初等整数論 (Instructor's Notes)

柳田 五夫

2017 年 8 月 22 日

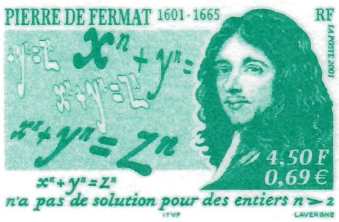


図 1　フェルマー

図 2　オイラー

$\mathbb{Z}$	整数全体の集合
$\mathbb{N}$	正の整数全体の集合
$\mathbb{N}_0$	非負整数全体の集合
$\mathbb{Q}$	有理数全体の集合
$\mathbb{R}$	実数全体の集合
$\mid A \mid$	集合 A の要素の個数（高校では $n(A)$ と表すことが多い）
$A \subset B$	集合 A は集合 B の真部分集合
$A \subseteq B$	集合 A は集合 B の部分集合
$A \setminus B,\ A - B$	差集合（集合 B に含まれない集合 A の要素全体の集合）
A^c	補集合（高校では $\overline{A}$ で表すことが多い）
$a \mid b$	a は b を割り切る（b は a で割り切れる）
$a \nmid b$	a は b を割り切らない（b は a で割り切れない）
$a \equiv b \pmod{p}$	a と b は m を法として合同（$m \mid a-b$）
$\gcd(a,b),\ (a,b)$	a と b の最大公約数
$\mathrm{lcm}(a,b),\ [a,b]$	a と b の最小公倍数
$[x],\ \lfloor x \rfloor$	x 以下の最大の整数
$\lceil x \rceil$	x 以上の最小の整数
$\{x\}$	x の小数部分，$\{x\} = x - [x]$
$p^\alpha \mid\mid n$	$p^\alpha \mid n$ かつ $p^{\alpha+1} \nmid n$
$v_p(a)$	a の素因数分解における素数 p の指数
μ	メビウス関数
φ	オイラーの φ 関数
$\displaystyle\sum_{d\mid m}$	m の全ての正の約数 d にわたる和
$\displaystyle\prod_{d\mid m}$	m の全ての正の約数 d にわたる積
$\overline{a_n a_{n-1}\cdots a_0}_{(b)}$	b 進法表示
$\binom{n}{r},\ {}_n\mathrm{C}_r$	二項係数
$\mathrm{ord}_m(a)$	m を法としたときの a の位数
$\left(\dfrac{a}{p}\right)$	ルジャンドルの記号

初等整数論は易しいか？　答えはノーである．

中学生にも理解できるのに，まだ証明されていない未解決問題が存在するのである．

- ゴールドバッハ予想

$n \geq 4$ であるすべての偶数は 2 つの素数の和で表せる．

- 双子素数予想

双子素数は無数に存在する．

p と $p+2$ が素数であるとき，これらの組は双子素数と呼ばれている．

- n^2+1 予想

n^2+1 の形をした素数が無数に存在する．

ここでは，$3n+1$ 予想ともいわれるコラッツ予想を紹介しておこう．

- コラッツ予想

n を 2 以上の正の整数とし，以下の操作をする．

(i) n が偶数ならば，n を 2 で割る．

(ii) n が奇数ならば，n を 3 倍して 1 を加える．

この操作を何回か繰り返すと，どのような正の整数も必ず 1 に到達するというのがコラッツ (Lothar O. Collatz) 予想である．これは 1930 年代に推測されたがまだに解決されていない．（筆者は高校時代に「大学への数学」でコラッツ予想を知ったが，それから 50 年近く経っている．）

例をあげると次のようになる．

```
 27 →  82 →  41 → 124 →  62 →  31 →  94 →  47 → 142 →  71 →
214 → 107 → 322 → 161 → 484 → 242 → 121 → 364 → 182 →  91 →
274 → 137 → 412 → 206 → 103 → 310 → 155 → 466 → 233 → 700 →
350 → 175 → 526 → 263 → 790 → 395 → 1186 → 593 → 1780 → 890 →
445 → 1336 → 668 → 334 → 167 → 502 → 251 → 754 → 377 → 1132 →
566 → 283 → 850 → 425 → 1276 → 638 → 319 → 958 → 479 → 1438 →
719 → 2158 → 1079 → 3238 → 1619 → 4858 → 2429 → 7288 → 3644 → 1822 →
911 → 2734 → 1367 → 4102 → 2051 → 6154 → 3077 → 9232 → 4616 → 2308 →
1154 →  577 → 1732 →  866 →  433 → 1300 →  650 →  325 →  976 →  488 →
244 →  122 →   61 →  184 →   92 →   46 →   23 →   70 →   35 →  106 →
 53 →  160 →   80 →   40 →   20 →   10 →    5 →   16 →    8 →    4 →
  2 →    1
```

- コラッツ予想についてポール・エルディシュは

Mathematics may not be ready for such problems.

(数学はこの種の問題に対する準備ができていない．)

と述べ，解決した人に 500 ドルを提供すると申し出た．

参考　コラッツ予想の操作の回数に関する問題が 2011 年のセンター試験の数 B の試験範囲で出題されている．

n を 2 以上の自然数とし，以下の操作を考える．

(i) n が偶数ならば，n を 2 で割る．
(ii) n が奇数ならば，n を 3 倍して 1 を加える．

与えられた 2 以上の自然数にこの操作を行い，得られた自然数が 1 でなければ，得られた自然数にこの操作を繰り返す．2 以上 10^5 以下の自然数から始めると，この操作を何回か繰り返すことで必ず 1 が得られることが確かめられている．たとえば，10 から始めると

$$10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$$

である．ただし，$a \to b$ は 1 回の操作で自然数 a から自然数 b が得られたことを意味する．
N を 2 以上 10^5 以下の自然数とするとき，$F(N)$ を N から始めて 1 が得られるまでの上記の操作の回数と定義する．また，$F(1) = 0$ とおく．たとえば，上の例から，$F(10) = 6$ である．

(1) $F(6) =$ [ア], $F(11) =$ [イウ] である．
(2) 10^5 以下の自然数 N について，$F(N)$ を求めるため，次のような〔プログラム〕を作った．ただし，INT(X) は X を超えない最大の整数を表す関数である．

〔プログラム〕

```
100 INPUT N
110 LET I=N
120 LET C=0
130 IF I=1 THEN GOTO [エ]
140 IF INT(I/2)*2=I THEN
150 [オ]
160   GOTO 190
170 END IF
180 LET I=3*I+1
190 [カ]
200 [キ]
210 PRINT "F(";N;")=";C
220 END
```

エ に当てはまるものを，次の⓪～⑤のうちから一つ選べ．

⓪ 130　① 140　② 150　③ 190　④ 200　⑤ 210

オ，カ，キ に当てはまるものを，次の⓪～⑧のうちからそれぞれ一つずつ選べ．

⓪ `LET C=1`
① `GOTO 130`
② `GOTO 140`
③ `GOTO 210`
④ `LET C=C+1`
⑤ `LET I=I+1`
⑥ `LET I=I/2`
⑦ `NEXT N`
⑧ `LET I=2*I+1`

〔プログラム〕を実行して，N に 24 を入力すると，180 行は ク 回実行される．

(3) M を 10^5 以下の自然数とする．(2) で作成した〔プログラム〕を変更して，M 以下の自然数 N のうち，$F(N) \leqq 10$ となるすべての N について，$F(N)$ の値を出力するプログラムを作成する．そのために，まず，〔プログラム〕の 100 行を次の二つの行で置き換える．

```
100 INPUT M
101 FOR N=1 TO M
```

さらに，210 行を次の二つの行で置き換える．

```
210 IF ケ THEN PRINT "F(";N;")=";C
211 コ
```

ケ に当てはまるものを，次の⓪～⑤のうちから一つ選べ．

⓪ `INT(I/2)=I`
① `C>10`
② `M>=C`
③ `N=I`
④ `C<=10`
⑤ `I=N`

コ に当てはまるものを，次の⓪～⑤のうちから一つ選べ．

⓪ `LET M=M+1`
① `GOTO 120`
② `NEXT M`
③ `NEXT N`
④ `LET C=C+1`
⑤ `NEXT I`

変更後のプログラムを実行して，M に 10 を入力すると，210 行の PRINT 文は サ 回実行される．

【解答】

ア	イウ	エ	オ	カ	キ	ク	ケ	コ	サ
8	14	5	6	4	1	2	4	3	8

(1) $6 \to 3 \to 10$ であるから

$$f(6) = 2 + f(10) = \mathbf{8} \qquad \cdots\cdots \text{ア}$$

$11 \to 34 \to 17 \to 52 \to 26 \to 13 \to 40 \to 20 \to 10$ であるから

$$f(11) = 8 + f(10) = \mathbf{14} \qquad \cdots\cdots \text{イウ}$$

(2) `I=1` のときは，操作の終了であるから，`F(n)` を出力する `210` 行に飛ぶ．すなわち［エ］は⑤ …… エ

`INT(I/2)*2=I` は，`I` が偶数であることを示すから，`I` を 2 で割った商で置き換える．すなわち［オ］は⑥ …… オ

［カ］は，操作の回数 `C` を 1 増やす，すなわち④ …… カ

しかるのち，再度 `I` が 1 になったかどうかの判定を行う `130` 行に飛ぶ．すなわち［キ］は① …… キ

$24 \to 12 \to 6 \to 3 \to 10$ となるから，24 に対してこの操作を行ったとき，1 以外の奇数が登場する回数は **2** 回である． …… ク

(3) 出力するのは，$C \leqq 10$ の場合であるから，［ケ］は④ …… ケ

しかるのち，次の `N` に対して調べることになるから，［コ］は③ …… コ

$f(1) = 0$, 問題はじめの例から

$$2 \to 1, 4 \to 2 \to 1, 5 \to 16 \to 8 \to 4 \to 2 \to 1,$$

$$10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$$

だから

$$f(2) = 1,\ f(4) = 2,\ f(5) = 5,\ f(8) = 3,\ f(10) = 6$$

となり，$f(2) \leqq 10, f(4) \leqq 10, f(5) \leqq 10, f(8) \leqq 10, f(10) \leqq 10$ を満たす．

$$3 \to 10 \text{ だから } f(3) = 1 + f(10) = 7 \leqq 10$$
$$6 \to 3 \text{ だから } f(6) = 1 + f(3) = 8 \leqq 10$$
$$7 \to 22 \to 11 \text{ だから } f(7) = 2 + f(11) = 16 > 10$$
$$9 \to 28 \to 14 \to 7 \text{ だから } f(9) = 3 + f(7) = 19 > 10$$

したがって，$f(N) \leqq 10$ を満たす 10 以下の自然数は 8 個であるから，`210` 行の `PRINT` 文は **8** 回実行される． …… サ

コラッツ予想の操作 (ii) を

(a) ***n*** **が奇数のときは，この数に 1 を加える．**

に変更したものが鳥取大学で出題されている．

1 より大きい自然数 n が与えられたときに，この n に対して次の操作を繰り返し行い，結果が 1 になるまで続ける．

(a) n が奇数のときは，この数に 1 を加える．
(b) n が偶数のときは，この数をを 2 で割る．

例えば，最初に与えられた自然数が 9 のときは

$$9 \to 10 \to 5 \to 6 \to 3 \to 4 \to 2 \to 1$$
$$(a) \quad (b) \quad (a) \quad (b) \quad (a) \quad (b) \quad (b)$$

と全部で 7 回の操作を行うことにより 1 になる．ただし，$n = 1$ の場合には 0 回の操作で 1 になると考える．次の問いに答えよ．

(1) どのような自然数 n を与えても必ず有限回の操作で 1 に到達することを，数学的帰納法を用いて証明せよ．
(2) 自然数 n が与えられたときに，この操作で 1 に到達ために必要な操作回数を $f(n)$ で表す．例えば $f(9) = 7$ である. また，1 から N までの自然数 n に対する $f(n)$ の和を $g(N)$ とする．すなわち，$g(N) = \sum_{n=1}^{N} f(n)$ である．$g(10)$ の値を求めよ．
(3) 任意の自然数 N について，(2) で与えた $g(N)$ が $g(2N) = 2g(N) + 3N - 2$ を満たすことを示せ．
(4) (3) の結果を用いて， $g(64)$ の値を求めよ． (2005 鳥取大・医・前期)

(5) を追加しておきます．
(5) $g\left(2^n\right)$ を n を用いて表せ．

[答] (2) $g(10) = 35$ (4) $g(64) = 450$ (5) $g\left(2^n\right) = (3n-4) \cdot 2^{n-1} + 2$

(5) は（3）で得られた式において，$N = 2^n$ とおくと

$$g\left(2^{n+1}\right) = 2g\left(2^n\right) + 3 \cdot 2^n - 2$$

となる．$x_n = g\left(2^n\right)$ とおくと，

$$x_{n+1} = 2x_n + 3 \cdot 2^n - 2$$

という漸化式になる．

目次

第1章

自然数・整数・有理数・無理数

1.1　自然数・整数

自然数の全体を $\mathbb{N}$ で表す:

$$\mathbb{N} = \Big\{1,\ 2,\ 3,\ 4,\ 5,\ \ldots\Big\}.$$

自然数を**正の整数**，**正整数** (positive integer) ともいう．

非負整数の全体を $\mathbb{N}_0$ で表す:

$$\mathbb{N}_0 = \Big\{0\Big\} \cup \mathbb{N} = \Big\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ \ldots\Big\}.$$

整数の全体を $\mathbb{Z}$ で表す：

$$\mathbb{Z} = \Big\{\ldots,\ -5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ \ldots\Big\}.$$

- 0 も自然数と見なしている英語の論文等も多いので，natural number(s) と書いてある場合には注意が必要である．
  ここでは，できるだけ自然数と言う用語を避け，正の整数や正整数と表現する．

$\mathbb{N}_0$ ($\mathbb{N}$) の整列性 (Well-Ordering Principle)

(1) $\mathbb{N}_0$ の空でない任意の部分集合には最小数が存在する．
(2) $\mathbb{N}$ の空でない任意の部分集合には最小数が存在する．

- **$\mathbb{N}_0$ ($\mathbb{N}$) の整列性**は当たり前のように使っているが，きちんと意識しておきたい．

定理 1.1.1　(数学的帰納法の原理 1)

$\mathbb{N}$ の部分集合 S が次の二つの性質 (i) と (ii) をもつとする．

(i)　1 は S に属する；$1 \in S$.

(ii)　k が S に属するときはいつでも次の整数 $k+1$ も S に属する；

$$k \in S \Longrightarrow k+1 \in S.$$

このとき $S = \mathbb{N}$ が成り立つ．

定理 1.1.1 の証明　T を S に属さないすべての正整数の集合として，T は空集合ではないと仮定する．$\mathbb{N}$ の整列性より，T には最小数が存在するからこれを a とおく．$1 \in S$ より $1 \notin T$ であるから $a > 1$ で，$0 < a-1 < a$ が成り立つ．a は T における最小数であったから，$a-1$ は T の要素ではない，すなわち S に属する．仮定から，S は $(a-1)+1 = a$ を含まなければならないが，これは a が T に属していることに矛盾する．
したがって，T は空集合でなければならず，$S = \mathbb{N}$ が成り立つことが言えた．　□

定理 1.1.2　(数学的帰納法の原理 2)

$\mathbb{N}$ の部分集合 S が次の二つの性質 (i) と (ii) をもつとする．

(i)　1 は S に属する；$1 \in S$.

(ii)　k 以下のすべての正整数 $1, 2, \ldots, k$ が S に属するならば，$k+1$ も S に属する；

$$\Big\{1,\ 2,\ \ldots,\ k\Big\} \subseteq S \Longrightarrow k+1 \in S.$$

このとき $S = \mathbb{N}$ が成り立つ．

定理 1.1.2 の証明　T を S に属さないすべての正整数の集合として，T は空集合ではないと仮定する．$\mathbb{N}$ の整列性より，T には最小数が存在するからこれを a とおく．$1 \in S$ より $1 \notin T$ であるから $a > 1$ で，$0 < a-1 < a$ が成り立つ．a は T における最小数であったから，$1, 2, \ldots, a-1$ のなかに T の要素はない．すなわち，$1, 2, \ldots, a-1$ はすべて S に属する．仮定から，S は $(a-1)+1 = a$ を含まなければならないが，これは a が T に属していることに矛盾する．
したがって，T は空集合でなければならず，$S = \mathbb{N}$ が成り立つことが言えた．　□

- 定理 1.1.1 において，性質 (i) の 1 を 任意の正整数 r にかえ，$\mathbb{N}$ を $\mathbb{N}_r = \Big\{r,\ r+1,\ r+2, r+3,\ \ldots\Big\}$ にかえても成り立つ．
- 定理 1.1.2 は次のようになる．
  定理 1.1.2' (数学的帰納法の原理 2)
  $\mathbb{N}$ の部分集合 S が次の二つの性質 (i) と (ii) をもつとする．

(i) $r \in \mathbb{N}$ は S に属する；$r \in S$.

(ii) k $(\geq r)$ 以下のすべての正整数 $r,\ r+1,\ \ldots,\ k$ が S に属するならば，$k+1$ も S に属する；

$$\Big\{r,\ r+1,\ \ldots,\ k\Big\} \subseteq S \Longrightarrow k+1 \in S.$$

このとき $S = \Big\{r,\ r+1,\ r+2, r+3,\ \ldots\Big\}$ が成り立つ．

異なる n 個のものから k 個とって作った組合せの総数 $\binom{n}{k} = {}_n\mathrm{C}_k$ は

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)\cdots 2\cdot 1}$$

を満たしている．

$\binom{n}{k}$ には，次の性質がある．

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \qquad (1 \leq k \leq n). \tag{1.1}$$

証明

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\
&= \frac{(n-k+1)\cdot n!}{k!(n-k+1)!} + \frac{k\cdot n!}{k!(n-k+1)!} \\
&= \frac{((n-k+1)+k)\,n!}{k!(n-k+1)!} \\
&= \frac{(n+1)n!}{k!(n-k+1)!} \\
&= \frac{(n+1)!}{k!(n-k+1)!} \\
&= \binom{n+1}{k}.
\end{aligned}$$

□

初めて等式 (1.1) の証明を試みる高校生には難しいかもしれない．

次のように結論から考えていくとわかりやすい．

$$\begin{aligned}
&\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \\
\Longleftrightarrow\quad &\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} = \frac{(n+1)!}{k!(n-k+1)!} \\
\Longleftrightarrow\quad &\frac{1}{k} + \frac{1}{n-k+1} = \frac{n+1}{k(n-k+1)}.
\end{aligned}$$

最後の等式を利用すると (1.1) は次のように証明できる．

(1.1) の証明

$$\frac{1}{k}+\frac{1}{n-k+1}=\frac{n+1}{k(n-k+1)}$$

の両辺に $\dfrac{n!}{(k-1)!(n-k)!}$ をかけると

$$\frac{n!}{k(k-1)!(n-k)!}+\frac{n!}{(k-1)(n-k+1)!(n-k)!}=\frac{(n+1)n!}{k(k-1)!(n-k+1)(n-k)!}.$$

これから

$$\frac{n!}{k!(n-k)!}+\frac{n!}{(k-1)!(n-k+1)!}=\frac{(n+1)!}{k!(n-k+1)!}$$

すなわち

$$\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}.$$ □

定理 1.1.3　(二項定理)

n を正の整数とするとき

$$(a+b)^n=\binom{n}{0}a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b^2+\cdots+\binom{n}{n-1}ab^{n-1}+\binom{n}{n}b^n$$

が成り立つ.

二項定理は

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k \tag{1.2}$$

とかくことができる.

定理 1.1.3 の証明　n に関する数学的帰納法で証明する.

(I) $n=1$ のとき

左辺$=a+b$，右辺$=\displaystyle\sum_{k=0}^{1}\binom{1}{k}a^{1-k}b^k=\binom{1}{0}a^1b^0+\binom{1}{1}a^0b^1=a+b.$

したがって，$n=1$ のとき，等式 (1.2) は成り立つ.

(II) $n=m$ のとき，等式 (1.2) が成り立つと仮定する．すなわち

$$(a+b)^m=\sum_{k=0}^{m}\binom{m}{k}a^{m-k}b^k$$

が成り立つと仮定する.

$$(a+b)^{m+1}=a(a+b)^m+b(a+b)^m$$

を利用する．帰納法の仮定を使うと

$$\begin{aligned}
a(a+b)^m &= \sum_{k=0}^{m} \binom{m}{k} a^{m+1-k} b^k \\
&= a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} a^{m+1-k} b^k, \\
b(a+b)^m &= \sum_{r=0}^{m} \binom{m}{r} a^{m-r} b^{r+1} \\
&= \sum_{r=0}^{m-1} \binom{m}{r} a^{m-r} b^{r+1} + b^{m+1} \\
&\quad (r = k-1) \\
&= \sum_{k=1}^{m} \binom{m}{k-1} a^{m+1-k} b^k + b^{m+1}.
\end{aligned}$$

よって，(1.1) を使うと

$$\begin{aligned}
(a+b)^{m+1} &= a(a+b)^m + b(a+b)^m \\
&= a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} a^{m+1-k} b^k + \sum_{k=1}^{m} \binom{m}{k-1} a^{m+1-k} b^k + b^{m+1} \\
&= a^{m+1} + \sum_{k=1}^{m} \left(\binom{m}{k} + \binom{m}{k-1} \right) a^{m+1-k} b^k + b^{m+1} \\
&= \binom{m+1}{0} a^{m+1} + \sum_{k=1}^{m} \binom{m+1}{k} a^{m+1-k} b^k + \binom{m+1}{m+1} b^{m+1} \\
&= \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k} b^k.
\end{aligned}$$

すなわち，(1.2) は $n = m+1$ のときも成り立つ．

(III) (I)，(II) から，すべての正整数 n について (1.2) は成り立つ． □

問題 1.1.1　n を正の整数とするとき，次の等式を組合せ論を用いて証明せよ．

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \qquad (1 \le k \le n).$$

問題 1.1.2　n を正の整数とするとき，等式 $(1+x)^{2n} = (1+x)^n (1+x)^n$ の両辺の展開式を利用して，次の等式が成り立つことを証明せよ．

$$\binom{2n}{n} = \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2.$$

問題 1.1.3　p は素数，r は正の整数とする．以下の問いに答えよ．

(1) $x_1, x_2, \ldots, x_r$ についての式 $(x_1 + x_2 + \cdots + x_r)^p$ を展開したときの単項式 $x_1^{p_1} x_2^{p_2} \cdots x_r^{p_r}$ の係数を求めよ．ここで，$p_1, p_2, \ldots, p_r$ は 0 または正の整数で，$p_1 + p_2 + \cdots + p_r = p$ を満たすとする．

(2) $x_1, x_2, \ldots, x_r$ が正の整数のとき，

$$(x_1 + x_2 + \cdots + x_r)^p - (x_1^p + x_2^p + \cdots + x_r^p)$$

は，p で割り切れることを示せ．

(3) r は p で割り切れないとする．このとき，$r^{p-1} - 1$ は p で割り切れることを示せ．　(2010 大阪大・理系・後期)

注 問題 1.1.3 の (1) は本質的に多項定理の証明である．次を多項定理という．

n, r が正の整数のとき，

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{p_1, p_2, \ldots, p_r} \frac{p!}{p_1! p_2! \cdots p_r!} x_1^{p_1} x_2^{p_2} \cdots x_r^{p_r}$$

が成り立つ．ここで，

$$0 \leq p_1 \leq n, 0 \leq p_2 \leq n, \ldots, 0 \leq p_r \leq n,\ p_1 + p_2 + \cdots + p_r = n$$

である．

$(x_1 + x_2 + \cdots + x_r)^n$ を展開したときの単項式 $x_1^{p_1} x_2^{p_2} \cdots x_r^{p_r}$ の係数が

$$\frac{n!}{p_1! p_2! \cdots p_r!}$$

となる　……(∗)

ことは，r に関する数学的帰納法でも証明できる．

証明 (I) $r = 1$ のとき，明らかに (∗) は成り立つ．

$r = 2$ のときは，二項定理を使うと，

$(x_1 + x_2)^n$ の展開式における $x_1^{p_1} x_2^{p_2} = x_1^{p_1} x_2^{n-p_1}$ の係数は

$$\binom{n}{p_1} = \frac{n!}{p_1!(n - p_1)!} = \frac{n!}{p_1! p_2!}$$

であるから (∗) は成り立つ．

(II) r のとき (∗) が成り立つと仮定する．

$(x_1 + x_2 + \cdots + x_r + x_{r+1})^n = ((x_1 + x_2 + \cdots + x_r) + x_{r+1})^n$ を展開したとき，

$(x_1+x_2+\cdots+x_r)^{p_1+p_2+\cdots+p_r}\,x_{r+1}^{n-(p_1+p_2+\cdots+p_r)}$ の係数は

$$\frac{n!}{(p_1+p_2+\cdots+p_r)!\,(n-(p_1+p_2+\cdots+p_r))!}=\frac{n!}{(p_1+p_2+\cdots+p_r)!p_{r+1}!}$$

である．

そして，$(x_1+x_2+\cdots+x_r)^{p_1+p_2+\cdots+p_r}$ の展開式における $x_1^{p_1}x_2^{p_2}\cdots x_r^{p_r}$ の係数は，仮定から

$$\frac{(p_1+p_2+\cdots+p_r)!}{p_1!p_2!\cdots p_r!}$$

だから，$x_1^{p_1}x_2^{p_2}\cdots x_r^{p_r}x_{r+1}^{p_{r+1}}$ の係数は

$$\frac{n!}{(p_1+p_2+\cdots+p_r)!p_{r+1}!}\cdot\frac{(p_1+p_2+\cdots+p_r)!}{p_1!p_2!\cdots p_r!}=\frac{n!}{p_1!p_2!\cdots p_r!\cdot p_{r+1}!}$$

となり，$r+1$ のときも $(*)$ は成り立つ．

(III) (I)，(II) から，すべての正整数 r に対して $(*)$ は成り立つ．　□

問題 1.1.3 の (2) は合同式の性質を表している．

p は素数，$x, y, x_1, \ldots, x_r$ は整数とする．このとき，次の合同式が成り立つ．

(i) $(x+y)^p \equiv x^p + y^p \pmod{p}$.
(ii) $(x_1+\cdots+x_r)^p \equiv x_1^p + x_2^p + \cdots + x_r^p \pmod{p}$.

(2) の証明は，$x, y, x_1, \ldots, x_r$ が正整数でなくて，$x, y, x_1, \ldots, x_r$ が整数でも通用する．

問題 1.1.3 の (3) は，フェルマーの小定理の正整数に対する証明になっている．フェルマーの小定理とは，次の定理である．

定理 4.3.1　p は素数，a は整数とするとき，次のことが成り立つ．

(i) $a^p \equiv a \pmod{p}$.
(ii) a と p が互いに素ならば $a^{p-1} \equiv 1 \pmod{p}$.

問題 1.1.4　　7^{9999} の下 3 桁 (しもみけた) を求めよ.

問題 1.1.5　$\left(x^3+\sqrt{2}\,x^2+\sqrt[3]{3}\,x+1\right)^{100}$ を展開したときの，x^{296} の係数を求めよ.

(1974 京都大・文)

問題 1.1.6　n を 4 以上の自然数とする．$\left(1+x+x^2+x^3+x^4\right)^n$ を展開したときの x^4 の係数を求めよ.

(1993 京都大・文・後期)

問題 1.1.7　数列 $\{a_n\}$ を次のように定義する.

$$\begin{cases} a_1=1, \\ a_{n+1}=\dfrac{1}{2}a_n+\dfrac{1}{n+1} \quad (n=1,2,\ldots\ldots) \end{cases}$$

このとき，各自然数 n に対して不等式 $a_n \leqq \dfrac{4}{n}$ が成り立つことを証明せよ.

(1993 京都大・文・後期)

問題 1.1.8　(2013 PUMaC)

数列 $\{a_n\}$, $\{b_n\}$ を次のように定義する.

$$a_1=2013,\ a_{n+1}=2013^{a_n} \quad (n=1,2,\ldots)$$

$$b_1=1,\ b_{n+1}=2013^{2012b_n} \quad (n=1,2,\ldots)$$

このとき，すべての正の整数 n に対して不等式 $a_n > b_n$ が成り立つことを証明せよ.

1.2 有理数・無理数

整数 m, n を用いて $\dfrac{m}{n}$ の形に表される数を**有理数**という．

整数 m は $\dfrac{m}{1}$ と表されるから有理数である．

有理数の全体を $\mathbb{Q}$ で表す．

また，有限小数や無限小数で表される数を，一般に**実数**といい，実数のうち，有理数でないものを，**無理数**という．

例題 1.2.1 $\sqrt{2}$ は無理数であることを証明せよ．

$\mathbb{N}$ の整列性を使って証明できる．

解答 $\sqrt{2}$ が有理数だと仮定すると，$\sqrt{2} = \dfrac{a}{b},\ a, b \in \mathbb{N}$ とかける．

$A = \left\{ n\sqrt{2} : n,\ n\sqrt{2} \in \mathbb{N} \right\}$ とおくと，$a = b\sqrt{2} \in \mathbb{N}, b \in \mathbb{N}$ より，$b\sqrt{2} \in A$ だから $A \neq \phi$.

よって，$\mathbb{N}$ の整列性より，A には最小の要素が存在するから，これを $j = k\sqrt{2}\ \ (k \in \mathbb{N}, j \in \mathbb{N})$ とおく．$j(\sqrt{2}-1)$ は正の数で，$j(\sqrt{2}-1) = j\sqrt{2} - j = 2k - j \in \mathbb{Z}$ より正の整数であることがわかる．

このことと，$j(\sqrt{2}-1) = j\sqrt{2} - j = j\sqrt{2} - k\sqrt{2} = (j-k)\sqrt{2}$ から $(j-k)\sqrt{2}$ も正の整数である．

また，$(j-k)\sqrt{2} = j(\sqrt{2}-1) < j$ であるから，$(j-k)\sqrt{2}$ は $(j-k)\sqrt{2} \in A$ で，j より小さいから，j が A のなかで最小であることに矛盾する．

したがって，$\sqrt{2}$ は無理数である． □

- 素因数分解を用いて証明することもできる．（例題 2.4.1 参照）

例題 1.2.2 $\log_2 3$ は無理数であることを証明せよ．

解答 $\log_2 3$ が有理数だと仮定すると，$\log_2 3 = \dfrac{m}{n}\ \ (m, n \in \mathbb{N})$ とかける．これは $3 = 2^{\frac{m}{n}}$ と書き直せる．この等式の両辺を n 乗すると

$$3^n = 2^m.$$

左辺は奇数，右辺は偶数となり，これは不可能である．ゆえに，この等式は成り立たない．したがって，$\log_2 3$ が有理数ではありえないから，$\log_2 3$ は無理数である． □

注 2 を法とする合同式で考えると，

$$2^n \equiv 0 \pmod 2,\ 3^m \equiv 1^m \equiv 1 \pmod 2$$

より $3^n = 2^m$ は成立しない．

例題 1.2.3　e は無理数であることを証明せよ.

解答　$e^x = \sum_{j=0}^{\infty} \frac{x^j}{j!}$ で $x = 1$ とおくと

$$e = \sum_{j=0}^{\infty} \frac{1}{j!} \qquad \cdots\cdots ①$$

が成り立つ.

e が有理数だと仮定すると，$e = \frac{a}{b}$, $a, b \in \mathbb{N}$ とかける.

①より

$$b!e = \sum_{j=0}^{b} \frac{b!}{j!} + \sum_{j=b+1}^{\infty} \frac{b!}{j!}$$

が成り立つから，

$$\theta = b!e - \sum_{j=0}^{b} \frac{b!}{j!} = \sum_{j=b+1}^{\infty} \frac{b!}{j!}$$

とおくと，$0 < \theta < 1$ が成り立つことを示す.

明らかに，$0 < \theta$ は成り立つから，$\theta < 1$ が成り立つことを示せばよい.

$$\begin{aligned}
\theta = \sum_{j=b+1}^{\infty} \frac{b!}{j!} &= \sum_{j=1}^{\infty} \frac{b!}{(b+j)!} \\
&= \sum_{j=1}^{\infty} \frac{1}{(b+j)(b+j-1)\cdots(b+1)} \\
&< \sum_{j=1}^{\infty} \frac{1}{(b+1)^j} \\
&= \frac{\dfrac{1}{b+1}}{1 - \dfrac{1}{b+1}} = \frac{1}{b} \leqq 1.
\end{aligned}$$

$0 < \theta < 1$ が成り立つことがわかったが，これは，

$$\theta = b!e - \sum_{j=0}^{b} \frac{b!}{j!} = (b-1)!a - \sum_{j=0}^{b} \frac{b!}{j!}$$

が整数であることに矛盾する.

したがって，e は無理数である.　□

例題 1.2.4　α が 1 以外の有理数，β が無理数のとき，α^β は無理数となるか.

$\alpha = 2$, $\beta = \log_2 3$ として α^β を考えよ.

例題 1.2.5 α が無理数，β が無理数のとき，α^β は無理数となるか．

$\alpha = \sqrt{2}^{\sqrt{2}}$, $\beta = \sqrt{2}$ として $\alpha^\beta = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$ を考えよ．

$$\alpha^\beta = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2.$$

$\alpha = \sqrt{2}^{\sqrt{2}}$ が無理数であることは，$\alpha = \sqrt{2}^{\sqrt{2}}$ が超越数であることからわかる．

注 $a_1 = \sqrt{2}$, $a_{k+1} = \sqrt{2}^{a_k}$ $(k = 1, 2, \dots)$ とおいたとき，$\alpha^\beta \neq a_3 = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}}$ に注意したい．

有理数係数の 0 でない方程式

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Q} \quad (i = 0, 1, \dots, n-1)$$

の根（解）になる複素数を**代数的数**といい，代数的数ではない複素数を**超越数**という．

1934 年にゲルフォントとシュナイダーが独立に証明した次の定理を使うと $\alpha = \sqrt{2}^{\sqrt{2}}$ が超越数であると言える．

定理 α, β が代数的数で，$\alpha \neq 0, 1$ かつ β が有理数ではないならば，α^β は超越数である．

注 $\alpha = \sqrt{2}^{\sqrt{2}}$ が超越数であることの説明

$\alpha_1 = \beta_1 = \sqrt{2}$ とおくと，$\alpha_1 = \beta_1 = \sqrt{2}$ は，代数方程式 $x^2 - 2 = 0$ の根だから，代数的数である．$\alpha_1 \neq 0, 1$ かつ β_1 が有理数ではないから，定理により，$\alpha = \alpha_1^{\beta_1} = \sqrt{2}^{\sqrt{2}}$ は超越数である．

ゲルフォントとシュナイダーの定理は，1966 年にベイカーによって一般化されている．ベイカーの定理とは，次のものである．

定理 $\alpha_1, \alpha_2, \dots, \alpha_n$ を 0 でない代数的数とする．少なくとも一つが 0 でない代数的数 $\beta_0, \beta_1, \dots, \beta_n$ に対して，

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n = 0$$

が成り立てば，

$$r_1 \log \alpha_1 + r_2 \log \alpha_2 + \cdots + r_n \log \alpha_n = 0$$

を満たす少なくとも一つが 0 でない有理数 $r_1, r_2, \dots, r_n$ が存在する．

問題 1.2.1　(1)　a, b, c, d が有理数のとき，$\sqrt{3} = \dfrac{a + b\sqrt{2}}{c + d\sqrt{2}}$ となることがあるか．

(2)　a, b, c, d が有理数で $a + \sqrt{2}\,b + \sqrt{3}\,c + \sqrt{6}\,d = 0$ となるのは，$a = b = c = d = 0$ のときに限ることを証明せよ．((2) のみ 1969 一橋大)

問題 1.2.2　自然数 n に対して，関数 $f_n(x) = x^n e^{1-x}$ と，その定積分 $a_n = \displaystyle\int_0^1 f_n(x)\,dx$ を考える．ただし，e は自然対数の底である．次の問いに答えよ．

(1)　区間 $0 \leqq x \leqq 1$ 上で $0 \leqq f_n(x) \leqq 1$ であることを示し，さらに $0 < a_n < 1$ が成り立つことを示せ．

(2)　a_1 を求めよ．$n > 1$ に対して a_n と a_{n-1} の間の漸化式を求めよ．

(3)　自然数 n に対して，等式　$\dfrac{a_n}{n!} = e - \left(1 + \dfrac{1}{1!} + \dfrac{1}{2!} + \cdots + \dfrac{1}{n!}\right)$ が成り立つことを証明せよ．

(4)　いかなる自然数 n に対しても，$n!e$ は整数とならないことを示せ．

(1997 大阪大・理・工・基礎工・後期)

- (1) の結果を使うと，$0 < \dfrac{a_n}{n!} < \dfrac{1}{n!}$ だから，$\lim\limits_{n\to\infty} \dfrac{a_n}{n!} = 0$.

  次に，(3) の結果を用いて $n \to \infty$ とすると

  $$\lim_{n\to\infty} \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}\right) = \lim_{n\to\infty} \left(e - \frac{a_n}{n!}\right) = e$$

  だから

  $$\boldsymbol{e = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \cdots}$$

  が得られる．

- (4) から，**e は無理数である**ことがわかる．

  e が有理数だと仮定して $e = \dfrac{a}{b}$, $a, b \in \mathbb{N}$ とおくと，$b!e$ は整数となるが，(4) の結果に矛盾する．

類題が電通大で出題されている．(大阪大と電通大の問題において，$1 - x = t$ とおけば，被積分関数は同じである．)

類題 e を自然対数の底とする．$2 < e < 3$ であることを既知として，e が有理数でないことを背理法を用いて証明しよう．数列 $\{A_n\}$ を

$$A_n = \frac{1}{n!} \int_0^1 e^x (1 - x)^n\,dx \ (n = 1, 2, 3, \dots)$$

により定めるとき，以下の問いに答えよ．

(1)　A_1, A_2 を求めよ．

(2) $n \geqq 2$ のとき，$0 \leqq x \leqq 1$ において $0 \leqq (1-x)^n \leqq (1-x)^2$ が成り立つことを用いて，$0 < n!A_n < 1$ であることを示せ．

(3) $n \geqq 2$ のとき，A_n を A_{n-1} を用いて表せ．

(4) 一般項 A_n を求めよ．（必要ならば和の記号 $\sum$ を用いてもよい．）

(5) e が有理数であると仮定すれば，e は整数ではないから，$e = \dfrac{M}{N}$ (M, N は互いに素な自然数で，$N \geqq 2$) という形で表せるはずである．この仮定のもとで $N!A_N$ は整数でなくてはならないことを示せ．

注意 ： (5) で e が有理数であると仮定して示したことは，(2) で示したことに矛盾する．よって，e が有理数でないことが証明された．　(2003 電通大・後期)

問題 1.2.3　(1)　$\log_5 3$ は無理数であることを示せ．

(2)　$\log_{10} r$ が有理数となる有理数 r は $r = 10^q$ ($q = 0, \pm 1, \pm 2, \dots$) に限ることを示せ．

(3)　任意の正の整数 n に対して，

$$\log_{10}\left(1 + 3 + 3^2 + \cdots + 3^n\right)$$

は無理数であることを示せ．

(1998 一橋大・商・経済・社会・後期)

問題 1.2.4 と問題 1.2.5 は π が無理数であることの証明問題である．
次の問題 1.2.4 から，π^2 が無理数であることがわかる．（Ivan Niven による証明方法である．）

問題 1.2.4　次の問いに答えよ．

(1)　正の整数 n に対して，関数 $f(x) = \dfrac{x^n(1-x)^n}{n!}$ を考える．

(a)　$f(x)$ は

$$f(x) = \frac{1}{n!}\left(a_n x^n + a_{n+1}x^{n+1} + \cdots + a_{2n}x^{2n}\right) \quad (a_n, a_{n+1}, \dots, a_{2n} \in \mathbb{Z}) \quad \cdots\cdots ①$$

という形の多項式であることを示せ．

(b)　$0 < x < 1$ で $0 < f(x) < \dfrac{1}{n!}$ であることを示し，さらに

$$0 < \int_0^1 f(x)\sin(\pi x)\,dx < \frac{1}{n!}$$

が成り立つことを示せ．

(c)　非負の整数 m に対して，$\dfrac{d^m f(0)}{dx^m}$, $\dfrac{d^m f(1)}{dx^m}$ はともに整数であることを示せ．

(2)　n, q を正の整数として，

$$F(x) = q^n \left(\pi^{2n} f(x) - \pi^{2n-2} f^{(2)}(x) + \pi^{2n-4} f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x) \right)$$

とおく．ただし，$f(x) = \dfrac{x^n(1-x)^n}{n!}$ とする．

(d)　$\dfrac{d}{dx}\left(F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)\right)$ を考えることにより，

$$F''(x) + \pi^2 F(x) = q^n \pi^{2n+2} f(x)$$

が成り立つことを示せ．

(e)　$q^n \pi^{2n+1} \displaystyle\int_0^1 f(x)\sin(\pi x)\,dx = F(0) + F(1)$ が成り立つことを示せ．

(f)　π^2 は無理数であることを証明せよ．

(g)　π は無理数であることを証明せよ．

問題 1.2.5　　π を円周率とする．次の積分について考える．

$$I_0 = \pi \int_0^1 \sin \pi t\,dt,\ I_n = \frac{\pi^{n+1}}{n!} \int_0^1 t^n (1-t)^n \sin \pi t\,dt\ (n = 1, 2, \dots)$$

(1)　n が自然数であるとき，不等式

$$1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} < e^x\ (x > 0)$$

が成立することを数学的帰納法により示せ．これを用いて，不等式

$$I_0 + uI_1 + u^2 I_2 + \cdots + u^n I_n < \pi e^{\pi u}\ (u > 0)$$

が成立することを示せ．

(2)　I_0, I_1 の値を求めよ．また，漸化式

$$I_{n+1} = \frac{4n+2}{\pi} I_n - I_{n-1}$$

が成立することを示せ．

(3)　π が無理数であることを背理法により証明しよう．π が無理数でないとし，正の整数 p, q によって $\pi = \dfrac{p}{q}$ として表されると仮定する．$A_0 = I_0, A_n = p^n I_n$ とおくとき，$A_0, A_1, A_2, \dots$ は正の整数になることを示せ．さらに，これから矛盾を導け．　　(2003 大阪大・理・工・基礎工・後期)

第2章

整除性の理論

2.1　基本概念と基本定理

整数 a, b に対して，$b = aq$ となる整数 q が存在するとき，a は b を**割り切る**あるいは b は a で**割り切れる**という．このとき a は b の**約数**，b は a の**倍数**という．

a が b を割り切ることを $\boldsymbol{a \mid b}$ と表し，a が b を割り切らないことを $\boldsymbol{a \nmid b}$ で表す．

正の整数 p が**素数**であるとは，$p > 1$ であって 1 と p 自身以外の正の整数で割りきれない場合をいう．

- $\boldsymbol{a \mid b}$ は便利な記号であるが，どちらがどちらを割り切るのか間違いやすいので注意したい．
- 1 は素数ではない．
- 偶数の素数は 2 だけであり，2 以外の素数は奇数である．

定理 2.1.1　整数 a，正の整数 b に対して

$$a = bq + r, \quad 0 \leq r < b \tag{2.1}$$

を満たすような整数 q, r がただ一組だけ存在する．

(2.1) を成り立たせる q を，a を b で割ったときの**商**，r を**余り**という．

もっと一般的に次の定理が成り立つ．

定理 2.1.2　整数 a と整数 $b \neq 0$ に対して

$$a = bq + r, \quad 0 \leq r < |b| \tag{2.2}$$

を満たすような整数 q, r がただ一組だけ存在する．

[定理 2.1.1 の証明]

◎ (2.1) を満たすような整数 q, r が存在することを示す.
整数列

$$\ldots,\ a-3b,\ a-2b,\ a-b,\ a,\ a+b,\ a+2b,\ a+3b,\ \ldots \qquad \cdots\cdots(*)$$

の中で，最小の非負の整数を r とすると，$r = a - qb$ となる整数 q が存在する．$(a-qb)-b$ は整数列 $(*)$ の中にあり，$(a-qb)-b < a-qb$ なので $(a-qb)-b < 0$ である．ゆえに，$r < b$ を得るが，$r \geq 0$ であったから，$a = bq + r,\quad 0 \leq r < b$ を満たす整数 q, r が存在することがわかった.

◎ 次に q と r の存在の一意性を示す.
$a = bq_1 + r_1,\quad q_1, r_1 \in \mathbb{Z}, 0 \leq r_1 < b,\quad a = bq_2 + r_2,\quad q_2, r_2 \in \mathbb{Z}, 0 \leq r_2 < b$
と 2 通りに表せたとする．等式 $a = bq_1 + r_1$, $a = bq_2 + r_2$ の差をとると

$$r_1 - r_2 = (q_2 - q_1)\, b.$$

これから，$b|(r_1 - r_2)$ が言える．ところで $-b < r_1 - r_2 < b$ であるから $b|(r_1 - r_2)$ となるのは $r_1 - r_2 = 0$ すなわち $r_1 = r_2$ のときしかない．$r_1 - r_2 = 0$ を $r_1 - r_2 = (q_2 - q_1)b$ に代入すると $(q_2 - q_1)b = 0$ となる．$b > 0$ であるから $q_2 - q_1 = 0$ すなわち $q_1 = q_2$.
以上のことから，定理における q と r の存在の一意性が示された. □

- ガウス記号を使うと $q = \left[\dfrac{a}{b}\right]$, $r = a - b\left[\dfrac{a}{b}\right]$ となる.
  $a = bq + r,\quad 0 \leq r < b$ から $qb \leq a < (q+1)b$ すなわち $q \leq \dfrac{a}{b} < q + 1$. よって，$q$ は $\dfrac{a}{b}$ 以下の最大の整数となるので

  $$q = \left\lfloor \frac{a}{b} \right\rfloor = \left[\frac{a}{b}\right]$$

  とかける.
- 実数全体の集合 $\mathbb{R}$ を

  $$\mathbb{R} = \bigcup_{q \in \mathbb{Z}} [qb,\ (q+1)b) = \cdots [-3b,\ -2b) \cup [-2b,\ -b) \cup [-b,\ 0) \cup [0,\ b) \cup [b,\ 2b) \cup \cdots$$

  のように分割する.
  整数 a はこれらの区間の中のただ一つに属するから，$a \in [qb,\ (q+1)b)$ を満たす整数 q がただ一つ存在する．このとき，$r = a - qb$ とおけば $0 \leq r < b$ となる.

系 2.1.1　整数 a，正の整数 b に対して

$$a = bq + r,\ -\frac{b}{2} \leq r < \frac{b}{2}$$

を満たすような整数 q, r がただ一組存在する.

証明 実数全体の集合 $\mathbb{R}$ を

$$\mathbb{R} = \bigcup_{q\in\mathbb{Z}} \left[qb - \frac{b}{2},\, qb + \frac{b}{2} \right)$$

のように分割する．
整数 a はこれらの区間の中のただ一つに属するから，$a \in \left[qb - \frac{b}{2},\, qb + \frac{b}{2} \right)$ を満たす整数 q がただ一つ存在する．このとき，$r = a - qb$ とおけば $-\frac{b}{2} \leq r < \frac{b}{2}$ となる．　□

系 2.1.2　整数 a，正の整数 b に対して

$$a = bq + r,\ -\frac{b}{2} < r \leq \frac{b}{2}$$

を満たすような整数 q, r がただ一組存在する．

証明 実数全体の集合 $\mathbb{R}$ を

$$\mathbb{R} = \bigcup_{q\in\mathbb{Z}} \left(qb - \frac{b}{2},\, qb + \frac{b}{2} \right]$$

のように分割する．
整数 a はこれらの区間の中のただ一つに属するから，$a \in \left(qb - \frac{b}{2},\, qb + \frac{b}{2} \right]$ を満たす整数 q がただ一つ存在する．このとき，$r = a - qb$ とおけば $-\frac{b}{2} < r \leq \frac{b}{2}$ となる．　□

- $-4 = 5\cdot(-1) + 1$ より -4 を 5 で割った商は -1，余りは 1 である．
- m, n, d はすべて整数とするとき，次のことが成り立つ．
  $d \mid m$ かつ $d \mid n \implies$ 任意の整数 a, b に対して $d \mid (am + bn)$.

  証明　$d \mid m$ かつ $d \mid n$ から $m = dm_1$, $n = dn_1$, $m_1, n_1 \in \mathbb{Z}$ とおける．
  このとき $am + bn = a\cdot dm_1 + b\cdot dn_1 = d(am_1 + bn_1)$ から $\mid (am + bn)$.　□

- a が奇数のとき，$a^2 - 1$ は 8 で割り切れる．

  証明　$a = 2k + 1$, $k \in \mathbb{Z}$ とおくと

  $$a^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4k(k+1).$$

  $k(k+1)$ は連続する 2 整数の積だから，2 の倍数である．したがって $4k(k+1)$ は 8 の倍数となるので，$a^2 - 1$ は 8 で割り切れる．　□

例題 2.1.1　連続する n 個の整数の積は $n!$ で割り切れる．

解答 連続する n 個の整数の積を $P=(m+1)(m+2)\cdots(m+n)$ とおく．

(a) 最初に $m+1, m+2, \ldots, m+n$ がすべて正の整数の場合を考える．$(m \geq 0, n \geq 2)$
二項係数の式を使うと

$$\binom{m+n}{n} = \frac{(m+n)!}{m!n!} = \frac{(m+n)(m+n-1)\cdots(m+1)}{n!} = \frac{P}{n!}.$$

$\binom{m+n}{n}$ は正の整数なので，P は $n!$ で割り切れる．

(b) 連続する n 個の整数 $m+1, m+2, \ldots, m+n$ の中に 0 がある場合は，$P=0$ となり，P は $n!$ で割り切れる．

(c) 連続する n 個の整数 $m+1, m+2, \ldots, m+n$ がすべて負の整数である場合は，P に $(-1)^n$ をかけることにより，$(-1)^n P$ は (a) の場合に帰着して，$n!$ で割り切れる．したがって，P は $n!$ で割り切れる．　□

[**定理 2.1.2 の証明**]

◎ (2.2) を満たすような整数 q, r が存在することを示す．
整数列

$$\ldots, a-3b, a-2b, a-b, a, a+b, a+2b, a+3b, \ldots \qquad \cdots(*)$$

の中で，最小の非負の整数を r とすると，$r=a-qb$ となる整数 q が存在する．$(a-qb)-|b|$ は整数列 $(*)$ の中にあり，$(a-qb)-|b|<a-qb$ なので $(a-qb)-|b|<0$ である．ゆえに，$r<|b|$ を得るが，$r \geq 0$ であったから，$a=bq+r, \quad 0 \leq r < |b|$ を満たす整数 q, r が存在することがわかった．

◎ 次に q と r の存在の一意性を示す．
$a=bq_1+r_1, \quad q_1, r_1 \in \mathbb{Z}, 0 \leq r_1 < |b|, \quad a=bq_2+r_2, \quad q_2, r_2 \in \mathbb{Z}, 0 \leq r_2 < |b|$
と 2 通りに表せたとする．等式 $a=bq_1+r_1, a=bq_2+r_2$ の差をとると

$$r_1 - r_2 = (q_2 - q_1)\, b.$$

これから，$b|(r_1-r_2)$ が言える．ところで $-|b|<r_1-r_2<|b|$ であるから $b|(r_1-r_2)$ となるのは $r_1-r_2=0$ すなわち $r_1=r_2$ のときしかない．$r_1-r_2=0$ を $r_1-r_2=(q_2-q_1)b$ に代入すると $(q_2-q_1)b=0$ となる．$b \neq 0$ であるから $q_2-q_1=0$ すなわち $q_1=q_2$．以上のことから，定理における q と r の存在の一意性が示された．　□

例題 2.1.2　実数 x の小数部分を，$0 \leqq y < 1$ かつ $x-y$ が整数となる実数 y のこととし，これを記号 $< x >$ で表す．実数 a に対して，無限数列 $\{a_n\}$ の各項 $a_n\,(n=1,2,3,\dots)$ を次のように順次定める．

$$\text{(i)}\quad a_1 =< a >$$

$$\text{(ii)}\quad \begin{cases} a_n \neq 0 \text{ のとき，} a_{n+1} = \left\langle \dfrac{1}{a_n} \right\rangle \\ a_n = 0 \text{ のとき，} a_{n+1} = 0 \end{cases}$$

(1)　$a=\sqrt{2}$ のとき，数列 $\{a_n\}$ を求めよ．

(2)　任意の自然数 n に対して $a_n = a$ となるような $\dfrac{1}{3}$ 以上の実数 a をすべて求めよ．

(3)　a が有理数であるとする． a を整数 p と自然数 q を用いて $a=\dfrac{p}{q}$ と表すとき，q 以上のすべての自然数 n に対して， $a_n = 0$ であることを示せ．

(2011 東京大・理・前期)

解答

(1) $a=\sqrt{2}$ のとき，$1<\sqrt{2}<2$ より，$\left[\sqrt{2}\right]=1$ なので，$a_1 = \left\langle \sqrt{2} \right\rangle = \sqrt{2}-1$,

$a_2 = \left\langle \dfrac{1}{\sqrt{2}-1} \right\rangle = \left\langle \sqrt{2}+1 \right\rangle$.

$2<\sqrt{2}+1<3$ より，$\left[\sqrt{2}+1\right]=2$ なので

$$a_2 = \left\langle \sqrt{2}+1 \right\rangle = \sqrt{2}+1-2 = \sqrt{2}-1 = a_1.$$

したがって，$a_{n+1}=a_n\ (n \geq 1)$ となるので

$$a_n = \sqrt{2}-1\ (n=1,2,\dots).$$

(2) $a_1 =< a >$ と $a_n = a\ (n=1,2,\dots)$ から

$$< a >= a \qquad \cdots\cdots ①$$

が成り立つ．等式①から，$0 \leq a < 1$ でなければならないから，$a \geq \dfrac{1}{3}$ とあわせて

$$\frac{1}{3} \leq a < 1. \qquad \cdots\cdots ②$$

②から $a_1 = a \neq 0$ なので，$a_2 = \left\langle \dfrac{1}{a_1} \right\rangle = \left\langle \dfrac{1}{a} \right\rangle$.

$a_n = a\ (n=1,2,\dots)$ を使うと

$$\left\langle \frac{1}{a} \right\rangle = a \qquad \cdots\cdots ③$$

が成り立つ．②から，$1 < \dfrac{1}{a} \leq 3$ なので $\left[\dfrac{1}{a}\right] \in \Big\{1,\ 2,\ 3\Big\}$.

(ア) $\left[\frac{1}{a}\right]=1$ の場合　　$1<\frac{1}{a}<2$ すなわち，$\frac{1}{2}<a<1$.
$\left\langle\frac{1}{a}\right\rangle=\frac{1}{a}-1$ となるから，③より

$$\frac{1}{a}-1=a \qquad a^2+a-1=0 \qquad a=\frac{-1\pm\sqrt{5}}{2}.$$

このうち，$\frac{1}{2}<a<1$ を満たすのは $a=\frac{-1+\sqrt{5}}{2}$.

(イ) $\left[\frac{1}{a}\right]=2$ の場合　　$2\leq\frac{1}{a}<3$ すなわち，$\frac{1}{3}<a\leq\frac{1}{2}$.
$\left\langle\frac{1}{a}\right\rangle=\frac{1}{a}-2$ となるから，③より

$$\frac{1}{a}-2=a \qquad a^2+2a-1=0 \qquad a=-1\pm\sqrt{2}.$$

このうち，$\frac{1}{3}<a\leq\frac{1}{2}$ を満たすのは $a=-1+\sqrt{2}$.

(ウ) $\left[\frac{1}{a}\right]=3$ の場合
$a=\frac{1}{3}$ で，$\left\langle\frac{1}{a}\right\rangle=<3>=0$ となり③を満たさない.

以上のことから，$a_2=a, a_1=a$ を満たす a の値は，$a=\frac{-1+\sqrt{5}}{2}, -1+\sqrt{2}$.

$a_2=a, a_1=a$ を満たすとき，①，②が成り立つから，$<a>=a, \left\langle\frac{1}{a}\right\rangle=a\neq 0$.

$a_k=a$ とすると，$a_{k+1}=\left\langle\frac{1}{a_k}\right\rangle=\left\langle\frac{1}{a}\right\rangle=a$ となるから，帰納的に $a_n=a$ $(n=1,2,\dots)$ が成り立つ.

よって，求める a の値は，$a=\frac{-1+\sqrt{5}}{2}, -1+\sqrt{2}$.

(3) $a_1=<a>=\left\langle\frac{p}{q}\right\rangle$.
整数 p を q で割った商を q_1，余りを r_1 とすると

$$p=qq_1+r_1 \quad (0\leq r_1<q)$$

とかける．これから，$\frac{p}{q}=q_1+\frac{r_1}{q}$, $0\leq\frac{r_1}{q}<1$ となるので

$$a_1=<a>=\left\langle\frac{p}{q}\right\rangle=\left\langle q_1+\frac{r_1}{q}\right\rangle=\frac{r_1}{q}.$$

$r_1=0$ のとき，$a_1=0$
$r_1\neq 0$ のとき，$a_1=\frac{r_1}{q}\neq 0$ なので，$a_2=\left\langle\frac{1}{a_1}\right\rangle=\left\langle\frac{q}{r_1}\right\rangle$.
整数 q を r_1 で割った商を q_2，余りを r_2 とすると

$$q=r_1q_2+r_2 \quad (0\leq r_2<r_1)$$

とかける．これから，$\dfrac{q}{r_1} = q_2 + \dfrac{r_2}{r_1}$, $0 \leq \dfrac{r_2}{r_1} < 1$ となるので

$$a_2 = \left\langle \frac{q}{r_1} \right\rangle = \left\langle q_2 + \frac{r_2}{r_1} \right\rangle = \frac{r_2}{r_1}.$$

$r_2 = 0$ のとき，$a_2 = 0$

$r_2 \neq 0$ のとき，$a_2 = \dfrac{r_2}{r_1} \neq 0$ なので，$a_3 = \left\langle \dfrac{1}{a_2} \right\rangle = \left\langle \dfrac{r_1}{r_2} \right\rangle$.

整数 r_1 を r_2 で割った商を q_3，余りを r_3 とすると

$$r_1 = r_2 q_3 + r_3 \quad (0 \leq r_3 < r_2)$$

とかける．これから，$\dfrac{r_1}{r_2} = q_3 + \dfrac{r_3}{r_2}$, $0 \leq \dfrac{r_3}{r_2} < 1$ となるので

$$a_3 = \left\langle \frac{r_1}{r_2} \right\rangle = \left\langle q_3 + \frac{r_3}{r_2} \right\rangle = \frac{r_3}{r_2}.$$

$r_3 = 0$ のとき，$a_3 = 0$

$r_3 \neq 0$ のとき，以下同様に操作を繰り返すと，有限回の操作で $r_m = 0$ となる正の整数 m が存在する．

$$0 = r_m < r_{m-1} < \cdots < r_1 < q$$

だから，最大でも q 回の操作で，$r_m = 0$ となるので，$1 \leq m \leq q$ が成り立つ．

$r_m = 0$ のとき，$a_m = 0$ だから，$0 = a_m = a_{m+1} = \ldots$ となる．

$q \geq m$ であったから，$0 = a_q = a_{q+1} = \ldots$ すなわち q 以上のすべての自然数 n に対して， $a_n = 0$ である． □

問題 2.1.1 (APMO 2002)

$\dfrac{a^2+b}{b^2-a}$, $\dfrac{b^2+a}{a^2-b}$ がともに整数となるような正の整数の組 (a, b) をすべて求めよ．

問題 2.1.2 (IMO 1992)

a, b, c は $1 < a < b < c$ を満たす整数とする．このとき，$(a-1)(b-1)(c-1)$ が $abc-1$ を割り切るような整数 a, b, c をすべて求めよ．

問題 2.1.3 整数を係数とする多項式 $f(x)$ について，次のことを証明しなさい．

(1) 任意の整数 m, n に対し $f(n+m) - f(n)$ は m の倍数である．

(2) 任意の整数 k, n に対し $f(n + f(n)k)$ は $f(n)$ の倍数である．

(3) 任意の自然数 n に対し $f(n)$ が素数であるならば，$f(x)$ は定数である．

(2002 慶応大・理工)

$f(x) = x^2 + x + 41$ に $x = 0, 1, 2, \ldots$ と代入していくと

n	$f(n)$	n	$f(n)$	n	$f(n)$
0	41	14	251	28	853
1	43	15	281	29	911
2	47	16	313	30	971
3	53	17	347	31	1033
4	61	18	383	32	1097
5	71	19	421	33	1163
6	83	20	461	34	1231
7	97	21	503	35	1301
8	113	22	547	36	1373
9	131	23	593	37	1447
10	151	24	641	38	1523
11	173	25	691	39	1601
12	197	26	743		
13	223	27	797		

$n = 0, 1, 2, \ldots, 39$ に対して，$f(n)$ は素数となるが，$n = 40$ と $n = 41$ のとき $f(n)$ は素数ではない．なぜならば，

$$f(40) = 40^2+40+41 = 40\cdot 41+41 = 41^2, f(41) = 41^2+41+41 = 41(41+1+1) = 41\cdot 43$$

となるからである．

「任意の正の整数 n に対してその値が素数になるような整数係数の素数生成多項式は定数以外には存在しない」というのが上の問題 2.1.3 である．

- $f(x) = x^2 + x + 41$ が無限個の素数を生成するかどうかはわかっていない．
- $f(x) = \left(x + \dfrac{1}{2}\right)^2 + \dfrac{163}{4}$ と変形できる．

「Aoba Scientia 研究室訪問」によれば

$$e^{\pi\sqrt{163}} = 262537412640768743.9999999999992\cdots$$

という数が整数に非常に近く（整数との差が 10^{-12} 未満）なっている．

素数生成多項式について調べたので，整数値多項式についても調べておこう．「数学の問題」([105]) の B の問題 12 を引用する．

次の (a) または (b) の問いに答えよ．

(a)　$g_0(x)=1,\ g_1(x)=x,\ g_2(x)=\dfrac{x(x-1)}{2!},\ \ldots,$

$g_n(x)=\dfrac{x(x-1)(x-2)\cdots(x-n+1)}{n!}$ と定義する．

(1) すべての整数 k に対して $g_n(k)$ は 整数であることを示せ．

(2) 任意の n 次多項式 $f(x)$ は $f(x)=\displaystyle\sum_{i=0}^{n}a_ig_i(x)$ の形で表せることを示せ．

(3) n を自然数，$P(x)$ を n 次の多項式とする．
$P(0), P(1), \ldots, P(n)$ が整数ならば，すべての整数 k に対し，$P(k)$ は整数であることを証明せよ．

(b) (1) $n\,(\geq 1)$ 次の整式 $P(x)$ に対して $P(x+1)-P(x)$ は $n-1$ 次の整式となることを示せ．

(2) n を自然数，$P(x)$ を n 次の多項式とする．
$P(0), P(1), \ldots, P(n)$ が整数ならば，すべての整数 k に対し，$P(k)$ は整数であることを証明せよ．

(a)(1) 例題 2.1.1 で扱っている．

解 (a)(1)　$k\geq n$ のとき　$g_n(k)={}_kC_n$ は整数である．

$0\leq k<n$ のとき　$g_n(k)=0$ は整数である．

$k<0$ のとき　$l=-k$ とおくと

$$\begin{aligned}g_n(k)&=\frac{-l(-l-1)(-l-2)\cdots(-l-n+1)}{n!}\\&=(-1)^n\frac{l(l+1)\cdots(l+n-1)}{n!}\\&=(-1)^n{}_{l+n-1}C_n\end{aligned}$$

は整数である．

(2) n に関する数学的次帰納法で示す．

(I) $n=0$ のとき，$f(x)=c$ は $f(x)=cg_0(x)$ と表せる．

(II) $n\leq m-1$ のとき成り立つとすると，任意の m 次多項式
$f(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m$ に対し，$f(x)-b_0m!g_m(x)$ は $m-1$ 次以下の多項式なので，帰納法の仮定から

$f(x)-b_0m!g_m(x)=\sum_{i=0}^{m-1}b_ig_i(x)$ とおける．よって，

$f(x)=\sum_{i=0}^{m-1}b_ig_i(x)+b_0m!g_m(x)$ となり，$n=m$ のときも成り立つ．

(III) (I)，(II) からすべての n について成り立つ．

(3)　$P(x)=\sum_{i=0}^{n}a_ig_i(x)$ とおくと，

$P(0)=a_0$,$P(1)=a_0+a_1$,

$P(2)=a_0+2a_1+a_2$,$P(3)=a_0+3a_1+3a_2+a_3$,

$\cdots\cdots$

$P(n)=a_0+{}_nC_1a_1+{}_nC_2a_2+\cdots\cdots+a_n$.

$P(0)$, $P(1)$, …, $P(n)$ が整数なので，a_0, a_1, …, a_n が整数となる．

($a_0=P(0)$ は整数で，$a_0,\ldots,a_{k-1}$ が整数ならば，

$a_k=P(k)-a_0-{}_kC_1a_1-\cdots-{}_kC_{k-1}a_{k-1}$ は整数となり，帰納的に a_0, a_1, …, a_n が整数となることが言える．)

また，整数 k に対し，$g_i(k)$ は整数であるから，$P(k)=\sum_{i=0}^{m}a_ig_i(k)$ は整数である．　□

解 (b) (1)　$P(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$, $a_0\neq0$ とおく．

$n=1$ のとき，$P(x)=a_0x+a_1$, $a_0\neq0$ とおくと，$P(x+1)-P(x)=a_0$ で 0 次式となり成り立つ．

$n\geq2$ のとき

$$\begin{aligned}P(x+1)-P(x)&=a_0\left\{nx^{n-1}+(n-2\text{ 次以下の整式})\right\}\\&\quad+a_1\left\{(n-1)x^{n-2}+(n-3\text{ 次以下の整式})\right\}\\&\quad+\cdots+a_{n-1}\\&=a_0nx^{n-1}+(n-2\text{ 次以下の整式}).\end{aligned}$$

よって，$P(x+1)-P(x)$ は $n-1$ 次の整式である．

(2) $P(x)$ の 次数 n についての数学的帰納法で証明する．

(I) $n=1$ のとき　$P(x)=ax+b$ について $P(0)=b$, $P(1)=a+b$ が整数だから a, b は整数となる．したがって，すべての整数 k に対し，$P(k)=ak+b$ は整数である．

(II) $n=m$ のとき成り立つと仮定する．$m+1$ 次多項式 $P(x)$ に対し，多項式 $Q(x)$ を $Q(x)=P(x+1)-P(x)$ とおく．

$Q(x)$ は m 次の多項式で，

$Q(0)=P(1)-P(0)$ $Q(1)=P(2)-P(1)$, …, $Q(m)=P(m+1)-P(m)$

はすべて整数であるから，数学的帰納法の仮定より，すべての整数 k に対し，$Q(k)$ は整数である．
したがって，$P(0)$ が整数であることと

$$P(-1)-P(-2),\ P(0)-P(-1),\ P(1)-P(0),\ P(2)-P(1),\ \cdots$$

がすべて整数であることから，すべての整数 k に対し，$P(k)$ は整数である．よって，$n=m+1$ のときも成り立つ．

(III) (I)，(II) からすべての n について成り立つ．　□

(b) の解法のポイントは

すべての整数 k に対し，$f(k)$ が整数

$$\Longleftrightarrow \begin{cases} f(0) \text{ が整数}\quad (\text{ ある整数 } k_0 \text{ について } f(k_0) \text{ が整数でもよい }) \text{ かつ} \\ \text{すべての整数 } k \text{ に対し，} f(k+1)-f(k) \text{ が整数} \end{cases}$$

と，$f(x)$ が $n\,(\geq 1)$ のとき，$\Delta f(x)=f(x+1)-f(x)$ が $n-1$ 次式となることである．

前半の部分

すべての整数 k に対し，$f(k)$ が整数

$$\Longleftrightarrow \begin{cases} f(0) \text{ が整数) かつ} \\ \text{すべての整数 } k \text{ に対し，} f(k+1)-f(k) \text{ が整数} \end{cases}$$

を証明しておく．

証明 $\Longrightarrow$ は明らかに成り立つから，$\Longleftarrow$ を示せばよい．

$f(0)$ は整数である．

整数 n について，$f(n)$ が整数であると，$f(n)-f(n-1)$, $f(n+1)-f(n)$ が整数であることから，$f(n-1)$, $f(n+1)$ は整数である．よって，数学的帰納法により，すべての整数 k について $f(k)$ は整数である．　□

一般の n 次式の場合は，東京工大の入試問題が有名である．

類題　n を自然数，$P(x)$ を n 次の多項式とする．$P(0),\ P(1),\ \cdots\cdots,\ P(n)$ が整数ならば，すべての整数 k に対し，$P(k)$ は整数であることを証明せよ．
（1993 東京工大・前期，2008 東京工大 AO）

「数学の問題」([105]) の B の問題 12 の類題をあげておく．

n は 3 以上の整数とする．

(1) $g(x)=(x+n-1)(x+n-2)\cdots\cdots(x+1)x$ を n 次多項式とする．1 以上のすべての整数 k に対し，$g(k)$ は $n!$ の倍数であることを示せ．

(2) $f(x)$ は x^n の係数を 1 とする n 次多項式とする．

$$f_1(x)=f(x+1)-f(x)$$

の x^{n-1} の係数および

$$f_2(x)=f_1(x+1)-f_1(x)$$

の x^{n-2} の係数をそれぞれ求めよ．

(3) a を 1 以上の整数，$f(x)$ を (2) の多項式とする．1 以上のすべての整数 k について $f(k)$ が整数で a を約数にもつとき，a は $n!$ の約数であることを示せ．

(1996 北海道大・理系・後期)

0 以上の任意の整数 i に対して，x の i 次式 $g_i(x)$ を

$i=0$ のとき $g_0(x)=1$, $i\geqq 1$ のとき $g_i(x)=\dfrac{x(x+1)\cdots\cdots(x+i-1)}{i!}$

と定義する．

(1) $f(x)=\displaystyle\sum_{i=0}^{n}a_ix^i$ （但し $a_n\neq 0$ ）を x に関する実数係数の $n\,(\geqq 0)$ 次式とする．このとき，等式 $f(x)=\displaystyle\sum_{i=0}^{n}c_ig_i(x)$ が任意の実数 x について成り立つような実数 $c_i\,(0\leqq i\leqq n$，但し $c_n\neq 0)$ が一意的に存在することを証明せよ．

(2) (1) において，$n>0$ のとき等式 $f(x)-f(x-1)=\displaystyle\sum_{i=1}^{n}c_ig_{i-1}(x)$ が成り立つことを証明せよ．

(3) $F(x)\,(\neq 0)$ を x に関する実数係数の $n\,(\geqq 0)$ 次式とし，任意の整数 a に対して $F(a)$ が整数であるとする．このとき，等式 $F(x)=\displaystyle\sum_{i=0}^{n}d_ig_i(x)$ が任意の実数 x について成り立つような整数 $d_i\,(0\leqq i\leqq n$，但し $d_n\neq 0)$ が一意的に存在することを証明せよ．

(2011 奈良県立医大)

次の問題では，原題に $C_0(x)=1$ を追加した．

x に関する多項式 $C_0(x)=1$, $C_n(x)=\dfrac{x(x-1)\cdots\cdots(x-n+1)}{n!}$ $(n\geqq 1)$ を用いて，関係式 $x\{f(x+1)-f(x)\}=rf(x)$ (r は自然数) を満たす多項式 $f(x)$ を求める．

1) 0 以上の整数 n に対して，次の命題が成立する．

$P(n)$: 任意の n 次多項式 $p(x)$ は $p(x)=\sum_{k=0}^{n} a_kC_k(x)$ (a_kは定数, $a_n\neq 0$) のように一通りに表される．

この命題 $P(n)$ を証明するためには次の数学的帰納法を用いる．

数学的帰納法：命題 $P(n)$ が 0 以上のすべての整数 n に対して成立することを示すには，以下を示せばよい．

[I]　$P(0)$ が成立する．

[II]　$0\leqq k\leqq n-1$ なるすべての整数 k に対して，$P(k)$ が成立するならば $P(n)$ が成立する．

命題 $P(n)$ の証明：$p(x)$ が定数の場合は明らかであるから，$P\left(\boxed{\text{ア}}\right)$ が成立する．次数が $\boxed{\text{イ}}$ 以下の多項式に関して命題が成立すると仮定する．$p(x)$ の n 次の係数を a とする．多項式 $n!C_n(x)$ は $\boxed{\text{ウ}}$ 次であり，$\boxed{\text{ウ}}$ 次の係数は $\boxed{\text{エ}}$ であるから，$q(x)=p(x)-\boxed{\text{オ}}\,n!C_n(x)$ は $\boxed{\text{カ}}$ または $\boxed{\text{カ}}$ でない $\boxed{\text{キ}}$ 次以下の多項式である．前者の場合，$p(x)=\boxed{\text{オ}}\,n!C_n(x)$ である．後者の場合，帰納法の仮定によって $q(x)=\sum_{k=0}^{m} a_kC_k(x)$($a_k$は定数, $a_m\neq 0$, $m\leqq n-1$) のように一通りに表される．

したがって，$p(x)=\boxed{\text{オ}}\,n!C_n(x)+q(x)$ となり $P(n)$ が成立する．

以上により命題が証明された．

2) さて，$f(x)$ を n 次多項式とし，1) の結果を用いて $f(x)=\sum_{k=0}^{\boxed{\text{ク}}} a_kC_k(x)$ $(a_n\neq 0)$ と表す．

$x\{C_k(x+1)-C_k(x)\}=\boxed{\text{ケ}}\,C_{k-1}(x)+\boxed{\text{コ}}\,C_k(x)$ $(1\leqq k)$ であるから，$f(x)$ の関係式と 1) の結果より $\boxed{\text{サ}}\,(a_k+a_{k+1})=\boxed{\text{シ}}\,a_k$ $(0\leqq k\leqq n-1)$ を得る．$n=\boxed{\text{ス}}, a_0=\boxed{\text{セ}}$ であり，よって $a_k={}_{r-1}\mathrm{C}_{\boxed{\text{ソ}}}\,a_1$ $(1\leqq k\leqq r)$ であることがわかる．したがって

$f(x)=a_r\sum_{k=1}^{r} {}_{r-1}\mathrm{C}_{\boxed{\text{ソ}}}C_{\boxed{\text{タ}}}(x)$ を得る．　(2001 慶応大・環境情報・改題)

2.2　最大公約数

m と n は整数で，少なくとも一方は 0 ではないものとする．m と n の**最大公約数**とは，m と n を割り切る最大の正整数をいう．

m と n の最大公約数を $\mathbf{gcd}(\boldsymbol{m}, \boldsymbol{n})$ または $(\boldsymbol{m}, \boldsymbol{n})$ で表す．

- $a, b \in \mathbb{Z}$，$a \neq 0$ または $b \neq 0$ のとき，$\gcd(a, b) = \gcd(|a|, |b|)$ が成り立つ．
- $c \in \mathbb{Z}$，$c \neq 0$ のとき，$\gcd(c, 0) = |c|$ が成り立つ．

定理 2.2.1　a, b は整数で少なくとも一方は 0 ではないものとする．

このとき，$ax_0 + by_0 = \gcd(a, b)$ を満たす整数 x_0, y_0 が存在する．さらに

$$\Big\{ax + by : x,\ y \in \mathbb{Z}\Big\} = \Big\{k(a,\ b) : k \in \mathbb{Z}\Big\}$$

が成り立つ．

証明　$S = \Big\{ax + by : x,\ y \in \mathbb{Z},\ ax + by > 0\Big\}$ とおく．

$$a = a \cdot 1 + b \cdot 0,\ -a = a \cdot (-1) + b \cdot 0,\ b = a \cdot 0 + b \cdot 1,\ -b = a \cdot 0 + b \cdot (-1).$$

a と b の少なくとも一方は 0 ではないから，a, $-a$, b, $-b$ の少なくとも一つは正の整数である．よって，a, $-a$, b, $-b$ の少なくとも一つは S に属するから，S は空集合ではない．したがって，S の中には最小なものが存在するから，これを d とおくと $d = ax_0 + by_0$ となる整数 x_0, y_0 が存在する．

$T = \Big\{ax + by : x,\ y \in \mathbb{Z}\Big\}$ とおく．

(a) $\Big\{kd : k \in \mathbb{Z}\Big\} \subseteq T$.

$kd = k(ax_0 + by_0) = a(kx_0) + b(ky_0)$, $kx_0, ky_0 \in \mathbb{Z}$ より $kd \in T$.

(b) $T \subseteq \Big\{kd : k \in \mathbb{Z}\Big\}$.

$t \in T$ とすると $t = ax_1 + by_1$, $x_1, y_1 \in \mathbb{Z}$ とかける．

t を d で割った商を q，余りを r とすると $t = dq + r$, $0 \leq r < d$ を満たす整数 q, r がある．よって

$$r = t - dq = ax_1 + by_1 - (ax_0 + by_0)q = a(x_1 - x_0q) + b(y_1 - y_0q) \in T.$$

d の S における最小性から $r = 0$ を得る．このとき，$t = dq$ となり $t \in \Big\{kd : k \in \mathbb{Z}\Big\}$.

(c) $d = (a, b)$.

(a)，(b) から $T = \Big\{kd : k \in \mathbb{Z}\Big\}$ が成り立つので $d = (a, b)$ を示す．

$g=(a,\,b)$ とおくと $a=ga_1,\,b=gb_1,\,a_1,b_1\in\mathbb{Z},\,(a_1,\,b_1)=1$ とかけるから，これを $d=ax_0+by_0$ に代入すると

$$d=ax_0+by_0=ga_1\cdot x_0+gb_1\cdot y_0=g(a_1x_0+b_1y_0).$$

これから，$g\mid d$ が言えて $g\le d$.
$a=a\cdot1+b\cdot0\in T,\,b=a\cdot0+b\cdot1\in T$ なので，(b) より $a,b\in\left\{kd:k\in\mathbb{Z}\right\}$ が言えて $d\mid a,\,d\mid b$ が成り立つ．
$(a,\,b)$ は $a,\,b$ を割り切る最大の正整数だから，$d\le(a,b)=g$ が成り立つ．$g\le d$ であったから，$d=g=(a,b)$.
これで，定理は証明された．　□

$a,\,b$ は整数で少なくとも一方は 0 ではないものとする．$a,\,b$ の最大公約数が 1 すなわち $\gcd(a,\,b)=1$ のとき a と b は**互いに素** (relatively prime または coprime) であるという．
定理 2.2.1 より次の系を得る．

系 2.2.1　a と b は互いに素な整数とする．
このとき，$ax+by=1$ を満たす整数 $x,\,y$ が存在する．

定理 2.2.2　a と b は互いに素な正整数とする．このとき，$au-bv=1$ を満たす正整数 $u,\,v$ が存在する．

証明　$a\ge2$ の場合

- $1\cdot a,2\cdot a,\ldots,(b-1)a$ を考える．これらの数を b で割ったときの余りは異なる．

もしも，そうでなければ

$$k_1a=bq_1+r,\;k_2a=bq_2+r,q_1,q_2\in\mathbb{Z},r\in\mathbb{N}_0,0\le r<b$$

を満たす $k_1,k_2,\;k_1>k_2,\,k_1,k_2\in\left\{1,\,2,\,\ldots,\,b-1\right\}$ が存在する．
すると

$$k_1a-k_2a=bq_1+r-(bq_2+r)=b(q_1-q_2)$$

から

$$(k_1-k_2)a=(q_1-q_2)b.$$

$(k_1-k_2)a$ は b で割り切れるが，a と b は互いに素であるから，k_1-k_2 は b で割り切れる．
ところが，$0<k_1-k_2<b$ であるから，k_1-k_2 は b で割り切れず，$b\mid k_1-k_2$ に矛盾する．

• $1\cdot a, 2\cdot a, \ldots, (b-1)a$ の中には b で割り切れるものが存在しない．
もしも，$ka = bq,\ q \in \mathbb{N}$ となる $k \in \{1, 2, \ldots, b-1\}$ が存在したとする．
$d = \gcd(k, q)$ とすると，$k = dk_1, q = dq_1, k_1, q_1 \in \mathbb{N}, \gcd(k_1, q_1) = 1$ とおけるから，
これらの式を $ka = bq$ に代入すると，$dk_1 a = bdq_1$ から

$$k_1 a = q_1 b.$$

$\gcd(a, b) = 1$ だから，$b \mid k_1$ が成り立つ．
すると，$b \leq k_1$ だから

$$b \leq k_1 \leq dk_1 = k < b$$

となり，矛盾が生じる．
$1\cdot a, 2\cdot a, \ldots, (b-1)a$ を b で割ったときの余りは異なり，これらの中には b で割り切れるものが存在しないから，$1\cdot a, 2\cdot a, \ldots, (b-1)a$ を b で割ったときの余りの集合は，$\{1, 2, \ldots, b-1\}$ と一致する．
よって，$1\cdot a, 2\cdot a, \ldots, (b-1)a$ の中の一つは b で割ったときの余りが 1 であるから，
$au = bv + 1$ となる $u \in \{1, 2, \ldots, b-1\}, v \in \mathbb{N}_0$ が存在する．

$$bv = au - 1 \geq a - 1 > 0 \qquad (\because a \geq 2)$$

より $v \geq 1$ である．
よって，$au - bv = 1$ を満たす正整数 u, v が存在する．

(2) $a = 1$ の場合
任意の正整数 v に対して，$u = bv + 1 (> 0)$ とおけば，$au - bv = 1$ が成り立つ． □

系 2.2.2　a と b は正整数とする．
このとき，$au - bv = \gcd(a, b)$ を満たす正整数 u, v が存在する．

証明　$g = \gcd(a, b)$ とすると，$a = ga_1, b = gb_2, a_1, b_1 \in \mathbb{N}, \gcd(a_1, b_1) = 1$ とおける．定理 2.2.2 より $a_1 u - b_1 v = 1$ を満たす正整数 u, v が存在する．この等式の両辺に g をかけると，$ga_1 u - gb_1 v = g$ すなわち $au - bv = \gcd(a, b)$ となる． □

定理 2.2.3　a, b, c は整数で，a と b の少なくとも一方は 0 ではないものとする．

(1)　a と b は互いに素で，$a \mid bc$ ならば $a \mid c$ が成り立つ．
(2)　$c \mid a$ かつ $c \mid b$ ならば $c \mid \gcd(a, b)$ が成り立つ．

証明　a と b は互いに素であるから，系 2.2.1 より $ax+by=1$ を満たす整数 $x,\ y$ が存在する．このとき，$c=c\cdot 1=c(ax+by)=acx+bcy$.

$a|ac,\ a|bc$ であるから，$a \mid acx+bcy=c$ すなわち $a \mid c$ が成り立つ．

(2) 定理 2.2.1 より $ax_0+by_0=\gcd(a,\ b)$ を満たす整数 $x_0,\ y_0$ が存在する．

$c \mid a$ かつ $c \mid b$ より $c \mid ax_0+by_0=\gcd(a,\ b)$ すなわち $c \mid \gcd(a,\ b)$ が成り立つ．　□

例題 2.2.1　座標平面において，x 座標，y 座標がともに整数である点を格子点と呼ぶ．四つの格子点 $\mathrm{O}(0,0),\mathrm{A}(a,b),\mathrm{B}(a,b+1),\mathrm{C}(0,1)$ を考える．ただし，a,b は正の整数で，その最大公約数は 1 である．

(1)　平行四辺形 OABC の内部（辺，頂点は含めない）に格子点はいくつあるか．

(2)　(1) の格子点全体を $\mathrm{P}_1,\mathrm{P}_2,\ldots,\mathrm{P}_t$ とするとき，$\triangle \mathrm{OP}_i\mathrm{A}\ (i=1,2,\ldots,t)$ の面積のうちの最小値を求めよ．ただし $a>1$ とする．　(1989 京都大・理・後期)

a と b が互いに素な正の整数のとき，$au-bv=1$ を満たす正の整数 u,v が存在することに気づきたい．

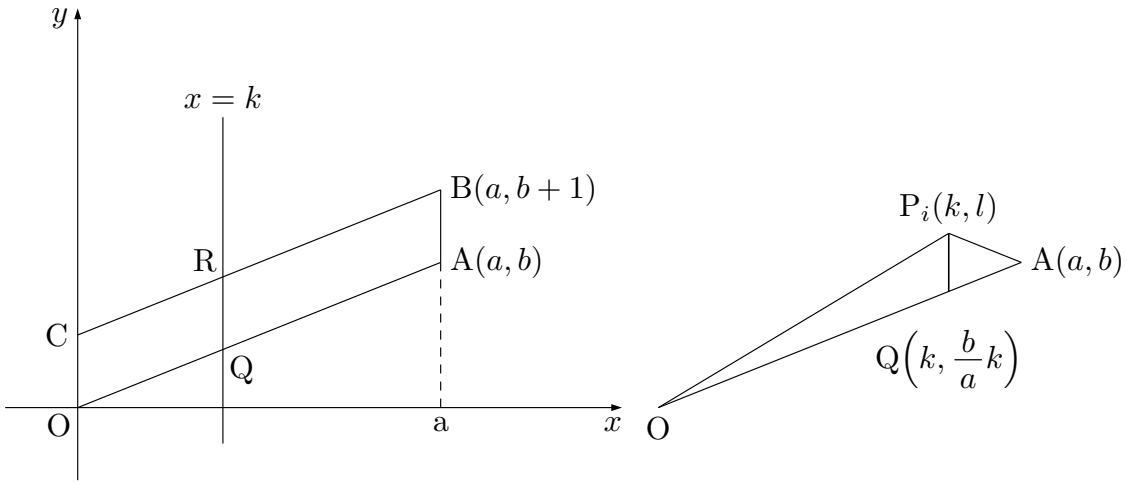
解答 (1) $a\geq 2$ のとき，$1\leq k\leq a-1$ を満たす整数 k に対して，$\mathrm{Q}\left(k,\ \dfrac{b}{a}k\right)$,

$\mathrm{R}\left(k,\ \dfrac{b}{a}k+1\right)$ とおくと $\mathrm{QR}=1$．a と b は互いに素で $1\leq k\leq a-1$ だから，$\dfrac{b}{a}k$ は整数にならないので，Q,R は格子点ではない．

よって，線分 QR(端点を除く) 上には格子点が 1 つだけ存在するから，平行四辺形 OABC の内部（辺，頂点は含めない）に格子点は $a-1$ 個ある．

$a=1$ のとき，平行四辺形 OABC の内部（辺，頂点は含めない）に格子点は 0 個である．

したがって，平行四辺形 OABC の内部（辺，頂点は含めない）に格子点は $a-1$ 個ある．



(2) $\mathrm{P}_i(k,l)$ $(1 \leq k \leq a-1)$ とおくと

$$\triangle \mathrm{OP}_i\mathrm{A} = \frac{1}{2}a\left(l - \frac{b}{a}k\right) = \frac{1}{2}(al - bk) \geq \frac{1}{2} \qquad \cdots\cdots(*)$$

が成り立つ．

次に $(*)$ で等号が成り立つ場合があることを示す．

すなわち，$al - bk = 1$ を満たす整数 k, l $\left(1 \leq k \leq a-1,\ \frac{b}{a}k < l < \frac{b}{a}k + 1\right)$ が存在することを示す．

a と b は互いに素であるから，$ax_0 - by_0 = 1$ を満たす整数 x_0, y_0 が存在する．

$ax - by = 1$ を満たす整数解は $ax - by - (ax_0 - by_0) = 1 - 1 = 0$ から，

$$a(x - x_0) = b(y - y_0).$$

a と b は互いに素であるから，l を整数として，$x - x_0 = bl, y - y_0 = al$ とかける．

$y \equiv y_0 \pmod{a}$ であるから，$1 \leq y_0 \leq a-1$ とすることができる．（$y_0 = 0$ だと，$ax_0 = 1$ となるが，$a > 1$ に矛盾する．）$k = y_0$ とすると，$ax_0 - bk = 1$.

$bk \equiv ax_0 - 1 \equiv -1 \equiv a - 1 \pmod{a}$ より，$bk = aq + a - 1$ $(q \in \mathbb{Z})$ とおける．この式は $l = q + 1$ とおくと，$al - bk = 1$ となる．

$l = \dfrac{bk+1}{a}$ だから，$\dfrac{b}{a}k < l < \dfrac{b}{a}k + 1$ を満たす． □

例題 2.2.2　xy 平面上，x 座標，y 座標がともに整数であるような点 (m, n) を格子点と呼ぶ．各格子点を中心として半径 r の円がえがかれており，傾き $\dfrac{2}{5}$ の任意の直線はこれらの円のどれかと共有点をもつという．このような性質をもつ実数 r の最小値を求めよ．　(1991 東京大・理)

2 と 5 が互いに素であるから，$2x_0 - 5y_0 = 1$ を満たす整数 x_0, y_0 が存在する．これから，任意の整数 k に対して $2(kx_0) - 5(ky_0) = k$ が成り立つので，任意の整数は $2x - 5y$ の形に表すことができる．

解答　点 (m, n) を中心とする半径 r の円が，傾き $\dfrac{2}{5}$ の直線 $2x - 5y - t = 0$ と共有点を持つための条件は

$$\frac{|2m - 5n - t|}{\sqrt{(-2)^2 + 5^2}} \leq r \qquad \cdots\cdots①$$

となることである．したがって，任意の実数 t に対して，①が成り立つような整数 m, n が存在するような r の最小値を求めればよい．

論理記号を使ってかくと次のようになる．

「$\forall t \in \mathbb{R},\ \exists m, n \in \mathbb{Z}\ ;\ \dfrac{|2m - 5n - t|}{\sqrt{29}} \leq r$」が成り立つような r の最小値を求める．

$2(3k)-5(k)=k$ より，任意の整数 k に対して，$m=2k, n=k$ とおけば，$2m-5n=k$ となるので，$2m-5n$ は任意の整数値をとれる．よって，$2m-5n=N$ とおくと，N は整数で，任意の整数値をとれる．

任意の実数 t に対して，

$$\frac{|N-t|}{\sqrt{29}} \leq r \qquad \cdots\cdots ②$$

が成り立つような整数 N が存在するような r の最小値を求めればよい．

数直線上で，任意の実数 t と整数との差を考えると，0.5 以下の整数が存在することに注意する．

$t=\dfrac{1}{2}$ のとき，$\dfrac{1}{2} \leq \left|N-\dfrac{1}{2}\right|$　(等号は $N=0$ または $N=1$ のときに成り立つ．)

これから

$$\frac{1}{2\sqrt{29}} \leq \frac{\left|N-\dfrac{1}{2}\right|}{\sqrt{29}} \leq r.$$

よって，

$$\frac{1}{2\sqrt{29}} \leq r \qquad \cdots\cdots ③$$

が成り立つ．

②は $t-\sqrt{29}\,r \leq N \leq t+\sqrt{29}\,r$ と同値で，③が成り立つとき，

$$t+\sqrt{29}\,r-\left(t-\sqrt{29}\,r\right)=2\sqrt{29}\,r \geq 1$$

となり，$t-\sqrt{29}\,r \leq N \leq t+\sqrt{29}\,r$ を満たす整数 N が存在することになる．

よって，r の最小値は $\dfrac{1}{2\sqrt{29}}$ である．　□

例題 2.2.3　(IMO 1979)

a, b は

$$\frac{a}{b}=1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{1318}+\frac{1}{1319}$$

を満たす正の整数とする．

$1979 \mid a$ であることを証明せよ．

解答 次の補題を示しておく．

n を正の整数とするとき，

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{2n-1}-\frac{1}{2n}=\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n} \quad \cdots①$$

が成り立つ．

補題の証明 1　n に関する数学的帰納法で証明する．

(1) $n=1$ のとき，左辺 $=1-\dfrac{1}{2}=\dfrac{1}{2}$，右辺 $=\dfrac{1}{2}$ であるから ①は成り立つ．

(2) n のとき成り立つと仮定して，①の両辺に $\dfrac{1}{2n+1}-\dfrac{1}{2n+2}$ を加えると

$$\begin{aligned}
&1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{2n-1}-\frac{1}{2n}+\frac{1}{2n+1}-\frac{1}{2n+2}\\
&=\underline{\frac{1}{n+1}}+\frac{1}{n+2}+\cdots+\frac{1}{2n}+\frac{1}{2n+1}-\underline{\frac{1}{2n+2}}\\
&=\frac{1}{n+2}+\cdots+\frac{1}{2n}++\frac{1}{2n+1}+\underline{\frac{1}{2n+2}}
\end{aligned}$$

となり，$n+1$ のときも①は成り立つ．

(3) (I)，(II) よりすべての正の整数 n に対して，①は成り立つ． ■

補題の証明 2　①は帰納法を使わなくても証明できる．

$$\begin{aligned}
&1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{2n-1}-\frac{1}{2n}\\
&=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{2n-1}+\frac{1}{2n}-2\cdot\frac{1}{2}-2\cdot\frac{1}{4}-2\cdot\frac{1}{6}-\cdots-2\cdot\frac{1}{2n}\\
&=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{2n-1}+\frac{1}{2n}-2\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\cdots+\frac{1}{2n}\right)\\
&=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{2n-1}+\frac{1}{2n}-\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}\right)\\
&=\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n}
\end{aligned}$$

から①は成り立つ． ■

補題を用いると

$$\begin{aligned}
\frac{a}{b}&=\left(1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{1318}\right)+\frac{1}{1319}\\
&=\frac{1}{659+1}+\frac{1}{659+2}+\cdots+\frac{1}{2\cdot659}+\frac{1}{1319}\\
&=\underbrace{\frac{1}{660}+\frac{1}{661}+\cdots+\frac{1}{1318}+\frac{1}{1319}}_{660}\\
&=\left(\frac{1}{660}+\frac{1}{1319}\right)+\left(\frac{1}{661}+\frac{1}{1318}\right)+\cdots+\left(\frac{1}{989}+\frac{1}{990}\right)\\
&=\frac{1319+660}{660\cdot1319}+\frac{1318+661}{661\cdot1318}+\cdots+\frac{990+989}{989\cdot990}\\
&=\frac{1979}{660\cdot1319}+\frac{1979}{661\cdot1318}+\cdots+\frac{1979}{989\cdot990}\\
&=1979\left(\underline{\frac{1}{660\cdot1319}+\frac{1}{661\cdot1318}+\cdots+\frac{1}{989\cdot990}}\right)
\end{aligned}$$

と変形できる．下線部を $\dfrac{a'}{b'}$ (a' と b' は互いに素) と表すと

$$\frac{a'}{b'}=\frac{1}{660\cdot1319}+\frac{1}{661\cdot1318}+\cdots+\frac{1}{989\cdot990}$$

から

$$\frac{a}{b} = 1979 \cdot \frac{a'}{b'} \text{ すなわち } a = 1979 \cdot a' \cdot \frac{b}{b'}.$$

1979 は素数で，b' は 1319 より小さい数を素因数にしているから，b' と 1979 は互いに素である．また，a' と b' は互いに素であるから，b' は b の約数である．

よって，1979 は a の約数となり，$1979 \mid a$ である． □

- 補題は，数 III で $\lim_{n\to\infty}\left(1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{2n-1}-\frac{1}{2n}\right)$ を求めるときに使われる等式である．

参考までに極限を求めると

$$\begin{aligned}
&\lim_{n\to\infty}\left(1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{2n-1}-\frac{1}{2n}\right)\\
&=\lim_{n\to\infty}\left(\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n}\right)\\
&=\lim_{n\to\infty}\frac{1}{n}\left(\frac{1}{1+\frac{1}{n}}+\frac{1}{1+\frac{2}{n}}+\cdots+\frac{1}{1+\frac{n}{n}}\right)\\
&=\int_0^1\frac{1}{1+x}\,dx\\
&=\Big[\log|1+x|\Big]_0^1\\
&=\log 2.
\end{aligned}$$

問題 2.2.1 a, b, c は整数で，a と b の少なくとも一方は 0 ではないものとする．このとき，次のことが成り立つことを示せ．

$$a \mid c,\ b \mid c,\ \gcd(a,\ b) = 1 \quad \Longrightarrow \quad ab \mid c.$$

2.3　ユークリッドの互除法

定理 2.3.1　a, b, q は整数で，a と b の少なくとも一方は 0 ではないものとする．このとき，

$$\gcd(a, b) = \gcd(a - qb, b)$$

が成り立つ．

証明　$r = a - qb$ とおき $(a, b) = (r, b)$ を示す．

$d = (a, b)$ とおくと，$d \mid a, d \mid b$ から $d \mid a - qb = r$ すなわち $d \mid r$.

ゆえに $d \mid b, d \mid r$ だから定理 2.2.3(2) より，$d \mid (r, b)$. これから $(a, b) \leq (r, b)$.

$d' = (r, b)$ とおくと，$d' \mid r, d' \mid b$ から $d' \mid qb + r = a$ すなわち $d' \mid a$.

ゆえに $d' \mid a, d' \mid b$ から，$d' \mid (a, b)$. これから $(r, b) \leq (a, b)$.

以上のことから，$(a, b) = (r, b)$ が成り立つ．　□

a を b で割った商を q，余りを r とおくと，$a = bq + r, 0 \leq r < b$ とかけるから，定理 2.3.1 より次のことが言える．

- a, b は正の整数で，$a > b > 0$ とする．このとき，a を b で割った商を q，余りを r とおくと

  $$\gcd(a, b) = \gcd(r, b)$$

  が成り立つ．
- 定理 2.3.1 において $q = 1$ とおくと $(a, b) = (a - b, b)$ が成り立つ．

  「a, b は正の整数で，$a > b > 0$ とすると，$(a, b) = (a - b, b)$ が成り立つ．」

  ことを扱っている高校の教科書もある．

a, b は整数で，a と b の少なくとも一方は 0 ではないものとする．このとき，

- $\gcd(a, b) = \gcd(|a|, |b|)$ が成り立つ．
- $c \in \mathbb{Z}$，$c \neq 0$ のとき，$\gcd(c, 0) = |c|$ が成り立つ．

を考慮すれば，a, b は正の整数で，$a > b > 0$ として $\gcd(a, b)$ を求めればよい．

$r_0 = a, r_1 = b$ とおき，r_0 を r_1 で割った商を q_1，余りを r_2 とおくと

$$r_0 = r_1 q_1 + r_2, \quad 0 \leq r_2 < r_1.$$

$r_2 \neq 0$ のときは，r_1 を r_2 で割った商を q_2，余りを r_3 とおくと

$$r_1 = r_2 q_2 + r_3, \quad 0 \leq r_3 < r_2.$$

$\cdots\cdots$

この操作を続けると，余りの列

$$a = r_0 > r_1 > r_2 > \cdots \geq 0$$

は a 個より多くの正整数を含み得ないから，いつかは余りは 0 となる．
すなわち

$$\left.\begin{aligned} r_0 &= r_1 q_1 + r_2, && 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, && 0 < r_3 < r_2 \\ &\vdots \qquad \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_n + r_{n+1}, && r_{n+1} = 0 \end{aligned}\right\} \tag{2.3}$$

となる正の整数 n が存在する．定理 2.3.1 より

$$(a,\, b) = (r_0,\, r_1) = (r_1,\, r_2) \cdots = (r_{n-1},\, r_n) = (r_n,\, \underbrace{r_{n+1}}_{=0}) = r_n$$

すなわち，$(a,\, b) = r_n$ が得られる．

定理 2.3.2　（**ユークリッドの互除法**）a, b, q は正の整数で，$a > b$ とする．
$r_0 = a$, $r_1 = b$ とおき，r_2, r_3, $\ldots$, r_{n+1} と n は

$$\left.\begin{aligned} r_0 &= r_1 q_1 + r_2, && 0 < r_2 < r_1, && q_1,\, r_2 \in \mathbb{N} \\ r_1 &= r_2 q_2 + r_3, && 0 < r_3 < r_2, && q_2,\, r_3 \in \mathbb{N} \\ &\vdots \qquad \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 < r_n < r_{n-1}, && q_{n-1},\, r_n \in \mathbb{N} \\ r_{n-1} &= r_n q_n + r_{n+1}, && r_{n+1} = 0, && q_n \in \mathbb{N} \end{aligned}\right\} \tag{2.4}$$

で定める．このとき

$$\gcd(a,\, b) = r_n$$

が成り立つ．

- (2.3) の式から $r_n = r_{n-2} - q_{n-1} r_{n-1}$ となり，r_n は r_{n-2} と r_{n-1} の線形結合で表せることがわかる．
  この式に $r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}$ を変形した $r_{n-1} = r_{n-3} - r_{n-2} q_{n-2}$ を代入すると

$$\begin{aligned} r_n &= r_{n-2} - q_{n-1} r_{n-1} \\ &= r_{n-2} - q_{n-1} \left(r_{n-3} - r_{n-2} q_{n-2} \right) \\ &= -q_{n-1} r_{n-3} + (1 + q_{n-2} q_{n-1}) r_{n-2} \end{aligned}$$

となり，r_n は r_{n-3} と r_{n-2} の線形結合で表せることがわかる．

この操作を続けて，$r_{n-2}, r_{n-3}, \ldots, r_2$ を消去していくと，$r_n = \gcd(a, b)$ は a と b の線形結合 $x_0a + y_0b$ で表せることになる．これは，定理 2.2.1 の前半部分の別証明になっている．

- gcd(803, 154) を求めよ．

$$\begin{aligned} &(803,\ 154) && 803 = 154 \times 5 + 33 \\ &= (154,\ 33) && 154 = 33 \times 4 + 22 \\ &= (33,\ 22) && 33 = 22 \times 1 + 11 \\ &= (22,\ 11) && 22 = 11 \times 2 + 0 \\ &= (11,\ 0) \\ &= 11 \end{aligned}$$

よって　$\gcd(803,\ 154) = 11$.

- 不定方程式 $803x + 154y = 11$ の特殊解を求めよ．

$33 = 22 \times 1 + 11$ から $11 = 33 - 22 \times 1$.

この式に $154 = 33 \times 4 + 22$ を変形した $22 = 154 - 33 \times 4$ を代入すると

$$\begin{aligned} 11 &= 33 - 22 \times 1 \\ 11 &= 33 - (154 - 33 \times 4) \times 1 \\ &= 33 \times 5 - 154. \end{aligned}$$

この式に $803 = 154 \times 5 + 33$ を変形した $33 = 803 - 154 \times 5$ を代入すると

$$\begin{aligned} 11 &= 33 \times 5 - 154 \\ &= (803 - 154 \times 5) \times 5 - 154 \\ &= 803 \times 5 + 154 \times (-26). \end{aligned}$$

不定方程式 $803x + 154y = 11$ の特殊解として $x = 5$, $y = -26$ が得られた．

- *Blankinship's method*

  Blankinship's method は $\gcd(a, b)$ と不定方程式 $ax + by = (a, b)$ の特殊解を求めるのに実用的である．

> a, b は正の整数で，$a > b$ とする．
>
> $$A = \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$$
>
> として，行に対する操作だけを行い，A を変形する．
> そして
> $$\begin{pmatrix} d & x_0 & y_0 \\ 0 & x_1 & y_1 \end{pmatrix} \quad \text{または} \quad \begin{pmatrix} 0 & x_1 & y_1 \\ d & x_0 & y_0 \end{pmatrix}$$
> の形になれば，$(a, b) = d$ となり，不定方程式 $ax + by = (a, b)$ の特殊解として $x = x_0, y = y_0$ が得られる．

  原理については，連立方程式を解く方法と同じ操作（加減法）を

$$\begin{cases} a = a \cdot 1 + b \cdot 0 \\ b = a \cdot 0 + b \cdot 1 \end{cases}$$

  に行っているだけである．

- $a = 803, b = 154$ に対して *Blankinship's method* を適用してみる．

$$\begin{aligned}
A &= \begin{pmatrix} 803 & 1 & 0 \\ 154 & 0 & 1 \end{pmatrix} \\
&\quad \downarrow \quad (\text{第 1 行}) - (\text{第 2 行}) \times 5 \qquad 803 = 154 \times 5 + 33 \\
&\begin{pmatrix} 33 & 1 & -5 \\ 154 & 0 & 1 \end{pmatrix} \\
&\quad \downarrow \quad (\text{第 2 行}) - (\text{第 1 行}) \times 4 \qquad 154 = 33 \times 4 + 22 \\
&\begin{pmatrix} 33 & 1 & -5 \\ 22 & -4 & 21 \end{pmatrix} \\
&\quad \downarrow \quad (\text{第 1 行}) - (\text{第 2 行}) \qquad 33 = 22 \times 1 + 11 \\
&\begin{pmatrix} 11 & 5 & -26 \\ 22 & -4 & 21 \end{pmatrix} \\
&\quad \downarrow \quad (\text{第 2 行}) - (\text{第 1 行}) \times 2 \qquad 22 = 11 \times 2 \\
&\begin{pmatrix} 11 & 5 & -26 \\ 0 & -14 & 73 \end{pmatrix}.
\end{aligned}$$

  $(803, 154) = 11$ で不定方程式 $803x + 154y = 11$ の特殊解として $x = 5, y = -26$ が得られた．

例題 2.3.1　次の方程式の整数解を求めよ．

$$821x + 1997y = 24047. \qquad \cdots\cdots ①$$

解答

$$A = \begin{pmatrix} 821 & 1 & 0 \\ 1997 & 0 & 1 \end{pmatrix}$$

$$\downarrow \quad (\text{第 2 行}) - (\text{第 1 行}) \times 2 \qquad 1997 = 821 \times 2 + 355$$

$$\begin{pmatrix} 821 & 1 & 0 \\ 355 & -2 & 1 \end{pmatrix}$$

$$\downarrow \quad (\text{第 1 行}) - (\text{第 2 行}) \times 2 \qquad 821 = 355 \times 2 + 111$$

$$\begin{pmatrix} 111 & 5 & -2 \\ 355 & -2 & 1 \end{pmatrix}$$

$$\downarrow \quad (\text{第 2 行}) - (\text{第 1 行}) \times 3 \qquad 355 = 111 \times 3 + 22$$

$$\begin{pmatrix} 111 & 5 & -2 \\ 22 & -17 & 7 \end{pmatrix}$$

$$\downarrow \quad (\text{第 1 行}) - (\text{第 2 行}) \times 5 \qquad 111 = 22 \times 5 + 1$$

$$\begin{pmatrix} 1 & 90 & -37 \\ 22 & -17 & 7 \end{pmatrix}$$

$$\downarrow \quad (\text{第 2 行}) - (\text{第 1 行}) \times 22 \qquad 22 = 1 \times 22$$

$$\begin{pmatrix} 1 & 90 & -37 \\ 0 & -1997 & 821 \end{pmatrix}.$$

$(821, 1997) = 1$ で不定方程式 $821x + 1997y = 1$ の特殊解として $x = 90$, $y = -37$ が得られた．

$$821 \cdot 90 + 1997 \cdot (-37) = 1. \qquad \cdots\cdots ①'$$

①′ の両辺に 24047 をかけて ① の特殊解を求めてもよいが，少し工夫しよう．

24047 を小さい数にすることを考える．

$$24047 = 821 \times 29 + 238,\ 24047 = 1997 \times 12 + 83$$

であるから，① を

$$821x + 1997(y - 12) = 83. \qquad \cdots\cdots ②$$

と変形する．

①′ の両辺に 83 をかけると

$$821 \cdot 7470 + 1997 \cdot (-3071) = 83. \qquad \cdots\cdots ②'$$

② − ②′ から，$821(x - 7470) + 1997(y + 3059) = 0$ すなわち

$$821(x - 7470) = -1997(y + 3059). \qquad \cdots\cdots ③$$

右辺は 1997 の倍数だから，左辺も 1997 の倍数である．821 と 1997 は互いに素だから $x-7470$ は 1997 の倍数となり，$x-7470=-1997t$ (t は整数) とおける．これを③に代入すると，$y+3059=821t$ となる．

よって，$x=7470-1997t,\ y=-3059+821t$　(t は任意の整数).

※　$x=7470-1997t=7470-1997(t-4)=-518-1997s$ と変形できる．ただし，$s=t-4$ とする．

$y=-3059+821t=-3059+3284+821(t-4)=225+821s$ より

$$x=-518-1997s,\ y=225+821s \quad (s \text{ は任意の整数})$$

と書くこともできる．

- n が正の整数のとき

$$\boldsymbol{x^n-y^n=(x-y)\left(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+xy^{n-2}+y^{n-1}\right)}$$

が成り立つ．

特に

$$\boldsymbol{x^n-1=(x-1)\left(x^{n-1}+x^{n-2}+x^{n-3}+\cdots+x+1\right).}$$

- n が正の**奇数**のとき

$$\boldsymbol{x^n+y^n=(x+y)\left(x^{n-1}-x^{n-2}y+x^{n-3}y^2-\cdots-xy^{n-2}+y^{n-1}\right)}$$

が成り立つ．

等式の証明は，右辺を展開すれば容易に左辺が得られるが，ここでは，まず

$$x^n-1=(x-1)\left(x^{n-1}+x^{n-2}+x^{n-3}+\cdots+x+1\right) \qquad \cdots\cdots①$$

を示す．

$x=1$ のときは，明らかに①は成り立つ．

$x\neq 1$ のときは，等比数列の和の公式を使うと

$$x^{n-1}+x^{n-2}+x^{n-3}+\cdots+x+1=1+x+x^2+\cdots+x^{n-1}=\frac{x^n-1}{x-1}$$

となるから，$x^{n-1}+x^{n-2}+x^{n-3}+\cdots+x+1=\dfrac{x^n-1}{x-1}$ が成り立つ．この等式の両辺に $x-1$ をかければ，①を得る．

次に，①において，x のところに $\dfrac{x}{y}$ を代入すれば，

$$\left(\frac{x}{y}\right)^n - 1 = \left(\frac{x}{y} - 1\right)\quad\left(\left(\frac{x}{y}\right)^{n-1} + \left(\frac{x}{y}\right)^{n-2} + \left(\frac{x}{y}\right)^{n-3} + \cdots + \frac{x}{y} + 1\right).$$

両辺に y^n をかければ，

$$x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}\right) \qquad \cdots\cdots ②$$

を得る．

n が正の奇数のとき，②において，y のところに $-y$ を代入すれば，

$$\begin{aligned} &x^n - (-y)^n \\ &= (x-(-y))\left(x^{n-1} + x^{n-2}(-y) + x^{n-3}(-y)^2 + \cdots + x(-y)^{n-2} + (-y)^{n-1}\right). \end{aligned}$$

n は奇数だから，

$$x^n + y^n = (x+y)\left(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \cdots - xy^{n-2} + y^{n-1}\right)$$

が得られる．

例 2.3.1　m, n は自然数で，$m < n$ を満たすものとする．$m^n + 1$，$n^m + 1$ がともに 10 の倍数となる，m, n を 1 組与えよ．　(1996 京都大・理・後期)

m, n が奇数のとき

$$m^n + 1 = (m+1)\left(m^{n-1} - m^{n-2} + m^{n-3} - \cdots - m + 1\right),$$
$$n^m + 1 = (n+1)\left(n^{m-1} - n^{m-2} + n^{m-3} - \cdots - n + 1\right)$$

から，m と n の 1 の位が 9 ならば，$m^n + 1$，$n^m + 1$ がともに 10 の倍数となる．例えば，$(m, n) = (9, 19)$.

例題 2.3.2　a, m, n が正の整数で，$a > 1$ のとき

$$\gcd\left(a^m - 1,\, a^n - 1\right) = a^{\gcd(m,\,n)} - 1 \tag{2.5}$$

が成り立つことを証明せよ．

解 1　$m = n$ のとき (2.5) は成り立つから，$m > n$ と仮定する．

$r_0 = m$, $r_1 = n$ とおき，r_0 を r_1 で割った商を q_1，余りを r_2 とすると，

$$r_0 = r_1 q_1 + r_2, \quad 0 \le r_2 < r_1 \qquad (m = nq_1 + r_2, \quad 0 \le r_2 < n)$$

が成り立つ．

定理 2.3.1 を使うと

$$(a^m-1,\, a^n-1) = \big(a^m-1-a^{m-n}(a^n-1),\, a^n-1\big) = \big(a^{m-n}-1,\, a^n-1\big)$$

が成り立つから，これを繰り返すと

$$\begin{aligned}(a^{r_0}-1,\, a^{r_1}-1) = (a^m-1,\, a^n-1) &= \big(a^{m-n}-1,\, a^n-1\big)\\ &= \big(a^{m-2n}-1,\, a^n-1\big)\\ &= \cdots\\ &= \big(a^{m-q_1 n}-1,\, a^n-1\big)\\ &= (a^{r_2}-1,\, a^{r_1}-1)\,.\end{aligned}$$

よって

$$(a^{r_0}-1,\, a^{r_1}-1) = (a^{r_1}-1,\, a^{r_2}-1)$$

が成り立つ．$r_2 \neq 0$ のとき，r_1 を r_2 で割った商を q_2，余りを r_3 とすると，

$$r_1 = r_2 q_2 + r_3, \quad 0 \leq r_3 < r_2$$

で上で示したことから

$$(a^{r_1}-1,\, a^{r_2}-1) = (a^{r_2}-1,\, a^{r_3}-1)$$

が成り立つ．

この操作を続けると余りの列

$$m = r_0 > r_1 > r_2 > \cdots \geq 0$$

は m 個より多くの正整数を含み得ないから，いつかは余りは 0 となる．

すなわち

$$\left.\begin{aligned} r_0 &= r_1 q_1 + r_2, && 0 < r_2 < r_1\\ r_1 &= r_2 q_2 + r_3, && 0 < r_3 < r_2\\ &\vdots && \vdots\\ r_{l-2} &= r_{l-1} q_{l-1} + r_l, && 0 < r_l < r_{l-1}\\ r_{l-1} &= r_l q_l + r_{l+1}, && r_{l+1} = 0 \end{aligned}\right\}$$

となる正の整数 l が存在する．

$r_l = \gcd(m, n)$ で

$$\begin{aligned}(a^m-1,\, a^n-1) = (a^{r_0}-1,\, a^{r_1}-1) &= (a^{r_1}-1,\, a^{r_2}-1)\\ &= \cdots\\ &= (a^{r_{l-1}}-1,\, a^{r_l}-1)\\ &= (a^{r_l}-1,\, a^{r_{l+1}}-1)\\ &= \big(a^{r_l}-1,\, a^0-1\big)\\ &= a^{r_l}-1 = a^{\gcd(m,\,n)}-1.\end{aligned}$$

したがって，(2.5) は成り立つ．　□

解 2　$g = \gcd(m, n)$ とすると，$m = gp$, $n = gq$, $p, q \in \mathbb{N}$, $(p, q) = 1$ とおける．

$$a^m - 1 = (a^g)^p - 1 = (a^g - 1)\left((a^g)^{p-1} + (a^g)^{p-2} + \cdots + 1\right).$$

同様にして

$$a^n - 1 = (a^g)^q - 1 = (a^g - 1)\left((a^g)^{q-1} + (a^g)^{q-2} + \cdots + 1\right)$$

と変形できるから

$$a^g - 1 \mid a^m - 1,\ a^g - 1 \mid a^n - 1.$$

よって，定理 2.2.3(2) より $a^g - 1 \mid \gcd(a^m - 1, a^n - 1)$ となり

$$a^g - 1 \leq \gcd(a^m - 1, a^n - 1) \qquad \cdots\cdots ①$$

が成り立つ．

系 2.2.2 より $mx - ny = g$ となる正整数 x, y が存在する．

$t = \gcd(a^m - 1, a^n - 1)$ とおくと，

$t \mid a^m - 1$, $t \mid a^n - 1$ から $t \mid a^m - 1 \mid a^{mx} - 1$, $t \mid a^n - 1 \mid a^{ny} - 1$ すなわち $t \mid a^{mx} - 1$, $t \mid a^{ny} - 1$ が成り立ち

$$t \mid a^{mx} - 1 - a^g(a^{ny} - 1) = a^{mx} - 1 - a^{g+ny} + a^g = a^g - 1.$$

よって，$t \leq a^g - 1$ すなわち

$$\gcd(a^m - 1, a^n - 1) \leq a^g - 1 \qquad \cdots\cdots ②$$

が成り立つ．

①，②より

$$\gcd(a^m - 1, a^n - 1) = a^g - 1 = a^{\gcd(m, n)} - 1$$

が成り立つ．　□

解 2 で用いたように次のことが成り立つ．

- a, b, m, n は正の整数とする．
  $m \mid n$ のとき，$a^m - 1 \mid a^n - 1$ が成り立つ．
  $m \mid n$ のとき，$a^m - b^m \mid a^n - b^n$ が成り立つ．

証明　$n = mq$ $(q \in \mathbb{N})$ とおくと

$$a^n - 1 = (a^m)^q - 1 = (a^m - 1)\left((a^m)^{q-1} + (a^m)^{q-2} + \cdots + 1\right)$$

と変形できるから

$$a^m - 1 \,|\, a^n - 1.$$

同様にして

$$a^n - b^n = (a^m)^q - (b^m)^q = (a^m - b^m)\left((a^m)^{q-1} + (a^m)^{q-2}\, b^m + \cdots + (b^m)^{q-1}\right)$$

と変形できるから

$$a^m - b^m \,|\, a^n - b^n$$

が成り立つ．　□

例題 2.3.3　p は奇素数，a, b が互いに素な正の整数とする．このとき

$$\gcd\left(a+b,\ \frac{a^p+b^p}{a+b}\right) = 1 \text{ または } p$$

であることを証明せよ．

解答　$p \geq 3$ は奇数であるから

$$a^p + b^p = (a+b)\left(a^{p-1} - a^{p-2}b + a^{p-3}b^2 - \cdots - ab^{p-2} + b^{p-1}\right)$$

が成り立つ．この式を変形すると

$$\frac{a^p+b^p}{a+b} = a^{p-1} - a^{p-2}b + a^{p-3}b^2 - \cdots - ab^{p-2} + b^{p-1}.$$

$a+b$ を法として考えると，$b \equiv -a \pmod{a+b}$ だから

$$\begin{aligned} & a^{p-1} - a^{p-2}b + a^{p-3}b^2 - \cdots - ab^{p-2} + b^{p-1} \\ \equiv\ & a^{p-1} + a^{p-1} + a^{p-1} + \cdots + a^{p-1} + a^{p-1} \\ \equiv\ & pa^{p-1} \pmod{a+b}. \end{aligned}$$

よって，

$$\frac{a^p+b^p}{a+b} = a^{p-1} - a^{p-2}b - \cdots - ab^{p-2} + b^{p-1} = pa^{p-1} + m(a+b) \quad (m \in \mathbb{Z})$$

とおけるから，

$$\gcd\left(a+b,\ \frac{a^p+b^p}{a+b}\right) = \gcd\left(pa^{p-1} + m(a+b), a+b\right) = \gcd\left(pa^{p-1}, a+b\right).$$

a, b が互いに素なので，$\gcd(a, a+b) = \gcd(a,b) = 1$ より $\gcd\left(a^{p-1}, a+b\right) = 1$ となる．よって，

$$\frac{a^p+b^p}{a+b} = \gcd\left(pa^{p-1}, a+b\right) = \gcd\left(p, a+b\right) = 1.$$

p は素数なので，$\gcd(p, a+b) = 1$ または p だから

$$\frac{a^p+b^p}{a+b} = \gcd\left(pa^{p-1}, a+b\right) = \gcd\left(p, a+b\right) = 1 \text{ または } p.$$　□

問題 2.3.1　(1)　$25m + 17n = 1623$ を満たす正の整数の組 $(m,\, n)$ を 1 つ求めなさい.
(2)　$25m + 17n = 1623$ を満たす正の整数の組 $(m,\, n)$ をすべて求めなさい.

問題 2.3.2　$p,\, q$ を互いに素な正整数とする.

(1)　任意の整数 x に対して，p 個の整数 $x - q,\, x - 2q,\, \ldots,\, x - pq$ を p で割った余りはすべて相異なることを証明せよ.
(2)　$x > pq$ なる任意の整数 x は，適当な正整数 $a,\, b$ を用いて $x = pa + qb$ と表せることを示せ.　(2008 奈良県立医大)

次の福井大の問題 (3) は，問題 2.3.2 で $p = 65,\, q = 31,\, pq = 65 \times 31 = 2015$ の場合である.

問題 2.3.3　以下の問いに答えよ.

(1)　方程式 $65x + 31y = 1$ の整数解をすべて求めよ.
(2)　$65x + 31y = 2016$ を満たす正の整数の組 $(x,\, y)$ を求めよ.
(3)　2016 以上の整数 m は，正の整数 $x,\, y$ を用いて $m = 65x + 31y$ と表せることを示せ.

(2016 福井大・教育地域科学)

問題 2.3.4　xy 平面上の点で x 座標，y 座標がともに整数である点を格子点という.
a, k は整数で $a \geq 2$ とし，直線 $L : ax + \left(a^2 + 1\right) y = k$ を考える.

(1)　直線 L 上の格子点を 1 つ求めよ.
(2)　$k = a\left(a^2 + 1\right)$ のとき，$x > 0,\, y > 0$ の領域に直線 L 上の格子点は存在しないことを示せ.
(3)　$k > a\left(a^2 + 1\right)$ ならば，$x > 0,\, y > 0$ の領域に直線 L 上の格子点が存在することを示せ.　(2000　京都大・理・医・薬・工・農・後期)

問題 2.3.5　(Putnam 2000)
$n \geq m \geq 1$ を満たすすべての正の整数の組 $(m,\, n)$ に対して

$$\frac{\gcd(m, n)}{n} \binom{n}{m}$$

は整数であることを証明せよ.

問題 2.3.6　(PUMAC 2013)
$2^{30^{10}} - 2$ と $2^{30^{45}} - 2$ の最大公約数が $2^x - 2$ の形に表されるとき，x を求めよ.

問題 2.3.7　a, m, n は正の整数で，$m \neq n$ のとき次のことを証明せよ．

$$\gcd\left(a^{2^m}+1, a^{2^n}+1\right) = \begin{cases} 1 & (a \text{ は偶数}) \\ 2 & (a \text{ は奇数}) \end{cases}.$$

問題 2.3.8　a, b, m, n が正の整数で $a > b$, $\gcd(a,b) = 1$ のとき

$$\gcd\left(a^m - b^m,\, a^n - b^n\right) = a^{\gcd(m,\,n)} - b^{\gcd(m,\,n)} \tag{2.6}$$

が成り立つことを証明せよ．

問題 2.3.9　2 つの奇数 a, b に対して，$m = 11a + b$, $n = 3a + b$ とおく．次の (1)，(2) を証明せよ．

(1)　m, n の最大公約数は，a, b の最大公約数を d として，$2d, 4d, 8d$ のいずれかである．
(2)　m, n がともに平方数であることはない．（整数の 2 乗である数を平方数という．）

(1989 京都大・医・薬・工・農・教・経・後期)

問題 2.3.10　$43x + 782y = 1$ と $2 < |x + 18y| < 12$ を満たす整数 x, y で，$\left|\dfrac{x}{y}\right|$ が最大であるものを求めよ．

(1987 芝浦工大・電気工・建築・工業経営)

問題 2.3.11　(Japan 1996)

m, n がは互いに素な正の整数とする．このとき

$$\gcd\left(5^m + 7^m,\, 5^n + 7^n\right)$$

を求めよ．

問題 2.3.12　(IMO 1983)

a, b, c はどの 2 つをとっても互いに素である正の整数とする．

$2abc - ab - bc - ca$ は $xbc + yca + zab$ $(x, y, z \in \mathbb{N}_0)$ と表されない最大の整数であることを示せ．

2.4　素因数分解

定理 2.4.1　p は素数で，a と b は整数とするとき，次のことが成り立つ．

$$p \mid ab \implies p \mid a \text{ または } p \mid b$$

証明　$ab = kp,\ k \in \mathbb{Z}$ とおき，$p \nmid a$ と仮定して $p \mid b$ が成り立つことを示す．
$p \nmid a$ で p は素数だから $(a, p) = 1$ となるので，系 2.2.1 より $ax + py = 1$ を満たす整数 x, y が存在する．

$$b = b \cdot 1 = b(ax + py) = abx + bpy = kpx + bpy = p(kx + by)$$

から $p \mid b$ が成り立つ．　□

定理 2.4.2　1 より大きい正の整数は有限個の素数の積として表される．しかもこの表し方は素因数の順序を除いて一意的である．

証明　まず，1 より大きい正の整数 n は有限個の素数の積として表されることを，n に関する数学的帰納法で示す．

$n = 2, 3$ のときは明らかに成り立つ．

$m \geq 3$ として m より小さいすべての n に対して，n は有限個の素数の積として表されると仮定する．

m が素数ならば明らかに成り立つ．

m が素数でないならば，$m = ab,\ a, b \in \mathbb{N},\ a \geq 2,\ b \geq 2$ とかける．仮定より a と b は有限個の素数の積と表せるから，$m = ab$ も有限個の素数の積で表せる．

次に，表し方が素因数の順序を除いて一意的であることを，n に関する数学的帰納法で示す．

$n = 2, 3$ のときは明らかに成り立つ．

$m \geq 3$ として m より小さいすべての n に対して，n は有限個の素数の積として素因数の順序を除いて一意的に表されると仮定する．

m が $p_1, \ldots, p_r$ と $q_1, \ldots, q_s$ を素数として

$$m = p_1 \cdots p_r = q_1 \cdots q_s$$

と表せたとする．

$p_1 \mid q_1 \cdots q_s$ が成り立つから，定理 2.4.1 より $p_1 \mid q_1$ または $p_1 \mid q_2 \cdots q_s$ が成り立つ．これを繰り返すと $p_1 \mid q_1$ または $p_1 | q_2$ または $p_1 | q_3 \cdots q_s$ が成り立つ．$\cdots\cdots$

よって，$p_1 \mid q_1$ または $p_1 \mid q_2$ または $\ldots$ または $p_1 \mid q_s$ となるから，

$$p_1 \mid q_j \text{ を満たす } j\ (1 \leq j \leq s)$$

が存在する．p_1 と q_j は素数だから $p_1 = q_j$ となる．

さて，

$$p_2 \cdots p_r = \frac{m}{p_1} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s$$

と帰納法の仮定から，$p_2, \ldots, p_r$ は $q_1, \ldots, q_{j-1}, q_{j+1}, \ldots, q_s$ の並べ替えたものにすぎない．

よって，m の有限個の素数の積としての表し方は素因数の順序を除いて一意的である．　□

- 1 より大きい正の整数 n は

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \quad (p_1, p_2, \ldots, p_r \text{は異なる素数}, e_1, e_2, \ldots, e_r \in \mathbb{N})$$

の形に素因数の順序を除いて一意的に表せる．

正の整数 $n \geq 2$ が与えられたとき，n の素因数分解は次のいずれかの形で表せる．

(i) $n = \displaystyle\prod_{i=1}^{r} p_i$,　　$p_1, \ldots, p_r$は素数（異なっている必要はない）

(ii) $n = \displaystyle\prod_{i=1}^{s} p_i^{\alpha_i}$,　　$p_1, \ldots, p_s$は異なる素数, $\alpha_1, \ldots, \alpha_s$は正の整数

(iii) $n = \displaystyle\prod_{i=1}^{t} p_i^{\alpha_i}$,　　$p_1, \ldots, p_t$は異なる素数, $\alpha_1, \ldots, \alpha_t$は非負の整数

(iii) はいくつかの整数を素因数分解するときに便利である．

m と n は整数で，$m \neq 0$, $n \neq 0$ とする．$m|l$ かつ $n|l$ を満たす整数 l を m と n の**公倍数**という．m と n の**最小公倍数**とは，m と n の最小の正の公倍数をいう．

m と n の最小公倍数を $\mathbf{lcm}(\boldsymbol{m}, \boldsymbol{n})$ または $[\boldsymbol{m}, \boldsymbol{n}]$ で表す．

- 1 より大きい 2 つの正の整数 m, n を

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \quad n = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$

ここに，$p_1, p_2, \ldots, p_r$ は異なる素数で，$e_1, e_2, \ldots, e_r \in \mathbb{N}_0$ ，$f_1, f_2, \ldots, f_r \in \mathbb{N}_0$ と素因数分解されるとき，次のことが成り立つ．

$$\gcd(m, n) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_r^{\min\{e_r, f_r\}}.$$

$$\mathrm{lcm}(m, n) = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_r^{\max\{e_r, f_r\}}.$$

2 つ以上の整数に対しても，最大公約数と最小公倍数は定義される．

- $a, b, \ldots, h \in \mathbb{Z}$ とし，少なくとも一つは 0 でないものとする．このとき，整数 $a, b, \ldots, h$ を割り切るような整数を，それらの公約数といい，公約数のなかで最

大のものは最大公約数と呼ばれ，記号 $\gcd(a, b, \ldots, h)$ または $(a, b, \ldots, h)$ で表される．

- $a, b, \ldots, h \in \mathbb{Z}$ とし，すべて 0 でないものとする．このとき，$a \mid l, b \mid l, \ldots, h \mid l$ を満たす整数を，それらの公倍数といい，正の公倍数のなかで最小のものは最小公倍数と呼ばれ，記号 $\mathrm{lcm}(a, b, \ldots, h)$ または $[a, b, \ldots, h]$ で表される．

例題 2.4.1　$\sqrt{2}$ は無理数であることを証明せよ．

証明　$\sqrt{2}$ が有理数であると仮定すると，

$$\sqrt{2} = \frac{m}{n} \ (m,\, n \in \mathbb{N})$$

とかける．$1 < \sqrt{2} < 2$ より，$m \neq 1$ かつ $n \neq 1$ であることがわかる．

$m = \sqrt{2}\, n$ の両辺を 2 乗すると，$m^2 = 2n^2$.

$m \geq 2,\, n \geq 2$ であるから，$m,\, n$ を次のように素因数分解する．

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \quad n = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_s}$$

ここで，$p_1,\, p_2,\, \ldots,\, p_r$ は異なる素数で，$q_1,\, q_2,\, \ldots,\, q_s$ も異なる素数とし，

$e_1,\, e_2,\, \ldots,\, e_r \in \mathbb{N}$，$f_1,\, f_2,\, \ldots,\, f_r \in \mathbb{N}$ とする．

これらの式を $m^2 = 2n^2$ に代入すると

$$p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r} = 2 q_1^{2f_1} q_2^{2f_2} \cdots q_r^{2f_s}.$$

左辺の 2 の指数は偶数個，右辺の 2 の指数は奇数個となり矛盾が生じる．

したがって，$\sqrt{2}$ は無理数である．　□

定理 2.4.3　$a,\, b,\, c$ は整数で少なくとも一つは 0 ではないものとする．

このとき，$ax_0 + by_0 + cz_0 = \gcd(a,\, b,\, c)$ を満たす整数 $x_0,\, y_0,\, z_0$ が存在する．さらに

$$\Big\{ax + by + cz : x,\ y,\ z \in \mathbb{Z}\Big\} = \Big\{k(a,\ b,\ c) : k \in \mathbb{Z}\Big\}$$

が成り立つ．

証明は定理 2.2.1 と同様にできる．

証明　$S = \Big\{ax + by + cz : x,\ y,\ z \in \mathbb{Z},\ ax + by + cz > 0\Big\}$ とおく．

$$a = a \cdot 1 + b \cdot 0 + c \cdot 0,\ -a = a \cdot (-1) + b \cdot 0 + c \cdot 0,$$
$$b = a \cdot 0 + b \cdot 1 + c \cdot 0,\ -b = a \cdot 0 + b \cdot (-1) + c \cdot 0,$$
$$c = a \cdot 0 + b \cdot 0 + c \cdot 1,\ -c = a \cdot 0 + b \cdot 0 + c \cdot (-1).$$

a, b, c の少なくとも一つは 0 ではないから，a, $-a$, b, $-b$, c, $-c$ の少なくとも一つは正の整数である．よって，a, $-a$, b, $-b$, c, $-c$ の少なくとも一つは S に属するから，S は空集合ではない．したがって，S の中には最小なものが存在するから，これを d とおくと $d = ax_0 + by_0 + cz_0$ となる整数 x_0, y_0, z_0 が存在する．

$T = \left\{ax + by + cz : x,\ y,\ z \in \mathbb{Z}\right\}$ とおく．

(a) $\left\{kd : k \in \mathbb{Z}\right\} \subseteq T$.

$kd = k(ax_0 + by_0 + cz_0) = a(kx_0) + b(ky_0) + c(kz_0)$, kx_0, ky_0, $kz_0 \in \mathbb{Z}$ より $kd \in T$.

(b) $T \subseteq \left\{kd : k \in \mathbb{Z}\right\}$.

$t \in T$ とすると $t = ax_1 + by_1 + cz_1$, x_1, y_1, $z_1 \in \mathbb{Z}$ とかける．

t を d で割った商を q，余りを r とすると $t = dq + r$, $0 \leq r < d$ を満たす整数 q, r がある．よって

$$\begin{aligned} r &= t - dq \\ &= ax_1 + by_1 + cz_1 - (ax_0 + by_0 + cz_0)q \\ &= a(x_1 - x_0q) + b(y_1 - y_0q) + c(z_1 - z_0q) \in T. \end{aligned}$$

d の S における最小性から $r = 0$ を得る．このとき，$t = dq$ となり $t \in \left\{kd : k \in \mathbb{Z}\right\}$.

(c) $d = (a, b, c)$.

(a)，(b) から $T = \left\{kd : k \in \mathbb{Z}\right\}$ が成り立つので $d = (a, b, c)$ を示す．

$g = (a, b, c)$ とおくと $a = ga_1$, $b = gb_1$, $c = gc_1$, $a_1, b_1, c_1 \in \mathbb{Z}$, $(a_1, b_1, c_1) = 1$ とかけるから，これを $d = ax_0 + by_0 + cz_0$ に代入すると

$$d = ax_0 + by_0 + cz_0 = ga_1 \cdot x_0 + gb_1 \cdot y_0 + gc_1 \cdot z_0 = g(a_1x_0 + b_1y_0 + c_1z_0).$$

これから，$g \mid d$ が言えて $g \leq d$.

$a = a \cdot 1 + b \cdot 0 + c \cdot 0 \in T$, $b = a \cdot 0 + b \cdot 1 + c \cdot 0 \in T$, $c = a \cdot 0 + b \cdot 0 + c \cdot 1 \in T$ なので，(b) より $a, b, c \in \left\{kd : k \in \mathbb{Z}\right\}$ が言えて $d \mid a$, $d \mid b$, $d \mid c$ が成り立つ．

(a, b, c) は a, b, c を割り切る最大の正整数だから，$d \leq (a, b, c) = g$ が成り立つ．

$g \leq d$ であったから，$d = g = (a, b, c)$.

これで，定理は証明された． □

定理 2.4.3 より次の系を得る．

系 2.4.1　a, b, c はどの 2 つをとっても互いに素な整数とする．

このとき，$ax + by + cz = 1$ を満たす整数 x, y, z が存在する．

例題 2.4.2　次の方程式の整数解を求めよ．

$$6x + 15y + 20z = 1.$$

解答　$6x + 15y + 20z = 1.$ ……①

①を

$$3(2x + 5y) = 1 - 20z$$

と変形すると，$1 - 20z$ は 3 の倍数になるから，$1 - 20z = 3k$ $(k \in \mathbb{Z})$ とおくと

$$2x + 5y = k,\ 20z + 3k = 1.$$

$2x + 5y = k = 2(-2k) + 5k$ から $2(x + 2k) + 5(y - k) = 0$．2 と 5 は互いに素だから，s を整数として，$x + 2k = 5s, y - k = -2s$ すなわち

$$x = 5s - 2k,\ y = -2s + k \quad \cdots\cdots ②$$

とおける．

$20z + 3k = 1 = 20 \cdot (-1) + 3 \cdot 7$ から $20(z + 1) + 3(k - 7) = 0$．20 と 3 は互いに素だから，t を整数として，$z + 1 = 3t, k - 7 = -20t$ すなわち

$$z = 3t - 1,\ k = -20t + 7 \quad \cdots\cdots ③$$

とおける．$k = -20t + 7$ を②に代入して

$$x = 5s + 40t - 14,\ y = -2s - 20t + 7,\ z = 3t - 1\ (s, t \in \mathbb{Z}).$$ □

例題 2.4.3　n, k は $n \geq k > 0$ を満たす正の整数とする．

$\binom{n}{k}, \binom{n+1}{k}, \ldots, \binom{n+k}{k}$ の最大公約数は 1 であることを証明せよ．

解 1　r に関する数学的帰納法で証明する．

(1) $k = 1$ のとき，$\binom{n}{1} = n, \binom{n+1}{1} = n + 1$ の最大公約数は 1 であるから成り立つ．

(2) k のとき成り立つと仮定する．

$\binom{n}{k+1}, \binom{n+1}{k+1}, \ldots, \binom{n+k+1}{k+1}$ の最大公約数を g とおくと，

$$g \,\Big|\, \binom{n}{k+1}, g \,\Big|\, \binom{n+1}{k+1}, \ldots, g \,\Big|\, \binom{n+k+1}{k+1}.$$

等式 (1.1) を使うと

$$
\begin{aligned}
&g \,\Big|\, \binom{n+1}{k+1} - \binom{n}{k+1} = \binom{n}{k},\\
&g \,\Big|\, \binom{n+2}{k+1} - \binom{n+1}{k+1} = \binom{n+1}{k},\\
&\cdots\cdots,\\
&g \,\Big|\, \binom{n+k+1}{k+1} - \binom{n+k}{k+1} = \binom{n+k}{k}
\end{aligned}
$$

すなわち

$$
g \,\Big|\, \binom{n}{k}, g \,\Big|\, \binom{n+1}{k}, \ldots, g \,\Big|\, \binom{n+k}{k}
$$

となる．帰納法の仮定より，$\binom{n}{k}, \binom{n+1}{k}, \ldots, \binom{n+k}{k}$ の最大公約数は 1 だから，$g = 1$ でなければならない．

よって，$k+1$ のときも成り立つ．

(3) (I)，(II) より証明された． □

解 2　次の補題を利用する．

n, k は $n \geq k > 0$ を満たす正の整数のとき

$$
\sum_{i=0}^{k} (-1)^i \binom{k}{i} \binom{n+i}{k} = (-1)^k
$$

が成り立つ．

補題の証明

$$
\begin{aligned}
\binom{k}{i}\binom{n+i}{k} &= \frac{k!}{(k-i)!i!} \cdot \frac{(n+i)!}{(n+i-k)!k!}\\
&= \frac{n!}{(k-i)!(n+i-k)!} \cdot \frac{(n+i)!}{i!n!}\\
&= \binom{n}{k-i}\binom{n+i}{n}
\end{aligned}
$$

だから

$$
\sum_{i=0}^{k} (-1)^i \binom{k}{i}\binom{n+i}{k} = \sum_{i=0}^{k} \binom{n}{k-i} \cdot (-1)^i \binom{n+i}{n}
$$

となる．

$\displaystyle\sum_{i=0}^{k}\binom{n}{k-i}\cdot(-1)^i\binom{n+i}{n}$ は

$$\begin{aligned}&\left(\binom{n}{n}x^n+\binom{n}{n-1}x^{n-1}+\cdots+\underline{\binom{n}{k}x^k+\cdots+\binom{n}{1}x+\binom{n}{0}}\right)\\&\quad\times\sum_{r=0}^{\infty}(-1)^r\binom{n+r}{n}x^r\\&=(1+x)^n\times\sum_{r=0}^{\infty}(-1)^r\binom{n+r}{n}x^r\qquad\cdots\cdots(*)\end{aligned}$$

の展開式における x^k の係数である．

$$(1+x)^{-n}=\sum_{r=0}^{\infty}(-1)^r\binom{n+r-1}{r}=\sum_{r=0}^{\infty}(-1)^r\binom{n+r-1}{n-1}$$

だから，

$$(1+x)^{-n-1}=\sum_{i=0}^{\infty}(-1)^i\binom{n+i}{n}$$

を用いると，$(*)$ は

$$(1+x)^n\cdot(1+x)^{-n-1}=\frac{1}{1+x}=\sum_{i=0}^{\infty}(-1)^ix^i$$

となる．したがって x^k の係数は $(-1)^k$ である． ■

$\binom{n}{k},\binom{n+1}{k},\ldots,\binom{n+k}{k}$ の最大公約数を d とおくと

$$d\,\Big|\,\binom{n}{k},\ d\,\Big|\,\binom{n+1}{k},\ \ldots,\ d\,\Big|\,\binom{n+k}{k}$$

だから

$$d\,\Big|\,\sum_{i=0}^{k}(-1)^i\binom{k}{i}\binom{n+i}{k}=(-1)^k$$

すなわち，$d\mid(-1)^k$ となるから，$d=1$. □

例題 2.4.4　　n,k は $n-1\geq k>0$ を満たす正の整数とする．

$$\gcd\left(\binom{n-1}{k-1},\binom{n}{k+1},\binom{n+1}{k}\right)=\gcd\left(\binom{n-1}{k},\binom{n+1}{k+1},\binom{n}{k-1}\right)$$

が成り立つことを証明せよ．

解答 $a=\binom{n-1}{k-1}, b=\binom{n}{k+1}, c=\binom{n+1}{k}, A=\binom{n-1}{k}, B=\binom{n+1}{k+1}, C=\binom{n}{k-1}$

$g=\gcd\left(\binom{n-1}{k-1},\binom{n}{k+1},\binom{n+1}{k}\right)$, $d=\gcd\left(\binom{n-1}{k},\binom{n+1}{k+1},\binom{n}{k-1}\right)$ とおく．

$\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k}$ より $\binom{n}{k}=a+A.$ ……①

$\binom{n+1}{k+1}=\binom{n}{k+1}+\binom{n}{k}$ より $B=b+\binom{n}{k}.$ ……②

$\binom{n+1}{k}=\binom{n}{k}+\binom{n}{k-1}$ より $c=\binom{n}{k}+C.$ ……③

また，$\binom{n}{k+1}=\frac{n}{k+1}\cdot\binom{n-1}{k}$ より $b=\frac{n}{k+1}\cdot A.$ ……④

$\binom{n+1}{k}=\frac{n+1}{k}\cdot\binom{n}{k-1}$ より $c=\frac{n+1}{k}\cdot C.$ ……⑤

$g\mid a, g\mid b, g\mid c$ が成り立っている．④，①を使うと

$$g\,\Big|\, b=\frac{n}{k+1}\cdot A\,\Big|\, nA=n\binom{n}{k}-na \quad \text{よって} \quad g\,\Big|\, n\binom{n}{k}.$$

⑤，③を使うと

$$g\,\Big|\, c=\frac{n+1}{k}\cdot C\,\Big|\, (n+1)C=(n+1)c-(n+1)\binom{n}{k} \quad \text{よって} \quad g\,\Big|\, (n+1)\binom{n}{k}.$$

したがって，$g\,\Big|\,(n+1)\binom{n}{k}-n\binom{n}{k}=\binom{n}{k}$ から $g\,\Big|\,\binom{n}{k}$ が成り立つので，①，②，③から $g\mid A, g\mid B, g\mid C$ が言えて，$g\le d.$

$g\mid A, g\mid B, g\mid C$ が成り立っている．④，②を使うと

$$d\,\Big|\, A=\frac{k+1}{n}\cdot b\,\Big|\, (k+1)B=(k+1)B-(k+1)\binom{n}{k} \quad \text{よって} \quad d\,\Big|\, (k+1)\binom{n}{k}.$$

⑤，③を使うと

$$d\,\Big|\, C=\frac{k}{n+1}\cdot c\,\Big|\, kc=k\binom{n}{k}+kC \quad \text{よって} \quad d\,\Big|\, k\binom{n}{k}.$$

したがって，$d\,\Big|\,(k+1)\binom{n}{k}-k\binom{n}{k}=\binom{n}{k}$ から $d\,\Big|\,\binom{n}{k}$ が成り立つので，①，②，③から $d\mid a, d\mid b, d\mid c$ が言えて，$d\le g.$

以上のことから，$g=d$ を得る．　□

第3章

数論的関数

3.1 $[x], \{x\}$

実数 x に対して，$\boldsymbol{\lfloor x \rfloor}$ または $\boldsymbol{[x]}$ で x 以下の最大の整数を表す.
実数 x に対して，$\boldsymbol{\lceil x \rceil}$ で x 以上の最小の整数を表す.
例　$[\,5\,]=5$,　$[\,2.4\,]=2$,　$\left[\,\sqrt{2}\,\right]=1$,　$[\,-2.75\,]=-3$.
整数 n に対して，$[x]=n$ となるような x は $n \leq x < n+1$ の範囲にあるので，不等式

$$[x] \leq x < [x]+1$$

すなわち

$$\boldsymbol{x-1 < [x] \leq x} \tag{3.1}$$

が成り立つ.
$[x]$ を x の整数部分と呼び，$x-[x]$ を x の小数部分と呼び $\boldsymbol{\{x\}}$ で表す.
例 $\{-2.75\}=-2.75-(-3)=0.25$.
$\{-2.75\} \neq -0.75$ ，$\{-2.75\} \neq 0.75$ であることに注意したい.

- (3.1) より $0 \leq x-[x] < 1$ なので $0 \leq \{x\} < 1$ である.

次の性質が成り立つ.

$x \in \mathbb{R}$, $a \in \mathbb{Z}$ のとき
1. $[x+a]=[x]+a$,　　$\lceil x+a \rceil = \lceil x \rceil + a$
2. $< x >= -[-x]$

証明

1. $[x]=n$ とおくと，$n \leq x < n+1$ から $n+a \leq x+a < n+a+1$ が成り立つから，
   $[x+a]=n+a=[x]+a$.

$\lceil x \rceil = n$ とおくと，$n-1 < x \leq n$ から $n+a-1 < x+a \leq n+a$ が成り立つから，$\lceil x+a \rceil = n+a = \lceil x \rceil + a$.

2. $< x >= n$ とおくと，$n-1 < x \leq n$ から $-n \leq -x < -n+1$ が成り立つから，$[-x] = -n = - < x >$. □

$\boldsymbol{v_p(a)}$ で a の素因数分解における素数 p の指数を表すことにする．もちろん $p \not| a$ のときは $v_p(a) = 0$ とする．

- $n!$ の素因数分解における素数 p の指数は

$$v_p\left(n!\right) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots \tag{3.2}$$

に等しい．

例題 3.1.1　p を素数，n を正の整数とするとき，$(p^n)!$ は p で何回割り切れるか．[*1]

(2009 京都大)

解答　p は素数なので，$p \geq 2$.

$$\begin{aligned} v_p\left((p^n)!\right) &= \left[\frac{p^n}{p}\right] + \left[\frac{p^n}{p^2}\right] + \cdots + \left[\frac{p^n}{p^n}\right] \\ &= p^{n-1} + p^{n-2} + \cdots + p + 1 = \frac{p^n - 1}{p-1} \end{aligned}$$

から，$(p^n)!$ は p で $\dfrac{p^n-1}{p-1}$ 回割り切れる． □

例題 3.1.2　n を正の整数とするとき，任意の実数 x に対して

$$[x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \cdots + \left[x + \frac{n-1}{n}\right] = [nx]$$

が成り立つことを証明せよ．(Hermite)

解 1　$[x] + \left[x + \dfrac{1}{n}\right] + \left[x + \dfrac{2}{n}\right] + \cdots + \left[x + \dfrac{n-1}{n}\right] = [nx]$ $\cdots\cdots(*)$

とおく．

$[x] = m$ とおくと，$m \leq x < m+1$ から $nm \leq nx < nm+n$ となるので，$[nx]$ は，$nm, nm+1, \ldots, nm+n-1$ の n 通りの値を取り得る．

$0 \leq i \leq n-1$ として，$m + \dfrac{i}{n} \leq x < m + \dfrac{i+1}{n}$ のときを考える．

(i) $i = 0$ の場合

[*1] 1969 年に同趣旨の問題が立教大学の理学部で出題されている．

$m \leq x < m + \dfrac{1}{n}$ より $m + \dfrac{k}{n} \leq x + \dfrac{k}{n} < m + \dfrac{k+1}{n}$.

$0 \leq k \leq n-1$ のとき，$m \leq m + \dfrac{k}{n} \leq x + \dfrac{k}{n} < m + \dfrac{k+1}{n} \leq m+1$ が成り立つから，$\left[x + \dfrac{k}{n}\right] = m$.

ゆえに，$\displaystyle\sum_{k=0}^{n-1} \left[x + \frac{k}{n}\right] = nm$.

また，$nm \leq nx < nm + 1$ だから，$[nx] = nm$.

したがって，$(*)$ は成り立つ．

(ii) $1 \leq i \leq n-1$ の場合

$0 \leq k \leq n-i-1$ では，

$$m + \frac{1}{n} \leq m + \frac{i}{n} + \frac{k}{n} \leq x + \frac{k}{n} < m + \frac{i+1}{n} + \frac{k}{n} \leq m + \frac{n}{n} = m+1$$

より $\left[x + \dfrac{k}{n}\right] = m$.

$n-i \leq k \leq n-1$ では

$$m+1 \leq m + \frac{i}{n} + \frac{k}{n} \leq x + \frac{k}{n} < m + \frac{i+1}{n} + \frac{k}{n} \leq m + \frac{2n-1}{n} < m+2$$

より $\left[x + \dfrac{k}{n}\right] = m+1$.

よって

$$\begin{aligned}\sum_{k=0}^{n-1} \left[x + \frac{k}{n}\right] &= \sum_{k=0}^{n-i-1} \left[x + \frac{k}{n}\right] + \sum_{k=n-i}^{n-1} \left[x + \frac{k}{n}\right] \\ &= \underbrace{m + \cdots + m}_{n-i} + \underbrace{(m+1) + \cdots + (m+1)}_{i} \\ &= (n-i)m + i(m+1) = nm + i.\end{aligned}$$

また，$nm + i \leq nx < nm + i + 1$ だから，$[nx] = nm + i$.

したがって，$(*)$ は成り立つ． □

解 2 $\quad [x] + \left[x + \dfrac{1}{n}\right] + \left[x + \dfrac{2}{n}\right] + \cdots + \left[x + \dfrac{n-1}{n}\right] = [nx]\,. \qquad \cdots\cdots (*)$

$f(x) = [x] + \left[x + \dfrac{1}{n}\right] + \left[x + \dfrac{2}{n}\right] + \cdots + \left[x + \dfrac{n-1}{n}\right] - [nx]$ とおく．$[t+1] = [t] + 1$ を使うと

$$\begin{aligned}f\left(x + \frac{1}{n}\right) &= \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \cdots + \left[x + \frac{n-1}{n}\right] + [x+1] - [nx+1] \\ &= \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \cdots + \left[x + \frac{n-1}{n}\right] + [x] + 1 - ([nx] + 1) \\ &= f(x).\end{aligned}$$

したがって，$f(x)$ は周期 $\dfrac{1}{n}$ の周期関数となるから，$0 \leq x < \dfrac{1}{n}$ の場合を考えればよい．

このとき，$0 \leq x < x + \dfrac{1}{n} < \cdots < x + \dfrac{n-1}{n} < 1$, $0 \leq nx < 1$ だから

$$[x] = \left[x + \frac{1}{n}\right] = \cdots = \left[x + \frac{n-1}{n}\right] = 0,\ [nx] = 0.$$

よって，$f(x) = 0$ となり，すべての x について，$(*)$ が成り立つ．　□

- $x = [x] + \{x\}$ を使うと

$$\begin{aligned}
&[x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \cdots + \left[x + \frac{n-1}{n}\right] = [nx] \\
\Leftrightarrow\ &[x] + \left[[x] + \{x\} + \frac{1}{n}\right] + \left[[x] + \{x\} + \frac{2}{n}\right] + \cdots + \left[[x] + \{x\} + \frac{n-1}{n}\right] = [n[x] + n\{x\}] \\
\Leftrightarrow\ &[x] + [x] + \left[\{x\} + \frac{1}{n}\right] + [x] + \left[\{x\} + \frac{2}{n}\right] + \cdots + [x] + \left[\{x\} + \frac{n-1}{n}\right] = n[x] + [n\{x\}] \\
\Leftrightarrow\ &\left[\{x\} + \frac{1}{n}\right] + \left[\{x\} + \frac{2}{n}\right] + \cdots + \left[\{x\} + \frac{n-1}{n}\right] = [n\{x\}] \\
\Leftrightarrow\ &\left[t + \frac{1}{n}\right] + \left[t + \frac{2}{n}\right] + \cdots + \left[t + \frac{n-1}{n}\right] = [nt] \quad (t = \{x\}).
\end{aligned}$$

したがって，$0 \leq x < 1$ に対して等式が成り立つことを示してもよいことがわかる．

解 1 がわかりにくければ，具体的に $n = 3$ ぐらいのときを考えるとよい．

- エルミートの恒等式 $(*)$ で x のところを $-x$ で置き換えると

$$[-x] + \left[-x + \frac{1}{n}\right] + \left[-x + \frac{2}{n}\right] + \cdots + \left[-x + \frac{n-1}{n}\right] = [-nx]\,.$$

$[-x] = -\lceil x \rceil$ を用いると

$$-\lceil x \rceil - \lceil x - \frac{1}{n} \rceil - \lceil x - \frac{2}{n} \rceil - \cdots - \lceil x - \frac{n-1}{n} \rceil = -\lceil nx \rceil$$

から

$$\lceil x \rceil + \left\lceil x - \frac{1}{n} \right\rceil + \left\lceil x - \frac{2}{n} \right\rceil + \cdots + \left\lceil x - \frac{n-1}{n} \right\rceil = \lceil nx \rceil.$$

この式で，x のところを $x + \dfrac{n-1}{n}$ で置き換えると

$$\begin{aligned}
&\lceil x \rceil + \left\lceil x + \frac{1}{n} \right\rceil + \left\lceil x + \frac{2}{n} \right\rceil + \cdots + \left\lceil x + \frac{n-1}{n} \right\rceil \\
&= \left\lceil n\left(x + \frac{n-1}{n}\right) \right\rceil = \lceil nx + n - 1 \rceil \\
&= \lceil nx \rceil + n - 1
\end{aligned}$$

から

$$\lceil x \rceil + \left\lceil x + \frac{1}{n} \right\rceil + \left\lceil x + \frac{2}{n} \right\rceil + \cdots + \left\lceil x + \frac{n-1}{n} \right\rceil = \left\lceil n\left(x + \frac{n-1}{n}\right) \right\rceil = \lceil nx \rceil + n - 1$$

を得る．

- エルミートの恒等式は大学入試問題としても出題されている．

実数 x に対して，その整数部分を $[x]$ で表す．すなわち，$[x]$ は不等式 $[x] \leq x < [x]+1$ を満たす整数である．

(1) 実数 x に対して，等式 $\quad [x]+\left[x+\dfrac{1}{3}\right]+\left[x+\dfrac{2}{3}\right]=[3x] \quad$ を示せ．

(2) 正の整数 n，実数 x に対して，等式

$$[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]=[nx]$$

を示せ．

(1998 奈良女子大・理・生活環境・前期)

任意の実数 x に対して，不等式 $a \leq x < a+1$ を満たす整数 a を記号 $[x]$ で表す．実数 x および正の整数 n が与えられたとき，

(1) 不等式 $\quad [x]+\dfrac{k}{n} \leq x < [x]+\dfrac{k+1}{n} \quad$ を満たす整数 k が存在することを示せ．

(2) 等式 $\quad [x]+\left[x+\dfrac{1}{n}\right]+\left[x+\dfrac{2}{n}\right]+\cdots+\left[x+\dfrac{n-1}{n}\right]=[nx] \quad$ が成立することを示せ．

(1971 名古屋市大・医・薬・経済)

実数 x に対し，x 以下の最大の整数を $[x]$，x 以上の最小の整数を $< x >$ で表すことにする．例えば，

$$\left[\frac{1}{2}\right]=0,\ \left\langle\frac{1}{2}\right\rangle=1,\ \left[-\frac{1}{2}\right]=-1,\ \left\langle-\frac{1}{2}\right\rangle=0,$$

$$[\,3\,]=<3>=3,\ [-3]=<-3>=-3$$

である．このとき，$f(x)=x-\dfrac{1}{2}\ ([x]+<x>)$ とおく．

(1) 整数 m と実数 x に対して，$f(x+m)=f(x)$ が成り立つことを示せ．

(2) 2 以上の整数 n と実数 x に対して，

$$[nx\,]=[x]+\left[x+\frac{1}{n}\,\right]+\cdots+\left[x+\frac{n-1}{n}\right]$$

が成り立つことを示せ．

(3) 2 以上の整数 n と実数 x に対して，

$$<nx>+n-1=<x>+\left\langle x+\frac{1}{n}\right\rangle+\cdots+\left\langle x+\frac{n-1}{n}\right\rangle$$

が成り立つことを示せ．

(4) 2 以上の整数 n と実数 x に対して，

$$f(nx) = f(x) + f\left(x + \frac{1}{n}\right) + \cdots + f\left(x + \frac{n-1}{n}\right)$$

が成り立つことを示せ．

(2010 九州大・理系・後期)

九州大の問題の $< x >$ は $< x >= \lceil x \rceil$ である．

例題 3.1.3　p は奇数の素数，q は p で割り切れない整数とする．

$f : \mathbb{N}_0 \longrightarrow \mathbb{R}$ は次の 2 つの条件

(i)　$\dfrac{f(k)}{p} \notin \mathbb{Z} \quad (k = 1, 2, \ldots, p-1)$.

(ii)　$k = 1, 2, \ldots, p-1$ に対して，$f(k) + f(p-k)$ は p で割り切れる整数である．

を満たすとき

$$\sum_{k=1}^{p-1} \left[f(k) \frac{q}{p} \right] = \frac{q}{p} \sum_{k=1}^{p-1} f(k) - \frac{p-1}{2}$$

が成り立つ．

解答 (ii) から $\dfrac{qf(k)}{p} + \dfrac{qf(p-k)}{p} \in \mathbb{Z}$.　……①

$k = 1, 2, \ldots, p-1$ に対して，(i) から，$\dfrac{qf(k)}{p} \notin \mathbb{Z}$, $\dfrac{qf(p-k)}{p} \notin \mathbb{Z}$ となる．

よって，$0 < \left\{ \dfrac{qf(k)}{p} \right\} + \left\{ \dfrac{qf(p-k)}{p} \right\} < 2$ が成り立つ．ここで，$\{x\}$ は x の小数部分を表す．

しかし，①から，$\left\{ \dfrac{qf(k)}{p} \right\} + \left\{ \dfrac{qf(p-k)}{p} \right\} \in \mathbb{Z}$ だから，

$$\left\{ \frac{qf(k)}{p} \right\} + \left\{ \frac{qf(p-k)}{p} \right\} = 1 \quad (k = 1, 2, \ldots, p-1).$$

この式において，$k = 1, 2, \ldots, p-1$ とおいた $p-1$ 個の等式を辺々加えると

$$\sum_{k=1}^{p-1} \left\{ \frac{qf(k)}{p} \right\} + \sum_{k=1}^{p-1} \left\{ \frac{qf(p-k)}{p} \right\} = p - 1$$

すなわち

$$2 \sum_{k=1}^{p-1} \left\{ \frac{qf(k)}{p} \right\} = p - 1$$

から

$$\sum_{k=1}^{p-1} \left\{ \frac{qf(k)}{p} \right\} = \frac{p-1}{2}.$$

よって，

$$\sum_{k=1}^{p-1}\frac{q}{p}f(k)=\sum_{k=1}^{p-1}\left[\frac{q}{p}f(k)\right]+\sum_{k=1}^{p-1}\left\{\frac{q}{p}f(k)\right\}=\sum_{k=1}^{p-1}\left[\frac{q}{p}f(k)\right]+\frac{p-1}{2}$$

より

$$\sum_{k=1}^{p-1}\left[f(k)\frac{q}{p}\right]=\frac{q}{p}\sum_{k=1}^{p-1}f(k)-\frac{p-1}{2}$$

が成り立つ． □

問題 3.1.1 (1) p は奇数の素数とする．このとき

$$\sum_{k=1}^{p-1}\left[\frac{k^3}{p}\right]=\frac{(p-2)(p-1)(p+1)}{4}$$

が成り立つことを示せ．(German Mathematical Olympiad 2002)

(2) p は奇数の素数，q は p で割り切れない整数とする．このとき

$$\sum_{k=1}^{p-1}\left[(-1)^k k^2\frac{q}{p}\right]=\frac{(p-1)(q-1)}{2}$$

が成り立つことを示せ．

問題 3.1.2 (1) 次のことを示せ．

(a) x が整数ならば， $[x]+[-x]=0$．

(b) x が整数でなければ， $[x]+[-x]=-1$．

(2) p と q が互いに素な整数のとき

$$\left[\frac{p}{q}\right]+\left[\frac{2p}{q}\right]+\cdots+\left[\frac{(q-1)p}{q}\right]=\frac{(p-1)(q-1)}{2}$$

が成り立つことを示せ．

問題 3.1.3 n が正の整数のとき

$$\sum_{k=0}^{\infty}\left[\frac{n+2^k}{2^{k+1}}\right]=n$$

を示せ．

問題 3.1.4 n が正の整数，x が実数のとき

$$\sum_{0\le i<j\le n}\left[\frac{x+i}{j}\right]$$

を簡単にせよ．

問題 3.1.5　n が正の整数，x が実数のとき

$$\sum_{k=0}^{2000}\left[\frac{3^k+2000}{3^{k+1}}\right]-\sum_{k=0}^{2000}\left[\frac{3^k-2000}{3^{k+1}}\right]$$

を簡単にせよ.

問題 3.1.6　n が正の整数のとき

$$\left[\frac{n}{3}\right]+\left[\frac{n+2}{6}\right]+\left[\frac{n+4}{6}\right]=\left[\frac{n}{2}\right]+\left[\frac{n+3}{6}\right]$$

が成り立つことを証明せよ.

問題 3.1.7　(Romania MO 2004)

(1)　次の方程式は有理数の解を無数にもつことを示せ.

$$\{x^2\}+\{x\}=0.99.$$

(2)　次の方程式は正の有理数解をもたないことを示せ.

$$\left\{x^2\right\}+\{x\}=1.$$

3.2 Möbius 関数

定義域が正の整数全体の集合 $\mathbb{N}$ である関数 f が**乗法的** (multiplicative) であるといわれるのは，

任意の互いに素な正の整数 m, n に対して

$$f(mn) = f(m)f(n)$$

が成り立つ場合である．

- f が乗法的関数で，恒等的に 0 ではない場合は $f(1) = 1$ である．
  $f(a) \neq 0$ となる $a \in \mathbb{N}$ が存在する． $\gcd(a, 1) = 1$ で f が乗法的であるから，$f(a) = f(a \cdot 1) = f(a)f(1)$ が成り立つ．両辺を $f(a)\,(\neq 0)$ で割ると $f(1) = 1$ を得る．
- f が乗法的で， $m_1, m_2, \ldots, m_r$ がどの 2 つをとっても互いに素なとき，

  $$f(m_1 m_2 \cdots m_r) = f(m_1)f(m_2)\cdots f(m_r)$$

  が成り立つことを数学的帰納法で示せる．

Möbius **関数** $\mu : \mathbb{N} \longrightarrow \{-1,\ 0,\ 1\}$ は次のように定義される．

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & n \text{ が } 1 \text{ と異なる平方数で割りきれる} \\ (-1)^k & n \text{ が } 1 \text{ と異なる平方数で割りきれず，} \\ & n \text{ が相異なる } k \text{ 個の素因数の積となっている} \end{cases}$$

- 例 $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$,
  $\mu(7) = -1$, $\mu(8) = 0$, $\mu(9) = 0$, $\mu(10) = 1$, $\mu(11) = -1$, $\mu(12) = 0$.
  p が素数のとき，$\mu(p) = -1$, $\mu\left(p^k\right) = 0\ (k \in \mathbb{N},\ k \geq 2)$
- μ の定義の表現をかえると

  $$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{ある素数 } p \text{ に対して } p^2 \mid n \\ (-1)^k & n = p_1 p_2 \cdots p_k\ (p_1, p_2, \ldots, p_k \text{は異なる素数}) \end{cases}$$

  となる．

定理 3.2.1 μ は乗法的関数である．

証明 互いに素な正の整数 m, n に対して

$$\mu(mn) = \mu(m)\mu(n) \qquad \cdots\cdots ①$$

が成り立つことを示す.

$m = 1$ または $n = 1$ のとき明らかに①は成り立つので，以下 $m, n \geq 2$ とする.

p を素数として，$p^2 \mid m$ または $p^2 \mid n$ ならば $p^2 \mid mn$ であるから， $\mu(mn) = 0 = \mu(m)\mu(n)$ となり①は成り立つ.

m と n が素数の 2 乗では割り切れないならば

$$m = p_1 \cdots p_r, \quad n = q_1 \cdots q_s \quad (p_1, \ldots, p_r, q_1, \ldots, q_s \text{ はすべて異なる素数})$$

とかける.

$$\mu(mn) = \mu(p_1 \cdots p_r q_1 \cdots q_s) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n)$$

となり①は成り立つ. □

m が正の整数のとき，記号 $\sum_{\boldsymbol{d \mid m}}$ でもって， m のすべての正の約数 d にわたる和を表すことにする.

定理 3.2.2　f を乗法的関数， $n \geq 2$ は正の整数で $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ と素因数分解できるとすると

$$\begin{aligned}\sum_{d \mid n} f(d) = &\left(1 + f(p_1) + f\left(p_1^2\right) + \cdots + f\left(p_1^{e_1}\right)\right) \\ &\left(1 + f(p_2) + f\left(p_2^2\right) + \cdots + f\left(p_2^{e_2}\right)\right) \\ &\qquad \cdots\cdots \\ &\left(1 + f(p_r) + f\left(p_r^2\right) + \cdots + f\left(p_r^{e_r}\right)\right)\end{aligned}$$

が成り立つ.

$n = 1$ のときは $\sum_{d \mid 1} f(d) = f(1) = 1$ である.

証明 証明すべき式の右辺を展開すると

$$f\left(p_1^{f_1}\right) f\left(p_2^{f_2}\right) \cdots f\left(p_r^{f_r}\right) = f\left(p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}\right)$$

$$(0 \leq f_1 \leq e_1, 0 \leq f_2 \leq e_2, \cdots, 0 \leq f_r \leq e_r, \quad f_1, f_2, \cdots, f_r \in \mathbb{N}_0)$$

という形の和になっているから，これは左辺に等しい. □

定理 3.2.3 n が正の整数のとき

$$\sum_{d|n}\mu(d)=\begin{cases}1 & (n=1)\\ 0 & (n\geq 2)\end{cases} \tag{3.3}$$

が成り立つ.

証明 $n=1$ のとき, $\sum_{d|1}\mu(d)=\mu(1)=1$ である.

$n\geq 2$ のときは, $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ と素因数分解すると, μ は乗法的なので定理 3.2.2 より

$$\begin{aligned}\sum_{d|n}\mu(d)=&\left(1+\mu\left(p_1\right)+\mu\left(p_1^2\right)+\cdots+\mu\left(p_1^{e_1}\right)\right)\\ &\left(1+\mu\left(p_2\right)+\mu\left(p_2^2\right)+\cdots+\mu\left(p_2^{e_2}\right)\right)\\ &\cdots\cdots\\ &\left(1+\mu\left(p_r\right)+\mu\left(p_r^2\right)+\cdots+\mu\left(p_r^{e_r}\right)\right)\end{aligned}$$

が成り立つ.

$i\in\left\{1,\ 2,\ \ldots,\ r\right\}$ に対して,

$$j\geq 2\text{ のとき}\mu\left(p_i^j\right)=0,\quad \mu\left(p_i\right)=-1$$

であるから

$$\begin{aligned}\sum_{d|n}\mu(d)=&\left(1+\mu\left(p_1\right)\right)\left(1+\mu\left(p_2\right)\right)\cdots\left(1+\mu\left(p_r\right)\right)\\ =&(1-1)(1-1)\cdots(1-1)\\ =&0.\end{aligned}$$

□

定理 3.2.4 Möbius の反転公式 (Möbius inversion formula)

F, f は定義域が $\mathbb{N}$ の関数で, $F(n)=\sum_{d|n}f(d)$ を満たすとき

$$f(n)=\sum_{d|n}F\left(\frac{n}{d}\right)\mu(d) \tag{3.4}$$

が成り立つ.

証明 $F\left(\frac{n}{d}\right)=\sum_{c|\frac{n}{d}}f(c)$ を使うと

$$\sum_{d|n}F\left(\frac{n}{d}\right)\mu(d)=\sum_{d|n}\left(\sum_{c|\frac{n}{d}}f(c)\right)\mu(d)=\sum_{d|n}\sum_{c|\frac{n}{d}}\mu(d)f(c)\qquad\cdots\cdots①$$

と変形できる.

- $d \mid n$ かつ $c \Big| \dfrac{n}{d} \iff c \mid n$ かつ $d \Big| \dfrac{n}{c}$ ……②
  が成り立つことを示す.
  ($\Longrightarrow$) $d \mid n$ かつ $c \Big| \dfrac{n}{d}$ から $n = dn_1$, $\dfrac{n}{d} = cn_2$ $(n_1, n_2 \in \mathbb{N})$ とおける.
  $\dfrac{n}{d} = cn_2$ から $n = cdn_2$ となるので $c \mid n$.
  $\dfrac{n}{d} = cn_2$ を $\dfrac{n}{c} = dn_2$ と変形して $\dfrac{n}{c} \in \mathbb{N}$ を使うと $d \Big| \dfrac{n}{c}$ が成り立つ.
  ($\Longleftarrow$) ($\Longrightarrow$) の証明で c と d の役割を入れかえれば成り立つことが分かる.

②を使うと ①は次のように変形できる.

$$\sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) f(c) = \sum_{c|n} \sum_{d|\frac{n}{c}} \mu(d) f(c) = \sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d) \right). \qquad \cdots\cdots ③$$

定理 3.2.3 より $\displaystyle\sum_{d|\frac{n}{c}} \mu(d)$ は $\dfrac{n}{c} = 1$ すなわち $c = n$ のときを除いて 0 になる.

$c = n$ のとき $\displaystyle\sum_{d|\frac{n}{c}} \mu(d) = \sum_{d|1} \mu(d) = \mu(1) = 1.$

よって, $c = n$ のとき③は $\displaystyle\sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d) \right) = f(n)$ となるから, (3.4) は成り立つ. □

m が正の整数のとき，記号 $\displaystyle\prod_{\boldsymbol{d|m}}$ でもって， m のすべての正の約数 d にわたる積を表すことにすると，定理 3.2.4 と同様に，次の定理が成り立つ.

定理 3.2.5　F, f は定義域が $\mathbb{N}$ の関数で，$F(n) = \displaystyle\prod_{d|n} f(d)$ を満たすとき

$$f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} \tag{3.5}$$

が成り立つ.

証明　$F\left(\dfrac{n}{d}\right) = \displaystyle\prod_{c|\frac{n}{d}} f(c)$ を使うと

$$\prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} \left(\prod_{c|\frac{n}{d}} f(c) \right)^{\mu(d)} = \prod_{d|n} \prod_{c|\frac{n}{d}} f(c)^{\mu(d)} \qquad \cdots\cdots ①$$

と変形できる.

$d \mid n$ かつ $c \Big| \dfrac{n}{d} \iff c \mid n$ かつ $d \Big| \dfrac{n}{c}$

が成り立つことを用いると ①は次のように変形できる．

$$\prod_{d|n}\sum_{c|\frac{n}{d}} f(c)^{\mu(d)} = \prod_{c|n}\prod_{d|\frac{n}{c}} f(c)^{\mu(d)} = \prod_{c|n} f(c)^{\sum\limits_{d|\frac{n}{c}}\mu(d)}. \qquad \cdots\cdots ②$$

定理 3.2.3 より $\sum\limits_{d|\frac{n}{c}}\mu(d)$ は $\dfrac{n}{c}=1$ すなわち $c=n$ のときを除いて 0 になる．

$c=n$ のとき $\sum\limits_{d|\frac{n}{c}}\mu(d)=\sum\limits_{d|1}\mu(d)=\mu(1)=1.$

よって，$c=n$ のとき②は $\prod\limits_{c|n} f(c)^{\sum\limits_{d|\frac{n}{c}}\mu(d)} = f(n)$ となるから，(3.5) は成り立つ． □

定理 3.2.6　F, f は定義域が $\mathbb{N}$ の関数とする．F は乗法的で，$F(n)=\sum\limits_{d|n} f(d)$ を満たすならば，f も乗法的である．

証明　m, n を互いに素な正の整数とする．

メビウスの反転公式より

$$f(n)=\sum_{d|n} F\left(\frac{n}{d}\right)\mu(d)$$

が成り立つ．

mn のすべての約数 d は

$$d=d_1d_2,\ d_1\mid m,\ d_2\mid n,\ \gcd(d_1,d_2)=1$$

の形にかける．$1=\gcd(m,n)=\gcd\left(\dfrac{m}{d_1}d_1,\dfrac{n}{d_2}d_2\right)$ だから，$\gcd\left(\dfrac{m}{d_1},\dfrac{n}{d_2}\right)=1.$

よって

$$\begin{aligned}
f(mn) &= \sum_{d|mn} F\left(\frac{mn}{d}\right)\mu(d)\\
&= \sum_{\substack{d_1|m\\ d_2|n}} F\left(\frac{mn}{d_1d_2}\right)\mu(d_1d_2)\\
&= \sum_{\substack{d_1|m\\ d_2|n}} F\left(\frac{m}{d_1}\right)F\left(\frac{n}{d_2}\right)\mu(d_1)\mu(d_2) \quad (F,\ \mu\text{は乗法的})\\
&= \sum_{d_1|m} F\left(\frac{m}{d_1}\right)\mu(d_1)\sum_{d_2|n} F\left(\frac{n}{d_2}\right)\mu(d_2)\\
&= f(m)f(n).
\end{aligned}$$

したがって，f は乗法的である． □

3.3　オイラー (Euler) の φ 関数

オイラーの φ 関数 $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ は

$\varphi(1) = 1$,

$n \geq 2$ のとき，$\varphi(n)$ は $1, 2, \ldots, n-1$ の中で n と互いに素なものの個数

で定義される．

例　$\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2,$
$\varphi(7) = 6, \varphi(8) = 4, \varphi(9) = 6, \varphi(10) = 4, \varphi(11) = 10, \varphi(12) = 4.$

- p が素数，e が正の整数のとき，$\varphi\left(p^e\right) = p^e - p^{e-1}$.
  特に $\varphi(p) = p - 1$.
  p^e より小さくて，p^e と互いに素でない正の整数は $p, 2p, 3p, \ldots, \left(p^{e-1} - 1\right)p$ の $p^{e-1} - 1$ 個であるから，p^e より小さくて p^e と互いに素な正の整数の個数は $\varphi\left(p^e\right) = \left(p^e - 1\right) - \left(p^{e-1} - 1\right) = p^e - p^{e-1}$.
- $n \geq 2$ のとき，$\varphi(n)$ は $1, 2, \ldots, n$ の中で n と互いに素なものの個数でもある．これを使うと，p が素数，e が正の整数のとき，$\varphi\left(p^e\right) = p^e - p^{e-1}$ は次のように示すことができる．
  p^e 以下で，p^e と互いに素でない正の整数は $p, 2p, 3p, \ldots, p^{e-1} \cdot p$ の p^{e-1} 個であるから，p^e 以下で p^e と互いに素な正の整数の個数は $\varphi\left(p^e\right) = p^e - p^{e-1}$.

有限集合の S 要素の個数を $|S|$ で表すことにする．$|A \cup B| = |A| + |B| - |A \cap B|$, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$ が成り立つが，一般的には定理 3.3.1 のようになる．

定理 3.3.1　$n \geq 2$ は正の整数，$A_1, A_2, \ldots, A_n$ を有限集合 A の部分集合とする．

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n| \tag{3.6}$$

が成り立つ．

${A_i}^c = A - A_i$ を A_i の補集合とすると

$$|{A_1}^c \cap {A_2}^c \cap \cdots \cap {A_n}^c| = |A| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \sum_{i<j<k} |A_i \cap A_j \cap A_k| + \cdots + (-1)^n |A_1 \cap A_2 \cap \cdots \cap A_n| \tag{3.7}$$

が成り立つ．

証明 (3.6) が成り立つことを n に関する数学的帰納法で示す.

(I) $n=2$ のとき $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ は成り立つ.
(II) $n=m$ のとき成り立つと仮定すると

$$\Big|\bigcup_{i=1}^{m} S_i\Big| = \sum_{1\le i\le m} |S_i| - \sum_{1\le i<j\le m} |S_i\cap S_j| + \sum_{1\le i<j<k\le m} |S_i\cap S_j\cap S_k| - \cdots + (-1)^{m-1}\Big|\bigcap_{i=1}^{m} S_i\Big|$$

が成り立つ.

$|T_1 \cup T_2| = |T_1| + |T_2| - |T_1 \cap T_2|$ で $T_1 = \bigcup_{i=1}^{m} A_i$, $T_2 = A_{m+1}$ とおき分配法則[*2]

を使うと, $T_1 \cap T_2 = \left(\bigcup_{i=1}^{m} A_i\right) \cap A_{m+1} = \bigcup_{i=1}^{m} (A_i \cap A_{m+1})$ だから

$$\left|\bigcup_{i=1}^{m+1} A_i\right| = \left|\bigcup_{i=1}^{m} A_i\right| + |A_{m+1}| - \left|\bigcup_{i=1}^{m} (A_i \cap A_{m+1})\right|.$$

ここで, $\left|\bigcup_{i=1}^{m} A_i\right|$, $\left|\bigcup_{i=1}^{m} (A_i \cap A_{m+1})\right|$ に対して帰納法の仮定を使うと

$$\begin{aligned}
&\left|\bigcup_{i=1}^{m+1} A_i\right| = \left|\bigcup_{i=1}^{m} A_i\right| + |A_{m+1}| - \left|\bigcup_{i=1}^{m} (A_i \cap A_{m+1})\right| \\
&= \sum_{1\le i\le m} |A_i| - \sum_{1\le i<j\le m} |A_i\cap A_j| + \sum_{1\le i<j<k\le m} |A_i\cap A_j\cap A_k| - \cdots + (-1)^{m-1}\left|\bigcap_{i=1}^{m} A_i\right| \\
&\quad + |A_{m+1}| - \sum_{1\le i\le m} |A_i\cap A_{m+1}| + \sum_{1\le i<j\le m} |A_i\cap A_j\cap A_{m+1}| \\
&\qquad - \sum_{1\le i<j<k\le m} |A_i\cap A_j\cap A_k\cap A_{m+1}| + \cdots + (-1)^{m}\left|\bigcap_{i=1}^{m+1} A_i\right| \\
&= \sum_{1\le i\le m} |A_i| + |A_{m+1}| - \sum_{1\le i<j\le m} |A_i\cap A_j| - \sum_{1\le i\le m} |A_i\cap A_{m+1}| \\
&\quad + \sum_{1\le i<j<k\le m} |A_i\cap A_j\cap A_k| + \sum_{1\le i<j\le m} |A_i\cap A_j\cap A_{m+1}| \\
&\qquad - \sum_{1\le i<j<k<l\le m} |A_i\cap A_j\cap A_k\cap A_l| - \sum_{1\le i<j<k\le m} |A_i\cap A_j\cap A_k\cap A_{m+1}| \\
&\qquad + \cdots + (-1)^{m}\left|\bigcap_{i=1}^{m+1} A_i\right| \\
&= \sum_{1\le i\le m+1} |A_i| - \sum_{1\le i<j\le m+1} |A_i\cap A_j| + \sum_{1\le i<j<k\le m+1} |A_i\cap A_j\cap A_k| - \cdots
\end{aligned}$$

[*2] $A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$, $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$.

$$+(-1)^m \left| \bigcap_{i=1}^{m+1} A_i \right|$$

となり，$n = m+1$ のときも成り立つ．

(III) (I)，(II) よりすべての正整数 $n \geq 2$ について (3.6) が成り立つ．

(3.7) は

$$\left| \bigcap_{i=1}^{m+1} {A_i}^c \right| = \left| \left(\bigcup_{i=1}^{m+1} A_i \right)^c \right| = |A| - \left| \bigcup_{i=1}^{m+1} A_i \right|$$

と (3.6) から得られる． □

(3.6) は包除原理 と呼ばれる．

定理 3.3.2　$n \geq 2$ の素因数分解を $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ とすると

$$\varphi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\cdots\left(p_r^{e_r} - p_r^{e_r-1}\right) \tag{3.8}$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \tag{3.9}$$

が成り立つ．

証明　$A_i = \left\{ d : d \text{ は } n \text{ 以下の } p_i \text{の倍数} \right\}$ $(1 \leq i \leq r)$ とおくと，

$$\varphi(n) = |{A_1}^c \cap {A_2}^c \cap \cdots \cap {A_r}^c|$$

である．

$|A_i| = \frac{n}{p_i}$ $(1 \leq i \leq r)$, $|A_i \cap A_j| = \frac{n}{p_i p_j}$ $(1 \leq i < j \leq r)$, $\ldots$, $|A_1 \cap \cdots \cap A_r| = \frac{n}{p_1 \cdots p_r}$

より

$$\begin{aligned}
\varphi(n) &= |{A_1}^c \cap {A_2}^c \cap \cdots \cap {A_n}^c| \\
&= n - \sum_{1 \leq i \leq r} \frac{n}{p_i} + \sum_{1 \leq i < j \leq r} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

次に $\varphi(n)$ を変形する．

$$\begin{aligned}
\varphi(n) &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{e_2}\left(1 - \frac{1}{p_2}\right)\cdots p_r^{e_r}\left(1 - \frac{1}{p_r}\right) \\
&= \left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\cdots\left(p_r^{e_r} - p_r^{e_r-1}\right).
\end{aligned}$$

□

定理 3.3.3　φ は乗法的関数である.

証明 互いに素な正の整数 m, n に対して

$$\varphi(mn) = \varphi(m)\varphi(n) \qquad \cdots\cdots ①$$

が成り立つことを示す.

$m = 1$ または $n = 1$ のとき明らかに①は成り立つので，以下 $m, n \geq 2$ とする.

m, n を素因数分解すると

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},\ n = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s} \quad (p_1, \ldots, p_r,\ q_1, \ldots, q_s \text{ はすべて異なる素数})$$

とおけるから

$$\begin{aligned} f(mn) &= f\left(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \cdot q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}\right) \\ &= \left(p_1^{e_1} - p_1^{e_1 - 1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r - 1}\right) \left(q_1^{f_1} - q_1^{f_1 - 1}\right) \cdots \left(q_s^{f_s} - q_s^{f_s - 1}\right) \\ &= f(m) f(n) \end{aligned}$$

が成り立つ. □

定理 3.3.4　n が正の整数のとき

$$\sum_{d|n} \varphi(d) = n \tag{3.10}$$

が成り立つ.

証明　$n = 1$ のとき，$\sum_{d|1} \varphi(d) = \varphi(1) = 1$ である.

$n \geq 2$ のときは，$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ と素因数分解すると，φ は乗法的なので定理 3.2.2 より

$$\begin{aligned} \sum_{d|n} \varphi(d) = &\left(1 + \varphi(p_1) + \varphi\left(p_1^2\right) + \cdots + \varphi\left(p_1^{e_1}\right)\right) \\ &\left(1 + \varphi(p_2) + \varphi\left(p_2^2\right) + \cdots + \varphi\left(p_2^{e_2}\right)\right) \\ &\quad \cdots\cdots \\ &\left(1 + \varphi(p_r) + \varphi\left(p_r^2\right) + \cdots + \varphi\left(p_r^{e_r}\right)\right) \\ = &\left(1 + (p_1 - 1) + \left(p_1^2 - p_1\right) + \cdots + \left(p_1^{e_1} - p_1^{e_1 - 1}\right)\right) \\ &\left(1 + (p_2 - 1) + \left(p_2^2 - p_2\right) + \cdots + \left(p_2^{e_2} - p_2^{e_2 - 1}\right)\right) \\ &\quad \cdots\cdots \\ &\left(1 + (p_r - 1) + \left(p_r^2 - p_r\right) + \cdots + \left(p_r^{e_r} - p_r^{e_r - 1}\right)\right) \\ &= p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \\ &= n. \end{aligned}$$

□

定理 3.3.5　n が正の整数のとき

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} \tag{3.11}$$

が成り立つ．

証明 (3.10) にメビウスの反転公式を用いれば (3.11) が得られる．　□

φ は乗法的関数であることの別証明

互いに素な正の整数 m, n に対して

$$\varphi(mn) = \varphi(m)\varphi(n) \qquad \cdots\cdots ①$$

が成り立つことを示す．

$m = 1$ または $n = 1$ のとき明らかに①は成り立つので，以下 $m, n \geq 2$ とする．
mn 個の正の整数 1, 2, ..., mn を次のように並べる．

1	2	3	...	k	...	m
$m+1$	$m+2$	$m+3$	...	$m+k$	...	$2m$
$2m+1$	$2m+2$	$2m+3$	...	$2m+k$	...	$3m$
...	...	...	...	...	...	...
$(n-1)m+1$	$(n-1)m+2$	$(n-1)m+3$	...	$(n-1)m+k$	...	nm

$\gcd(m, n) = 1$ であるから，$r \in \mathbb{N}$ に対して

$$\gcd(r, mn) = 1 \Longleftrightarrow \gcd(r, m) = 1 \text{ かつ } \gcd(r, n) = 1$$

が成り立つので，まず上の表から m と互いに素なものを決定し，次にそれらの中から n と互いに素なものを見つける．

第 1 行目には $\varphi(m)$ 個の m と互いに素な正の整数がある．これらの中から任意の i $(1 \leq i < m,\ \gcd(i, m) = 1)$ をとると，その下の 2 行目から n 行目の数 (2 行 i 列の数，3 行 i 列の数，..., n 行 i 列の数) $jm + i$ $(1 \leq j \leq n-1)$ は m と互いに素になる．

なぜならば，定理 2.3.1 を使うと

$$(jm + i, m) = (jm + i - jm, m) = (i, m) = 1$$

となるからである．

したがって，第 1 行で m と互いに素な $\varphi(m)$ 個の正の整数を含む列の正の整数はすべて m と互いに素である．

上の議論と全く同様にして，第 1 行目には $m-\varphi(m)$ 個の m と互いに素でない整数がある．これらの中から，任意の i' $(1 < i' \leq m,\ \gcd(i',\, m) > 1)$ をとると，その下の 2 行目から n 行目の数 $jm + i'$ $(1 \leq j \leq n-1)$ は m と互いに素ではない．

なぜならば，

$$(jm + i',\, m) = (jm + i' - jm,\, m) = (i',\, m) > 1$$

となるからである．

したがって，第 1 行で m と互いに素でない $m-\varphi(m)$ 個の正の整数を含む列の正の整数はすべて m と互いに素ではない．

以上のことから，上の表でと互いに素になっている正の整数は，第 1 行で m と互いに素な $\varphi(m)$ 個の正の整数を含む列の正の整数のみであることがわかった．

再び第 1 行目で m と互いに素になっている正の整数のうちから，任意の i $(1 \leq i < m,\ \gcd(i,\, m) = 1)$ をとり，第 i 列を考える．

i 列目の n 個の正の整数 $i,\, m+i,\, 2m+i,\, \ldots,\, (n-1)m+i$ の中には，n と互いに素なものが $\varphi(n)$ 個あることを示す．

$0 \leq p,\, q \leq n-1$ に対して $pm+i$ と $qm+i$ を n で割った余りが異なることを示す．

もしも，$pm+i$ と $qm+i$ を n で割った余りが等しくなったとすると，$pm+i-(qm+i) = (p-q)m$ は n で割り切れる．m と n は互いに素であるから，$p-q$ は n で割り切れる．

$-n+1 \leq p-q \leq n-1$ なので，$p-q$ が n で割り切れるのは $p=q$ のときしかない．

以上のことから

$$0 \leq p,\, q \leq n-1,\ p \neq q \Longrightarrow pm+i \text{ と } qm+i \text{ を } n \text{ で割った余りは異なる．}$$

よって，$i,\, m+i,\, 2m+i,\, \ldots,\, (n-1)m+i$ を n で割った余り $r_0,\, r_1,\, \ldots, r_{n-1}$ は $0,\, 1,\, 2,\, \ldots,\, n-1$ を並べ替えたものに等しい．また

$$(n,\, i) = (n,\, r_0),\ (n,\, m+i) = (n,\, r_1),\ \ldots,\ (n,\, (n-1)m+i) = (n,\, r_{n-1})$$

が成り立つから

$$\begin{aligned}
&\Big\{(n,\ i),\ (n,\ m+i),\ (n,\ 2m+i),\ \ldots,\ (n,\ (n-1)m+i)\Big\} \\
&= \Big\{(n,\ r_0),\ (n,\ r_1),\ (n,\ r_2),\ \ldots,\ (n,\ r_{n-1})\Big\} \\
&= \Big\{(n,\ 0)(=n),\ (n,\ 1),\ (n,\ 2),\ \ldots,\ (n,\ n-1)\Big\}.
\end{aligned}$$

この集合の要素で 1 となるものの個数は，$n-1$ 以下で n と互いに素な正の整数の個数 $\varphi(n)$ に等しい．

したがって，m と互いに素な列には $\varphi(n)$ 個の n と互いに素な正の整数が存在するから，$\varphi(mn) = \varphi(m)\varphi(n)$ が成り立つ．　□

第4章

合同式

4.1　合同式

m を固定した正の整数とする．2つの整数 a, b に対して，m が $a-b$ を割り切るとき，すなわち $m|a-b$ のとき，a と b は **m を法として合同** (congruent modulo m) であるといい，$\boldsymbol{a \equiv b \pmod{m}}$ と表す．

命題 4.1.1　m を正の整数とする．2つの整数 a, b に対して，$a \equiv b \pmod{m}$ となるための必要十分条件は，a と b を m で割った余りが等しくなることである．

証明　$a \equiv b \pmod{m}$ とすると $a = b + km,\ k \in \mathbb{Z}$ とかける．b を m で割った商を q，余りを r とすると，

$$b = mq + r, \quad 0 \leq r < m$$

となる整数 q, r が存在する．この式を $a = b + km$ に代入すると

$$a = b + km = mq + r + km = m(q + k) + r$$

が成り立ち $0 \leq r < m$ であったから，a を m で割った余りは r である．よって，a と b を m で割った余りは等しい．

a と b を m で割った余りは等しいと仮定すると，

$$a = mq_1 + r, \quad b = mq_2 + r, \quad 0 \leq r < m$$

となる整数 q_1, q_2, r が存在する．

$$a - b = (mq_1 + r) - (mq_2 + r) = m(q_1 - q_2)$$

から，$m|a-b$ すなわち $a \equiv b \pmod{m}$ が成り立つ．　□

命題 4.1.2　$m \in \mathbb{N},\ a,\ b,\ c \in \mathbb{Z}$ とすると次のことが成り立つ．

(1)　$a \equiv a \pmod{m}$.
(2)　$a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$.
(3)　$a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$.
(4)　$a \equiv b \pmod{m} \implies a + c \equiv b + c \pmod{m},\quad ca \equiv cb \pmod{m}$.

証明 定義に基づいて丁寧に証明しておきたい．

(1) $a - a = 0 = m \cdot 0$ より $m \mid a - a$ となるから $a \equiv a \pmod{m}$.
(2) $a \equiv b \pmod{m}$ のとき $m \mid a - b$ であるから $a - b = mq$ となる整数 q が存在する．このとき $b - a = -(a - b) = m \cdot (-q)$ より $m \mid b - a$ すなわち $b \equiv a \pmod{m}$.
(3) $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m}$ のとき $m \mid a - b,\ m \mid b - c$ であるから $a - b = mq_1,\ b - c = mq_2$ となる整数 q_1, q_2 が存在する．このとき $a - c = (a - b) + (b - c) = mq_1 + mq_2 = m(q_1 + q_2)$ となるから $m \mid a - c$ すなわち $a \equiv c \pmod{m}$.
(4) $a \equiv b \pmod{m}$ のとき $m \mid a - b$ であるから $a - b = mq$ となる整数 q が存在する．このとき $(a + c) - (b + c) = a - b = mq,\quad ca - cb = c(a - b) = mcq$ となるから $m|(a+c)-(b+c),\ m \mid ca-cb$ すなわち $a+c \equiv b+c \pmod{m},\ ca \equiv cb \pmod{m}$.

□

定理 4.1.1　$m \in \mathbb{N},\ a,\ b,\ c,\ d \in \mathbb{Z}$ とすると次のことが成り立つ．

(1)　$a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m} \implies a + c \equiv b + d \pmod{m}$.
(2)　$a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$.
(3)　$ca \equiv cb \pmod{m}$ かつ $\gcd(c,\ m) = 1 \implies a \equiv b \pmod{m}$.

証明 (1), (2)　$a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m}$ のとき $a-b = mq_1,\ c-d = mq_2$ となる整数 q_1, q_2 が存在する．このとき，

$$(a + c) - (b + d) = (a - b) + (c - d) = mq_1 + mq_2 = m(q_1 + q_2),$$
$$ac - bd = (a - b)c + (c - d)b = mq_1 \cdot c + mq_2 \cdot b = m(q_1c + q_2b)$$

より $a + c \equiv b + d \pmod{m},\ ac \equiv bd \pmod{m}$.

(3) $ca \equiv cb \pmod{m}$ のとき $ca - cb = mq$ となる整数 q が存在する．$ca - cb = mq$ を変形した $c(a - b) = qm$ から $c \mid qm$ が成り立つ．c と m は互いに素なので，定理 2.2.3(1) より $c \mid q$ が言える．よって

$$a - b = \frac{q}{c} \cdot m,\quad \frac{q}{c} \in \mathbb{Z}$$

から $m \mid a-b$ すなわち $a \equiv b \pmod{m}$. □

※ 命題 4.1.2 を使うと (1)，(2) は次のように示すことができる．
$a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m}$ の両辺にそれぞれ c, b を加えると，

$$a+c \equiv b+c \pmod{m}, \quad b+c \equiv b+d \pmod{m}.$$

よって $a+c \equiv b+d \pmod{m}$.
$a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m}$ の両辺にそれぞれ c, b をかけると，

$$ac \equiv bc \pmod{m}, \quad bc \equiv bd \pmod{m}.$$

よって $ac \equiv bd \pmod{m}$.

- 合同記号 $\equiv$ を用いた加法，減法，乗法を含む計算は，等号 $=$ のときと同じようにできることがわかる．ただし，割り算は定理 4.1.1 (3) のようにしかできない．

系 4.1.1 $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ とすると次のことが成り立つ．
$a \equiv b \pmod{m} \implies$ 任意の $n \in \mathbb{N}$ について，$a^n \equiv b^n \pmod{m}$.
さらに，整数係数の n 次の多項式 $f(x)$ に対して，次のことが成り立つ．
$a \equiv b \pmod{m} \implies f(a) \equiv f(b) \pmod{m}$.

証明 n に関する数学的帰納法で証明する．

(I) $n=1$ のとき明らかに成り立つ．
(II) $n=k$ のとき成り立つと仮定すると，$a^k \equiv b^k \pmod{m}$.
この式と $a \equiv b \pmod{m}$ に対して，定理 4.1.1(2) を使うと

$$a^k \cdot a \equiv b^k \cdot b \pmod{m} \text{ すなわち } a^{k+1} \equiv b^{k+1} \pmod{m}$$

となり，$n=k+1$ のときも成り立つ．

(III) (I)，(II) から，すべての正の整数 n に対して成り立つ．

$f(x) = p_n x^n + p_{n-1}x^{n-1} + \cdots + p_1 x + p_0$ $(p_0, p_1, \ldots, p_n \in \mathbb{Z})$ とおくと，
$k \in \{1, 2, \ldots, n\}$ のとき，$a^k \equiv b^k \pmod{m}$ が成り立つから $p_k a^k \equiv p_k b^k \pmod{m}$.
この式で $k = n, n-1, \ldots, 1$ とおいたものと $p_0 \equiv p_0 \pmod{m}$ を辺々加えると

$$p_n a^n + p_{n-1}a^{n-1} + \cdots + p_1 a + p_0 \equiv p_n b^n + p_{n-1}b^{n-1} + \cdots + p_1 b + p_0 \pmod{m}.$$

よって，$f(a) \equiv f(b) \pmod{m}$. □

定理 4.1.2　m を正の整数，a を m と互いに素な整数とすると，

$$ax \equiv 1 \pmod{m}$$

を満たす整数 x が存在する．

証明　a と m は互いに素であるから，$ax + my = 1$ を満たす整数 x, y が存在する．
このとき

$$ax = 1 - my \equiv 1 \pmod{m}.$$ □

• 定理 4.1.2 における x のことを，$\boldsymbol{m}$ **を法とする** $\boldsymbol{a}$ **の逆数** (inverse of a modulo m) といい，$\boldsymbol{a^{-1}}$ で表す．

$\gcd(a, m) = 1$ でなければ，m を法とする a の逆数は存在しない．
なぜならば，もし存在したとすると，$ax - 1 = my$ となる $x, y \in \mathbb{Z}$ が存在する．
$(a, m)|a$, $(a, m)|m$ から $(a, m)|ax + by = 1$ となり $(a, m) > 1$ に矛盾する．

例題 4.1.1　(Frobenius)
a, b は互いに素な正の整数とする．このとき，非負の整数 r, s を用いて，$ar + bs = m$ の形に表せない正の整数 m の個数は $\dfrac{(a-1)(b-1)}{2}$ に等しい．

解答　$A = \left\{ n : ar + bs = n,\ r, s \in \mathbb{N}_0 \right\}$ とおく．
非負の整数を次のように並べて，

	0 列	1 列	2 列	...	k 列	...	$a-1$ 列
0 行	0	1	2	...	k	...	$a-1$
1 行	a	$a+1$	$a+2$	...	$a+k$	...	$2a-1$
2 行	$2a$	$2a+1$	$2a+2$	...	$2a+k$	...	$3a-1$
...	...	...	...	...	...	...	...

という配列を考える．各列の数列は，公差 a の等差数列である．

- $n \in A$ が第 k 列の第 m 行にあるとすると，k 列の第 m' $(> m)$ 行にある数 n' は A に属する．
  $n = ma + k, n' = m'a + k$ $(m \in \mathbb{N}_0, m' \in \mathbb{N}, m' > m)$ とかける．
  $n \in A$ より，$ar_0 + bs_0 = n$ を満たす $r_0, s_0 \in \mathbb{N}_0$ が存在する．
  よって

$$\begin{aligned} n' &= k + m'a \\ &= ma + k + (m' - m)a \end{aligned}$$

$$\begin{aligned} &= n + (m' - m)a \\ &= ar_0 + bs_0 + (m' - m)a \\ &= (r_0 + m' - m)a + bs_0 \end{aligned}$$

となり，$r_0 + m' - m \in \mathbb{N}, s_0 \in \mathbb{N}_0$ であるから，$n' \in A$ となる．

- $mb \in A \quad (m = 0, 1, \ldots, a-1)$.
  $m \in \{0,\ 1,\ \ldots,\ a-1\}$ のとき，

$$mb = 0 \cdot a + m \cdot b \in A.$$

- 異なる mb, nb $(0 \leq m < n \leq a-1)$ は異なる列に存在する．
  もしも mb, nb が同じ列にあったとすると，$mb \equiv nb \pmod{a}$ から，

$$(n-m)b \equiv 0 \pmod{a}.$$

  a と b は互いに素なので，$n - m \equiv 0 \pmod{a}$ から $a \mid n - m$.
  $0 < n - m \leq a - 1 < a$ であるから，$n - m$ は a の倍数にならないから，$a \mid n - m$ に矛盾する．
- ab 以上の整数はすべて A に属する．
  $mb \in A$ $(m = 0, 1, \ldots, a-1)$ で，第 0 列から第 $a-1$ 列には mb $(m = 0, 1, \ldots, a-1)$ のどれか 1 つだけ存在し，mb が存在する配列の位置から下にある数はすべて A に属するから，ab 以上の整数はすべて A に属する．
- $m \in \{0,\ 1,\ \ldots,\ a-1\}$ で mb が第 i 行，第 j 列にあるとすると，第 i' $(i' < i)$ 行，第 j 列の数は A に属さない．(mb より上にある，mb と同じ列の数は A に属さない．)
  mb より上にある，mb と同じ列の数は $mb - ka$ $(k \in \mathbb{N})$ と表せる．もしも，$mb - ka \in A$ だとすると，

$$ax + by = mb - ka \qquad \cdots ①$$

  を満たす非負の整数 x, y が存在する．①から，a を法として考えると

$$(m - y)b = (x + k)a \equiv 0 \pmod{a}$$

  から

$$(m-y)b \equiv 0 \pmod{a}.$$

  a と b は互いに素なので，$m - y \equiv 0 \pmod{a}$ から $a \mid m - y$.
  また，①より

$$by \leq ax + by = mb - ka < mb \qquad y < m.$$

よって，$0 \leq y < m \leq a-1 < a$ より $0 < m-y < a$ なので，$a \mid m-y$ に矛盾する．

	0 列	1 列	2 列	...	j 列	...	$a-1$ 列
0 行	0	1	2	...	$j(\times)$	...	$a-1$
1 行				...	$a+j(\times)$	...	
				...	$\ldots(\times)$	...	
i 行				...	$ia+j=mb(\bigcirc)$	...	
				...	$\ldots(\bigcirc)$	...	

- A に属さない数の個数は，$\displaystyle\sum_{m=1}^{a-1}\left[\frac{mb}{a}\right]$ である．

  $m \in \{0, 1, \ldots, a-1\}$ に対して，mb が第 i 行，第 j 列にあるとすると, 第 j 列で A に属さない数の個数は i 個ある．

  $mb = ia + j,\ 0 \leq j \leq a-1$ より j は mb を a で割った余りであるから，$j = mb - a\left[\dfrac{mb}{a}\right]$．

  したがって，$i = \dfrac{mb-j}{a} = \left[\dfrac{mb}{a}\right]$ となるので，求める個数は

$$\sum_{m=0}^{a-1}\left[\frac{mb}{a}\right] = \sum_{m=1}^{a-1}\left[\frac{mb}{a}\right]$$

  となる．

- $\displaystyle\sum_{m=1}^{a-1}\left[\frac{mb}{a}\right] = \frac{(a-1)(b-1)}{2}$.

  問題 3.1.2 より，a と b が互いに素なとき，

$$\left[\frac{b}{a}\right] + \left[\frac{2b}{a}\right] + \cdots + \left[\frac{(a-1)b}{a}\right] = \frac{(a-1)(b-1)}{2}$$

  が成り立つ．　□

A に属さない最大の整数は，$(a-1)b$ のすぐ上の数であるから，$(a-1)b-a = ab-a-b$ である．また，$ab-a-b$ より大きい正の整数 n は非負の整数 r, s を用いて $n = ar + bs$ と表せることがわかる．

r, s を非負の整数から正の整数にするために，$r = x-1, s = y-1$ とおくと，$n = ar+bs$ は $n = a(x-1) + b(y-1)$ すなわち $n + a + b = ax + by$ となるから，次の結果を得る．

a と b が互いに素な正の整数とき，次のことが成り立つ．

(1) $ab-a-b$ より大きい正の整数 n は非負の整数 r,s を用いて $n=ar+bs$ と表せる．
(2) ab より大きい正の整数 n は正の整数 x,y を用いて $n=ax+by$ と表せる．

(2) は，問題 2.3.2，問題 2.3.3(3) で扱った．(1) を 3 変数にしたのが，問題 2.3.12 である．

問題 4.1.1　$n\in\mathbb{N}_0$ として，N を十進法 (じっしんほう) でかかれた $n+1$ 桁の正の整数

$$\begin{aligned}N&=a_na_{n-1}\dots a_1a_{0(10)}=\overline{a_na_{n-1}\dots a_1a_0}\\&=a_n\cdot10^n+a_{n-1}\cdot10^{n-1}+\dots+a_1\cdot10+a_0\end{aligned}$$

とすると，次のことが成り立つことを示せ．

(1)　N が 2 の倍数 $\iff$ 下 1 桁 (しもひとけた) が 2 の倍数
(2)　N が 3 の倍数 $\iff$ $a_0+a_1+\dots+a_n$ が 3 の倍数
(3)　N が 4 の倍数 $\iff$ 下 2 桁 (しもふたけた) が 4 の倍数
(4)　N が 5 の倍数 $\iff$ 下 1 桁 (しもひとけた) が 0 か 5
(5)　N が 8 の倍数 $\iff$ 下 3 桁 (しもみけた) が 8 の倍数
(6)　N が 9 の倍数 $\iff$ $a_0+a_1+\dots+a_n$ が 9 の倍数
(7)　N が 11 の倍数 $\iff$ $a_0-a_1+a_2-a_3+\dots+(-1)^na_n$ が 11 の倍数

問題 4.1.2　どのような負でない 2 つの整数 m と n をもちいても $x=3m+5n$ とは表すことができない正の整数 x をすべて求めよ．

(2000 大阪大・理・医・歯・薬・工・基礎工・前期)

- 問題 2.3.2，問題 2.3.3 も参照．

問題 4.1.3　n を自然数とする．以下の各問いに答えよ．

(1)　n を 3 で割った余りが 1 ならば，すべての自然数 m に対して n^m を 3 で割った余りは 1 であることを示せ．
(2)　n を 3 で割った余りが 2 ならば，すべての奇数 m に対して n^m を 3 で割った余りは 2 であることを示せ．
(3)　n^m を 3 で割った余りが 2 となる自然数 m があれば，n を 3 で割った余りも 2 であることを示せ．

(2007 お茶の水女子大・理・前期)

4.2　完全剰余系

m を固定した正の整数とする．任意の整数 a に対して，

$$C(a) = \Big\{x : x \equiv a \pmod{m},\ x \in \mathbb{Z}\Big\}$$

を m を法とする**剰余類**という．

命題 4.1.1 より，$x \equiv a \pmod{m}$ となるための必要十分条件は，x と a を m で割った余りが等しくなることであるから，整数を m で割った余りで分類する．

$r \in \mathbb{N}_0$ を $0 \leq r \leq m-1$ として

$$C(r) = \Big\{x : x \equiv r \pmod{m},\ x \in \mathbb{Z}\Big\} = \Big\{x : x = mq + r,\ q \in \mathbb{Z}\Big\}$$

を考えると

$$\mathbb{Z} = C(0) \cup C(1) \cup \cdots \cup C(m-1),\ C(i) \cap C(j) = \phi \quad (i \neq j)$$

剰余類 $C(0),\ C(1),\ \ldots,\ C(m-1)$ の集合を $\mathbb{Z}/\boldsymbol{m}\mathbb{Z}$ または $\mathbb{Z}_{\boldsymbol{m}}$ で表す．

$$\mathbb{Z}/m\mathbb{Z} = \Big\{C(0),\ C(1),\ \ldots,\ C(m-1)\Big\}.$$

$0 \leq r \leq m-1$ として，各剰余類 $C(r)$ から 1 つずつ代表元 x_r を取り出して作った集合

$$\Big\{x_0,\ x_1,\ \ldots,\ x_{m-1}\Big\}$$

を m を法とする**完全剰余系**という．特に $\Big\{0,\ 1,\ \ldots,\ m-1\Big\}$ は m を法とする完全剰余系の一つである．

命題 4.2.1　m を正の整数とするとき，次のことが成り立つ．

(1)　$C(a) = C(b) \iff a \equiv b \pmod{m}$.

(2)　任意の整数 a に対して

$$C(a) = C(r), \quad 0 \leq r < m$$

を満たす整数 r がただ一つ存在する．

(3)　(a)　$m = 2k$ $(k \in \mathbb{N})$ ならば

$$\Big\{-(k-1),\ -(k-2),\ \ldots,\ -1,\ 0,\ 1,\ 2,\ \ldots,\ k-1,\ k\Big\}$$

は m を法とする完全剰余系である．

(b) $m = 2k+1$ $(k \in \mathbb{N}_0)$ ならば

$$\Big\{ -k,\ -(k-1),\ \ldots,\ -1,\ 0,\ 1,\ 2,\ \ldots,\ k-1,\ k \Big\}$$

は m を法とする完全剰余系である.

証明 (1) $C(a) = C(b)$ が成り立つと仮定する.

$x \in C(a) = C(b)$ とすると, $x \equiv a \pmod m$, $x \equiv b \pmod m$ が成り立つから, $a \equiv b \pmod m$.

$a \equiv b \pmod m$ と仮定すると

$$x \equiv a \pmod m \iff x \equiv b \pmod m$$

であるから, $C(a) = C(b)$.

(2) a を m で割った商を q, 余りを r とすると, $a = mq + r$, $0 \le r < m$ とかける.

これから $a \equiv r \pmod m$ となるので, (1) より $C(a) = C(r)$.

$C(a) = C(r)$, $C(a) = C(r')$, $0 \le r < m$, $0 \le r' < m$ となる r, r' が存在したとする. $C(r) = C(r')$ が成り立つから, (1) より $r \equiv r' \pmod m$.ところが, $0 \le r < m$, $0 \le r' < m$ だから, $r = r'$ でなければならない.

(3) (a) $m = 2k$ $(k \in \mathbb{N})$ であるから

$$\mathbb{Z}/m\mathbb{Z} = \Big\{ C(0),\ C(1),\ \ldots,\ C(k),\ C(k+1),\ \ldots,\ C(2k-1) \Big\}.$$

$C(k+1) = C\left(-(k-1)\right)$, $C(k+2) = C\left(-(k-2)\right)$, $\ldots$, $C(2k-1) = C(-1)$ すなわち $C(k+i) = C\left(-(k-i)\right)$ $(1 \le i \le k-1)$ を示せばよい.

$(k+i) - \left(-(k-i)\right) = 2k = m \equiv 0 \pmod m$ だから $k+i \equiv -(k-i) \pmod m$ が成り立つ. したがって, (1) より $C(k+i) = C\left(-(k-i)\right)$ $(1 \le i \le k-1)$.

(b) $m = 2k+1$ $(k \in \mathbb{N}_0)$ であるから

$$\mathbb{Z}/m\mathbb{Z} = \Big\{ C(0),\ C(1),\ \ldots,\ C(k),\ C(k+1),\ \ldots,\ C(2k) \Big\}.$$

$C(k+1) = C\left(-k\right)$, $C(k+2) = C\left(-(k-1)\right)$, $\ldots$, $C(2k) = C(-1)$ すなわち $C(k+i) = C\left(-(k-i+1)\right)$ $(1 \le i \le k)$ を示せばよい.

$(k+i) - \left(-(k-i+1)\right) = 2k+1 = m \equiv 0 \pmod m$ だから $k+i \equiv -(k-i+1) \pmod m$ が成り立つので, (1) より $C(k+i) = C\left(-(k-i+1)\right)(1 \le i \le k)$. □

- 命題 4.2.1 (3) より m が奇数である場合

$$\Big\{ -\frac{m-1}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m-1}{2} \Big\}$$

は m を法とする完全剰余系である．

m が偶数である場合

$$\left\{-\frac{m}{2}+1,\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m}{2}\right\}$$

は m を法とする完全剰余系であることがわかったが，

$$\left\{-\frac{m}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m}{2}-1\right\}$$

も m を法とする完全剰余系である．

これら三つの完全剰余系は絶対値が最小である剰余系で，絶対最小剰余系と呼ばれる．

定理 4.2.1　$m \in \mathbb{N}$ とする．m 個の整数の要素からなる集合 $\left\{a_0,\ a_1,\ \ldots,\ a_{m-1}\right\}$ が m を法とする完全剰余系となるための必要十分条件は，

すべての $i, j\ (0 \leq i < j \leq m-1)$ について，$a_i \not\equiv a_j \pmod{m}$ となることである．

証明　$\left\{a_0,\ a_1,\ \ldots,\ a_{m-1}\right\}$ が m を法とする完全剰余系であると仮定する．

すべての $i, j\ (0 \leq i < j \leq m-1)$ について，$a_i \equiv i' \pmod{m}$，$a_j \equiv j' \pmod{m}$ $(0 \leq i', j' \leq m-1,\ i' \neq j')$ となる $i', j' \in \mathbb{N}_0$ が存在する．

もしも，$a_i \equiv a_j \pmod{m}$, $i \neq j$ となる $i, j \in \mathbb{N}_0$ があったとすると，$i' \equiv j' \pmod{m}$ が成り立つ．$-m+1 \leq i'-j' \leq m-1$ であるから $i'-j'$ が m の倍数になるのは $i'-j'=0$ のときだけであるが，これは $i' \neq j'$ に矛盾する．

よって，すべての $i, j\ (0 \leq i < j \leq m-1)$ について，$a_i \not\equiv a_j \pmod{m}$ である．

すべての $i, j\ (0 \leq i < j \leq m-1)$ について，$a_i \not\equiv a_j \pmod{m}$ が成り立つと仮定する．

各 $i\,(0 \leq i \leq m-1)$ に対して，a_i を m で割った余りを r_i とすると，すべての $i, j\ (0 \leq i < j \leq m-1)$ について，$r_i \not\equiv r_j \pmod{m}$ が成り立つ．もしも $r_i \equiv r_j \pmod{m}$ となる $i, j\ (0 \leq i < j \leq m-1)$ があったとすると，$a_i \equiv r_i \pmod{m}$, $a_j \equiv r_j \pmod{m}$ が成り立つから，$a_i \equiv a_j \pmod{m}$ となってしまい，$a_i \not\equiv a_j \pmod{m}$ に矛盾する．

したがって，m 個の整数の要素からなる集合 $\left\{a_0,\ a_1,\ \ldots,\ a_{n-1}\right\}$ は $0 \leq r \leq m-1$ として，各剰余類 $C(r)$ から 1 つずつ元を取り出して作った集合となるので，$\left\{a_0,\ a_1,\ \ldots,\ a_{m-1}\right\}$ は m を法とする完全剰余系となる．　□

定理 4.2.2　m は正の整数，a は m と互いに素な整数とする．

$\left\{a_0,\ a_1,\ \ldots,\ a_{m-1}\right\}$ が m を法とする完全剰余系ならば，$\left\{aa_0,\ aa_1,\ \ldots,\ aa_{m-1}\right\}$ も m を法とする完全剰余系である．

証明 定理 4.2.1 より，すべての i, j $(0 \leq i < j \leq m-1)$ について，$aa_i \not\equiv aa_j \pmod{m}$ が成り立つことを示せばよい．

もしも，ある i, j $(0 \leq i < j \leq m-1)$ について，$aa_i \equiv aa_j \pmod{m}$ が成り立つとする．$aa_i \equiv aa_j \pmod{m}$ を変形すると $a(a_i - a_j) \equiv 0 \pmod{m}$. a と m は互いに素であるから，$a_i - a_j \equiv 0 \pmod{m}$ すなわち $a_i \equiv a_j \pmod{m}$. 定理 4.2.1 より $\left\{a_0,\ a_1,\ \ldots,\ a_{m-1}\right\}$ が m を法とする完全剰余系ではなくなり，$\left\{a_0,\ a_1,\ \ldots,\ a_{m-1}\right\}$ が m を法とする完全剰余系であることに矛盾する．

したがって，すべての i, j $(0 \leq i < j \leq m-1)$ について，$aa_i \not\equiv aa_j \pmod{m}$ が成り立つ． □

$a \in C(r)$ とすると $a \equiv r \pmod{m}$ から $a = mq + r$ を満たす $q \in \mathbb{Z}$ が存在する．このとき

$$(a,\, m) = (mq + r,\, m) = (mq + r - mq,\, m) = (r,\, m)$$

が成り立つ．この $\gcd(r, m)$ が 1 に等しいような剰余類は，特に重要である．

m を法とする剰余類 $C(0), C(1), \ldots, C(m-1)$ の中で $\gcd(r, m) = 1$ を満たす $C(r)$ を m を法とする**既約剰余類**という．

m を法とする既約剰余類 $C(r_1), C(r_2), \ldots, C(r_t)$ の各々から代表元を一つずつ取り出してできる集合 $\left\{x_1,\ x_2,\ \ldots,\ x_t\right\}$ を m を法とする**既約剰余系**という．

$m \geq 2$ のとき，オイラー関数 φ を使うと，m を法とする既約剰余類は $\varphi(m)$ 個あることがわかる．

定理 4.2.3 m は正の整数，a は m と互いに素な整数とする．

$\left\{x_1,\ x_2,\ \ldots,\ x_t\right\}$ が m を法とする既約剰余系ならば，$\left\{ax_1,\ ax_2,\ \ldots,\ ax_t\right\}$ も m を法とする既約剰余系である．

証明 $k \in \left\{1,\ 2,\ \ldots,\ t\right\}$ のとき，$(x_k, m) = 1$ かつ $(a, m) = 1$ より $(ax_k, m) = 1$ が成り立つ．m を法とする既約剰余類は t 個であるから，$ax_1, ax_2, \ldots, ax_t$ の中からどの 2 つをとっても，m を法として合同ではないことを示せばよい．

もしも，ある i, j $(0 \leq i < j \leq t)$ について，$ax_i \equiv ax_j \pmod{m}$ が成り立つとする．$ax_i \equiv ax_j \pmod{m}$ を変形すると $a(x_i - x_j) \equiv 0 \pmod{m}$. a と m は互いに素であるから，$x_i - x_j \equiv 0 \pmod{m}$ すなわち $x_i \equiv x_j \pmod{m}$． 命題 4.2.1 より $C(x_i) = C(x_j)$ となり矛盾が生じる．

したがって，すべての i, j $(0 \leq i < j \leq t)$ について，$ax_i \not\equiv ax_j \pmod{m}$ が成り立つ． □

4.3　フェルマーの小定理

定理 4.3.1　p は素数，a は整数とするとき，次のことが成り立つ．

(1)　$a^p \equiv a \pmod{p}$.

(2)　$(a, p) = 1$ ならば $a^{p-1} \equiv 1 \pmod{p}$.

証明 (1) まず $a > 0$ として，a に関する数学的帰納法で証明する．

(I) $a = 1$ とき $a^1 \equiv a \pmod{p}$ は成り立つ．

(II) $a = k$ のとき成り立つと仮定すると，$k^p \equiv k \pmod{p}$.

$a = k + 1$ のとき，二項定理より

$$(k+1)^p = k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots + \binom{p}{p-1}k + 1.$$

これを

$$(k+1)^p - k^p - 1 = \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots + \binom{p}{p-1}k \quad \cdots\cdots ①$$

と変形する．

ところで，$1 \leq i \leq p-1$ のとき

$$\binom{p}{i} = \frac{p!}{(p-i)!i!} = \frac{p}{i} \cdot \frac{(p-1)!}{(p-i)!(i-1)!} = \frac{p}{i}\binom{p-1}{i-1}$$

から

$$\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1} \qquad \cdots\cdots (*)$$

を得る．

p は素数で，p と $i\,(1 \leq i \leq p-1)$ は互いに素なので，$(*)$ より $\binom{p}{i}$ は p の倍数になる．

よって，①の右辺は p の倍数になり，①の左辺も p の倍数になるから

$$(k+1)^p - k^p - 1 \equiv 0 \pmod{p}$$

すなわち

$$(k+1)^p \equiv k^p + 1 \pmod{p}.$$

ここで，帰納法の仮定 $k^p \equiv k \pmod{p}$ を使うと

$$(k+1)^p \equiv k^p + 1 \equiv k + 1 \pmod{p}.$$

ゆえに，$a = k + 1$ のときも成り立つことがわかった．

(III) (I)，(II) よりすべての正の整数に対して，$a^p \equiv a \pmod{p}$ が成り立つ．

$a = 0$ のときは明らかに成り立つ．

$a < 0$ のときは $a \equiv b \pmod{p}$ となる正の整数 b をとると，$b^p \equiv b \equiv a \pmod{p}$ かつ $a^p \equiv b^p \pmod{p}$ から $a^p \equiv a \pmod{p}$ が成り立つ．

(2) (1) から $a^p \equiv a \pmod{p}$ が成り立つ．この式を $a(a^{p-1} - 1) \equiv 0 \pmod{p}$ と変形する．a と p は互いに素だから，$a^{p-1} - 1 \equiv 0 \pmod{p}$ すなわち $a^{p-1} \equiv 1 \pmod{p}$. □

(1) の証明のなかで

$$\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1} \qquad \cdots\cdots(*)$$

を使い，次のことを示した．

> p は素数で，$1 \leq i \leq p-1$ のとき $\binom{p}{i}$ は p の倍数になる．

$\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}$ を使わない場合は次のように示せばよい．

$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 1}$ において，p は素数であり，分母の $i, i-1, \ldots, 1$ はすべて p より小さい正整数なので，分子の p は約分されないで残る．よって，$\binom{p}{i}$ は p の倍数になる．

例題 4.3.1　a, b は $a > b$ を満たす自然数とし，p, d は素数で $p > 2$ とする．このとき，$a^p - b^p = d$ であるならば，d を $2p$ で割った余りが 1 であることを示せ．

(1995 京都大 総合人間（理系）・理・医・薬・工・農・前期)

解答　$d = a^p - b^p = (a-b)\left(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}\right)$ が素数で，$p > 2$, $a > b \geq 1$ より $a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} > 1$ だから，$a - b = 1$ でなければならない．

p は素数だから，フェルマーの小定理より，$a^p \equiv a \pmod{p}$, $b^p \equiv b \pmod{p}$ が成り立つから

$$d = a^p - b^p \equiv a - b \equiv 1 \pmod{p}$$

すなわち

$$p \mid d - 1. \qquad \cdots\cdots①$$

$a - b = 1$ より a と b の偶奇は異なる．また，p は奇素数である．

a が偶数，b が奇数のとき，$d = a^p - b^p \equiv 0^p - 1^p \equiv -1 \equiv 1 \pmod{2}$.

a が奇数，b が偶数のとき，$d = a^p - b^p \equiv 1^p - 0^p \equiv 1 \pmod 2$.
いずれにしても

$$2 \mid d - 1. \qquad \cdots\cdots ②$$

p は奇素数だから，$\gcd(p, 2) = 1$ で，①，②より，$2p \mid d - 1$ すなわち d を $2p$ で割った余りが 1 である．□

注　$d - 1$ が p で割り切れるところを，フェルマーの小定理を使わなければ，次のように解くことになるだろう．

$$d = a^p - b^p = (b+1)^p - b^p = \sum_{i=0}^{p-1} \binom{p}{i} b^i = 1 + \sum_{i=1}^{p-1} \binom{p}{i} b^i.$$

「p は素数で，$1 \le i \le p-1$ のとき $\binom{p}{i}$ は p の倍数になる」ことから，$\displaystyle\sum_{i=1}^{p-1} \binom{p}{i} b^i$ は p で割り切れる．よって，$d - 1$ が p で割り切れる．□

命題 4.3.1　p は素数，a, b は整数とする．
$(a, p) = 1$ ならば $ax \equiv b \pmod p$ は解をもつ．

証明 フェルマーの小定理より，$a^{p-1} \equiv 1 \pmod p$ が成り立つ．$ax \equiv b \pmod p$ の両辺に a^{p-2} をかけると

$$a^{p-1}x \equiv a^{p-2}b \pmod p \text{ すなわち } x \equiv a^{p-2}b \pmod p.$$

$ax \equiv b \pmod p$ は解 $x \equiv a^{p-2}b \pmod p$ をもつ．□

※ フェルマーの小定理は $a^{-1} \equiv a^{p-2} \pmod p$ であることを教えてくれる．

例題 4.3.2　すべての素数 p に対して，$2^n + 3^n + 6^n - 1$ が p で割り切れるような，正の整数 n が存在することを示せ．

解答　$p = 2$ のとき $n = 2$ とすると $2^2 + 3^2 + 6^2 - 1 \equiv 0^2 + 1^2 + 0^2 - 1 \equiv 0 \pmod 2$.
$p = 3$ のとき $n = 2$ とすると $2^2 + 3^2 + 6^2 - 1 \equiv (-1)^2 + 0^2 + 0^2 - 1 \equiv 0 \pmod 3$.
$p \ge 5$ のとき $(2, p) = (3, p) = (6, p) = 1$ なので，フェルマーの小定理より

$$2^{p-1} \equiv 1 \pmod p,\ 3^{p-1} \equiv 1 \pmod p,\ 6^{p-1} \equiv 1 \pmod p$$

が成り立つので，$n = p - 2$ とすると

$$\begin{aligned} 6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) &= 3 \cdot 2^{p-1} + 2 \cdot 3^{p-2} + 6^{p-1} - 6 \\ &\equiv 3 \cdot 1 + 2 \cdot 1 + 1 - 6 \pmod p \\ &\equiv 0 \pmod p. \end{aligned}$$

□

フェルマーの小定理の証明を定理 4.3.1 の証明のようにする大学入試問題が多いが，次の慶応大学の入試問題の証明方法も興味深い．

問題 4.3.1　選択肢から最も適切なものを選びその番号を解答欄に記入しなさい．

相異なる自然数 a と b が 1 以外に共通の約数を持たないとき，a と b は互いに素であるという．自然数 n を素数 p で割った余りを $M_p(n)$ で表すことにする．また $p-1$ 以下の自然数 x, y に対して $x \otimes y = M_p(xy)$ と演算 $\otimes$ を定義する．ただし右辺の xy は通常の積である．例えば，$M_{11}\left(6 \times \boxed{\text{ア}}\right) = 2$ である．この演算 $\otimes$ は交換法則 $\boxed{\text{イウ}}$ や結合法則 $\boxed{\text{エオ}}$ を満たす．ここで，x, y, z は $p-1$ 以下の然数である．

次の命題はフェルマーの小定理と呼ばれている．

命題　自然数 a と素数 p が互いに素ならば a^{p-1} を p で割った余りは 1 である．

この命題を証明しよう．上の記号を用いれば $M_p\left(\boxed{\text{カ}}\right) = \boxed{\text{キ}}$ を示せばよい．以下，M_p の添字 p は省略する．x, y は $p-1$ 以下の然数とする．

$M(ax) = M(ay)$ ならば $a(x-y)$ は $\boxed{\text{クケ}}$ の $\boxed{\text{コサ}}$ となる．よって $x = y$ でなければならない．この $\boxed{\text{シス}}$ を考えれば，$\boxed{\text{セソ}}$ ならば $\boxed{\text{タチ}}$ である．このことから

$$M(1a),\ M(2a),\ \ldots\ldots,\ M((p-1)a)$$

は異なった自然数である．よって

$$M(1a) \otimes M(2a) \otimes \cdots\cdots \otimes M((p-1)a) = 1 \otimes 2 \otimes \cdots\cdots \otimes \boxed{\text{ツテ}}$$

となる．

一方，M の性質を使えば

$$M(1a) \otimes M(2a) \otimes \cdots\cdots \otimes M((p-1)a) = M\left(\boxed{\text{ト}}\right) \otimes 1 \otimes 2 \otimes \cdots\cdots \otimes \boxed{\text{ナニ}}$$

となる．$x \otimes y = y$ のとき，$x = \boxed{\text{ヌ}}$ となることに注意すれば，$M\left(\boxed{\text{カ}}\right) = \boxed{\text{キ}}$ を得る．

[選択肢]

(1)　1	(2)　2	(3)　3	(4)　4	(5)　0
(6)　a	(7)　a^{p-1}	(8)　a^p	(9)　a^{p+1}	(10)　$x-y$
(11)　$x \otimes y$	(12)　xy	(13)　$x+y$		
(14)　$x \fallingdotseq y$	(15)　$M(ax) = M(ay)$	(16)　$x = y$		
(17)　$p+1$	(18)　p	(19)　$p-1$		
(20)　$M(ax) \fallingdotseq M(ay)$	(21)　逆	(22)　対偶		
(23)　裏	(24)　否定	(25)　矛盾		

(26)　倍数　　(27)　約数　　(28)　素数

(29)　互いに素　　(30)　$p-1$ 以下　　(31)　$x \otimes y = 0$

(32)　$x \otimes y = y \otimes x$　　(33)　$x \otimes y \otimes z = y \otimes z \otimes x = z \otimes x \otimes y$

(34)　$x \otimes (y \otimes z) = (x \otimes y) \otimes z$　　(35)　$x \otimes (y + z) = x \otimes y + x \otimes z$

(2005 慶応大・総合政策)

4.4　オイラーの定理

定理 4.4.1　（オイラーの定理）m は正の整数，a は m と互いに素な整数とすると

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

が成り立つ．

証明　$m = 1$ のときは明らかに成り立つので，$m \geq 2$ と仮定する．m を法とする既約剰余系 $\left\{x_1,\ x_2,\ \ldots,\ x_{\varphi(m)}\right\}$ を考える．$(a, m) = 1$ であるから定理 4.2.3 より，$\left\{ax_1,\ ax_2,\ \ldots,\ ax_{\varphi(m)}\right\}$ も既約剰余系である．したがって，$ax_1, ax_2, \ldots, ax_{\varphi(m)}$ は $x_1, x_2, \ldots, x_{\varphi(m)}$ のある並べ替えと m を法として合同である．これらのすべての積を考えて

$$x_1x_2\cdots x_{\varphi(m)} \equiv (ax_1)(ax_2)\cdots(ax_{\varphi(m)}) \equiv a^{\varphi(m)}x_1x_2\cdots x_{\varphi(m)} \pmod{m}.$$

$x_1, x_2, \ldots, x_{\varphi(m)}$ はすべて m と互いに素であることより，$x_1x_2\ldots x_{\varphi(m)}$ と m は互いに素なので

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

を得る．　□

既約剰余系の知識を借りなければ，次のように証明することになる（実質的には同じことをやっているのだが）．

証明　$m = 1$ のときは明らかに成り立つので，$m \geq 2$ と仮定する．$\left\{a_1,\ a_2,\ \ldots,\ a_{\varphi(m)}\right\}$ を m 以下で m と互いに素な $\varphi(m)$ 個の正の整数とする．このとき，$aa_1, aa_2, \ldots, aa_{\varphi(m)}$ を要素とする集合 $C = \left\{aa_1,\ aa_2,\ \ldots,\ aa_{\varphi(m)}\right\}$ を考える．

- C の中のどの 2 つの要素も m を法として合同ではない．
  もしも，$aa_i \equiv aa_j \pmod{m}$ となる i, j $(1 \leq i, j \leq \varphi(m))$ があったとすると，$a(a_i - a_j) \equiv 0 \pmod{m}$ で a と m は互いに素であるから $a_i - a_j \equiv 0 \pmod{m}$ すなわち $a_i \equiv a_j \pmod{m}$.
  $1 \leq a_i, a_j \leq \varphi(m) < m$ より $-m < a_i - a_j < m$ であるから，$a_i - a_j$ が m で割り切れるのは $a_i - a_j = 0$ すなわち $i = j$ のときしかない．
- 各 $j \in \left\{1,\ 2,\ \ldots,\ \varphi(m)\right\}$ に対して $aa_j \equiv a_k \pmod{m}$, $k \in \left\{1,\ 2,\ \ldots,\ \varphi(m)\right\}$ を満たす k が存在する．
  aa_j を m で割った商を q，余りを r とおくと $aa_j = mq + r$, $0 \leq r < m$ が成り立つ．この式から $aa_j \equiv r \pmod{m}$, $(aa_j, m) = (m, r)$.
  $(a, m) = 1$, $(a_j, m) = 1$ より $(aa_j, m) = 1$ となるから，$(m, r) = (aa_j, m) = 1$.

$m \geq 2$ より $r \neq 0$ でもある．
ゆえに，$r = a_k$ となる $k \in \left\{1,\ 2,\ \ldots,\ \varphi(m)\right\}$ 存在して $aa_j \equiv r \equiv a_k \pmod{m}$.

以上のことから，$aa_1, aa_2, \ldots, aa_{\varphi(m)}$ は $a_1, a_2, \ldots, a_{\varphi(m)}$ のある並べ替えと m を法として合同である．これらのすべての積を考えて

$$a_1 a_2 \cdots a_{\varphi(m)} \equiv (aa_1)(aa_2)\cdots(aa_{\varphi(m)}) \equiv a^{\varphi(m)} a_1 a_2 \cdots a_{\varphi(m)} \pmod{m}.$$

$a_1, a_2, \ldots, a_{\varphi(m)}$ はすべて m と互いに素であることより，$a_1 a_2 \ldots a_{\varphi(m)}$ と m は互いに素なので

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

を得る．　□

- オイラーの定理を使うと，フェルマーの小定理の (2)
  「p は素数，a は p と互いに素な整数とすると，$a^{p-1} \equiv 1 \pmod{p}$.」
  が得られる．
  オイラーの定理で，$m = p$ とおくと，$\varphi(p) = p-1$ であるから，$a^{p-1} \equiv 1 \pmod{p}$
  が成り立つからである．

定理 4.4.2　m は正の整数，a, b は整数とする．
$(a, m) = 1$ ならば $ax \equiv b \pmod{m}$ は m を法としてただ一つの解をもつ．

証明　m を法とする完全剰余系 $\left\{0,\ 1,\ \ldots,\ m-1\right\}$ をとれば，定理 4.2.2 により $\left\{a\cdot 0,\ a\cdot 1,\ \ldots,\ a\cdot(m-1)\right\}$ も完全剰余系である．
よって，ただ一つの j $(0 \leq j \leq m-1)$ が存在して

$$a \cdot j \equiv b \pmod{m}$$

となる．したがって，$ax \equiv b \pmod{m}$ は m を法としてただ一つの解をもつことが言えた．　□

※　$S = \left\{0,\ 1,\ \ldots,\ m-1\right\}$ とおくと，$ax \equiv b \pmod{m}$ は S の中に解があることがわかる．

オイラーの定理より，$a^{\varphi(m)} \equiv 1 \pmod{m}$ が成り立つ．$ax \equiv b \pmod{m}$ の両辺に $a^{\varphi(m)-1}$ をかけると

$$a^{\varphi(m)} x \equiv a^{\varphi(m)-1} b \pmod{m} \text{ すなわち } x \equiv a^{\varphi(m)-1} b \pmod{m}.$$

$ax \equiv b \pmod{n}$ は解 $x \equiv a^{\varphi(m)-1} b \pmod{m}$ をもつことがわかり，オイラーの定理は $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$ であることを教えてくれる．

4.5　中国の剰余定理

定理 4.5.1　$m_1, m_2, \ldots, m_k$ は正の整数で，どの 2 つをとっても互いに素であるとする．

このとき，任意の整数 $a_1, a_2, \ldots, m_k$ に対し

$$(*)\quad \begin{cases} x \equiv a_1 & (\mathrm{mod}\ m_1) \\ x \equiv a_2 & (\mathrm{mod}\ m_2) \\ \cdots & \\ x \equiv a_k & (\mathrm{mod}\ m_k) \end{cases}$$

は $m_1 m_2 \cdots m_k$ を法としてただ一つの解をもつ．

証明　$M = m_1 m_2 \cdots m_k$ とおく．

$i \in \left\{1,\ 2,\ \ldots,\ k\right\}$ に対して $M_i = \dfrac{M}{m_i} = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$ とおく．まず

$$\begin{cases} x \equiv 1 & (\mathrm{mod}\ m_1) \\ x \equiv 0 & (\mathrm{mod}\ m_2) \\ \cdots & \\ x \equiv 0 & (\mathrm{mod}\ m_k) \end{cases}$$

の解を求める．2 番目以下の式から，x は $m_2, m_3, \ldots, m_k$ で割り切れる．$m_2, m_3, \ldots, m_k$ はどの 2 つをとっても互いに素であるから，x はその積 $m_2 m_3 \cdots m_k = M_1$ で割り切れる．

$x = yM_1$ $(y \in \mathbb{Z})$ とかけるから，これを $x \equiv 1\ (\mathrm{mod}\ m_1)$ に代入すると，$yM_1 \equiv 1\ (\mathrm{mod}\ m_1)$ となる．M_1 と m_1 は互いに素であるから，定理 4.4.2 より $yM_1 \equiv 1\ (\mathrm{mod}\ m_1)$ を満たす整数 y が存在する．$yM_1 \equiv 1\ (\mathrm{mod}\ m_1)$ を満たす y を ${M_1}'$，この ${M_1}'$ に対応する x を x_1 とすると，$x_1 = M_1 {M_1}'$.

次に

$$\begin{cases} x \equiv 0 & (\mathrm{mod}\ m_1) \\ x \equiv 1 & (\mathrm{mod}\ m_2) \\ x \equiv 0 & (\mathrm{mod}\ m_3) \\ \cdots & \\ x \equiv 0 & (\mathrm{mod}\ m_k) \end{cases}$$

の解を $x_2 = M_2 {M_2}'$ とする．

このようにして，各 $i \in \left\{1,\ 2,\ \ldots,\ k\right\}$ に対して，$M_i {M_i}' \equiv 1\ (\mathrm{mod}\ m_i)$ を満たす M_i' をとり，$x_i = M_i {M_i}'$ とする．

$x_1, x_2, \ldots, x_k$ を用いて

$$x = a_1x_1 + a_2x_2 + \cdots + a_kx_k = \sum_{i=1}^{k} a_iM_i{M_i}'$$

を作ると，これが求める答えである．

- $x = \sum_{i=1}^{k} a_iM_i{M_i}'$ が解になっていることを示す．
  各 $i \in \{1,\ 2,\ \ldots,\ k\}$ に対して，$j \neq i$ ならば $M_j \equiv 0 \pmod{m_i}$ が成り立つから

$$\begin{aligned} x &= a_1M_1{M_1}' + a_2M_2{M_2}' + \cdots + a_kM_k{M_k}' \\ &\equiv a_iM_i{M_i}' \pmod{m_i} \\ &\equiv a_i \pmod{m_i} \end{aligned}$$

  となるので，$x = \sum_{i=1}^{k} a_iM_i{M_i}'$ は $(*)$ の解になっている．
- 一意性を示す．
  各 $i \in \{1,\ 2,\ \ldots,\ k\}$ に対して，$y \equiv a_i \pmod{m_i}$ を満たすとする．$x \equiv a_i \pmod{m_i}$ でもあるから，$y - x \equiv 0 \pmod{m_i}$.
  $m_1, m_2, \ldots, m_k$ はどの 2 つをとっても互いに素であるから，$y - x$ はその積 $m_1m_2\cdots m_k = M$ で割り切れる．よって $M \mid y - x$ から $y \equiv x \pmod{M}$ である．　□

次の証明 2 は解の構成方法がすこし違っているだけである．

証明 2　$M = m_1m_2\cdots m_k$ とおく．
$i \in \{1,\ 2,\ \ldots,\ k\}$ に対して $M_i = \dfrac{M}{m_i} = m_1\cdots m_{i-1}m_{i+1}\cdots m_k$ とおく．まず

$$\begin{cases} x \equiv a_1 & \pmod{m_1} \\ x \equiv 0 & \pmod{m_2} \\ \cdots & \\ x \equiv 0 & \pmod{m_k} \end{cases}$$

の解を求める．2 番目以下の式から，x は $m_2, m_3, \ldots, m_k$ で割り切れる．$m_2, m_3, \ldots, m_k$ はどの 2 つをとっても互いに素であるから，x はその積 $m_2m_3\cdots m_k = M_1$ で割り切れる．
$x = yM_1$ $(y \in \mathbb{Z})$ とかけるから，これを $x \equiv a_1 \pmod{m_1}$ に代入すると，$yM_1 \equiv a_1 \pmod{m_1}$ となる．M_1 と m_1 は互いに素であるから，定理 4.4.2 より $yM_1 \equiv a_1 \pmod{m_1}$ を満たす整数 y が存在する．$yM_1 \equiv a_1 \pmod{m_1}$ を満たす y を ${M_1}'$，この ${M_1}'$ に対応する x を x_1 とすると，$x_1 = M_1{M_1}'$.

次に

$$\begin{cases} x \equiv 0 & (\mathrm{mod}\ m_1) \\ x \equiv a_2 & (\mathrm{mod}\ m_2) \\ x \equiv 0 & (\mathrm{mod}\ m_3) \\ \cdots & \\ x \equiv 0 & (\mathrm{mod}\ m_k) \end{cases}$$

の解を $x_2 = M_2 M_2{}'$ とする．

このようにして，各 $i \in \{1,\ 2,\ \ldots,\ k\}$ に対して，$M_i M_i{}' \equiv 1\ (\mathrm{mod}\ m_i)$ を満たす M_i' をとり，$x_i = M_i M_i{}'$ とする．

$x_1, x_2, \ldots, x_k$ を用いて

$$x = x_1 + x_2 + \cdots + x_k = \sum_{i=1}^{k} M_i M_i{}'$$

を作ると，これが求める答えである．

- $x = \sum_{i=1}^{k} M_i M_i{}'$ が解になっていることを示す．
  各 $i \in \{1,\ 2,\ \ldots,\ k\}$ に対して，$j \neq i$ ならば $M_j \equiv 0\ (\mathrm{mod}\ m_i)$ が成り立つから

  $$\begin{aligned} x &= M_1 M_1{}' + M_2 M_2{}' + \cdots + M_k M_k{}' \\ &\equiv M_i M_i{}' \pmod{m_i} \\ &\equiv a_i \pmod{m_i} \end{aligned}$$

  となるので，$x = \sum_{i=1}^{k} M_i M_i{}'$ は $(*)$ の解になっている．
- 一意性を示す．
  各 $i \in \{1,\ 2,\ \ldots,\ k\}$ に対して，$y \equiv a_i\ (\mathrm{mod}\ m_i)$ を満たすとする．$x \equiv a_i\ (\mathrm{mod}\ m_i)$ でもあるから，$y - x \equiv 0\ (\mathrm{mod}\ m_i)$.
  $m_1, m_2, \ldots, m_k$ はどの 2 つをとっても互いに素であるから，$y - x$ はその積 $m_1 m_2 \cdots m_k = M$ で割り切れる．よって $M \mid y - x$ から $y \equiv x\ (\mathrm{mod}\ M)$ である．　□

例題 4.5.1　次の連立 1 次合同式を解け．

$$\begin{cases} x \equiv a_1 & (\mathrm{mod}\ 3) \\ x \equiv a_2 & (\mathrm{mod}\ 5) \\ x \equiv a_3 & (\mathrm{mod}\ 7) \end{cases}$$

解答 $3,5,7$ はどの 2 つをとっても互いに素で，$3\cdot5\cdot7=35\cdot3=21\cdot5=15\cdot7$ である．

$$35\cdot2\equiv1 \pmod 3,\ 21\cdot1\equiv1 \pmod 5,\ 15\cdot1\equiv1 \pmod 7$$

より，$x_1=35\cdot2,\ x_2=21\cdot1,\ x_3=15\cdot1$ で，解は

$$x\equiv35\cdot2\cdot a_1+21\cdot1\cdot a_2+15\cdot1\cdot a_3\equiv70a_1+21a_2+15a_3 \pmod{105}$$

となる．□

例えば，連立 1 次合同式

$$\begin{cases} x\equiv2 & \pmod 3\\ x\equiv3 & \pmod 5\\ x\equiv2 & \pmod 7 \end{cases}$$

の解は

$$x\equiv70\cdot2+21\cdot3+15\cdot2\equiv140+63+30\equiv35+63+30\equiv128\equiv23 \pmod{105}.$$

例題 4.5.2　1032^{1032} の下 2 桁 (しもふたけた) を求めよ．

mod 100 で考えるわけであるが，mod 4 と mod 25 で分けるとよい．

解答　$x=1032^{1032}$ とおく．

$1032\equiv0 \pmod 4$ から $x=1032^{1032}\equiv0 \pmod 4$.

$1032\equiv\ \ 32\equiv7 \pmod{25}$ より

$$x=1032^{1032}\equiv7^{1032}\equiv\left(7^2\right)^{516}\equiv(-1)^{516}\equiv1 \pmod{25}.$$

よって，$x\equiv0 \pmod 4,\ x\equiv1 \pmod{25}$.

$$25\cdot1\equiv1 \pmod 4,\quad 4\cdot(-6)\equiv1 \pmod{25}$$

であるから，中国の剰余定理より

$$x=1032^{1032}\equiv0\cdot25\cdot1+1\cdot4\cdot(-6)\equiv-24\equiv76 \pmod{100}.$$

したがって，1032^{1032} の下 2 桁は 76 である．□

例題 4.5.3　格子点 (a,b) は，a と b の最大公約数が 1 のとき visible であると言うことにする．

$$(x,y)=(a+m,b+n),\ 0\le m,n\le99$$

の形の格子点の中に visible であるものがないような，整数 a,b が存在することを示せ．

原題「If a and b are integers, then the point (a, b) is called a *lattice point*. A *visible* lattice point is one for which $\gcd(a, b) = 1$ (it is visible from the origin). Prove that there are circles (or squares) in the plane which are arbitrarily large and have the property that each lattice point in the circles (or squares) is not visible. (Use that there are infinitely many primes.)」より易しくしてある.

解答　$\{p_j\}$ は異なる素数の無限数列とする.

$(a, b), (a, b+1), \ldots, (a, b+99)$ が visible な格子点でないように,

$a \equiv 0 \left(\mod \prod_{i=1}^{100} p_i \right)$ とし,

$$\begin{cases} b \equiv 0 & (\mod p_1) \\ b+1 \equiv 0 & (\mod p_2) \\ \cdots & \\ b+99 \equiv 0 & (\mod p_{100}) \end{cases}$$

とおく.

$(a+1, b), (a+1, b+1), \ldots, (a+1, b+99)$ が visible な格子点でないように,

$a+1 \equiv 0 \left(\mod \prod_{i=101}^{200} p_i \right)$ とし,

$$\begin{cases} b \equiv 0 & (\mod p_{101}) \\ b+1 \equiv 0 & (\mod p_{102}) \\ \cdots & \\ b+99 \equiv 0 & (\mod p_{200}) \end{cases}$$

とおく. これを繰り返し, $(a+99, b), (a+99, b+1), \ldots, (a+99, b+99)$ が visible な格子点でないように,

$a+99 \equiv 0 \left(\mod \prod_{i=9901}^{10000} p_i \right)$ とし,

$$\begin{cases} b \equiv 0 & (\mod p_{9901}) \\ b+1 \equiv 0 & (\mod p_{9902}) \\ \cdots & \\ b+99 \equiv 0 & (\mod p_{10000}) \end{cases}$$

とおく.

したがって

$$\begin{cases} a \equiv 0 \left(\mod \prod_{i=1}^{100} p_i \right) \\ a+1 \equiv 0 \left(\mod \prod_{i=101}^{200} p_i \right) \\ \cdots \\ a+99 \equiv 0 \left(\mod \prod_{i=9901}^{10000} p_i \right) \end{cases} \quad \text{かつ} \quad \begin{cases} b \equiv 0 \left(\mod \prod_{i=0}^{99} p_{100i+1} \right) \\ b+1 \equiv 0 \left(\mod \prod_{i=0}^{99} p_{100i+2} \right) \\ \cdots \\ b+99 \equiv 0 \left(\mod \prod_{i=0}^{100} p_{100i+100} \right) \end{cases}$$

を満たす整数 a, b が存在することを示せばよく，これは中国の剰余定理により，存在が保証される．　□

4.6　ウィルソンの定理

定理 4.6.1　(ウィルソンの定理) p を素数とするとき，

$$(p-1)! \equiv -1 \pmod{p}$$

が成り立つ．

証明　$p=2$ のとき $(2-1)! = 1 \equiv -1 \pmod 2$, $p=3$ のとき $(3-1)! = 2 \equiv -1 \pmod 3$

となり，定理の式は成り立つから，以下 $p \geq 5$ とする．

$S = \left\{1,\ 2,\ \ldots,\ p-1\right\}$ とおくと，すべての $a \in S$ に対して $(a,\, p) = 1$ だから，定理 4.4.2 より $aa' \equiv 1 \pmod p$ を満たす $a' \in S$ がただ一つ存在する．

$a' = a$ となる場合を調べる．

このとき $a^2 \equiv 1 \pmod p$ となるから $(a-1)(a+1) \equiv 0 \pmod p$.

p は素数なので $p \mid a-1$ または $p \mid a+1$ すなわち $a \equiv 1 \pmod p$ または $a \equiv -1 \equiv p-1 \pmod p$ となる．

よって $a = 1$ または $a = p-1$ のときは $a' = a$ となる．

残りの $S - \left\{1,\ p-1\right\} = \left\{2,\ 3,\ \ldots,\ p-2\right\}$ の要素を $\dfrac{p-3}{2}$ 個の組

$$(a_1,\, a_1'),\ \ldots,\ \left(a_{\frac{p-3}{2}},\, {a_{\frac{p-3}{2}}}'\right)$$

に分けると

$$\begin{aligned}(p-1)! &\equiv 1 \times (p-1) \times (a_1 a_1') \times \cdots \times \left(a_{\frac{p-3}{2}} {a_{\frac{p-3}{2}}}'\right) \\ &\equiv 1 \times (p-1) \\ &\equiv -1 \pmod p.\end{aligned}$$

□

ウィルソンの定理の別証明をする．そのために次の補助定理を用意する．

補助定理 4.6.1　n が正の整数のとき，

$$n! = n^n - \binom{n}{1}(n-1)^n + \binom{n}{2}(n-2)^n - \cdots + (-1)^{n-2}\binom{n}{n-2}2^n + (-1)^{n-1}\binom{n}{n-1}$$

が成り立つ．

証明 二項定理を使うと

$$(e^x-1)^n = e^{nx} - \binom{n}{1}e^{(n-1)x} + \binom{n}{2}e^{(n-2)x} - \cdots + (-1)^{n-2}\binom{n}{n-2}e^{2x} + (-1)^{n-1}\binom{n}{n-1}e^x + (-1)^n.$$

$e^x = 1 + \dfrac{x}{1!} + \dfrac{x^2}{2!} + \cdots + \dfrac{x^n}{n!} + \cdots$ だから

$$\begin{aligned}
&\left(\frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots\right)^n \\
&= \left[1 + \frac{nx}{1!} + \frac{(nx)^2}{2!} + \cdots + \frac{(nx)^n}{n!} + \cdots\right] \\
&\quad - \binom{n}{1}\left[1 + \frac{(n-1)x}{1!} + \frac{((n-1)x)^2}{2!} + \cdots + \frac{((n-1)x)^n}{n!} + \cdots\right] \\
&\quad + \binom{n}{2}\left[1 + \frac{(n-2)x}{1!} + \frac{((n-2)x)^2}{2!} + \cdots + \frac{((n-2)x)^n}{n!} + \cdots\right] + \cdots \\
&\quad + (-1)^{n-2}\binom{n}{n-2}\left[1 + \frac{2x}{1!} + \frac{(2x)^2}{2!} + \cdots + \frac{(2x)^n}{n!} + \cdots\right] \\
&\quad + (-1)^{n-1}\binom{n}{n-1}\left[1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots\right] + (-1)^n.
\end{aligned}$$

両辺の x^n の係数を比較すると

$$\frac{1}{1!} = \frac{n^n}{n!} - \binom{n}{1}\frac{(n-1)^n}{n!} + \binom{n}{2}\frac{(n-2)^n}{n!} - \cdots + (-1)^{n-2}\binom{n}{n-2}\frac{2^n}{n!} + (-1)^{n-1}\binom{n}{n-1}\frac{1}{n!}.$$

両辺に $n!$ をかけると

$$n! = n^n - \binom{n}{1}(n-1)^n + \binom{n}{2}(n-2)^n - \cdots + (-1)^{n-2}\binom{n}{n-2}2^n + (-1)^{n-1}\binom{n}{n-1}$$

を得る．　□

注 異なる r 個のものを同じ種類の n 個の箱に，空き箱をつくらないように入れる入れ方の数を $S(r,n)$ で表し，**第 2 種のスターリング数**と呼ばれている．

$$S(r,n) = \frac{1}{n!}\sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^r$$

が成り立つことが知られており，$r=n$ とおくと，明らかに $S(n,n)=1$ であるから，補助定理 4.6.1 の等式になる．なお，等式 $S(r,n) = \dfrac{1}{n!}\sum\limits_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^r$ については，C.L. リウ著　[101] P.40 参照.

ウィルソンの定理の別証明　$p=2$ のとき $(2-1)!=1\equiv -1 \pmod 2$ となり定理は成り立つので，以下 $p\geq 3$ とする．

補助定理 4.6.1 で $n=p-1$ とおくと，

$$\begin{aligned}&(p-1)!\\ &=(p-1)^{p-1}-\binom{p-1}{1}(p-2)^{p-1}+\binom{p-1}{2}(p-3)^{p-1}\\ &\qquad -\cdots+(-1)^{p-3}\binom{p-1}{p-3}2^{p-1}+(-1)^{p-2}\binom{p-1}{p-2}. \qquad (*)\end{aligned}$$

フェルマーの小定理より，$\gcd(a,p)=1$ のとき，$a^{p-1}\equiv 1 \pmod p$ が成り立つから

$$(p-1)^{p-1}\equiv 1 \pmod p,(p-2)^{p-1}\equiv 1 \pmod p,\ldots,2^{p-1}\equiv 1 \pmod p.$$

よって，$\bmod p$ で考えると

$$\begin{aligned}&(p-1)^{p-1}-\binom{p-1}{1}(p-2)^{n}+\binom{p-1}{2}(p-3)^{p-1}-\cdots+(-1)^{p-2}\binom{p-1}{p-2}\\ &\equiv 1-\binom{p-1}{1}+\binom{p-1}{2}-\cdots+(-1)^{p-2}\binom{p-1}{p-2}\\ &\equiv 1-\binom{p-1}{1}+\binom{p-1}{2}-\cdots+(-1)^{p-2}\binom{p-1}{p-2}+(-1)^{p-1}\binom{p-1}{p-1}-(-1)^{p-1}\binom{p-1}{p-1}\\ &\equiv (1-1)^{p-1}-(-1)^{p-1}\binom{p-1}{p-1}\\ &\equiv -(-1)^{p-1}\\ &\equiv -1 \pmod p \qquad (p-1 \text{ は偶数})\end{aligned}$$

となるので，$(*)$ より

$$(p-1)!\equiv -1 \pmod p$$

が成り立つ．　□

例題 4.6.1　(ウィルソンの定理の逆)

n を 2 以上の整数とするとき，次のことが成り立つことを示せ．

$$(n-1)!\equiv -1 \pmod n \quad\Longrightarrow\quad n \text{ は素数}.$$

解答　n が素数でないと仮定すると，$n=n_1n_2$ $(n_1,\,n_2\in\mathbb{N},\,n_1,\,n_2\geq 2)$ とおける．

$n_1\mid n\mid (n-1)!+1$ より $n_1\mid (n-1)!+1$.

ところで

$$\begin{aligned}(n-1)!+1 &= \underbrace{1\cdot 2\cdots n_1\cdots(n-1)}_{n_1\text{で割り切れる}}+1\\ &\equiv 0+1\\ &\equiv 1 \pmod{n_1}\end{aligned}$$

は $n_1 \mid (n-1)!+1$ に矛盾する．　□

定理 4.6.2　p は奇素数とする．

$x^2 \equiv -1 \pmod{p}$ が整数解をもつための必要十分条件は $p \equiv 1 \pmod{4}$ となることである．

証明　$x^2 \equiv -1 \pmod{p}$ が整数解をもつと仮定する．

$p \geq 3$ は奇数より，$\dfrac{p-1}{2}$ は正の整数なので，$x^2 \equiv -1 \pmod{p}$ の両辺を $\dfrac{p-1}{2}$ 乗すると，　$\left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ から

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}. \qquad \cdots\cdots ①$$

$x^2 \equiv -1 \pmod{p}$ から $(x, p) = 1$ がわかるので，フェルマーの小定理より

$$x^{p-1} \equiv 1 \pmod{p}. \qquad \cdots\cdots ②$$

①，②から

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

よって，$\dfrac{p-1}{2}$ は偶数で $\dfrac{p-1}{2} = 2l$ $(l \in \mathbb{N})$ とおくと $p = 1+4l$ となり，$p \equiv 1 \pmod{4}$ である．

$p \equiv 1 \pmod{4}$ と仮定する．

p は奇素数だから，ウィルソンの定理より

$$(p-1)! \equiv -1 \pmod{p}$$

が成り立つ．この式を使うと，$x^2 \equiv -1 \pmod{p}$ は

$$x^2 \equiv (p-1)! \pmod{p}$$

となる．

ところで，p を法として考えると

$$\begin{aligned}(p-1)! &= (1\cdot(p-1))\,(2\cdot(p-2))\cdots\Big(\Big(\frac{p-1}{2}\Big)\cdot\Big(\frac{p+1}{2}\Big)\Big)\\ &\equiv (1\cdot(-1))\,(2\cdot(-2))\cdots\Big(\Big(\frac{p-1}{2}\Big)\cdot\Big(-\frac{p-1}{2}\Big)\Big)\\ &\equiv \underset{p\equiv 1 \pmod 4 \text{ なので}=1}{\underbrace{(-1)^{\frac{p-1}{2}}}}\Big(\Big(\frac{p-1}{2}\Big)!\Big)^2\\ &\equiv \Big(\Big(\frac{p-1}{2}\Big)!\Big)^2 \pmod p.\end{aligned}$$

よって，$x=\left(\frac{p-1}{2}\right)!$ は $x^2\equiv(p-1)!\pmod p$ の解になっている． □

$p=2$ のとき，$x^2\equiv -1\pmod p$ は $x=1$ を整数解にもつから，定理 4.6.2 より，次の定理を得る．

定理 4.6.3　p は素数とする．

$x^2\equiv -1\pmod p$ が整数解をもつための必要十分条件は $p=2$ または $p\equiv 1\pmod 4$ となることである．

系 4.6.1　$4k+1$ の形の素数は無限に存在する．

証明　n を整数として，n^2+1 を考えると，定理 4.6.3 より n^2+1 の素因数は 2 または $4k+1$ の形の素数である．

$4k+1$ の形の素数は有限個しかないと仮定する．$4k+1$ の形の最大の素数を p として，p 以下の $4k+1$ の形の素数を $p_1,\ldots,p_r$ $(p_r=p)$ とする．

$$a=(2\cdot p_1\cdots p_r)^2+1=4(p_1\cdots p_r)^2+1$$

とおく．

a が素数ならば，a は $4k+1$ の形の素数で p より大きい．

a が合成数ならば，$a=n^2+1$ の形の整数だから，定理 4.6.3 より $a=n^2+1$ の素因数 q は 2 または $4k+1$ の形の素数である．$2\nmid a$ であるから，q は $4k+1$ の形の素数である．しかし，a は $p_1,\ldots,p_r\,(=p)$ で割り切れないから，$q>p$.

いずれにしても，$q>p$ となり，$4k+1$ の形の最大の素数が p であることに矛盾する．

したがって，$4k+1$ の形の素数は無限に存在する． □

定理 4.6.4　p は素数とする．

(1)　$p=x^2+y^2$ を満たす整数 x,y が存在すれば，$p=2$ または $p\equiv 1\pmod 4$ である．

(2)　素数 p が $p\equiv 1\pmod 4$ を満たすときは，$p=x^2+y^2$ を満たす整数 x,y が存在する．

証明 (1) $p \neq 2$ とすると p は奇素数となる．x, y がともに偶数，あるいは，ともに奇数であるとすると $x^2+y^2=p$ は偶数になるので，p は奇素数であることに矛盾する．
よって，x, y の一方が偶数でもう一方が奇数となる．対称性から，x が偶数で y が奇数と仮定しても一般性を失わない．
$x=2l$, $y=2m+1$ $(l,\, m \in \mathbb{Z})$ とおくと

$$p = x^2+y^2 = (2l)^2+(2m+1)^2 = 4\left(l^2+m^2+m\right)+1$$

となり，$p \equiv 1 \pmod 4$ である．

(2) $p \equiv 1 \pmod 4$ ならば， 定理 4.6.3 より，$x^2 \equiv -1 \pmod p$ は整数解をもつから，$a^2+1=pk$ を満たす正の整数 a, k が存在する．
ここで，

$$S = \left\{x+ay : 0 \leq x,\ y < \sqrt{p},\ x \in \mathbb{Z},\ y \in \mathbb{Z}\right\},$$

$$T = \left\{(x,\ y) : 0 \leq x,\ y < \sqrt{p},\ x \in \mathbb{Z},\ y \in \mathbb{Z}\right\}$$

とおくと，T の要素の個数は $\left(\left[\sqrt{p}\right]+1\right)^2$ である．
$(x_1,\, y_1)$, $(x_2,\, y_2) \in T$, $(x_1,\, y_1) \neq (x_2,\, y_2)$ でも $x_1+ay_1 = x_2+ay_2$ となる可能性があるので，S の要素の個数は $\left(\left[\sqrt{p}\right]+1\right)^2$ 以下である．

(i) $(x_1,\, y_1)$, $(x_2,\, y_2) \in T$, $(x_1,\, y_1) \neq (x_2,\, y_2,\ x_1+ay_1 = x_2+ay_2$ となる $(x_1,\, y_1)$, $(x_2,\, y_2)$ が存在する場合は，明らかに

$$x_1+ay_1 \equiv x_2+ay_2 \pmod p, \quad (x_1,\, y_1) \neq (x_2,\, y_2)$$

となる S の要素が存在する．

(ii) (i) のような $(x_1,\, y_1)$, $(x_2,\, y_2)$ が存在しない場合
S の要素の個数は $\left(\left[\sqrt{p}\right]+1\right)^2$ で，$\left(\left[\sqrt{p}\right]+1\right)^2 > \left(\sqrt{p}\right)^2 = p$ をみたしている．0 以上の整数を p で割った余りは $0,\, 1,\, \ldots,\, p-1$ の p 通りだから，鳩の巣原理により，p で割った余りが等しくなる S の中の異なる 2 数 x_1+ay_1, x_2+ay_2 が存在して

$$x_1+ay_1 \equiv x_2+ay_2 \pmod p, \quad (x_1,\, y_1) \neq (x_2,\, y_2)$$

(i)，(ii) のいずれにしても

$$x_1+ay_1 \equiv x_2+ay_2 \pmod p, \quad (x_1,\, y_1) \neq (x_2,\, y_2)$$

となる S の要素が存在する．
$x=x_1-x_2$, $y=y_1-y_2$ とおくと，$x_1+ay_1 \equiv x_2+ay_2 \pmod p$ から

$$(x_1-x_2)+a(y_1-y_2) \equiv 0 \pmod p \text{ すなわち } x+ay \equiv 0 \pmod p.$$

また，$|x| < \sqrt{p}$, $|y| < \sqrt{p}$ $(x \neq 0$ または $y \neq 0)$ が成り立つ．
このとき，

$$(x+ay)(x-ay) = x^2 - a^2y^2 = x^2 - (pk-1)y^2 = x^2 + y^2 - pky^2$$

から

$$x^2 + y^2 = (x+ay)(x-ay) + pky^2 \equiv 0 \cdot (x-ay) - 0 \equiv 0 \pmod{p}.$$

ゆえに，$x^2 + y^2$ は p の倍数である．
さらに，$|x| < \sqrt{p}$, $|y| < \sqrt{p}$ $(x \neq 0$ または $y \neq 0)$ から $0 < x^2 + y^2 < 2\left(\sqrt{p}\right)^2 = 2p$ なので $x^2 + y^2 = p$ が得られる． □

定理 4.6.4(2) の別証明（無限降下法で証明する．）
$p \equiv 1 \pmod 4$ ならば， 定理 4.6.3 より，

$$x^2 \equiv -1 \pmod{p} \qquad \cdots\cdots ①$$

となる整数 x が存在する．

◎ ①の解を $-\dfrac{p}{2} \leq x < \dfrac{p}{2}$ の範囲でとることができる．
系 2.1.1 より x を p で割った余り r を $-\dfrac{p}{2} \leq r < \dfrac{p}{2}$ のようにとれる．$x \equiv r \pmod p$ から $r^2 \equiv x^2 \equiv -1 \pmod p$ となるので，最初から①の解を $-\dfrac{p}{2} \leq x < \dfrac{p}{2}$ の範囲としてもよい．

p は奇数なので $-\dfrac{p}{2} \leq x < \dfrac{p}{2}$ は

$$-\frac{p}{2} < x < \frac{p}{2} \qquad \cdots\cdots ②$$

とできる．
①から $x^2 + 1$ は p の倍数なので

$$x^2 + 1 = kp \qquad \cdots\cdots ③$$

を満たす正の整数 k が存在する．
②を用いると

$$1 < x^2 + 1 < \frac{p^2}{4} + 1 < p^2$$

が成り立つので，③から

$$1 \leq k < p \qquad \cdots\cdots ④$$

であることがわかる．

いま，$y = 1$ とおくと

$$x^2 + y^2 = kp \qquad \cdots\cdots ⑤$$

が成り立つ．⑤において，$k = 1$ ならば証明は終了する．

$k \geq 2$ と仮定する．④は

$$2 \leq k < p \qquad \cdots\cdots ⑥$$

となる．x, y を k で割って

$$x = ku + r,\ y = kv + s,\ -\frac{k}{2} \leq r,\ s < \frac{k}{2},\ u,\ v,\ r,\ s \in \mathbb{Z}$$

と表すことができるから，

$$x \equiv r \pmod{k},\ y \equiv s \pmod{k} \qquad \cdots\cdots ⑦$$

となる整数 r, s がとれたことになる．

⑤，⑦から

$$r^2 + s^2 \equiv x^2 + y^2 \equiv kp \equiv 0 \pmod{k}$$

となるので

$$r^2 + s^2 = kk_1 \qquad \cdots\cdots ⑧$$

を満たす整数 k_1 が存在する．

⑧から $k_1 \geq 0$ である．もしも $k_1 = 0$ となったとすると，⑧から $r = s = 0$ となる．

すると，⑦から $x \equiv 0 \pmod{k}$, $y \equiv 0 \pmod{k}$ となり，x, y は k の倍数である．

$x = ki$, $y = kj$ $(i,\ j \in \mathbb{Z})$ とおき，⑤に代入すると，$k^2\left(i^2 + j^2\right) = kp$ から

$$k\left(i^2 + j^2\right) = p$$

となる．p は奇素数なのに，約数 $k\,(2 \leq k < p)$ をもつことになり矛盾が生じる．

したがって，$k_1 \neq 0$ でなければならないので，$k_1 \geq 1$ である．

$-\dfrac{k}{2} \leq r,\ s < \dfrac{k}{2}$ であったから

$$kk_1 = r^2 + s^2 \leq \frac{k^2}{4} + \frac{k^2}{4} = \frac{k^2}{2}.$$

よって，$k_1 \leq \dfrac{k}{2} < k$ が得られる．$k_1 \geq 1$ とあわせて

$$1 \leq k_1 < k \qquad \cdots\cdots ⑨$$

が成り立つ．恒等式 $\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac + bd)^2 + (ad - bc)^2$ を利用すると

$$\left(r^2 + s^2\right)\left(x^2 + y^2\right) = (rx + sy)^2 + (ry - sx)^2$$

が成り立つ．$X = rx + sy,\ Y = ry - sx$ とおくと

$$X^2 + Y^2 = \left(r^2 + s^2\right)\left(x^2 + y^2\right) = kk_1 \cdot kp = k^2 k_1 p \qquad \cdots\cdots ⑩$$

が得られる．

一方，⑦より

$$\begin{aligned} X &= rx + sy \equiv x \cdot x + y \cdot y \equiv x^2 + y^2 \equiv kp \equiv 0 \pmod{k} \\ Y &= ry - sx \equiv x \cdot y - y \cdot x \equiv 0 \pmod{k} \end{aligned}$$

となるから，X, Y はともに k の倍数なので，$X = kx_1,\ Y = ky_1\ (x_1,\ y_1 \in \mathbb{Z})$ とおき，⑩ に代入して，両辺を k^2 で割ると

$$x_1^2 + y_1^2 = k_1 p \qquad \cdots\cdots ⑪$$

を得る．

以上より $k \geq 2$ の場合には，$x^2 + y^2 = kp$ が成り立つことから，$0 < k_1 < k$ となる整数 k_1 が存在して，$x_1^2 + y_1^2 = k_1 p$ を満たす整数 $x_1,\ y_1$ があることが示された．

$k_1 = 1$ ならば証明は終了する．

$k_1 \geq 2$ ならば，上の操作を繰り返すと，有限回で

$$k_1 > k_2 > \cdots > k_m = 1$$

となる正の整数 m が存在する．このとき，整数 $x_m,\ y_m$ が存在して，$x_m^2 + y_m^2 = p$ となる． □

定理 4.6.4(2) において，$p = 2$ のときは，$2 = 1^2 + 1^2$ となるので，$p = x^2 + y^2$ を満たす整数 $x,\ y$ は存在する．したがって，定理 4.6.4 は次のようにまとめることができる．

定理 4.6.5　p は素数とする．

p が 2 つの平方数の和となるための必要十分条件は，$p = 2$ または $p \equiv 1 \pmod{4}$ となることである．

命題 4.6.1　$S = \left\{a^2 + b^2 : a,\ b \in \mathbb{Z}\right\}$ とする．

$$m,\ n \in S \implies mn \in S$$

が成り立つ．

証明　$m,\ n \in S$ より $m = a^2 + b^2,\ n = c^2 + d^2\ (a,\ b,\ c,\ d \in \mathbb{Z})$ とかける．このとき

$$mn = \left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac + bd)^2 + (ad - bc)^2 \in S. \qquad \square$$

命題 4.6.2　p は $p \equiv 3 \pmod 4$ を満たす素数とする．

$v_p(n)$ が奇数ならば，n は 2 つの平方数の和にはならない．

証明 背理法で証明する．

$n = x^2 + y^2 \ (x, y \in \mathbb{Z})$ ……①

と表せたと仮定する．

$x = p^k x_1,\ y = p^k y_1,\ k \in \mathbb{N}_0,\ x_1, y_1 \in \mathbb{Z},$ (x_1と y_1の少なくとも一方は p で割り切れない)

とおき，①に代入すると

$$n = p^{2k}\left(x_1^2 + y_1^2\right)$$

となる．$n' = x_1^2 + y_1^2$ とおくと n は p の奇数乗で割り切れるから，n' は p の奇数乗で割り切れる．

よって

$$x_1^2 + y_1^2 \equiv 0 \pmod p \quad \cdots\cdots ②$$

が成り立つ．

x_1と y_1の少なくとも一方は p で割り切れないが，対称性から x_1 が p で割り切れないと仮定しても一般性は失われない．$p \nmid x_1$ で p は素数だから，x_1 と p は互いに素になるので，p を法とする x_1 の逆数 x_1^{-1} が存在する．

②の両辺に $\left(x_1^{-1}\right)^2$ をかけると

$$1 + \left(x_1^{-1} y_1\right)^2 \equiv 0 \pmod p$$

すなわち

$$\left(x_1^{-1} y_1\right)^2 \equiv -1 \pmod p.$$

定理 4.6.3 より $p = 2$ または $p \equiv 1 \pmod 4$ となるが，これは $p \equiv 3 \pmod 4$ に矛盾する．

したがって，n は 2 つの平方数の和にはならない．　□

どのような正の整数が 2 つの平方数の和で表されるか？という問いの答えは次のようになる．

定理 4.6.6　正の整数 n が 2 つの平方数の和で表されるための必要十分条件は，n が

(∗)　$n = n_1^2 n_2,\ n_1, n_2 \in \mathbb{N},$ n_2は 4 を法として 3 と合同な素因数をもたない

と表せることである．

※　$n(\geq 2)$ を素因数分解して考えると，定理は次のように表現することもできる．

正の整数 $n(\geq 2)$ が 2 つの平方数の和で表されるための必要十分条件は，

$p \equiv 3 \pmod 4$ となるすべての素数が n を偶数回割り切ることである．

証明　n が $(*)$ のように表せないとすると，明らかに $n \neq 1$ だから n を素因数分解すると，$p \equiv 3 \pmod 4$ となる素数 p で，$v_p(n)$ が奇数であるものが存在するということだから，命題 4.6.2 より，n は 2 つの平方数の和にはならない．

対偶をとると，n が 2 つの平方数の和で表されるならば，n は $(*)$ のように表されることが言えたことになる．

n は $(*)$ のように表されると仮定する．

$n = 1$ のときは $n_1 = n_2 = 1$ で $n = 1 = 1^2 + 0^2$ と 2 つの平方数の和で表される．

$n \geq 2$ とする．n_2 は次のように表せる．

$n_2 = p_1 \cdots p_r$　($p_1, \ldots, p_r$ はすべて素数で，すべての $i \in \left\{1, \ \ldots, \ r\right\}$ について $p_i = 2$ または $p_i \equiv 1 \pmod 4$ である．)

定理 4.6.5 より $p_1, \ldots, p_r$ はすべて 2 つの平方数の和で表せるから，命題 4.6.1 より $n_2 = p_1 \cdots p_r$ も 2 つの方数の和で表される．$n_2 = a^2 + b^2$ $(a, b \in \mathbb{Z})$ とおくと

$$n = n_1^2 n_2 = n_1^2 \left(a^2 + b^2\right) = (n_1 a)^2 + (n_1 b)^2$$

となり，n は 2 つの平方数の和で表される．　□

「4 で割ると 1 余る素数 $p = 4k + 1$ はある 2 つの正の整数 x, y により $p = x^2 + y^2$ と表せる.」ことに対する Don Zagier の証明方法が慶応大学の医学部で出題されている．

例題 4.6.2　設問 (1) から (2) に答えなさい．

4 で割ると余りが 1 になるような素数 $p, p = 4k + 1,$ を 1 つとる．これに対し，等式

(Q)　　$a^2 + 4bc = p$

を満たす自然数 3 つの組 (a, b, c) の全体を考える，両辺の絶対値を比べればわかるように，このような自然数の 3 つの組の可能性は有限通りしかありえない．

いま等式 (Q) を満たす自然数 3 つの組 (a, b, c) から新しく自然数 3 つの組を作る手続きを次の (i)，(ii)，(iii) により定める：

(i) $a < b - c$ ならば $(a + 2c, c, b - a - c)$ を作る；

(ii) $b - c < a < 2b$ ならば $(2b - a, b, a - b + c)$ を作る；

(iii) $a > 2b$ ならば $(a - 2b, a - b + c, b)$ を作る；

(1)　(a, b, c) が等式 (Q) を満たす自然数の組で (i) の条件 $a < b - c$ を満たすとする．このとき，上の (i) より得られる $(a + 2c, c, b - a - c)$ もまた等式 (Q) を満たすことを示しなさい．

(2)　等式 (Q) を満たす自然数の組 (a, b, c) は $a = b - c$ や $a = 2b$ を満たすことはないことを示しなさい．

(3)　等式 (Q) を満たす自然数の組 (a, b, c) の中には，上の手続きを施しても変化しないという性質を持つものが存在する．$p = 4k + 1$ と表すとき，この性質を持つ (a, b, c) を k を用いて具体的に与え，かつそれがただ 1 組しか存在しないことを示しなさい．

(4)　等式 (Q) を満たす自然数の組 (a, b, c) に対して上の手続きを 2 回繰り返して施すとどうなるか，結論を簡潔に説明しなさい．また，この観察をもとに等式 (Q) を満たす自然数 3 つの組の全体の個数が偶数か奇数かを決定し，そう判断できる理由を述べなさい．ただし，等式 (Q) を満たす自然数 3 つの組から上の手続きにより新しく作られた自然数 3 つの組は (i)，(ii)，(iii) のどの場合でも再び等式 (Q) を満たすという事実についてはここでは証明なしに用いてよい．

(5)　素数 $p = 4k + 1$ をある 2 つの自然数 a, b により

$$p = a^2 + (2b)^2$$

と表すことができることを示しなさい．　(2002 慶応大・医)

解答

(1) (a, b, c) が等式 (Q) を満たすから，

$$(a + 2c)^2 + 4c(b - a - c) = a^2 + 4bc = p$$

となるから，$(a + 2c, c, b - a - c)$ も等式 (Q) を満たす．

(2) (a, b, c) が等式 (Q) を満たすから，$a^2 + 4bc = p$.

$a = b - c$ とすると，$p = a^2 + 4bc = (b - c)^2 + 4bc = (b + c)^2$.

$b + c \geq 2$ は自然数なので，p が素数であることに矛盾する．

$a = 2bc$ とすると，$p = a^2 + 4bc = (2bc)^2 + 4bc = 4b^2c^2 + 4bc = 4bc(bc + 1)$ は素数ではないから，p が素数であることに矛盾する．

よって，等式 (Q) を満たす自然数の組 (a, b, c) は $a = b - c$ や $a = 2b$ を満たすことはない．

(3) (i) のとき，$a + 2c > a$ であるから，手続きによって，自然数の組は変化する．

また，(iii) のときも，$a - 2b < a$ であるから，手続きによって，自然数の組は変化する．

よって，変化しない手続きは，(ii) の場合で，

$$b - c < a < 2b \qquad \cdots\cdots ①$$

で

$$2b - a = a \qquad \cdots\cdots ②$$

かつ

$$a - b + c = c \qquad \cdots\cdots ③$$

となる場合である．

②，③より，$a=b$ であり，このとき，①は成り立つ．

(Q) より，

$$p=a^2+4bc=a^2+4ac=a(a+4c).$$

p が素数で，$a+4c\geq 5$ だから，$a=1$ でなけらばならない．

このとき，$p=1+4c$ となるから，$p=1+4c=4k+1$ より $c=k$.

したがって，手続きを施しても変化しないという性質を持つ組はただ 1 組しか存在せず，それは，$(a,b,c)=(1,1,k)$ である．

(4) 等式 (Q) を満たす自然数の組 (a,b,c) に対して上の手続きを 1 回施したものを (a',b',c')，2 回繰り返して施したものを (a'',b'',c'') とする．

(ア) $a<b-c$ の場合

(i) より，$a'=a+2c, b'=c, c'=b-a-c$.

このとき，$a'>2b'$ だから，(iii) より，

$$\begin{aligned}a''&=a'-2b'=(a+2c)-2c=a\\ b''&=a'-b'+c'=(a+2c)-c+(b-a-c)=b\\ c''&=b'=c.\end{aligned}$$

(イ) $b-c<a<2b$ の場合

(ii) より，$a'=2b-a, b'=b, c'=a-b+c$.

このとき，$b-(a-b+c)=2b-a-c<2b-a<2b$ だから，$b'-c'<a'<2b'$.

(ii) より，

$$\begin{aligned}a''&=2b'-a'=2b-(2b-a)=a\\ b''&=b'=b\\ c''&=a'-b'+c'=2b-a-b+(a-b+c)=c.\end{aligned}$$

(ウ) $a>2b$ の場合

(iii) より，$a'=a-2b, b'=a-b+c, c'=b$.

このとき，$a-2b<a-2b+c=(a-b+c)-b$ だから，$a'<b'-c'$．(i) より，

$$\begin{aligned}a''&=a'+2c'=a-2b+2b=a\\ b''&=c'=b\\ c''&=b'-a'-c'=a-b+c-(a-2b)-b=c.\end{aligned}$$

よって，等式 (Q) を満たす自然数の組 (a,b,c) に対して上の手続きを 2 回繰り返すと元の組 (a,b,c) に戻る．

したがって，等式 (Q) を満たす自然数の組 (a, b, c) は，手続きによって変わらないものと，手続きによって互いに移りあう異なるものしか存在しない．

手続きによって変わらないものは 1 個，手続きによって互いに移りあう異なるものは 2 つずつペアにして考えれば，偶数個あるから，等式 (Q) を満たす自然数の組 (a, b, c) の個数は奇数である．

(5) 等式 (Q) を満たす自然数の組 (a, b, c) に対して，(a, c, b) もまた等式 (Q) を満たす．(等式 (Q) は b と c に関して対称である．)

もしもすべての組 (a, b, c) が $b \neq c$ ならば，(a, b, c) と (a, c, b) の 2 つずつペアにして考えれば，そのような組の個数は偶数個になり，(4) の結果に矛盾する．

したがって，等式 (Q) を満たす自然数の組 (a, b, c) の中には，$b = c$ となるものが存在する．このとき，

$$p = a^2 + 4bc = a^2 + 4b^2 = a^2 + (2b)^2$$

と表すことができる． □

上の例題 4.6.2 の (5) より，$x = a, y = 2b$ とおくと

「4 で割ると 1 余る素数 $p = 4k + 1$ はある 2 つの正の整数 x, y により $p = x^2 + y^2$ と表すことができる．」

ことがわかる．

類題が旭川医科大で出題されている．

問題 4.6.1　正の奇数 p に対して，3 つの自然数の組 (x, y, z) で，$x^2 + 4yz = p$ を満たすものの全体の集合を S とおく．すなわち，

$$S = \left\{ (x,\, y,\, z) \,|\, x,\, y,\, z \text{ は自然数},\, x^2 + 4yz = p \right\}$$

次の問いに答えよ．

(1)　S が空集合でないための必要十分条件は，$p = 4k + 1$ (k は自然数) と書けることであることを示せ．

(2)　S の要素の個数が奇数ならば S の要素 (x, y, z) で $y = z$ となるものが存在することを示せ．　(2012　旭川医大)

4.7　例題と問題

次の命題はベキ乗の問題を解くときに便利である．

命題 4.7.1　a, b, m, n, n_1 は正の整数で，$\gcd(a, m) = 1$ とする．
$n \equiv n_1 \pmod{\varphi(m)}$ のとき，$a^n \equiv a^{n_1} \pmod{m}$ が成り立つ．
さらに，$a \equiv b \pmod{m}$ のとき，$a^n \equiv b^{n_1} \pmod{m}$ が成り立つ．

使いやすいように，次の形で書いておく．

$\gcd(a, m) = 1,\ a, m, n \in \mathbb{N}$ のとき

$$a^n \equiv a^{n \pmod{\varphi(m)}} \pmod{m}$$

が成り立つ．

証明　$\gcd(a, m) = 1$ だから，オイラーの定理より，$a^{\varphi(m)} \equiv 1 \pmod{m}$.
$n \equiv n_1 \pmod{\varphi(m)}$ より，$n = n_1 + k\varphi(m)$ $(k \in \mathbb{Z})$ とおけるから，
$k > 0$ のとき，　mod m で考えると

$$a^n = a^{n_1 + k\varphi(m)} = a^{n_1} \left(a^{\varphi(m)}\right)^k \equiv a^{n_1} \cdot 1^k \equiv a^{n_1} \pmod{m}.$$

$k < 0$ のときは，$n_1 = n - k\varphi(m)$ で考えればよい．
さらに，$a \equiv b \pmod{m}$ のときは，$a^n \equiv a^{n_1} \equiv b^{n_1} \pmod{m}$.　□

例題 4.7.1　(USAMO 1991)
正の整数 n を固定するとき，数列

$$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}, \ldots$$

は n を法として，いずれは定数となることを示せ．
(ただし，指数の塔は $a_1 = 1, a_{i+1} = 2^{a_i}$ により定義される．)

解答 正の整数 n に対して，数列 $\{b_k\}$ を次のように定める．
b_1 は $b_1 \mid n$ を満たす最大の奇数とする．
$i \geq 1$ のとき，b_{i+1} は $b_{i+1} \mid \varphi(b_i)$ を満たす最大の奇数とする．
すると，$b_i > 1$ のとき，$\varphi(b_i) < b_i$ と $b_{i+1} \mid \varphi(b_i)$ から $b_{i+1} \leq \varphi(b_i) < b_i$ が成り立つ．
$b_i = 1$ のときは，$\varphi(b_i) = 1$ だから，$b_{i+1} = b_i$ である．
以上のことから，ある正の整数 m_0 が存在して，$b_{m_0} = 1$ となる．
準備ができたので，十分大きな n に対して，$a_{m+1} \equiv a_m \pmod{n}$ を示そう．

$n = 2^{k_1}b_1$ ($k_1 \in \mathbb{N}_0, b_1 \in \mathbb{N}, b_1$は奇数) とおくと，$\gcd(2, b_1) = 1$.

よって

$$a_{m+1} \equiv a_m \pmod{2^{k_1}} \quad \cdots\cdots ①$$

$$a_{m+1} \equiv a_m \pmod{b_1} \quad \cdots\cdots ②$$

を示せばよいことになる．m を十分大きくとれば，$a_{m+1} \equiv a_m \equiv 0 \pmod{2^{k_1}}$ となるから，①は成り立つ．

②は，$2^{a_m} \equiv 2^{a_{m-1}} \pmod{b_1}$ と変形できる．$\gcd(2, b_1) = 1$ だから，命題 4.7.1 より

$$a_m \equiv a_{m-1} \pmod{\varphi(b_1)}$$

が言えれば，$2^{a_m} \equiv 2^{a_{m-1}} \pmod{b_1}$ は成り立つことになる．

$\varphi(b_1) = 2^{k_2}b_2$ ($k_2 \in \mathbb{N}_0, b_2 \in \mathbb{N}, b_2$は奇数) とおくと，$\gcd(2, b_2) = 1$.

よって，$a_m \equiv a_{m-1} \pmod{\varphi(b_1)}$ を示すには，

$$a_m \equiv a_{m-1} \pmod{2^{k_2}} \quad \cdots\cdots ③$$

$$a_m \equiv a_{m-1} \pmod{b_2} \quad \cdots\cdots ④$$

を示せばよいことになる．m を十分大きくとれば，$a_m \equiv a_{m-1} \equiv 0 \pmod{2^{k_2}}$ となるから，③は成り立つ．

④は，$2^{a_{m-1}} \equiv 2^{a_{m-2}} \pmod{b_2}$ と変形できる．$\gcd(2, b_2) = 1$ だから，命題 4.7.1 より

$$a_{m-1} \equiv a_{m-2} \pmod{\varphi(b_2)}$$

が言えれば，$2^{a_{m-1}} \equiv 2^{a_{m-2}} \pmod{b_2}$ は成り立つことになる．

この操作を $b_{m_0} = 1$ となるまで繰り返し行うと

$$a_{m-m_0+1} \equiv a_{m-m_0} \pmod{2^{k_{m_0}}} \quad \cdots\cdots ⑤$$

$$a_{m-m_0+1} \equiv a_{m-m_0} \pmod{b_{m_0}} \quad \cdots\cdots ⑥$$

となる．

m を十分大きくとれば，これらの合同式⑤，⑥は成り立つ．

したがって，数列

$$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}, \ldots$$

は n を法として，いずれは定数となる．　□

例題 4.7.2 $n \geq 3$ を正の整数とするとき，

$$n^{n^{n^n}} - n^{n^n}$$

は 1989 で割り切れることを示せ．

解答 $1989 = 3^2 \cdot 13 \cdot 17$.

- $n^{n^{n^n}} \equiv n^{n^n} \pmod 9$ ……①

  が成り立つことを示す．

  $3 \mid n$ のとき，①は明らかに成り立つ．

  $3 \nmid n$ のとき，$\gcd(n, 9) = 1$ で $\varphi(9) = 3^2 - 3 = 6$ である．命題 4.7.1 より，

  $$n^{n^n} \equiv n^n \pmod 6 \quad \cdots\cdots ②$$

  が言えれば，①は成り立つ．②と同値な

  $$n^{n^n} \equiv n^n \pmod 2 \quad \cdots\cdots ③$$

  $$n^{n^n} \equiv n^n \pmod 3 \quad \cdots\cdots ④$$

  を示せばよい．

  $2 \mid n$ のとき，③は明らかに成り立つ．

  $2 \nmid n$ のとき，$n \equiv 1 \pmod 2$ であるから，$n^{n^n} \equiv 1 \pmod 2$, $n^n \equiv 1 \pmod 2$.

  ゆえに，③は成り立つ．

  $3 \mid n$ のとき，④は明らかに成り立つ．

  $3 \nmid n$ のとき，$\gcd(n, 3) = 1$ で $\varphi(3) = 2$ である．命題 4.7.1 より，

  $$n^n \equiv n \pmod 2 \quad \cdots\cdots ⑤$$

  が言えれば，④は成り立つ．

  $2 \mid n$ のとき，⑤は明らかに成り立つ．

  $2 \nmid n$ のとき，$n \equiv 1 \pmod 2$ であるから，$n^n \equiv 1 \pmod 2$, $n \equiv 1 \pmod 2$.

  ゆえに，⑤は成り立つ．

- $n^{n^{n^n}} \equiv n^{n^n} \pmod{13}$ ……⑥

  が成り立つことを示す．

  $13 \mid n$ のとき，⑥は明らかに成り立つ．

  $13 \nmid n$ のとき，$\gcd(n, 13) = 1$ で $\varphi(13) = 12$ である．命題 4.7.1 より，

  $$n^{n^n} \equiv n^n \pmod{12} \quad \cdots\cdots ⑦$$

が言えれば，⑥は成り立つ．⑦と同値な

$$n^{n^n} \equiv n^n \pmod 3 \qquad \cdots\cdots ⑧$$

$$n^{n^n} \equiv n^n \pmod 4 \qquad \cdots\cdots ⑨$$

を示せばよい．

$3 \mid n$ のとき，⑧は明らかに成り立つ．

$3 \nmid n$ のとき，④が成り立つことから，⑧は成り立つ．

$2 \mid n$ のとき，⑨は明らかに成り立つ．

$2 \nmid n$ のとき，$\gcd(n, 4) = 1$ で $\varphi(4) = 2^2 - 2 = 2$ である．命題 4.7.1 より，

$$n^n \equiv n \pmod 2$$

を示せばよく，⑤が成り立つことから，この合同式は成り立つ．

- $n^{n^{n^n}} \equiv n^{n^n} \pmod{17}$ $\cdots\cdots ⑩$

が成り立つことを示す．

$17 \mid n$ のとき，⑩は明らかに成り立つ．

$17 \nmid n$ のとき，$\gcd(n, 17) = 1$ で $\varphi(17) = 16$ である．命題 4.7.1 より，

$$n^{n^n} \equiv n^n \pmod{16} \qquad \cdots\cdots ⑪$$

が言えれば，⑩は成り立つ．

$2 \mid n$ のとき，⑪は明らかに成り立つ．

$2 \nmid n$ のとき，$\gcd(n, 16) = 1$ で $\varphi(16) = 2^4 - 2 - 3 = 8$ である．命題 4.7.1 より，

$$n^n \equiv n \pmod 8 \qquad \cdots\cdots ⑫$$

を示せばよい．

$2 \nmid n$ より，n は奇数なので，$n^2 \equiv 1 \pmod 8$.

ゆえに，$n^{n-1} \equiv 1 \pmod 8$ から $n^n \equiv n \pmod 8$ すなわち⑫が成り立つ．　□

例題 4.7.3　(Canada 2003)

$2003^{2002^{2001}}$ の下 3 桁を求めよ．

解答　mod 1000 で $2003^{2002^{2001}}$ を計算することになるが，$1000 = 8 \cdot 125$ より mod 8 と　mod 125 の 2 つの場合に分けて考えてみる．

- mod 8 で考える．$\varphi(8) = 2^3 - 2^2 = 4$.

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod 8$$

が成り立つ．$\gcd(3,4)=1$，$2002^{2001}\equiv 0 \pmod 4$ だから，命題 4.7.1 より，

$$3^{2002^{2001}}\equiv 3^0\equiv 1 \pmod 8.$$

ゆえに，$2003^{2002^{2001}}\equiv 3^{2002^{2001}}\equiv 1 \pmod 8$ から

$$2003^{2002^{2001}}\equiv 1 \pmod 8. \qquad \cdots\cdots ①$$

- mod 125 で考える．$\varphi(125)=5^3-5^2=100$.

$$2003^{2002^{2001}}\equiv 3^{2002^{2001}} \pmod{125}$$

が成り立つ．

2002^{2001} を mod 100 で計算する．$100=4\cdot 25$ なので mod 4 と mod 25 で計算する．

$$2002^{2001}\equiv 2^{2001}\equiv 0 \pmod 4.$$

$\gcd(2,25)=1, \varphi(25)=5^2-5=20$ だから，オイラーの定理より，$2^{20}\equiv 1 \pmod{25}$ が成り立つ．

$$2002^{2001}\equiv 2^{2001}\equiv 2^1\cdot\left(2^{20}\right)^{100}\equiv 2^1\cdot\left(1^{20}\right)^{100}\equiv 2 \pmod{25}$$

から

$$2002^{2001}\equiv 2 \pmod{25}.$$

$25\cdot 0\equiv 0 \pmod 4$, $4\cdot 13\equiv 2 \pmod{25}$ だから，中国の剰余定理より

$$2002^{2001}\equiv 25\cdot 0+4\cdot 13\equiv 52 \pmod{100}.$$

よって，$\gcd(3,125)=1$，$2002^{2001}\equiv 52 \pmod{100}$ だから，命題 4.7.1 より

$$3^{2002^{2001}}\equiv 3^{52} \pmod{125}$$

が成り立つ．

$3^{52}\equiv\left(3^5\right)^{10}\cdot 3^2\equiv(-7)^{10}\cdot 9\equiv\left(49^2\right)^2\cdot 49\cdot 9\equiv 26^2\cdot 49\cdot 9\equiv 51\cdot 9\cdot 49\equiv 84\cdot 49\equiv 116 \pmod{125}$

より

$$2003^{2002^{2001}}\equiv 116 \pmod{125}. \qquad \cdots\cdots ②$$

$125\cdot 5\equiv 1 \pmod 8$, $8\cdot 77\equiv 116 \pmod{125}$[*1]だから，中国の剰余定理より

$$2003^{2002^{2001}}\equiv 125\cdot 5+8\cdot 77\equiv 625+616\equiv 1241\equiv 241 \pmod{1000}.$$

よって，$2003^{2002^{2001}}$ の下 3 桁は，241. □

[*1] $8t\equiv 116 \pmod{125}$ を満たす t は $2t\equiv 29 \pmod{125}$ から探す．

注 中国の剰余定理を使うところは，次のように合同式を用いてもよい．

$x = 2002^{2001}$ とおくと，$x \equiv 0 \pmod 4$, $x \equiv 2 \pmod{25}$ より，

$$x = 4l = 25m + 2,\ l, m \in \mathbb{Z}$$

とおける．　mod 4 で考えると，

$$0 \equiv 4l \equiv 25m + 2 \equiv m + 2 \pmod 4$$

より，$m \equiv -2 \equiv 2 \pmod 4$.

ゆえに，$m = 4m_1 + 2$, $m_1 \in \mathbb{Z}$ とおけて，

$$x = 25m + 2 = 25(4m_1 + 2) + 2 = 100m_1 + 52$$

から

$$x \equiv 52 \pmod{100}.$$

$y = 2003^{2002^{2001}}$ とおくと，$y \equiv 1 \pmod 8$, $y \equiv 116 \pmod{125}$ より，

$$x = 8l + 1 = 125m + 116,\ l, m \in \mathbb{Z}$$

とおける．　mod 8 で考えると，

$$1 \equiv 8l + 1 \equiv 125m + 116 \equiv 5m + 4 \pmod 8$$

より，$5m + 4 \equiv 1 \pmod 8$.

これから，$5m \equiv 1 - 4 \equiv -3 \equiv 5 \pmod 8$．5 と 8 は互いに素だから，$m \equiv 1 \pmod 8$ となる．

ゆえに，$m = 8m_1 + 1$, $m_1 \in \mathbb{Z}$ とおけて，

$$x = 125m + 116 = 125(8m_1 + 1) + 116 = 1000m_1 + 241$$

から

$$y \equiv 241 \pmod{1000}.$$ □

問題 4.7.1 $a_1 = 7,\ a_n = 7^{a_{n-1}}$ で定義される数列 $\{a_n\}$ において，a_{1001} の下 2 桁を求めよ．

類題（Putnam 1985）

$a_1 = 3,\ a_n = 3^{a_{n-1}}$ で定義される数列 $\{a_n\}$ がある．大きな n に対して a_n を 100 で割ったときの余りを求めよ．

問題 4.7.2 (Senior Hanoi Open MO 2006)

$2005^{11} + 2005^{112} + \cdots + 2005^{2006}$ の下 3 桁を求めよ．

問題 4.7.3 (PuMAC^a)

$2008^{2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}}$ の下 3 桁を求めよ．

(Princeton University Mathematics Competition)

問題 4.7.4 (PuMAC2008)

$f(x) = x^{x^{x^x}}$ と定義する．$f(17) + f(18) + f(19) + f(20)$ の下 2 桁を求めよ．

問題 4.7.5 (AoPS)

c は整数，p は素数とする．このとき，合同式 $x^x \equiv c \pmod{p}$ は解を持つことを示せ．

問題 4.7.6 (Putnam 1997)

2 以上の正の整数 n に対して

$$\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n} \equiv \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n-1} \pmod{n}$$

が成り立つことを証明せよ．

第5章

平方剰余

5.1　法 m での位数

m は 2 以上の整数で，a は m と互いに素な整数とする．

a と m は互いに素であるから，オイラーの定理より，$a^{\varphi(m)} \equiv 1 \pmod{m}$ が成り立つので，$a^n \equiv 1 \pmod{m}$ となるような正整数 n が存在することがわかる．

$a^n \equiv 1 \pmod{m}$ となるような正整数のなかで，最小のものを $\boldsymbol{m}$ **を法とする位数**といい，$\mathrm{ord}_{\boldsymbol{m}}(\boldsymbol{a})$ で表す．

例 5.1.1　7 を法とする 2 の位数

7 を法とする 2 のべきを計算すると

2	2^2	2^3
2	4	1

という表が得られるから，$\mathrm{ord}_7(2) = 3$ となる．

13 を法とする 2 の位数

13 を法とする 2 のべきを計算すると

2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
2	4	8	3	6	12	11	9	5	10	7	1

という表が得られるから，$\mathrm{ord}_{13}(2) = 12$ となる．

※ 2 と 7 は互いに素であるから，オイラーの定理より，$2^{\varphi(7)} \equiv 1 \pmod{7}$ すなわち $2^6 \equiv 1 \pmod{7}$ が成り立つ．この場合は，$\mathrm{ord}_7(2) < \varphi(7)$ で，$\mathrm{ord}_7(2)(= 3)$ は $\varphi(7)(= 6)$ の約数である．

2 と 13 も互いに素であるから，オイラーの定理より，$2^{\varphi(13)} \equiv 1 \pmod{13}$ すなわち

$2^{12} \equiv 1 \pmod{13}$ が成り立つ．この場合は，$\mathrm{ord}_{13}(2) = \varphi(13)$ となっている．

命題 5.1.1　m は 2 以上の整数で，a は m と互いに素な整数とし，$d = \mathrm{ord}_m(a)$ とおくと，次のことが成り立つ．

(1)　正の整数 k について，$a^k \equiv 1 \pmod{m}$ となるための必要十分条件は，d が k を割り切ることである．
($a^k \equiv 1 \pmod{m} \iff d \mid k$.)

(2)　d は $\varphi(m)$ の約数である．($d \mid \varphi(m)$.)

証明

(1) $a^k \equiv 1 \pmod{m}$ が成り立つと仮定する．正の整数 k を d で割った商を q，余りを r とすると

$$k = dq + r,\ q, r \in \mathbb{Z},\ 0 \leq r < d$$

とかける．このとき，$a^d \equiv 1 \pmod{m}$ を用いると

$$a^k = a^{dq+r} = \left(a^d\right)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{m}$$

から

$$a^k \equiv a^r \pmod{m}$$

が成り立つ．$a^k \equiv 1 \pmod{m}$ が成り立つことを用いると

$$a^r \equiv 1 \pmod{m}.$$

$r \neq 0$ だとすると，$0 < r < d$ で，$a^r \equiv 1 \pmod{m}$ が成り立つことになり，$d = \mathrm{ord}_m(a)$ に矛盾する．
よって $r = 0$ で $k = dq$ となり d が k を割り切る．

　d が k を割り切ると仮定する．
$k = dq$ $(q \in \mathbb{Z})$ とおける．

$$a^k = a^{dq} = \left(a^d\right)^q \equiv 1^q \equiv 1 \pmod{m}$$

から $a^k \equiv 1 \pmod{m}$ が成り立つ．

(2) a と m は互いに素だから，オイラーの定理より，$a^{\varphi(m)} \equiv 1 \pmod{m}$ が成り立つ．
(1) の結果から d が $\varphi(m)$ を割り切る．　□

命題 5.1.2　m は 2 以上の整数で，a は m と互いに素な整数とし，$d = \mathrm{ord}_m(a)$ とおくと，次のことが成り立つ．
$a^i \equiv a^j \pmod{m}$ となるための必要十分条件は，$i \equiv j \pmod{d}$ となることである．

証明 $a^i \equiv a^j \pmod{m}$ $(i \geq j)$ とする．$a^i \equiv a^j \pmod{m}$ を変形すると

$$a^j \left(a^{i-j} - 1\right) \equiv 0 \pmod{m}.$$

a と m は互いに素だから，$a^{i-j} - 1 \equiv 0 \pmod{m}$. 命題 5.1.1 より，$d \mid i-j$ すなわち $i \equiv j \pmod{d}$ が成り立つ．

$i \equiv j \pmod{d}$ $(i \geq j)$ とすると，$i = j + kd$ $(k \in \mathbb{N}_0)$ とかける．$a^d \equiv 1 \pmod{m}$ を用いると

$$a^i = a^{j+dk} = \left(a^d\right)^k \cdot a^j \equiv 1^k \cdot a^j \equiv a^j \pmod{m}. \qquad \square$$

命題 5.1.3 m は 2 以上の整数で，a は m と互いに素な整数とし，$d = \mathrm{ord}_m(a)$ とおくと，次のことが成り立つ．

$a, a^2, \ldots, a^d$ の中には，m を法として合同なものは存在しない．

証明 もしも $a^i \equiv a^j \pmod{m}$ $(1 \leq i \leq j \leq d)$ が成り立つとすると，命題 5.1.2 より，$i \equiv j \pmod{d}$ となる．$1 \leq i \leq j \leq d$ から $-d < i - j < d$ なので，$i - j$ が d の倍数になるのは $i - j = 0$ のときしかない． $\square$

例題 5.1.1 $p > 3$ を素数とする．$\dfrac{2^p + 1}{3}$ の正の約数はすべて $2kp + 1$ の形であることを示せ．

解答 p は奇素数だから，

$$\frac{2^p + 1}{3} = 2^{p-1} - 2^{p-2} + 2^{p-3} - \cdots - 2 + 1$$

は整数である．

$q \left| \dfrac{2^p + 1}{3} \right.$ を満たす任意の素数 q をとる．

$q \left| \dfrac{2^p + 1}{3} \right. \left| 2^p + 1 \mid (2^p + 1)(2^p - 1) = 2^{2p} - 1 \right.$ が成り立つから，$2^{2p} \equiv 1 \pmod{q}$.

これから，$\mathrm{ord}_q(2)$ が存在し，

$$\mathrm{ord}_q(2) \mid 2p$$

を満たす．p は素数なので，$\mathrm{ord}_q(2) \in \left\{1, 2, p, 2p\right\}$ となる．

(1) $\mathrm{ord}_q(2) = 1$ の場合 $q \mid 2^1 - 1 = 1$ から $q = 1$ となり，q が素数であることに矛盾する．

(2) $\mathrm{ord}_q(2) = 2$ の場合 $q \mid 2^2 - 1 = 3$ で q は素数だから，$q = 3$.

$q \left| \dfrac{2^p + 1}{3} \right.$ から $9 \mid 2^p + 1$.

$p > 3$ は奇素数なので，6 で割った余りで考えると，$p = 6j + 1$ か $p = 6j + 5$ の形にかける．

$p = 6j+1$ $(j \in \mathbb{N})$ のとき，

$$2^p = 2^{6j+1} = 2 \cdot \left(2^3\right)^{2j} \equiv 2 \cdot (-1)^{2j} \equiv 2 \pmod 9$$

から $2^p + 1 \equiv 3 \not\equiv 0 \pmod 9$.

$p = 6j+5$ $(j \in \mathbb{N}_0)$ のとき，

$$2^p = 2^{6j+5} = 2^5 \cdot \left(2^3\right)^{2j} \equiv 5 \cdot (-1)^{2j} \equiv 5 \pmod 9$$

から $2^p + 1 \equiv 6 \not\equiv 0 \pmod 9$.

いずれの場合も，$9 \mid 2^p + 1$ は成り立たない．

(3) $\mathrm{ord}_q(2) = p$ の場合 $q \mid 2^p - 1$.

$q \mid 2^p + 1$ でもあるから，$q \mid (2^p+1) - (2^p-1) = 2$.

q は素数だから，$q = 2$．このとき，$2 = q \mid 2^p + 1$ は成り立たない．

(4) $\mathrm{ord}_q(2) = 2p$ の場合

$$2^{2p} - 1 \equiv 1 \pmod q, \quad 2^k - 1 \not\equiv 0 \pmod q \ (k = 1, 2, \ldots, 2p-1).$$

q は素数で，$q \mid 2^p + 1$ より $\gcd(q, 2) = 1$ となるので，フェルマーの小定理より，$2^{q-1} \equiv 1 \pmod q$ が成り立つので，

$$2p = \mathrm{ord}_q(2) \mid q - 1.$$

よって，$q - 1 = k \cdot 2p$ $(k \in \mathbb{N})$ すなわち $q = 2kp + 1$ の形にかける．

$r \left| \dfrac{2^p+1}{3} \right.$ となる正の整数 r をとる．

$r = 1$ のときは，$r = 2 \cdot 0 \cdot p + 1$ とかける．

$r > 1$ のときは，

$$r = q_1 q_2 \cdots q_s \ (q_1, q_2, \ldots, q_s \text{ は素数})$$

と素因数分解すると，$q_i = 2k_i p + 1$ $(k_i \in \mathbb{N})$ の形にかける．

$\mathcal{A} = \left\{ 2kp + 1 : k \in \mathbb{N} \right\}$ とおくと，$2kp+1, 2lp+1 \in \mathcal{A}$ のとき，$k, l \in \mathbb{N}$ で

$$(2kp+1)(2lp+1) = 2(2klp + k + l)p + 1, \quad 2klp + k + l \in \mathbb{N}$$

より $(2kp+1)(2lp+1) \in \mathcal{A}$.

この結果を使うと，$q_1, q_2, \ldots, q_s \in \mathcal{A}$ だから $q_1 q_2 \cdots q_s \in \mathcal{A}$，すなわち，$r$ も $2kp+1$ $(k \in \mathbb{N})$ の形にかける． □

例題 5.1.2 (IMO Shortlist 2006)
次の方程式を満たす整数 x, y をすべて求めよ，

$$\frac{x^7-1}{x-1} = y^5 - 1.$$

解答 $x \neq 1$ のとき，$x-1$ と x^7-1 は同符号であるから，$\dfrac{x^7-1}{x-1} > 0$ である．

- p を $p \Big| \dfrac{x^7-1}{x-1}$ を満たす素数とすると，$p \equiv 1 \pmod 7$ または $p = 7$ が成り立つ．

  $p \Big| \dfrac{x^7-1}{x-1}$ より，$p \mid x^7-1$ すなわち $x^7 - 1 \equiv 0 \pmod p$. これから，$\mathrm{ord}_p(x)$ が存在することがわかるので，$m = \mathrm{ord}_p(x)$ とおくと

  $$m \mid 7. \qquad \cdots\cdots ①$$

  また，$p \mid x^7 - 1$ から $\gcd(p, x) = 1$ がわかるので，フェルマーの小定理より，$x^{p-1} - 1 \equiv 0 \pmod p$ が成り立つ．よって

  $$m \mid p - 1. \qquad \cdots\cdots ②$$

  ①，②より

  $$m \mid \gcd(p-1, 7). \qquad \cdots\cdots ③$$

  $p - 1 \not\equiv 0 \pmod 7$ のとき，$\gcd(p-1, 7) = 1$ だから，③より，$m \mid 1$ すなわち，$m = 1$ となる．
  よって，$p \mid x^1 - 1$ から，$x \equiv 1 \pmod p$ となるので

  $$0 \equiv \frac{x^7-1}{x-1} = x^6 + x^5 + \cdots + x + 1 \equiv 1 + 1 + \cdots + 1 + 1 \equiv 7 \pmod p.$$

  よって，$p \mid 7$ となる．p は素数だから，$p = 7$ を得る．

  以上のことから，

- d を $d \Big| \dfrac{x^7-1}{x-1}$ を満たす整数とすると，$d \equiv 0 \pmod 7$ または $d \equiv 1 \pmod 7$ が成り立つ．
  $d > 1$ として，$d = p_1 \cdots p_s$ ($p_1, \ldots, p_s$は素数) と素因数分解できたとすると

  $$p_i = 7 \text{ または } p_i \equiv 1 \pmod 7 \quad (i = 1, \ldots, s)$$

  である．$p_1, \cdots, p_s$ のなかに，7 に等しいものがあれば，$d \equiv 0 \pmod 7$ で，すべて $p_i \equiv 1 \pmod 7$ であれば，$d = p_1 \cdots p_s \equiv 1 \pmod 7$ である．

$\dfrac{x^7-1}{x-1}=y^5-1$ が整数解をもつとすると，

$$y^5-1=(y-1)\left(y^4+y^3+\cdots+y+1\right)$$

から

$$y-1\equiv 0 \pmod 7 \text{ または } y-1\equiv 1 \pmod 7 \qquad \cdots\cdots④$$

かつ

$$y^4+y^3+\cdots+y+1\equiv 0 \pmod 7 \text{ または } y^4+y^3+\cdots+y+1\equiv 1 \pmod 7 \quad \cdots⑤$$

でなければならない．

④から，$y\equiv 1 \pmod 7$ または $y\equiv 2 \pmod 7$ となる．

$y\equiv 1 \pmod 7$ のとき，$y^4+y^3+\cdots+y+1\equiv 1+1+\cdots+1+1\equiv 5 \pmod 7$,

$y\equiv 2 \pmod 7$ のとき，$y^4+y^3+\cdots+y+1\equiv 2^4+2^2+\cdots+2+1\equiv 31\equiv 3 \pmod 7$

となり，⑤に矛盾する．

したがって，$\dfrac{x^7-1}{x-1}=y^5-1$ は整数解をもたない． □

系 8.4.2 を使うと次のことが言える．

p,q は素数，$x\neq 1$ は整数とする．
$q \mid \dfrac{x^p-1}{x-1}$ ならば，$q=p$ または $q\equiv 1 \pmod p$ が成り立つ．

例題 5.1.3　(APMO 2012)

$\dfrac{n^p+1}{p^n+1}$ が整数となるような素数 p と正の整数 n の組をすべて求めよ，

解答　$\dfrac{n^p+1}{p^n+1}$ が正の整数となるから，$\dfrac{n^p+1}{p^n+1}\geq 1$ すなわち $p^n\leq n^p$ となる．

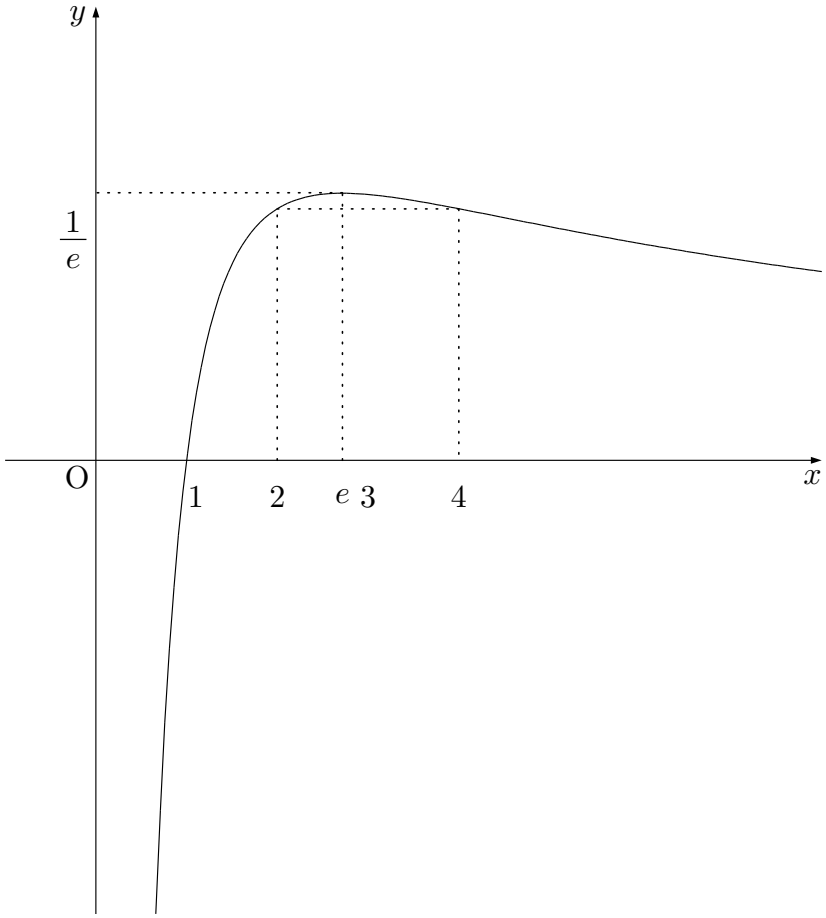
$$p^n\leq n^p \Longleftrightarrow \log p^n\leq \log n^p \Longleftrightarrow \frac{\log p}{p}\leq \frac{\log n}{n}.$$

$f(x)=\dfrac{\log x}{x}$ とおくと $f'(x)=\dfrac{1-\log x}{x^2}$.

x	0		e	
$f'(x)$		$+$	0	$-$
$f(x)$		↗	極大	↘

$x=e$ で極大値 $\dfrac{1}{e}$ をとる．また，$\lim\limits_{x\to+0} f(x)=-\infty$，$\lim\limits_{x\to+\infty} f(x)=0$

よって，$y=f(x)$ のグラフの概形は次のようになる．(実は y 軸方向に 8 倍拡大してある．)



(1) $p=2$ のとき，$n\in\left\{2,\,3,\,4\right\}$ で $\dfrac{n^p+1}{p^n+1}=\dfrac{n^2+1}{2^n+1}$ が正の整数となるのは，$n=2,4$ のときである．

(2) $p=3$ のとき，$n=3$.

(3) $p\geq 5$ のとき，p は奇素数で，$2\leq n\leq p$ である．

p^n+1 は偶数だから，n^p+1 も偶数となり，n は奇数である．

したがって，$p+1\mid p^n+1$ が成り立つことを用いると，$p+1\mid p^n+1\mid n^p+1$ から

$$n^p\equiv -1 \pmod{p+1}. \qquad \cdots\cdots ①$$

①の両辺を平方して

$$n^{2p}\equiv 1 \pmod{p+1}.$$

$\mathrm{ord}_{p+1}(n)$ が存在するから，$d=\mathrm{ord}_{p+1}(n)$ とおくと，$d\mid 2p$ が成り立つから，$d\in\left\{1,\,2,\,p,\,2p\right\}$.

$d=1$ のとき，$n^1 \equiv 1 \pmod{p+1}$ となるが，これは①に矛盾する．
$d=p$ のとき，$n^p \equiv 1 \pmod{p+1}$ となり，①とから，$1 \equiv -1 \pmod{p+1}$.
これから，$p+1 \mid 2$ となり，$p+1 \leq 2$ となるが，$p \geq 5$ に矛盾する．
よって，$d \in \left\{2,\, 2p\right\}$.
①から，$\gcd(n, p+1)=1$ だから，オイラーの定理より，$n^{\varphi(p+1)} \equiv 1 \pmod{p+1}$ が成り立つ．
よって，$d \mid \varphi(p+1)$ で $d \leq p+1 < p+1 < 2p$ だから，$d=2$ となる．
ゆえに，$n^2 \equiv 1 \pmod{p+1}$.
①から

$$-1 \equiv n^p \equiv n^{2\cdot\frac{p-1}{2}+1} \equiv \left(n^2\right)^{\frac{p-1}{2}} \cdot n \equiv 1^{\frac{p-1}{2}} \cdot n \equiv n \pmod{p+1}.$$

ゆえに，$p+1 \mid n+1$ となり，$p+1 \leq n+1$ から $p \leq n$ を得る．
$n \leq p$ であったから，$n=p$ となる．

（1），（2），（3）から，$(p,n)=(2,4),(p,p)$. □

5.2 原始根

p は素数とする．整数 a の p を法とする位数 $\mathrm{ord}_p(a)$ は，命題 5.1.1 より，$\varphi(p)$ の約数となるが，$\varphi(p) = p - 1$ に等しいとき，a は p を法とする**原始根**であるという．

例 5.2.1　13 を法として 1^k を計算した表

k	1
1^k	1

13 を法として 2^k を計算した表

k	1	2	3	4	5	6	7	8	9	10	11	12
2^k	2	4	8	3	6	12	11	9	5	10	7	1

13 を法として 3^k を計算した表

k	1	2	3
3^k	3	9	1

13 を法として 4^k を計算した表

k	1	2	3	4	5	6
4^k	4	3	12	9	10	1

13 を法として 5^k を計算した表

k	1	2	3	4
5^k	5	12	8	1

13 を法として 6^k を計算した表

k	1	2	3	4	5	6	7	8	9	10	11	12
6^k	6	10	8	9	2	12	7	3	5	4	11	1

13 を法として 7^k を計算した表

k	1	2	3	4	5	6	7	8	9	10	11	12
7^k	7	10	5	9	11	12	6	3	8	4	2	1

13 を法として 8^k を計算した表

k	1	2	3	4
8^k	8	12	5	1

13 を法として 9^k を計算した表

k	1	2	3
9^k	9	3	1

13 を法として 10^k を計算した表

k	1	2	3	4	5	6
10^k	10	9	12	3	4	1

13 を法として 11^k を計算した表

k	1	2	3	4	5	6	7	8	9	10	11	12
11^k	11	4	5	3	7	12	2	9	8	10	6	1

13 を法として 12^k を計算した表

k	1	2
12^k	12	1

2, 6, 7, 11 が 13 を法とする原始根になっている．

原始根は次の重要な性質をもっている．

命題 5.2.1　p は素数で，g は p を法とする原始根とする．
このとき，p と互いに素な整数 a に対して

$$g^k \equiv a \pmod{p} \quad (0 \leq k \leq p-2)$$

を満たす整数 k がただ一つ存在する．

証明 まず，$g^0 = 1, g^1, g^2, \ldots, g^{p-2}$ の中には p を法として合同になるものはないことを示す．

$\mathrm{ord}_p(g) = p-1$ から $g^{p-1} \equiv 1 \pmod{p}$ が成り立つので，

$$g^0 = 1 \not\equiv 0 \pmod{p},\ g^1 \not\equiv 0 \pmod{p},\ g^2 \not\equiv 0 \pmod{p},\ \ldots,\ g^{p-2} \not\equiv 0 \pmod{p}$$

である．命題 5.1.3 より，$g^1, g^2, \ldots, g^{p-2}, g^0 = 1 \equiv g^{p-1} \pmod{p}$ の中には p を法として合同になるものはない．

a と p は互いに素であるから， a は $p-1$ 個の整数 $1, 2, \ldots, p-1$ のどれかと合同である．よって，$p-1$ 個の整数 $g^0 = 1, g^1, g^2, \ldots, g^{p-2}$ のどれかが p を法として a と合同になるから

$$g^k \equiv a \pmod{p} \quad (0 \leq k \leq p-2)$$

を満たす整数 k が存在する．

次に一意性を示す．

$$g^{k_1} \equiv a \pmod{p},\ g^{k_2} \equiv a \pmod{p} \quad (0 \leq k_1 \leq k_2 \leq p-2)$$

が成り立つとすると，$g^{k_1} \equiv g^{k_2} \pmod{p}$ である．
これを，$g^{k_1}\left(g^{k_2-k_1} - 1\right) \equiv 0 \pmod{p}$ と変形する．
g と p は互いに素であるから，$g^{k_2-k_1} - 1 \equiv 0 \pmod{p}$.
g は p を法とする原始根なので，$\mathrm{ord}_p(g) = p-1$ が成り立つ．命題 5.1.1 より $p \mid k_2 - k_1$.
$0 \leq k_2 - k_1 < p-2$ なので $k_2 - k_1$ が p の倍数となるのは $k_2 - k_1 = 0$ のときだけである．
したがって $g^k \equiv a \pmod{p}$ を満たす k はただ一つしかない． □

注 $g^0 = 1, g^{p-1} \equiv 1 \pmod{p}$ なので，命題 5.2.1 において，$g^k \equiv a \pmod{p}$ $(0 \leq k \leq p-2)$ のかわりに $g^k \equiv a \pmod{p}$ $(1 \leq k \leq p-1)$ としてもよい．

例 5.2.2 $p = 13$ の場合を考えてみる．

13 を法として 2^k を計算すると

k	1	2	3	4	5	6	7	8	9	10	11	12
2^k	2	4	8	3	6	12	11	9	5	10	7	1

13 を法とする 2 の位数は $12 = \varphi(13)$ であるから，2 は 13 を法とする原始根になっている．

$\gcd(a, 13) = 1$ となる正の整数 a は $1, 2, \ldots, 12$ の値をとるが, 表から $2^k \equiv a \pmod{p}$ を満たす $k(1 \leq k \leq 12)$ は一つしかない．

命題 5.2.2 p は素数で, a, b は p と互いに素な整数とする．このとき, $\mathrm{ord}_p(a)$ と $\mathrm{ord}_p(b)$ が互いに素ならば，次のことが成り立つ．

$$\mathrm{ord}_p(ab) = \mathrm{ord}_p(a)\mathrm{ord}_p(b).$$

証明 $\mathrm{ord}_p(a) = s, \mathrm{ord}_p(b) = t, \mathrm{ord}_p(ab) = u$ とおく．
$(ab)^u \equiv 1 \pmod{p}$ から $(ab)^{su} \equiv 1 \pmod{p}$ すなわち $(a^s)^u b^{su} \equiv 1 \pmod{p}$ が成り立

つ．$a^s \equiv 1 \pmod{p}$ であることを用いると $b^{su} \equiv 1 \pmod{p}$ を得る．$\mathrm{ord}_p(b) = t$ であったから，$t \mid su$ が成り立つ．s と t は互いに素だから，$t \mid u$ となる．
同様にして $s \mid u$ が成り立つ．s と t は互いに素だから，

$$st \mid u. \qquad \cdots\cdots ①$$

$a^s \equiv 1 \pmod{p}$, $b^t \equiv 1 \pmod{p}$ から

$$(ab)^{st} = (a^s)^t \left(b^t\right)^s \equiv 1^t \cdot 1^s \equiv 1 \pmod{p}.$$

$u = \mathrm{ord}_p(ab)$ であったから

$$u \mid st. \qquad \cdots\cdots ②$$

①，②から $u = st$ すなわち $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a)\mathrm{ord}_p(b)$ が成り立つ．　□

数学的帰納法を使えば，次の命題が得られる．

命題 5.2.3　n は 2 以上の整数，p は素数で，$a_1, a_2, \ldots, a_n$ は p と互いに素な整数とする．このとき，$\mathrm{ord}_p(a_1), \mathrm{ord}_p(a_2), \ldots, \mathrm{ord}_p(a_n)$ のどの 2 つも互いに素ならば，次のことが成り立つ．

$$\mathrm{ord}_p(a_1 a_2 \cdots a_n) = \mathrm{ord}_p(a_1)\mathrm{ord}_p(a_2) \cdots \mathrm{ord}_p(a_n).$$

定理 5.2.1　p は素数とし，$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ は整数係数の n 次式で，$p \nmid a_n$ とする．
このとき，$f(x) \equiv 0 \pmod{p}$ の p を法とする解は n 個以下である．

証明　n に関する数学的帰納法で証明する．

(I) $n = 1$ のとき，$f(x) = a_1 x + a_0$, $p \nmid a_1$.
$f(x) \equiv 0 \pmod{p}$ とおくと，$a_1 x \equiv -a_0 \pmod{p}$.
p と a_1 は互いに素であるから，定理 4.4.2 より，p を法としてただ 1 個の解をもつ．

(II) $n-1$ 次の多項式について成り立つと仮定して，$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ を整数係数の n 次式で，$p \nmid a_n$ とする．
$f(x) \equiv 0 \pmod{p}$ が p を法として解をもたなければ，ここで証明は終わる．
よって，$f(x) \equiv 0 \pmod{p}$ が p を法として解をもつ場合を考える．解を x_1 とする．
$f(x)$ を $x - x_1$ で割った商を $f_1(x)$ とすると，余りは $f_1(x_1)$ だから

$$f(x) = (x - x_1)f_1(x) + f_1(x_1)$$

は x についての恒等式である．

$f_1(x)$ は整数係数の $n-1$ 次式で，$n-1$ 次の係数は a_n で $p \nmid a_n$ である．
$x \equiv x_1 \pmod{p}$ は $f(x) \equiv 0 \pmod{p}$ の解なので $f(x_1) \equiv 0 \pmod{p}$ が成り立つ．
よって，$f(x) \equiv 0 \pmod{p}$ は $(x-x_1)f_1(x) + f_1(x_1) \equiv 0 \pmod{p}$ すなわち

$$(x-x_1)f_1(x) \equiv 0 \pmod{p}$$

となる．p は素数なので

$$x - x_1 \equiv 0 \pmod{p} \text{ または } f_1(x) \equiv 0 \pmod{p}.$$

$x \equiv x_1 \pmod{p}$ 以外の解は $f_1(x) \equiv 0 \pmod{p}$ の解である．仮定から，$f_1(x) \equiv 0 \pmod{p}$ は p を法として $n-1$ 個以下の解しかもたないから，$f(x) \equiv 0 \pmod{p}$ の p を法とする解は n 個以下である．
すなわち，n のときも成り立つ．

(III) (I)，(II) よりすべての正の整数に対して成り立つ． □

定理 5.2.2 p は素数とし，d を $p-1$ の正の約数とする．このとき，$x^d - 1 \equiv 0 \pmod{p}$ は p を法として，ちょうど d 個の解をもつ．

証明 フェルマーの小定理より，$x^{p-1} - 1 \equiv 0 \pmod{p}$ は p を法として，$p-1$ 個の解 $1, 2, \ldots, p-1$ をもつ．
$d \mid p-1$ より $p-1 = de$ $(e \in \mathbb{N})$ とおくと

$$x^{p-1} - 1 = x^{de} - 1 = \left(x^d\right)^e - 1 = \left(x^d - 1\right)\left(\left(x^d\right)^{e-1} + \left(x^d\right)^{e-2} + \cdots + x^d + 1\right)$$

が成り立つ．

$$\begin{aligned} g(x) &= \left(x^d\right)^{e-1} + \left(x^d\right)^{e-2} + \cdots + x^d + 1 \\ &= x^{de-d} + x^{de-2d} + \cdots + x^d + 1 \\ &= x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1 \end{aligned}$$

とおくと

$$x^{p-1} - 1 \equiv 0 \pmod{p} \iff x^d - 1 \equiv 0 \pmod{p} \text{ または } g(x) \equiv 0 \pmod{p}$$

が成り立ち，定理 5.2.1 より，$x^d - 1 \equiv 0 \pmod{p}$ の解は p を法として d 個以下，$g(x) \equiv 0 \pmod{p}$ の解は p を法として $p-1-d$ 個以下だから，$x^{p-1} - 1 \equiv 0 \pmod{p}$ の解は p を法として $d + (p-1-d) = p-1$ 個以下となる．

ところで，最初に確認したように，$x^{p-1} - 1 \equiv 0 \pmod{p}$ の解は p を法として $p-1$ 個あったから，$x^d - 1 \equiv 0 \pmod{p}$ の解は p を法として d 個，$g(x) \equiv 0 \pmod{p}$ の解は p を法として $p-1-d$ 個でなければならない． □

これで準備が整ったので，次の定理が証明できる．

定理 5.2.3　すべての素数 p に対して，p を法とする原始根が存在する．

証明　$p = 2$ のときは，2 を法として 1 が原始根になっている．

以下，$p \geq 3$ とする．

$p - 1$ を素因数分解して

$$p - 1 = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \quad (p_1,\, p_2,\, \ldots,\, p_r \text{は異なる素数}, e_1,\, e_2,\, \ldots,\, e_r \in \mathbb{N})$$

とおく．

$$\mathrm{ord}_p(a_i) = p_i^{e_i} \quad (i = 1,\, 2,\, \ldots,\, r) \qquad \cdots\cdots ①$$

となる $a_i \in \mathbb{N}$ が存在することが証明できれば，

$r = 1$ のとき，$g = a_1$ とおくと，$\mathrm{ord}_p(g) = \mathrm{ord}_p(a_1) = p_1^{e_1} = p - 1$.

$r \geq 2$ のときは，$g = a_1 a_2 \cdots a_r$ とおく．$\mathrm{ord}_p(a_1),\, \mathrm{ord}_p(a_2),\, \ldots,\, \mathrm{ord}_p(a_r)$ のどの 2 つも互いに素であるから，命題 5.2.3 より

$$\mathrm{ord}_p(g) = \mathrm{ord}_p(a_1 a_2 \cdots a_r) = \mathrm{ord}_p(a_1)\mathrm{ord}_p(a_2) \cdots \mathrm{ord}_p(a_r) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = p - 1$$

となり，g は p を法とする原始根になる．

したがって，①を満たす $a_i \in \mathbb{N}$ が存在することを証明すればよい．

$i \in \left\{1,\, 2,\, \ldots,\, r\right\}$ を固定する．

$p_i^{e_i}$ は $p - 1$ の正の約数だから，定理 5.2.2 より，$x^{p_i^{e_i}} - 1 \equiv 0 \pmod{p}$ は p を法として，ちょうど $p_i^{e_i}$ 個の解をもつ．

また，$p_i^{e_i - 1}$ も $p - 1$ の正の約数だから，定理 5.2.2 より，$x^{p_i^{e_i - 1}} - 1 \equiv 0 \pmod{p}$ は p を法として，ちょうど $p_i^{e_i - 1}$ 個の解をもつ．

$p_i^{e_i} > p_i^{e_i - 1}$ であるから，

$$a_i{}^{p_i^{e_i}} - 1 \equiv 0 \pmod{p} \text{ かつ } a_i{}^{p_i^{e_i - 1}} - 1 \not\equiv 0 \pmod{p}$$

を満たす正の整数 a_i が存在することになる．

命題 5.1.1 より $\mathrm{ord}_p(a_i) \mid p_i^{e_i}$ かつ $\mathrm{ord}_p(a_i) \nmid p_i^{e_i - 1}$ であるから，$\mathrm{ord}_p(a_i) = p_i^{e_i}$ が成り立つ．　□

5.3　平方剰余

合同式 $x^2 \equiv a \pmod{m}$,　$\gcd(a, m) = 1$ が整数解をもつとき，整数 a のことを m を法とする**平方剰余** (quadratic residue modulo m) と呼び，整数解がない場合には a のことを m を法とする**平方非剰余** (quadratic nonresidue modulo m) と呼ぶ.

mod 17 で考えると

$1^2 \equiv 16^2 \equiv 1,\ 2^2 \equiv 15^2 \equiv 4,\ 3^2 \equiv 14^2 \equiv 9,\ 4^2 \equiv 13^2 \equiv 16,$

$5^2 \equiv 12^2 \equiv 8,\ 6^2 \equiv 11^2 \equiv 2,\ 7^2 \equiv 10^2 \equiv 15,\ 8^2 \equiv 9^2 \equiv 13.$

$6^2 \equiv 2 \pmod{17}$ から 2 は 17 を法とする平方剰余である.

また，$x^2 \equiv 3 \pmod{17}$ には整数解がないから，3 は 17 を法とする平方非剰余である.

まず，奇数の素数 p を法とする合同式

$$x^2 \equiv a \pmod{p}, \quad \gcd(a, p) = 1$$

を考えよう.

定理 5.3.1　p は奇数の素数，a は p と互いに素な整数とする．合同式 $x^2 \equiv a \pmod{p}$ は p を法として，2 つの解をもつか，解をまったくもたないかのどちらかである.

証明 定理 5.2.1 より，$x^2 \equiv a \pmod{p}$ の p を法とする解は 2 個以下である.

合同式 $x^2 \equiv a \pmod{p}$ が解 $x \equiv x_1 \pmod{p}$ をもつと

$$(-x_1)^2 \equiv x_1^2 \equiv a \pmod{p}$$

より $x \equiv -x_1 \pmod{p}$ も $x^2 \equiv a \pmod{p}$ の解である.

そして，これらの解は異なる.

なぜならば，$x_1 \equiv -x_1 \pmod{p}$ だとすると $2x_1 \equiv 0 \pmod{p}$ となる.

p は奇素数であるから $x_1 \equiv 0 \pmod{p}$ となり，$a \equiv x_1^2 \equiv 0 \pmod{p}$.

これは $\gcd(a, p) = 1$ に矛盾する.　□

命題 5.3.1　p は奇数の素数，a は p と互いに素な整数とする.

法 p に関する既約剰余系は，$1^2, 2^2, \ldots, \left(\dfrac{p-1}{2}\right)^2$ と合同な $\dfrac{p-1}{2}$ 個の平方剰余と，$\dfrac{p-1}{2}$ 個の平方非剰余からなる集合である.

証明 $A = \left\{ -\dfrac{p-1}{2},\ \ldots,\ -2,\ -1,\ 1,\ 2,\ \ldots,\ \dfrac{p-1}{2} \right\}$　……①

は法 p に関する既約剰余系の一つである．

$$\begin{aligned} p-1 &\equiv -1 \pmod{p} \\ p-2 &\equiv -2 \pmod{p} \\ &\vdots \\ \frac{p+1}{2} = p - \frac{p-1}{2} &\equiv -\frac{p-1}{2} \pmod{p} \end{aligned}$$

が成り立つから

$(*)$

$$\begin{aligned} 1^2 &\equiv 1^2 \pmod{p} \\ 2^2 &\equiv 2^2 \pmod{p} \\ &\vdots \\ \left(\frac{p-1}{2}\right)^2 &\equiv \left(\frac{p-1}{2}\right)^2 \pmod{p} \\ \left(\frac{p+1}{2}\right)^2 &\equiv \left(\frac{p-1}{2}\right)^2 \pmod{p} \\ &\vdots \\ (p-2)^2 &\equiv 2^2 \pmod{p} \\ (p-1)^2 &\equiv 1^2 \pmod{p}. \end{aligned}$$

$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ と p を法として合同なものを

$$r_1, r_2, \ldots, r_{\frac{p-1}{2}} \quad \left(-\frac{p-1}{2} \leq r_i \leq \frac{p-1}{2},\ r_i \neq 0,\ 1 \leq i \leq \frac{p-1}{2}\right)$$

とすると，$r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ はすべて異なる．

$B = A \setminus \left\{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\right\}$ とおくと B の要素は平方非剰余である．

もしも，$s \in B$ が平方剰余であったならば，$x^2 \equiv s \pmod{p}$ となる $x \in A$ がある．

上で調べた $(*)$ から，s は $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ のいずれかと p を法として合同となり，$s \in \left\{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\right\}$.

したがって，$s \notin B$ となり $s \in B$ に矛盾する．

法 p に関する既約な剰余系の中で平方剰余になっているものは，①の要素の平方と合同なものであり，かつこれらだけに限る． □

定理 5.3.2　p は奇数の素数，a は p と互いに素な整数とする．

a が p を法とする平方剰余であれば，$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$,

a が p を法とする平方非剰余であれば，$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

が成り立つ．

証明 フェルマーの小定理により，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つから

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

p は素数なので

$$a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \text{ または } a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$$

が成り立ち，これらが同時に成立することはない．
なぜならば，$a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$, $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$ が同時に成立するとき

$$2 = \left(a^{\frac{p-1}{2}} + 1\right) - \left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \mod p$$

から $p \mid 2$ となる．これは，p が奇数の素数だから $p \nmid 2$ に矛盾する．

a が p を法とする平方剰余のとき，$x^2 \equiv a \pmod{p}$ を満たす整数 x が存在する．

$a \equiv x^2 \pmod{p}$ の両辺を $\dfrac{p-1}{2}$ 乗すると

$$a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} = x^{p-1} \pmod{p}.$$

$x^2 \equiv a \pmod{p}$, $\gcd(a, p) = 1$ から $p \nmid x$ すなわち $\gcd(x, p) = 1$ となるから，フェルマーの小定理より

$$x^{p-1} \equiv 1 \pmod{p}.$$

これと $a^{\frac{p-1}{2}} \equiv x^{p-1} \pmod{p}$ から

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

を得る．

命題 5.3.1 より，合同式 $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ の解は，$\dfrac{p-1}{2}$ 個の平方剰余によってつくされていることがわかる．

なぜならば，$\dfrac{p-1}{2}$ 次の合同式の解は $\dfrac{p-1}{2}$ 個以下だからである．

それゆえ，平方非剰余は合同式 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ を満たす． □

5.4　ルジャンドル (Legendre) の記号

平方剰余について考察するためには次の記号が便利である．

p を奇数の素数，a は p と互いに素な整数とするとき，記号 $\left(\frac{a}{p}\right)$ を次のように定める．

a が p を法として平方剰余である場合には $\left(\frac{a}{p}\right) = 1$ とし，

a が p を法として平方非剰余である場合には $\left(\frac{a}{p}\right) = -1$ とする．

- $6^2 \equiv 2 \pmod{17}$ が成り立つので $\left(\frac{2}{17}\right) = 1$.

  $x^2 \equiv 3 \pmod{17}$ は整数解をもたないから $\left(\frac{3}{17}\right) = -1$
- ルジャンドルの記号を使うと，定理 4.6.2 は

  $p \equiv 1 \pmod 4$ ならば $\left(\frac{-1}{p}\right) = 1$

  $p \equiv 3 \pmod 4$ ならば $\left(\frac{-1}{p}\right) = -1$

  と書き直すことができる．

定理 5.4.1　p は奇数の素数，a, b は p と互いに素な整数とするとき，次のことが成り立つ．

(1)　$a \equiv b \pmod p$ ならば $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2)　$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.　(Euler's Criterion)

(3)　$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

証明

(1) $a \equiv b \pmod p$ のとき

$$x^2 \equiv a \pmod p \Longleftrightarrow x^2 \equiv b \pmod p$$

であるから，$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) a が p を法として平方剰余である $\Longleftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$ を示せばよい．これは定理 5.3.2 からわかるが，原始根を用いて証明する．

a が p を法として平方剰余であると仮定する．$x^2 \equiv a \pmod p$ は解をもつから，これを $x \equiv x_1 \pmod p$ とおく．$(a, p) = 1$ であるから $(x_1, p) = 1$ となる．よって，

フェルマーの小定理より $x_1^{p-1} \equiv 1 \pmod{p}$ が成り立つから，

$$a^{\frac{p-1}{2}} \equiv \left(x_1^2\right)^{\frac{p-1}{2}} \equiv x_1^{p-1} \equiv 1 \pmod{p}.$$

$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ が成り立つと仮定する．

定理 5.2.3 より，p を法とする原始根 g が存在する．すなわち，$g^k \equiv a \pmod{p}$ を満たす正の整数 k $(1 \leq k \leq p-1)$ が存在する．これから

$$g^{\frac{k(p-1)}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

$\mathrm{ord}_p(g) = p-1$ は $\frac{k(p-1)}{2}$ を割り切るから $\frac{k(p-1)}{2} = (p-1)j$ $(j \in \mathbb{N})$ すなわち $k = 2j$ $(j \in \mathbb{N})$ とかける．

$$\left(g^j\right)^2 = g^{2j} = g^k \equiv a \pmod{p}$$

から g^j は $x^2 \equiv a \pmod{p}$ の解であることがわかるので，a は p を法とする平方剰余である．

(3) (2) の結果を用いると

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

さて，ルジャンドルの記号は 1 か -1 の値しかとらないから，$\left(\frac{ab}{p}\right) \neq \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ ならば，$1 \equiv -1 \pmod{p}$ すなわち $2 \equiv 0 \pmod{p}$ となる．これは，$p > 2$ に矛盾する．

よって，$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ が成り立つ．　□

系 5.4.1　$n \geq 2$ は正の整数，p は奇数の素数，a, a_1, a_2, …, a_n は p と互いに素な整数とするとき，次のことが成り立つ．

(1) $\left(\frac{a_1 a_2 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$.

(2) $\left(\frac{a^2}{p}\right) = 1, \quad \left(\frac{1}{p}\right) = 1.$

(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

証明

(1) 定理 5.4.1(3) と n に関する数学的帰納法で証明できる．

(2) 定理 5.4.1(3) で $b = a$ とおくと

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2 = (\pm 1)^2 = 1.$$

特に $a = 1$ とおくと，$\left(\frac{1}{p}\right) = 1$.

(3) 定理 5.4.1(2) で $a = -1$ とおくと

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

$\left(\frac{-1}{p}\right)$ と $(-1)^{\frac{p-1}{2}}$ はともに 1 か -1 の値しかとらないから，$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

□

- 系 5.4.1(1) と (2) から

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)^2 = \left(\frac{a}{p}\right)$$

となるので，ルジャンドルの記号の分子において，平方因数を棄ててもよい.

5.5　ガウスの補題

定理 5.5.1　p は奇数の素数，a, b は p と互いに素な整数とする．

a, $2a$, $3a$, …, $\dfrac{p-1}{2}a$ を p で割った余りを $-\dfrac{p-1}{2}$ と $\dfrac{p-1}{2}$ の間にとる．そうしてできた $\dfrac{p-1}{2}$ 個の余りのうち，負であるものの個数 w をとする．このとき

$$\left(\frac{a}{p}\right) = (-1)^w$$

が成り立つ．

※　系 2.1.1 より p で割った余り r は $-\dfrac{p}{2} \leq r < \dfrac{p}{2}$ の範囲でとれるが，p は奇素数なので

$-\dfrac{p-1}{2} \leq r \leq \dfrac{p-1}{2}$ の範囲になる．

証明　$1 \leq k \leq \dfrac{p-1}{2}$ を満たす整数 k に対して，ka を p で割った余り r を

$$-\frac{p-1}{2} \leq r \leq \frac{p-1}{2}$$

の範囲にとって，r の符号が正のときは 1，負のときは -1 をとる関数を $s(k)$ とし，r の絶対値を $f(k)$ とする．(ka は p で割り切れないので，$f(k) \neq 0$.) このとき

$$ka \equiv s(k)f(k) \pmod{p}, \quad s(k) \in \Big\{1,\ -1\Big\}, \quad 1 \leq f(k) \leq \frac{p-1}{2}.$$

w の定義から

$$w = (s(k) = -1 \text{ となる } k \text{ の個数})$$

である．

$$ka \equiv s(k)f(k) \pmod{p}$$

において，$k = 1, 2, \ldots, \dfrac{p-1}{2}$ としたものを辺々かけあわせると

$$\left(\frac{p-1}{2}\right)! \, a^{\frac{p-1}{2}} \equiv (-1)^w f(1)f(2)\cdots f\left(\frac{p-1}{2}\right) \qquad \cdots\cdots ①$$

が成り立つ．

$f(1)$, $f(2)$, …, $f\left(\frac{p-1}{2}\right)$ の中には等しいものがないことを示す．

もしも

$$f(k) = f(k'), \quad k, k' \in \Big\{1,\ 2,\ \ldots,\ \frac{p-1}{2}\Big\}$$

となったとすると，

$$ka \equiv s(k)f(k) \pmod{p},\ k'a \equiv s(k')f(k') \equiv s(k')f(k) \pmod{p},$$
$$s(k), s(k') \in \left\{1,\ -1\right\}$$

が成り立つ．

これから

$$ka \equiv k'a \pmod{p} \text{ または } ka \equiv -k'a \pmod{p}.$$

a と p は互いに素であるから

$$k \equiv k' \pmod{p} \text{ または } k \equiv -k' \pmod{p}.$$

$k, k' \in \left\{1,\ 2,\ \ldots,\ \dfrac{p-1}{2}\right\}$ から $-(p-1) \leq k - k' \leq p-1$, $2 \leq k + k' \leq p-1$ となるので $k - k' = 0$ でなければならない．

したがって，$f(1), f(2), \ldots, f\left(\frac{p-1}{2}\right)$ の中には等しいものは存在しない．

$f(1), f(2), \ldots, f\left(\dfrac{p-1}{2}\right)$ はすべて異なり，すべて 1 以上 $\dfrac{p-1}{2}$ 以下の整数だから，$1, 2, \ldots, \dfrac{p-1}{2}$ を並べ替えたものに等しい．よって，

$$f(1)f(2)\cdots f\left(\frac{p-1}{2}\right) = 1 \cdot 2 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)!$$

これを①に使うと

$$\left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \equiv (-1)^w \left(\frac{p-1}{2}\right)! \pmod{p}$$

となる．p と $\left(\dfrac{p-1}{2}\right)!$ は互いに素だから

$$a^{\frac{p-1}{2}} \equiv (-1)^w \pmod{p}$$

を得る．定理 5.4.1(2) より $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ が成り立つから

$$\left(\frac{a}{p}\right) \equiv (-1)^w \pmod{p}.$$

$\left(\dfrac{a}{p}\right)$ と $(-1)^w$ は 1 か -1 の値しかとらないことと，p が奇数であることから

$$\left(\frac{a}{p}\right) = (-1)^w$$

が成り立つ．　□

- ある整数を p でわった余り r を，0 以上 $p-1$ で考えた場合，r が $\frac{p}{2}$ より大きいならば，それから p を引くと，$-\frac{p}{2} < r' < 0$ となる．

  $a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a$ を p で割った余りを 1 と $p-1$ の間にとる．そうしてできた $\frac{p-1}{2}$ 個の余りのうち，$\frac{p}{2}$ より大きいものの個数が w となる．

定理 5.5.2　p が奇数の素数ならば

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 8 \text{ または } p \equiv 7 \pmod 8 \\ -1 & p \equiv 3 \pmod 8 \text{ または } p \equiv 5 \pmod 8 \end{cases} \tag{5.1}$$

が成り立つ．

証明　$1\cdot 2,\ 2\cdot 2,\ 3\cdot 2,\ \ldots,\ \frac{p-1}{2}\cdot 2$ を p で割った余りを，$-\frac{p-1}{2}$ と $\frac{p-1}{2}$ の間にとる．

$$\begin{aligned} \frac{p+1}{2} &= p\times 1 - \frac{p-1}{2}, & \frac{p-1}{2} &= p\times 0 + \frac{p-1}{2} \\ \frac{p+3}{2} &= p\times 1 - \frac{p-3}{2}, & \frac{p-3}{2} &= p\times 0 + \frac{p-3}{2} \\ &\vdots & &\vdots \\ p-1 &= p\times 1 - 1, & 1 &= p\times 0 + 1 \end{aligned}$$

であるから，$k\cdot 2 \quad \left(k \in \left\{1,\ 2,\ \ldots,\ \frac{p-1}{2}\right\}\right)$ を p で割った余りが負になるための条件は，

$$2k \geq \frac{p+1}{2}$$

であるから，結局

$$\frac{p+1}{4} \leq k \leq \frac{p-1}{2} \qquad \cdots\cdots ① \tag{①}$$

となる．①を満たす k の個数を w とすると，$\left(\frac{a}{p}\right) = (-1)^w$ だから，①を満たす k の個数を調べる．

l を整数として

$p = 8l+1$ のとき，$2l+1 \leq k \leq 4l$ から $w = 2l,\ (-1)^w = 1$,

$p = 8l+3$ のとき，$2l+1 \leq k \leq 4l+1$ から $w = 2l+1,\ (-1)^w = -1$,

$p = 8l+5$ のとき，$2l+2 \leq k \leq 4l+2$ から $w = 2l+1,\ (-1)^w = -1$,

$p = 8l+7$ のとき，$2l+2 \leq k \leq 4l+3$ から $w = 2l+2,\ (-1)^w = 1$.

$\left(\dfrac{a}{p}\right) = (-1)^w$ だから，

$p \equiv 1 \pmod 8$ または $p \equiv 7 \pmod 8$ のとき $\left(\dfrac{a}{p}\right) = 1$,

$p \equiv 3 \pmod 8$ または $p \equiv 5 \pmod 8$ のとき $\left(\dfrac{a}{p}\right) = -1$

となる．□

$p \equiv 1 \pmod 8$ または $p \equiv 7 \equiv -1 \pmod 8$ のとき，$p = 8k \pm 1$ の形だから

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k \text{ は偶数となり } (-1)^{\frac{p^2-1}{8}} = 1.$$

$p \equiv 3 \pmod 8$ または $p \equiv 5 \equiv -3 \pmod 8$ のとき，$p = 8k \pm 3$ の形だから

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1 \text{ は奇数となり}$$

$(-1)^{\frac{p^2-1}{8}} = -1.$

したがって，次の系を得る．

系 5.5.1　p が奇数の素数ならば

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

が成り立つ．

5.6　平方剰余の相互法則

定理 5.6.1　p は奇数の素数，a は p と互いに素な奇数とする．このとき

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]}$$

が成り立つ．

証明　$S = \left\{a,\ 2a,\ \ldots,\ \dfrac{p-1}{2}a\right\}$ とおく．各 $ka \in S$ $\left(1 \leq k \leq \dfrac{p-1}{2}\right)$ を p で割った商を q_k，余りを r_k とおくと

$$ka = pq_k + r_k, \quad 1 \leq r_k \leq p-1$$

と書ける．ここで $q_k = \left[\dfrac{ka}{p}\right]$ だから，$ka = p\left[\dfrac{ka}{p}\right] + r_k$ が成り立つ．

余り $r_1, \ldots, r_{\frac{p-1}{2}}$ の中で $\dfrac{p}{2}$ より小さいものを $s_1, \ldots, s_m$ とし，$\dfrac{p}{2}$ より大きいものを $t_1, \ldots, t_n$ とする．

$ka = p\left[\dfrac{ka}{p}\right] + r_k$ で $k = 1, 2, \ldots, \dfrac{p-1}{2}$ とおいたものの辺々の和をとると

$$\sum_{k=1}^{\frac{p-1}{2}} ka = p\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] + \sum_{k=1}^{m} s_k + \sum_{k=1}^{n} t_k \qquad \cdots\cdots ①$$

◎ $\dfrac{p-1}{2}$ 個の数 $s_1, \ldots, s_m,\ p-t_1, \ldots, p-t_n$ は $k = 1, 2, \ldots, \dfrac{p-1}{2}$ の並べ替えたものである．

まず，$1 \leq k < k' \leq p-1$ のとき，$r_k \neq r_{k'}$ であることを示す．

もしも $r_k = r_{k'}$ が成り立つとすると，$ka - pq_k = k'a - pq_{k'}$ から

$$(k'-k)a = p(q_{k'} - q_k).$$

a と p は互いに素であるから，$p \mid k'-k$ となる．ところが，$0 < k'-k < \dfrac{p-1}{2} < p$ であるから，$k'-k$ が p で割り切れることはない．したがって，$r_k \neq r_{k'}$ である．

これから，$s_1, \ldots, s_m$ はすべて異なり，$t_1, \ldots, t_n$ もすべて異なることがわかる．

もしも $s_i = p - t_j,\ i \in \left\{1,\ \ldots,\ m\right\},\ j \in \left\{1,\ \ldots,\ n\right\}$ と成り立つとすると，$s_i + t_j = p$ が成り立つ．

$s_i = r_{k_1},\ t_j = r_{r_{k_2}}$ となる r_{k_1}, r_{k_2}，$k_1, k_2 \in \left\{1,\ \ldots,\ \dfrac{p-1}{2}\right\}$ があるので，$r_{k_1} + r_{k_2} = p$.

r_{k_1}, r_{k_2} に対応して，$k_1 a = pq_{k_1} + r_{k_1}$，$k_2 a = pq_{k_2} + r_{k_2}$ が成り立つので，これらの式の辺々を加えると

$$(k_1 + k_2)a = p(q_{k_1} + q_{k_2}) + r_{k_1} + r_{k_2} = p(q_{k_1} + q_{k_2}) + p = p(q_{k_1} + q_{k_2} + 1).$$

a と p は互いに素であるから，$p \mid k_1 + k_2$. ところが $2 \leq k_1 + k_2 \leq p-1$ であるから，$k_1 + k_2$ はで割り切れない．したがって，$1 \leq i \leq m, 1 \leq j \leq n$ のとき $s_i \neq p - t_j$ である．

$\dfrac{p-1}{2}$ 個の数 $s_1, \ldots, s_m, p - t_1, \ldots, p - t_n$ は $k = 1, 2, \ldots, \dfrac{p-1}{2}$ の並べ替えたものであるから

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{m} s_k + \sum_{k=1}^{n} (p - t_k) = pn + \sum_{k-1}^{m} s_k - \sum_{k=1}^{n} t_k \qquad \cdots\cdots ②$$

が成り立つ．① − ② から

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] - n\right) + 2\sum_{k=1}^{n} t_k \qquad \cdots\cdots ③$$

$p \equiv 1 \pmod 2$, $a \equiv 1 \pmod 2$ であるから，③を 2 を法とする合同式に直すと

$$0 \cdot \sum_{k=1}^{\frac{p-1}{2}} k \equiv 1 \cdot \left(\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] - n\right) + 0 \pmod 2$$

すなわち

$$n \equiv \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] \pmod 2$$

を得る．定理 5.5.1(ガウスの補題) より

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}} [\frac{ka}{p}]}$$

となる． □

定理 5.6.2　（平方剰余の相互法則）

p と q は異なる奇数の素数とする．このとき

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \left(-1\right)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

が成り立つ．

証明 定理 5.6.1 より

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]}\cdot(-1)^{\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right]}=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right]} \quad \cdots\cdots ①$$

が成り立つ．

xy 平面で $D=\left\{(x,\ y):0<x<\dfrac{p}{2},\ 0<y<\dfrac{p}{2}\right\}$ とおき，D 内にある格子点の個数を 2 通りの方法で数える．

p と q は両方とも奇数であるから， D 内にある格子点はすべて

$$(x,\,y),\ 1\leq x\leq\frac{p-1}{2},\ 1\leq y\leq\frac{q-1}{2}\ \ (x,\,y\in\mathbb{N})$$

の形をしているから，D 内にある格子点の個数は

$$\frac{p-1}{2}\cdot\frac{q-1}{2} \quad \cdots\cdots ②$$

である．

2 点 $O(0,\,0)$, $P\,(p/2,\,q/2)$ を通る直線 l の方程式は $y=\dfrac{q}{p}x$ すなわち $py=qx$ となる．

$\gcd(p,\,q)=1$ であるから，D 内で l 上に格子点は存在しない．領域 D を直線 l で 2 つの部分に分け，l の下側の部分を T_1，上側の部分を T_2 とする．

T_1 に含まれる格子点の個数を求める．いま，直線 $x=k\ \left(1\leq k\leq\dfrac{p-1}{2},\ k\in\mathbb{N}\right)$ で切ると，$0<y<\dfrac{kq}{p}$ を満たす整数 y の個数は $\left[\dfrac{kq}{p}\right]$ である．

したがって，T_1 に含まれる格子点の個数は

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right] \quad \cdots\cdots ③$$

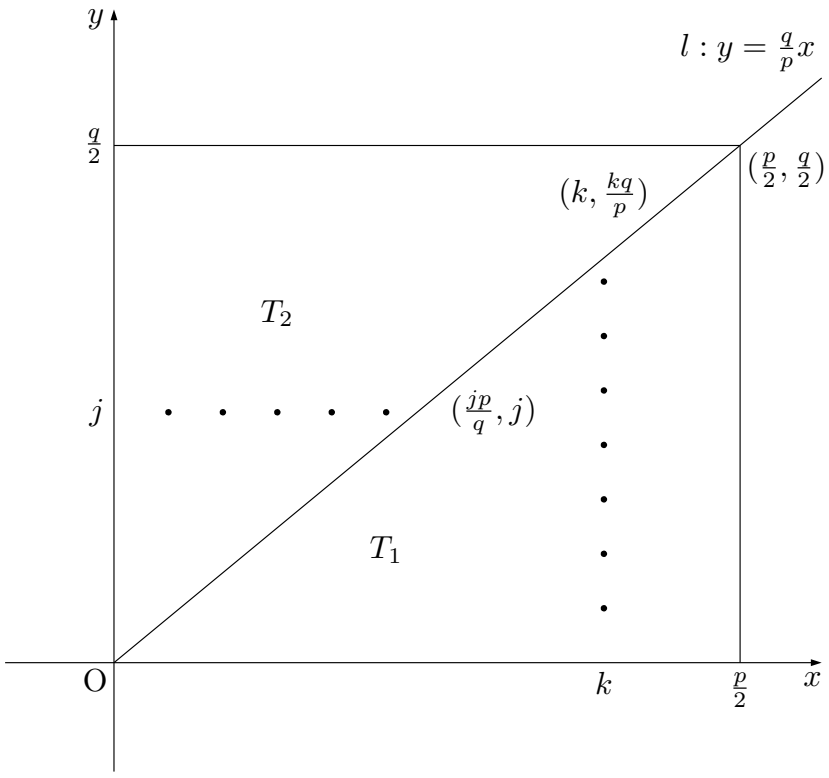
となる．

同様にして,T_2 に含まれる格子点の個数を求める．直線 $y=j\ \left(1\leq j\leq\dfrac{q-1}{2},\ j\in\mathbb{N}\right)$ で切ると，$0<x<\dfrac{jp}{q}$ を満たす整数 x の個数は $\left[\dfrac{jp}{q}\right]$ である．

したがって，T_2 に含まれる格子点の個数は

$$\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{jp}{q}\right]=\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right] \quad \cdots\cdots ④$$

となる．



D 内の格子点の総数は③と④の和

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right] + \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right]$$

で，これは②に等しいから

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right] + \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

が成り立つ.

これを①に使うと

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \left(-1\right)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

が成り立つ. □

- 明らかに T_1 と T_2 に含まれる格子点の個数は等しいので

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right] = \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right] = \frac{(p-1)(q-1)}{8} \tag{5.2}$$

が成り立つ.

- 定理 5.6.2，系 5.4.1(3)，系 5.5.1，系 5.4.1(2) より
  p, q を異なる奇数の素数とすれば，次のことが成り立つ．

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \left(-1\right)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{5.3}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{5.4}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{5.5}$$

$$\left(\frac{1}{p}\right) = 1 \tag{5.6}$$

(5.3) を平方剰余の相互法則，(5.4) をその第一補充法則，(5.5) を第二補充法則という．

(5.3) の両辺に $\left(\frac{p}{q}\right)$ をかけて，$\left(\frac{p}{q}\right)^2 = 1$ を用いると，次のことが言える．

p, q を異なる奇数の素数とすれば，

$$\left(\frac{q}{p}\right) = \left(-1\right)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) \tag{5.7}$$

が成り立つ．

系 5.6.1　p, q を異なる奇数の素数とすれば，

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \text{ または } q \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \text{ かつ } q \equiv 3 \pmod 4 \end{cases}$$

が成り立つ．

証明　$\frac{p-1}{2}\cdot\frac{q-1}{2}$ は整数 p, q がともに $4k+3$ という形である場合にのみ奇数になり，

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \left(-1\right)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1.$$

p, q の中に一つでも $4k+1$ という形であれば，$\frac{p-1}{2}\cdot\frac{q-1}{2}$ は偶数になり，

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \left(-1\right)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1.$$ □

例題 5.6.1　(1)　$\left(\dfrac{3}{53}\right)$ の値を計算せよ.

(2)　$\left(\dfrac{31}{641}\right)$ の値を計算せよ.

解答

(1)

$$\begin{aligned}\left(\frac{3}{53}\right) &= \left(-1\right)^{\frac{53-1}{2}\cdot\frac{3-1}{2}}\left(\frac{53}{3}\right)\\ &= \left(\frac{53}{3}\right)\\ &= \left(\frac{2}{3}\right) \qquad 53 \equiv 2 \pmod 3\\ &= (-1)^{\frac{3^2-1}{8}}\\ &= -1.\end{aligned}$$

(2)

$$\begin{aligned}\left(\frac{31}{641}\right) &= \left(-1\right)^{\frac{641-1}{2}\cdot\frac{31-1}{2}}\left(\frac{641}{31}\right)\\ &= \left(\frac{641}{31}\right)\\ &= \left(\frac{21}{31}\right) \qquad 641 \equiv 21 \pmod{31}\\ &= \left(\frac{3}{31}\right)\left(\frac{7}{31}\right) \qquad 21 = 3\cdot 7\end{aligned}$$

となるので, $\left(\dfrac{3}{31}\right)$ と $\left(\dfrac{7}{31}\right)$ を計算する.

$$\begin{aligned}\left(\frac{3}{31}\right) &= \left(-1\right)^{\frac{31-1}{2}\cdot\frac{3-1}{2}}\left(\frac{31}{3}\right)\\ &= -\left(\frac{31}{3}\right)\\ &= -\left(\frac{1}{3}\right) \qquad 31 \equiv 1 \pmod 3\\ &= -1.\end{aligned}$$

$$\begin{aligned}\left(\frac{7}{31}\right) &= \left(-1\right)^{\frac{31-1}{2}\cdot\frac{7-1}{2}}\left(\frac{31}{7}\right)\\ &= -\left(\frac{31}{7}\right)\\ &= -\left(\frac{3}{7}\right) \qquad 31 \equiv 3 \pmod 7\end{aligned}$$

$$\begin{aligned}
&= -\Big(-1\Big)^{\frac{7-1}{2}\cdot\frac{3-1}{2}}\left(\frac{7}{3}\right)\\
&= \left(\frac{7}{3}\right)\\
&= \left(\frac{1}{3}\right) \qquad\qquad 7 \equiv 1 \pmod 3\\
&= 1.
\end{aligned}$$

よって，$\left(\dfrac{31}{641}\right) = -1$. □

問題 5.6.1　(1)　$p \neq 3$ を奇数の素数とすれば，

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{12} \\ -1 & p \equiv \pm 5 \pmod{12} \end{cases}$$

が成り立つことを示せ．

(2)　$p \neq 3$ を奇数の素数とすれば，

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 6 \\ -1 & p \equiv -1 \pmod 6 \end{cases}$$

が成り立つことを示せ．

(3)　p を奇数の素数とすれば，

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 8 \text{ または } p \equiv 3 \pmod 8 \\ -1 & p \equiv 5 \pmod 8 \text{ または } p \equiv 7 \pmod 8 \end{cases}$$

が成り立つことを示せ．

問題 5.6.2　(Vietnam TST 2003)

任意の正の整数 n に対して，$2^n + 1$ は $8k - 1$ の形をした素数の約数をもたないことを証明せよ．

問題 5.6.3　(Gabriel Dospinescu)

任意の正の整数 n に対して，$2^{3^n} + 1$ は $8k + 3$ の形をした素数の約数を少なくとも n 個もつことを証明せよ．

問題 5.6.4　(Taiwan Mathematical Olympiad 1997)

ある正の整数 n に対して，$k = 2^{2^n} + 1$ とおく．このとき，k が素数となるための必要十分条件は，k が $3^{\frac{k-1}{2}} + 1$ の因数であることを証明せよ．

第6章

Vieta-Jumping

6.1 Vieta-Jumping

例題 6.1.1 (IMO 1988)

a と b は正の整数で， $ab+1$ は a^2+b^2 を割り切るものとする．このとき， $\dfrac{a^2+b^2}{ab+1}$ は平方数であることを示せ．

解答 a と b は正の整数で， $ab+1$ は a^2+b^2 を割り切るものとする．

$$k=\frac{a^2+b^2}{ab+1}$$

とおくと，k は正の整数であるが，平方数となることを証明しなければならない．

k を固定して，$k=\dfrac{a^2+b^2}{ab+1}$ を満たすすべての正の整数 a,b を考察する．

$$S(k)=\left\{(a,\,b):a,\,b\in\mathbb{N},\ \frac{a^2+b^2}{ab+1}=k\right\}$$

とおき，k が平方数でない $S(k)$ が存在したと仮定して矛盾が生じることを示す．

$S(k)$ の要素の中で $a+b$ が最小となるものが存在するから，これを $(A,B)\in S(k)$ とする．

$(A,B)\in S(k)$ から $\dfrac{A^2+B^2}{AB+1}=k$ が成り立つ．対称性から，$A\geq B$ と仮定できる．

ここで，方程式 $\dfrac{x^2+B^2}{xB+1}=k$ すなわち，2 次方程式

$$x^2-kBx+B^2-k=0 \qquad \cdots\cdots ①$$

を考える．

$x=A$ は①の解であるから，他の解を a_1 とすると

$$A+a_1=kB,\quad Aa_1=B^2-k \qquad \cdots\cdots ②$$

が成り立つ.

◎ a_1 は正の整数である.

②から $a_1 = kB - A$ は整数である.

次に $a_1 > 0$ を示す.

$a_1 = 0$ だとすると，②から $k = B^2$ で k が平方数となり，k は平方数でないことに矛盾する．よって $a_1 \neq 0$ である.

もしも $a_1 < 0$ だとする．$a_1^2 - kBa_1 + B^2 - k = 0$ が成り立つことを用いると

$$0 = a_1^2 - kBa_1 + B^2 - k \geq a_1^2 + k + B^2 - k = a_1^2 + B^2 > 0$$

となり矛盾が生じる.

したがって，$a_1 > 0$ が言えて，a_1 は正の整数である.

◎ $(a_1, B) \in S(k)$.

$a_1, B \in \mathbb{N}$ で $a_1^2 - kBa_1 + B^2 - k = 0$ から

$$\frac{a_1^2 + B^2}{a_1 B + 1} = k$$

が成り立つので，$(a_1, B) \in S(k)$ が言える.

◎ $a_1 < A$.

②と $A \geq B$, $k > 0$ から $a_1 = \dfrac{B^2 - k}{A} < \dfrac{A^2}{A} = A$.

よって，$a_1 + B < A + B$ で $(a_1, B) \in S(k)$ だから，$S(k)$ における $A + B$ の最小性に矛盾する.

したがって，k が平方数でないような $S(k)$ は存在しない. □

例題 6.1.2 (CRUX, Problem 1420)

a, b, c は正の整数で， $0 < a^2 + b^2 - abc \leq c$ を満たすものとする．
このとき， $a^2 + b^2 - abc$ は平方数であることを示せ．

解答 a, b, c は正の整数で， $0 < a^2 + b^2 - abc \leq c$ を満たすものとする．

$k = a^2 + b^2 - abc$ とおくと，k は $0 < k \leq c$ を満たす正の整数であるが，平方数となることを証明しなければならない．

いま，c と k $(0 < k \leq c)$ を固定して

$$S(c, k) = \left\{(a,\, b) : a,\, b \in \mathbb{N},\ \ a^2 + b^2 - abc = k\right\}$$

とおき，k が平方数でない $S(c, k)$ が存在したと仮定して矛盾が生じることを示す．

$S(c, k)$ の要素の中で $a + b$ が最小となるものが存在するから，これを $(A, B) \in S(c, k)$ とする．

$(A, B) \in S(c, k)$ から $A^2 + B^2 - ABc = k$ が成り立つ．対称性から，$A \geq B$ と仮定できる．

ここで，2 次方程式 $x^2 + B^2 - xBc = k$ すなわち

$$x^2 - xBc + B^2 - k = 0 \qquad \cdots\cdots ①$$

を考える．$x = A$ は①の解であるから，他の解を a_1 とすると

$$A + a_1 = Bc, \quad Aa_1 = B^2 - k \qquad \cdots\cdots ②$$

が成り立つ．

◎ a_1 は正の整数である．

②から $a_1 = Bc - A$ は整数である．

次に $a_1 > 0$ を示す．

$a_1 = 0$ だとすると，②から $k = B^2$ で k が平方数となり，k は平方数でないことに矛盾する．よって $a_1 \neq 0$ である．

もしも $a_1 < 0$ だとする．$a_1^2 - Bca_1 + B^2 - k = 0$ が成り立つことを用いると

$$k = a_1^2 - Bca_1 + B^2 \geq a_1^2 + Bc + B^2 > c$$

となり $k \leq c$ に矛盾する．

したがって，$a_1 > 0$ が言えて，a_1 は正の整数である．

◎ $(a_1, B) \in S(k)$.

◎ $a_1 < A$.

②と $A \geq B,\ k > 0$ から $a_1 = \dfrac{B^2 - k}{A} < \dfrac{A^2}{A} = A.$

よって，$a_1 + B < A + B$ で $(a_1, B) \in S(k)$ だから，$S(c,k)$ における $A+B$ の最小性に矛盾する．
したがって，k が平方数でないような $S(c,k)$ は存在しない．　□

- CRUX の問題は IMO 1998 の問題の一般化になっている．
  CRUX の問題の不等式 $0 < a^2 + b^2 - abc \leq c$ を等式 $a^2 + b^2 - abc = c$ にしたものが IMO の問題である．

例題 6.1.3 a と b は正の整数で， ab は a^2+b^2+1 を割り切るものとする．

このとき， $\dfrac{a^2+b^2+1}{ab}=3$ であることを示せ．

解答 a と b は正の整数で， ab は a^2+b^2+1 を割り切るものとする．

$$k=\frac{a^2+b^2+1}{ab}$$

とおくと，k は正の整数であるが，$k=3$ となることを証明しなければならない．

k を固定して，$k=\dfrac{a^2+b^2+1}{ab}$ を満たすすべての正の整数 a,b を考察する．

$$S(k)=\left\{(a,\,b):a,\,b\in\mathbb{N},\ \frac{a^2+b^2+1}{ab}=k\right\}$$

とおき，$k\neq 3$ であるような $S(k)$ が存在したと仮定して矛盾が生じることを示す．

$S(k)$ の要素の中で $a+b$ が最小となるものが存在するから，これを $(A,B)\in S(k)$ とする．

$(A,B)\in S(k)$ から $\dfrac{A^2+B^2+1}{AB}=k$ が成り立つ．対称性から，$A\geq B$ と仮定できる．

ここで，方程式 $\dfrac{x^2+B^2+1}{xB}=k$ すなわち，2 次方程式

$$x^2-kBx+B^2+1=0 \qquad \cdots\cdots①$$

を考える．

$x=A$ は①の解であるから，他の解を a_1 とすると

$$A+a_1=kB,\quad Aa_1=B^2+1 \qquad \cdots\cdots②$$

が成り立つ．

◎ a_1 は正の整数である．

②から $a_1=kB-A$ は整数である．

次に $a_1>0$ を示す．

②から $a_1=\dfrac{B^2+1}{A}>0$.

したがって，$a_1>0$ が言えて，a_1 は正の整数である．

◎ $(a_1,B)\in S(k)$.

$a_1,B\in\mathbb{N}$ で $a_1^2-kBa_1+B^2+1=0$ から

$$\frac{a_1^2+B^2}{a_1B}=k$$

が成り立つので，$(a_1,B)\in S(k)$ が言える．

◎ $A = B$.

$A > B$ だと仮定すると，$A \geq B + 1$ が成り立つ．

②から

$$a_1 = \frac{B^2 + 1}{A} \leq \frac{(A-1)^2 + 1}{A} = A - 2 + \frac{2}{A} < A.$$

よって，$a_1 + B < A + B$ で $(a_1, B) \in S(k)$ だから，$S(k)$ における $A + B$ の最小性に矛盾する．

したがって，$A = B$ でなければならない．

$\dfrac{A^2 + B^2 + 1}{AB} = k$ に $B = A$ を代入すると，

$$k = \frac{2A^2 + 1}{A^2} = 2 + \frac{1}{A^2}.$$

この式から，$\dfrac{1}{A^2}$ は整数でなければならないから，$A = 1$ すなわち，$k = 3$ となり $k \neq 3$ に矛盾する．

したがって，$k \neq 3$ であるような $S(k)$ は存在しない．　□

例題 6.1.4 a, b は $ab-1 \neq 1$ を満たす正の整数で， $ab-1$ は a^2+b^2 を割り切るものとする．このとき， $\dfrac{a^2+b^2}{ab-1} = 5$ であることを示せ．

解答 a, b は $ab-1 \neq 1$ を満たす正の整数で， $ab-1$ は a^2+b^2 を割り切るものとする．

$$k = \frac{a^2+b^2}{ab-1}$$

とおくと，k は正の整数であるが，$k=5$ となることを証明しなければならない．

k を固定して，$k = \dfrac{a^2+b^2}{ab-1}$ を満たすすべての正の整数 a, b を考察する．

$$S(k) = \left\{ (a,\, b) : a,\, b \in \mathbb{N},\ \frac{a^2+b^2}{ab-1} = k \right\}$$

とおき，$k \neq 5$ であるような $S(k)$ が存在したと仮定して矛盾が生じることを示す．

$S(k)$ の要素の中で $a+b$ が最小となるものが存在するから，これを $(A, B) \in S(k)$ とする．

$(A, B) \in S(k)$ から $\dfrac{A^2+B^2}{AB-1} = k$ が成り立つ．対称性から，$A \geq B$ と仮定できる．

ここで，方程式 $\dfrac{x^2+B^2}{xB-1} = k$ すなわち，2 次方程式

$$x^2 - kBx + B^2 + k = 0 \qquad \left(x \neq \frac{1}{B}\right) \qquad \cdots\cdots ①$$

を考える．$x = \dfrac{1}{B}$ のとき，

$$x^2 - kBx + B^2 + k = \left(\frac{1}{B}\right)^2 - kB \cdot \frac{1}{B} + B^2 + k = B^2 + \frac{1}{B^2} > 0$$

となり，$x = \dfrac{1}{B}$ は $x^2 - kBx + B^2 + k = 0$ の解にならないから，①のかわりに 2 次方程式

$$x^2 - kBx + B^2 + k = 0 \qquad \cdots\cdots ②$$

を考えてよい．

$x = A$ は②の解であるから，他の解を a_1 とすると

$$A + a_1 = kB, \quad Aa_1 = B^2 + k \qquad \cdots\cdots ③$$

が成り立つ．

◎ a_1 は正の整数である．

③から $a_1 = kB - A$ は整数である．

次に $a_1 > 0$ を示す．

③から $a_1 = \dfrac{B^2 + k}{A} > 0$.

したがって，$a_1 > 0$ が言えて，a_1 は正の整数である．

◎ $(a_1, B) \in S(k)$.

$a_1, B \in \mathbb{N}$ で $a_1^2 - kBa_1 + B^2 + k = 0$ から

$$\frac{a_1^2 + B^2}{a_1 B - 1} = k$$

が成り立つので，$(a_1, B) \in S(k)$ が言える．

◎ $A = B + 1$.

$(a_1, B) \in S(k)$ と $S(k)$ における $A + B$ の最小性から $a_1 \geq A$ でなければならない．

$a_1 = \dfrac{B^2 + k}{A}$ を $a_1 \geq A$ に代入すると $\dfrac{B^2 + k}{A} \geq A$ すなわち $B^2 + k \geq A^2$ と変形できる．

この不等式 $B^2 + k \geq A^2$ に $k = \dfrac{A^2 + B^2}{AB - 1}$ を代入すると

$$B^2 + \frac{A^2 + B^2}{AB - 1} \geq A^2.$$

$AB - 1 (> 0)$ を両辺にかけると

$$B^2(AB - 1) + A^2 + B^2 \geq A^2(AB - 1) \text{ から } 2A^2 + AB^3 \geq A^3 B.$$

A で両辺を割ると

$$2A + B^3 \geq A^2 B.$$

$A = B + l$ $(l \in \mathbb{N}_0)$ とおき，上の不等式に代入して変形する．

$2(B + l) + B^3 \geq (B + l)^2 B$ から

$$2B + 2l \geq 2lB^2 + l^2 B \qquad \cdots\cdots ④$$

もしも $l \geq 2$ だとすると

$$2lB^2 + l^2 B \geq 2l + 4B > 2l + 2B$$

となり④に矛盾する．

よって，$l = 0$ または $l = 1$ となる．

$l = 0$ の場合，$A = B$ で

$$k = \frac{A^2 + B^2}{AB - 1} = \frac{2A^2}{A^2 - 1} = 2 + \frac{2}{A^2 - 1}.$$

$A \geq 2$ だから $A^2 - 1 \geq 3$ で，$A^2 - 1$ は 2 の約数にならないから，k は整数にならず適さない．

よって，$l = 1$ で $A = B + 1$ となる．

$l = 1$ を④に代入すると $2B + 2 \geq 2B^2 + B$ から

$$2B^2 \leq B + 2.$$

$B \geq 2$ だと $2B^2 \geq 4B > B + 2$ だから $2B^2 \leq B + 2$ を満たさない．よって，$B = 1$.

$B = 1$ のとき $A = 2$ で $k = \dfrac{A^2 + B^2}{AB - 1} = \dfrac{2^2 + 1^2}{2 \cdot 1 - 1} = 5$ となり $k \neq 5$ に矛盾する．

したがって，$k \neq 5$ であるような $S(k)$ は存在しない． □

例題 6.1.5 (IMO 2007)

a と b は正の整数とする．

$4ab-1$ が $\left(4a^2-1\right)^2$ を割り切るならば，$a=b$ であることを示せ．

解答 $(b, 4ab-1)=(b, 4ab-1-4ab)=(b,-1)=(b,1)=1$ なので

$$4ab-1 \mid \left(4a^2-1\right)^2 \iff 4ab-1 \mid b^2\left(4a^2-1\right)^2.$$

$\bmod (4ab-1)$ で考えると

$$\begin{aligned} 0 \equiv b^2\left(4a^2-1\right)^2 &\equiv 16a^4b^2-8a^2b^2+b^2 \\ &\equiv 16a^2b^2\cdot a^2-4ab\cdot 2ab+b^2 \\ &\equiv (4ab)^2\cdot a^2-4ab\cdot 2ab+b^2 \\ &\equiv 1^2\cdot a^2-1\cdot 2ab+b^2 \\ &\equiv (a-b)^2 \pmod{4ab-1}. \end{aligned}$$

a, b は正の整数で，$4ab-1$ が $(a-b)^2$ を割り切るものとする．

$$k=\frac{(a-b)^2}{4ab-1}$$

とおくと，k は非負の整数であるが，$k=0$ となることを証明しなければならない．

k を固定して，$k=\dfrac{(a-b)^2}{4ab-1}$ を満たすすべての正の整数 a, b を考察する．

$$S(k)=\left\{(a,\, b) : a,\, b \in \mathbb{N},\ \frac{(a-b)^2}{4ab-1}=k\right\}$$

とおき，$k \neq 0$ であるような $S(k)$ が存在したと仮定して矛盾が生じることを示す．

$S(k)$ の要素の中で $a+b$ が最小となるものが存在するから，これを $(A, B) \in S(k)$ とする．

$(A, B) \in S(k)$ から $\dfrac{(A-B)^2}{4AB-1}=k$ が成り立つ．対称性から，$A \geq B$ と仮定できる．

$k \neq 0$ であるから，$A>B$ となる．ここで，方程式 $\dfrac{(x-B)^2}{4xB-1}=k$ すなわち，2 次方程式

$$(x-B)^2=k(4Bx-1) \quad \left(x \neq \frac{1}{4B}\right)$$

を変形した

$$x^2-(2B+4kB)x+B^2+k=0 \quad \left(x \neq \frac{1}{4B}\right) \qquad \cdots\cdots ①$$

を考える．$x=\dfrac{1}{4B}$ のとき，

$$(x-B)^2-k(4Bx-1)=\left(\frac{1}{4B}-B\right)^2=\left(\frac{1-4B^2}{4B}\right)^2 \neq 0$$

であるから，$(x-B)^2=k(4Bx-1)$ は $x=\dfrac{1}{4B}$ を解にもたないから①のかわりに 2 次方程式

$$x^2-(2B+4kB)x+B^2+k=0 \qquad \cdots\cdots ②$$

を考えてよい.

$x=A$ は②の解であるから，他の解を a_1 とすると

$$A+a_1=2B+4kB,\quad Aa_1=B^2+k \qquad \cdots\cdots ③$$

が成り立つ.

◎ a_1 は正の整数である.

③から $a_1=2B+4kB-A$ は整数である.

次に $a_1>0$ を示す.

③から $a_1=\dfrac{B^2+k}{A}>0$.

したがって，$a_1>0$ が言えて，a_1 は正の整数である.

◎ $(a_1,B)\in S(k)$.

$a_1,B\in\mathbb{N}$ で $a_1^2-(2B+4kB)a_1+B^2+k=0$ から

$$\frac{(a_1-B)^2}{4a_1B-1}=k$$

が成り立つので，$(a_1,B)\in S(k)$ が言える.

$(a_1,B)\in S(k)$ と $S(k)$ における $A+B$ の最小性から $a_1\geq A$ でなければならない.

$a_1=\dfrac{B^2+k}{A}$ を $a_1\geq A$ に代入すると $\dfrac{B^2+k}{A}\geq A$ すなわち $k\geq A^2-B^2$ と変形できる.

この不等式 $k\geq A^2-B^2$ に $k=\dfrac{(A-B)^2}{4AB-1}$ を代入すると

$$\frac{(A-B)^2}{4AB-1}\geq A^2-B^2.$$

$A>B$ だから両辺を $A-B(>0)$ で割ると

$$\frac{A-B}{4AB-1}\geq A+B.$$

両辺に $4AB-1(>0)$ をかけると

$$A-B\geq(A+B)(4AB-1). \qquad \cdots\cdots ④$$

ところで

$$(A+B)(4AB-1) \geq (A+B)(4\cdot 2\cdot 1-1) = 7(A+B) > A+B > A-B$$

であるから，④に矛盾する．

したがって，$k \neq 0$ であるような $S(k)$ は存在しない． □

- Vieta-Jumping が使えるとすれば，4 次式 $(4a^2-1)^2$ を a と b の 2 次の対称式にしなければならないので，$(a-b)^2 \equiv 0 \pmod{4ab-1}$ を導いた．

例題 6.1.6 (Romania 2005)

a, b, m, n は正の整数とする．

$$a^m b^n = (a+b)^2 + 1$$

を満たす (a, b, m, n) をすべて求めよ．

解答 $a^m b^n = (a+b)^2 + 1$ の両辺を ab で割ると

$$a^{m-1}b^{n-1} = \frac{(a+b)^2+1}{ab} = \frac{a^2+b^2+1}{ab} + 2. \qquad \cdots\cdots ①$$

これから，$\dfrac{a^2+b^2+1}{ab}$ は整数となる．例題 6.1.3 より

$$\frac{a^2+b^2+1}{ab} = 3 \qquad \cdots\cdots ②$$

となる．このとき①は

$$a^{m-1}b^{n-1} = 5 \qquad \cdots\cdots ③$$

となる．

③から $a = 5$ または $b = 5$ であることがわかる．

(i) $a = 5$ のとき②に代入すると，$b^2 - 15b + 26 = 0$. $(b-2)(b-13) = 0$ から $b \in \left\{2,\ 13\right\}$.
よって，③から $m - 1 = 1, n - 1 = 0$ でなければならない．
したがって，$(a, b, m, n) = (5, 2, 2, 1), (5, 13, 2, 1)$.

(ii) $b = 5$ のときもと同様にして，$(a, b, m, n) = (2, 5, 1, 2), (13, 5, 1, 2)$.

(i)，(ii) から解は

$$(a, b, m, n) = (5, 2, 2, 1), (5, 13, 2, 1), (2, 5, 1, 2), (13, 5, 1, 2). \qquad \square$$

6.2 ペルの方程式

例題 6.1.3 にあらわれた

$$\frac{a^2+b^2+1}{ab}=3$$

を満たす正の整数をすべて求めるには，ペル方程式の知識が必要になる．なぜならば，$a^2-3ab+b^2+1=0$ を $(2a-3b)^2-5b^2=-4$ 変形すると，$x^2-5y^2=-4$ の整数解を求めなければならないからである．

ペル方程式は，$x^2-Dy^2=1$ の形をした方程式で，D は平方数ではない正の整数とする．

定理 6.2.1 D は平方数ではない正の整数とする．

(1) ペル方程式

$$x^2-Dy^2=1 \tag{6.1}$$

は正の整数解をもつ．

(2) (6.1) を満足する正の整数の組 (x,y) なかで，x が最小のものを (x_1,y_1) とすれば，(6.1) のすべての正の整数解 (x_n,y_n) は

$$x_n+y_n\sqrt{D}=\left(x_1+y_1\sqrt{D}\right)^n \qquad (n=1,2,\dots)$$

から得られる．

定理 6.2.1 を証明するのに，次のディリクレの近似定理を使用する．

定理 6.2.2 α が正の無理数のとき，

$$|x-\alpha y|<\frac{1}{y}$$

を満たす正の整数の組 (x,y) が無数に存在する．

証明 n を $n>\dfrac{1}{\alpha}$ を満たす任意の正の整数とし，$[0,1)$ を n 個の区間

$$\left[0,\frac{1}{n}\right),\left[\frac{1}{n},\frac{2}{n}\right),\dots,\left[\frac{n-1}{n},1\right) \qquad \cdots\cdots ①$$

に分割する．

$s=0,1,\dots,n$ に対して

$$0\le \alpha s-[\alpha s]<1$$

が成り立つから，$n+1$ 個の $\alpha\cdot 0-[\alpha\cdot 0],\alpha\cdot 1-[\alpha\cdot 1],\ldots,\alpha\cdot n-[\alpha\cdot n]$ は n 個の区間①のどれかに属するから，ある区間 $\left[\dfrac{i-1}{n},\dfrac{i}{n}\right)$, $i\in\left\{1,2,\ldots,n\right\}$ には 2 つ以上の $\alpha s-[\alpha s]$ が属する．これを，$\alpha s_1-[\alpha s_1],\alpha s_2-[\alpha s_2]$ $(s_1>s_2)$ とおくと

$$|(\alpha s_1-[\alpha s_1])-(\alpha s_2-[\alpha s_2])|<\frac{1}{n}\ \text{ すなわち }\ |\alpha(s_1-s_2)-([\alpha s_1]-[\alpha s_2])|<\frac{1}{n}.$$

$s_1>s_2$ のときは，$y_1=s_1-s_2(>0), x_1=[\alpha s_1]-[\alpha s_2](\geq 0)$ とおけば，

$$|x_1-\alpha y_1|<\frac{1}{n}.$$

$x_1=[\alpha s_1]-[\alpha s_2]=0$ だとすると，$\dfrac{1}{n}>|x_1-\alpha y_1|=\alpha y_1\geq\alpha$ から $n<\dfrac{1}{\alpha}$ となり，$n>\dfrac{1}{\alpha}$ に矛盾する．したがって，$x_1>0$ である．

また，$0<y_1\leq n$ が成り立つ．

以上のことから，$n>\dfrac{1}{\alpha}$ を満たす正の整数 n に対して，

$$|x_1-\alpha y_1|<\frac{1}{n}\qquad\cdots\cdots②$$

を満たす正の整数 $x_1,y_1,(0<y_1\leq n)$ が存在することがわかった．

$0<y_1\leq n$ から，$\dfrac{1}{n}\leq\dfrac{1}{y_1}$ なので，②から

$$|x_1-\alpha y_1|<\frac{1}{y_1}$$

を満たす正の整数 $x_1,y_1,(0<y_1\leq n)$ が存在することがわかった．

n を大きくとるたびに，$|x-\alpha y|<\dfrac{1}{n}$ を満たす新たな正の整数 x と y が得られる．なぜならば，正の整数 x と y を定めたとき，不等式 $(0<)\,|x-\alpha y|<\dfrac{1}{n}$ は $n<\dfrac{1}{|x-\alpha y|}$ でないと成り立たないからである．

$n_1>\dfrac{1}{\alpha}$ を満たす正の整数 n_1 に対して，

$$|x_1-\alpha y_1|<\frac{1}{n_1}\left(\leq\frac{1}{y_1}\right)$$

を満たす正の整数の組 (x_1,y_1) $(0<y_1\leq n_1)$ をとる．

$n_2>\dfrac{1}{|x_1-\alpha y_1|}>n_1$ となる正の整数 n_2 に対して

$$|x_2-\alpha y_2|<\frac{1}{n_2}\left(\leq\frac{1}{y_2}\right)$$

を満たす正の整数の組 (x_2,y_2) $(0<y_2\leq n_2)$ をとる．

すると，$|x_2-\alpha y_2|<\dfrac{1}{n_2}<|x_1-\alpha y_1|$ より $(0<)\,|x_2-\alpha y_2|<|x_1-\alpha y_1|$ である．

以下，同様な操作を繰り返すことにより，

$$|x-\alpha y|<\frac{1}{y}$$

を満たす正の整数の組 (x,y) が無数に存在することがわかる．　□

定理 6.2.1 の証明

(1) 定理 6.2.2 より

$$\left|x-y\sqrt{D}\right|<\frac{1}{y} \qquad \cdots\cdots ①$$

を満たす正の整数の組 (x,y) が無数に存在する．①から $x<y\sqrt{D}+\dfrac{1}{y}$ が成り立つから

$$x+y\sqrt{D}<2y\sqrt{D}+\frac{1}{y}.$$

この不等式と $\left|x-y\sqrt{D}\right|<\dfrac{1}{y}$ から

$$\left|x^2-Dy^2\right|<\left(2y\sqrt{D}+\frac{1}{y}\right)\cdot\frac{1}{y}=2\sqrt{D}+\frac{1}{y^2}\leq 2\sqrt{D}+1.$$

$T=\left[2\sqrt{D}+1\right]$ とおくと，x^2-Dy^2 の値は

$$-T,-T+1,\ldots,-1,0,1,\ldots,T-1,T$$

のどれかをとる．①を満たす正の整数の組 (x,y) は無数にあるから，$l=-T,-T+1,\ldots,-1,0,1,\ldots,T-1,T$ に対して，方程式 $x^2-Dy^2=l$ の少なくとも一つは正の整数解を無数にもつ．

$x^2-Dy^2=M,\ M\in\mathbb{Z},\ -T\leq M\leq T$ が正の整数解を無数にもつとする．$\sqrt{D}$ は無理数だから $M\neq 0$ である．

正の整数解の組を $(x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n),\ldots$ とし $x_i,y_i\ (i=1,2,\ldots,n,\ldots)$ を $|M|$ で割った余りを考える．$|M|$ で割った余りの組は $(A,B),0\leq A,B\leq|M|-1$ の M^2 個であるから，ある剰余の組 (A,B) に無数の (x_i,y_i) が存在する．よって，異なる 2 組の (x_j,y_j) と (x_k,y_k) が存在して，

$$x_k\equiv x_j \pmod{|M|},\ y_k\equiv y_j \pmod{|M|} \qquad \cdots\cdots ②$$

が成り立つ．

②から $x_ky_j\equiv x_jy_k \pmod{|M|}$ が成り立つから，

$$x_ky_j-x_jy_k=MY$$

を満たす整数 Y が存在する．

また，$x_j^2-Dy_j^2=M$, $x_k^2-Dy_k^2=M$ から $\left(x_j^2-Dy_j^2\right)\left(x_k^2-Dy_k^2\right)=M^2$ すなわち

$$(x_jx_k-Dy_jy_k)^2-D(x_ky_j-x_jy_k)^2=M^2 \qquad \cdots\cdots ③$$

$x_ky_j-x_jy_k=MY$ を使うと $(x_jx_k-Dy_jy_k)^2-D\cdot M^2Y^2=M^2$ が成り立つから，$x_jx_k-Dy_jy_k$ は M で割り切れる．

$$x_jx_k-Dy_jy_k=MX$$

を満たす整数 X が存在するから，これを $(x_jx_k-Dy_jy_k)^2-D\cdot M^2Y^2=M^2$ に代入すると

$$M^2X^2-M^2DY^2=M^2.$$

両辺を M^2 で割ると

$$X^2-DY^2=1.$$

X,Y は整数で，$X<0$ のときは $-X$，$Y<0$ のときは $-Y$ を考えることにより，$X^2-DY^2=1$ の整数解として (X,Y) $(X\geq 0, Y\geq 0)$ となるものがとれる．

$X^2-DY^2=1$ を変形した $X^2=DY^2+1\geq 1$ から $X\geq 1$ である．

もしも，$Y=0$ だとすると，$x_ky_j-x_jy_k=0$ から $x_k^2y_j^2=x_j^2y_k^2$.

この式に $x_j^2=Dy_j^2+M, x_k^2=Dy_k^2+M$ を代入すると，

$$\left(Dy_k^2+M\right)y_j^2=\left(Dy_j^2+M\right)y_k^2$$

から $My_j^2=My_k^2$ すなわち $y_j=y_k$ を得る．すると

$$x_j^2=Dy_j^2+M=Dy_k^2+M=x_k^2$$

から $x_j=x_k$ も成り立ち，$(x_j,y_j)=(x_k,y_k)$ となり $(x_j,y_j)\neq(x_k,y_k)$ に矛盾する．

よって，$Y\neq 0$ となり $Y\geq 1$ である．

これで，$x^2-Dy^2=1$ は正の整数解をもつことが証明された．

(2) (6.1) を満たす正の整数の組 (x,y) のうちで x が最小のものを (x_1,y_1) とし，(u,v) を (6.1) の任意の正の整数解とする．

$z=x_1+y_1\sqrt{D}$, $r=u+v\sqrt{D}$ とおくと，$r=z^k$ となる正の整数 k が存在することを示す．

$z>1$ であるから，$z,z^2,\ldots,z^n,\ldots$ は増加数列で，$\lim_{n\to\infty} z^n=\infty$ をみたしている．

したがって

$$z^k\leq r<z^{k+1} \qquad \cdots\cdots ④$$

を満たす正の整数 k が存在する．

$$z^k \leq r < z^{k+1} \iff k\log_{10} z \leq \log_{10} r < (k+1)\log_{10} z$$
$$\iff k \leq \frac{\log_{10} r}{\log_{10} z} < k+1$$

より，$k = \left[\dfrac{\log_{10} r}{\log_{10} z}\right]$ とすればよいことがわかる．

④の両辺を z^k で割って

$$1 \leq \frac{r}{z^k} < z \qquad \cdots\cdots ⑤$$

とする．

$n \geq 2$ のとき，二項定理[*1]を使うと

$$\begin{aligned}
&\left(x_1 + y_1\sqrt{D}\right)^n \\
&= \sum_{r=0}^{n} \binom{n}{r} x_1^{n-r} \left(y_1\sqrt{D}\right)^r \\
&= \sum_{\substack{r=0 \\ r:\text{偶数}}}^{n} \binom{n}{r} x_1^{n-r} \left(y_1\sqrt{D}\right)^r + \sum_{\substack{r=0 \\ r:\text{奇数}}}^{n} \binom{n}{r} x_1^{n-r} \left(y_1\sqrt{D}\right)^r \\
&= \sum_{r=0}^{[n/2]} \binom{n}{2r} x_1^{n-2r} \left(y_1\sqrt{D}\right)^{2r} + \sum_{r=0}^{[(n-1)/2]} \binom{n}{2r+1} x_1^{n-2r-1} \left(y_1\sqrt{D}\right)^{2r+1} \\
&= \sum_{r=0}^{[n/2]} \binom{n}{2r} x_1^{n-2r} y_1^{2r} D^r + \sum_{r=0}^{[(n-1)/2]} \binom{n}{2r+1} x_1^{n-2r-1} y_1^{2r+1} D^r\sqrt{D}
\end{aligned}$$

となる．正の整数の項と，$\sqrt{D}$ を含む項を別々にまとめて，

$$x_n = \sum_{r=0}^{[n/2]} \binom{n}{2r} x_1^{n-2r} y_1^{2r} D^r, \quad y_n = \sum_{r=0}^{[(n-1)/2]} \binom{n}{2r+1} x_1^{n-2r-1} y_1^{2r+1} D^r$$

とおくと，x_n, y_n は正の整数で

$$\left(x_1 + y_1\sqrt{D}\right)^n = x_n + y_n\sqrt{D} \qquad (n = 2, 3, \dots)$$

と表せる．$n = 1$ のときは明らかに成り立つから，

$$\left(x_1 + y_1\sqrt{D}\right)^n = x_n + y_n\sqrt{D} \qquad (n = 1, 2, 3, \dots)$$

を満たす正の整数 x_n, y_n が存在する．

[*1] 数学的帰納法を使う方法については後述．

同様にして，$n \geq 2$ のとき，二項定理を使うと

$$\begin{aligned}
&\left(x_1 - y_1\sqrt{D}\right)^n \\
&= \sum_{r=0}^{n} \binom{n}{r} x_1^{n-r} \left(-y_1\sqrt{D}\right)^r \\
&= \sum_{\substack{r=0 \\ r:\text{偶数}}}^{n} \binom{n}{r} x_1^{n-r} \left(-y_1\sqrt{D}\right)^r + \sum_{\substack{r=0 \\ r:\text{奇数}}}^{n} \binom{n}{r} x_1^{n-r} \left(-y_1\sqrt{D}\right)^r \\
&= \sum_{r=0}^{[n/2]} \binom{n}{2r} x_1^{n-2r} \left(-y_1\sqrt{D}\right)^{2r} + \sum_{r=0}^{[(n-1)/2]} \binom{n}{2r+1} x_1^{n-2r-1} \left(-y_1\sqrt{D}\right)^{2r+1} \\
&= \sum_{r=0}^{[n/2]} \binom{n}{2r} x_1^{n-2r} y_1^{2r} D^r - \sum_{r=0}^{[(n-1)/2]} \binom{n}{2r+1} x_1^{n-2r-1} y_1^{2r+1} D^r \sqrt{D} \\
&= x_n - y_n\sqrt{D}
\end{aligned}$$

となるから

$$\left(x_1 - y_1\sqrt{D}\right)^n = x_n - y_n\sqrt{D} \qquad (n = 2, 3, \dots)$$

と表せる．$n = 1$ のときは明らかに成り立つから，

$$\left(x_1 - y_1\sqrt{D}\right)^n = x_n - y_n\sqrt{D} \qquad (n = 1, 2, 3, \dots)$$

以上のことから

$$z^k = \left(x_1 + y_1\sqrt{D}\right)^k = x_k + y_k\sqrt{D} \qquad \cdots\cdots ⑥$$

$$\left(x_1 - y_1\sqrt{D}\right)^k = x_k - y_k\sqrt{D} \qquad \cdots\cdots ⑦$$

が得られる．⑥と⑦をかけあわせると

$$\begin{aligned}
\left(x_k + y_k\sqrt{D}\right)\left(x_k - y_k\sqrt{D}\right) &= \left(x_1 + y_1\sqrt{D}\right)^k \left(x_1 - y_1\sqrt{D}\right)^k \\
&= \left(x_1 + y_1\sqrt{D}\right)\left(x_1 - y_1\sqrt{D}\right)^k \\
&= \left(x_1^2 - Dy_1^2\right)^k \\
&= 1^k = 1
\end{aligned}$$

から

$$x_k^2 - Dy_k^2 = \left(x_k + y_k\sqrt{D}\right)\left(x_k - y_k\sqrt{D}\right) = 1.$$

これから，$\dfrac{1}{z^k} = x_k - y_k\sqrt{D}$ が成り立つので

$$\begin{aligned}\frac{r}{z^k} &= \left(u + v\sqrt{D}\right)\left(x_k - y_k\sqrt{D}\right)\\ &= (ux_k - Dvy_k) + (vx_k - uy_k)\sqrt{D}\end{aligned}$$

となるので，$s = ux_k - Dvy_k, t = vx_k - uy_k$ とおくと，$s, t \in \mathbb{Z}$ で，⑤より

$$1 \leq s + t\sqrt{D} < z \qquad \cdots\cdots ⑧$$

が成り立つ．

また，

$$\begin{aligned}s^2 - Dt^2 &= (ux_k - Dvy_k)^2 - D(vx_k - uy_k)^2\\ &= \left(x_k^2 - Dy_k^2\right)\left(u^2 - Dv^2\right)\\ &= 1 \cdot 1 = 1\end{aligned}$$

から

$$s^2 - Dt^2 = 1 \qquad \cdots\cdots ⑨$$

が成り立つ．

◎ $s = 1$ かつ $t = 0$ を示す．

⑨から $\left(s + t\sqrt{D}\right)\left(s - t\sqrt{D}\right) = 1$.

⑧から $s + t\sqrt{D} > 0$ だから，上の等式より $s - t\sqrt{D} > 0$ が言える．

よって，$2s = \left(s + t\sqrt{D}\right) + \left(s - t\sqrt{D}\right) > 0$ から，$s > 0$ すなわち $s \geq 1$ が言えた．

もしも $t < 0$ だとすると，⑧から $s + t\sqrt{D} \geq 1$ なので

$$1 = s^2 - Dt^2 = \left(s - t\sqrt{D}\right)\left(s + t\sqrt{D}\right) > \left(s + t\sqrt{D}\right)^2 \geq 1$$

と矛盾が生じる．

よって $t \geq 0$ である．

$t > 0$ だとすると，(s, t) は (6.1) の正整数解となるので，x_1 の最小性から，$s \geq x_1$ でなければならない．

このとき，

$$t^2 = \frac{s^2 - 1}{D} \geq \frac{x_1^2 - 1}{D} = y_1^2$$

から $t \geq y_1$ が成り立つ．

すると，$s + t\sqrt{D} \geq x_1 + y_1\sqrt{D} = z$ となり，⑧の $s + t\sqrt{D} < z$ に矛盾する．

よって，$t = 0$ でなければならず，このとき⑨より $s = 1$ となる．

$s=1$ かつ $t=0$ より，$\dfrac{r}{z^k}=s+t\sqrt{D}=1$ で，$u+v\sqrt{D}=r=z^k$ となる．　□

命題 6.2.1　D は平方数ではない正の整数，x_1,y_1 も正の整数とする．

正の整数 n に対して

$$\left(x_1+y_1\sqrt{D}\right)^n=a_n+b_n\sqrt{D},$$
$$\left(x_1-y_1\sqrt{D}\right)^n=a_n-b_n\sqrt{D}$$

を満たす正の整数 a_n,b_n が存在する．

証明　n に関する数学的帰納法で証明する．

(I) $n=1$ のときは，$a_1=x_1,b_1=y_1$ とおけば成り立つ．

(II) $n=m$ のとき成り立つと仮定すると

$$\left(x_1+y_1\sqrt{D}\right)^m=a_m+b_m\sqrt{D},\ \left(x_1-y_1\sqrt{D}\right)^m=a_m-b_m\sqrt{D}$$

を満たす正の整数 a_m,b_m が存在する．

$$\begin{aligned}\left(x_1+y_1\sqrt{D}\right)^{m+1}&=\left(x_1+y_1\sqrt{D}\right)^m\left(x_1+y_1\sqrt{D}\right)\\&=\left(a_m+b_m\sqrt{D}\right)\left(x_1+y_1\sqrt{D}\right)\\&=(x_1a_m+Db_m)+(y_1a_m+x_1b_m)\sqrt{D}\\\left(x_1-y_1\sqrt{D}\right)^{m+1}&=\left(x_1-y_1\sqrt{D}\right)^m\left(x_1-y_1\sqrt{D}\right)\\&=\left(a_m-b_m\sqrt{D}\right)\left(x_1-y_1\sqrt{D}\right)\\&=(x_1a_m+Db_m)-(y_1a_m+x_1b_m)\sqrt{D}\end{aligned}$$

から

$$a_{m+1}=x_1a_m+Db_m,\ b_{m+1}=y_1a_m+x_1b_m$$

とおくと，a_{m+1},b_{m+1} は正の整数で

$$\left(x_1+y_1\sqrt{D}\right)^{m+1}=a_{m+1}+b_{m+1}\sqrt{D},\ \left(x_1-y_1\sqrt{D}\right)^{m+1}=a_{m+1}-b_{m+1}\sqrt{D}$$

とかける．

よって，$n=m+1$ のときも成り立つ．

(III) (I)，(II) からすべての正の整数 n について成り立つ．　□

問題 6.2.1 整数 x, y が $x^2 - 2y^2 = 1$ を満たすとき，次の問いに答えよ．

(1) 整数 a, b, u, v が $\left(a + b\sqrt{2}\right)\left(x + y\sqrt{2}\right) = u + v\sqrt{2}$ を満たすとき，u, v を a, b, x, y で表せ．さらに $a^2 - 2b^2 = 1$ のときの $u^2 - 2v^2$ の値を求めよ．ともに答えのみでよい．

(2) $1 < x + y\sqrt{2} \leqq 3 + 2\sqrt{2}$ のとき，$x = 3, y = 2$ となることを示せ．

(3) 自然数 n に対して，$\left(3 + 2\sqrt{2}\right)^{n-1} < x + y\sqrt{2} \leqq \left(3 + 2\sqrt{2}\right)^n$ のとき，$x + y\sqrt{2} = \left(3 + 2\sqrt{2}\right)^n$ を示せ．

(2015 早稲田大・理工)

問題 6.2.2 $A = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$ とする．

（1） $\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$ で，$x^2 - 3y^2 = 1, x > 0, y \geqq 1$ ならば，

$x'^2 - 3y'^2 = 1, 0 \leqq y' < y$ が成立することを示せ．

（2） x, y が $x^2 - 3y^2 = 1$ を満たす自然数ならば，ある自然数 n をとると

$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = A^n \begin{pmatrix} x \\ y \end{pmatrix}$ となることを示せ． （1988 京都大）

同趣旨の問題が 1967 年にも出題されている．

問題 6.2.3 次の□の中に適当な数または式を入れよ．また (イ)〜(ホ) の「 」で囲まれた文章の理由を，最後の (イ)〜(ホ) の解答のところで述べよ．

方程式 $x^2 - 3y^2 = 1$ ……①

を満たす整数の組 (x, y) を求めることを考える（以下この方程式の整数解を単に解と略称する）．準備のために次のことを確かめておく．

(イ) 「a, b, c, d が整数であって，$a + b\sqrt{3} = c + d\sqrt{3}$ ならば，$a = c, b = d$ である．」

次に (x, y) が解であれば，$(x, -y), (-x, y), (-x, -y)$ も解であることは，方程式①により明らかであるから，(x, y) がともに負でない解を求めることが基本的である．それで，そのような解を求める手段として

$(2 + \sqrt{3})^n = x_n + y_n\sqrt{3}$ ……②

(x_n, y_n は負でない整数，$n = 0, 1, 2, \ldots$) とおく．そうすると (イ) によって

$x_0 = 1, y_0 = 0, x_1 = 2, y_1 = 1$ ……③

$x_2 = \square, y_2 = \square, x_3 = \square, y_3 = \square$ である．

一方，$(2 + \sqrt{3})^2$ と $(2 - \sqrt{3})^2, (2 + \sqrt{3})^3$ と $(2 - \sqrt{3})^3$ などを比較することに

よって，一般に

$$(2-\sqrt{3}\,)^n = x_n - y_n\sqrt{3},\ n = 0, 1, \cdots \qquad \cdots\cdots\cdots ④$$

であることがわかる．

② と④ と $(2+\sqrt{3}\,)(2-\sqrt{3}\,) = 1$ とを使って

$$1 = (2+\sqrt{3}\,)^n(2-\sqrt{3}\,)^n = {x_n}^2 - 3{y_n}^2$$

となるから，② で定まる (x_n, y_n) は方程式 ① の解であることがわかる．とくに，x, y の一方が 0 となるような負でない解は，明らかに $x = 1, y = 0$ で，それは③の (x_0, y_0) に外ならない．

次に (x_{n-1}, y_{n-1}) と (x_n, y_n) との関係を求めてみる $(n \geqq 1)$ ．

$$x_n + y_n\sqrt{3} = (2+\sqrt{3}\,)^n = (x_{n-1} + y_{n-1}\sqrt{3}\,)(2+\sqrt{3}\,) = \boxed{\qquad\qquad}$$

ゆえに，$x_n = \boxed{\quad}, y_n = \boxed{\quad}$

したがって，(x_0, y_0) から出発して，負でない解 (x_1, y_1)，(x_2, y_2)，$\ldots$，$(x_n, y_n), \ldots\ldots$ を順次求めて行くことができる．しかも $y_1 < y_2 < y_3 < \ldots$ である．

以上のことで負でない解を多数みつけたのであるが，これらで負でない解が尽くされているかどうかを次に吟味する．

いま任意の正の解 $(x, y), (x > 0, y > 0)$ をとると

$$(x + y\sqrt{3}\,)(2-\sqrt{3}\,) = (2x - 3y) + (2y - x)\sqrt{3}$$

(ロ)　「$x' = 2x - 3y, y' = 2y - x$ とおくとき，(x', y') も解である．」

(ハ)　「そして，$x > x' > 0, y > y' \geqq 0$ である．」

(ニ)　「それで，任意の正の解 (x, y) から出発して，(ロ) における (x', y') を求める操作を順次行うことによって，③に示す負でない解 (x_0, y_0) に達する．」

(ホ)　「したがって，任意の負でない解 (x, y) は式②によって定まる (x_n, y_n) $(n = 0, 1, 2, \ldots)$ のどれか 1 つである．」　（1967　京都大）

6.3 $x^2 - 5y^2 = -4$ の正の整数解

D は平方数ではない正の整数とする．

ペル方程式 $x^2 - Dy^2 = 1$ は正の整数解をもち，正の整数の組 (x, y) なかで，x が最小のものを (x_1, y_1) とすれば，$x^2 - Dy^2 = 1$ のすべての正の整数解 (x_n, y_n) は

$$x_n + y_n\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)^n \qquad (n = 1, 2, \dots)$$

から得られることがわかった．

ところで，方程式の右辺の値が 1 ではないとき整数解はどうなるのであろうか．$N \in \mathbb{N}$ として $x^2 - Dy^2 = N^2$ は無数に整数解をもとことは容易にわかる．それは，$x_n^2 - Dy_n^2 = 1$ から $(Nx_n)^2 - D(Ny_n)^2 = N^2$ が成り立つからである．$N = 2$ の場合を練習問題とした．

しかし，右辺の値が負のときは状況が変わる．$x^2 - 3y^2 = -1$ は整数解をもたないのである．これは，

$$\left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$$

で $x^2 \equiv -1 \pmod 3$ が整数解をもたないことからわかる．同様に，D が $4m + 3$ の形の素数のとき

$$\left(\frac{-1}{D}\right) = (-1)^{\frac{4m+3-1}{2}} = (-1)^{2m+1} = -1$$

で，$x^2 - Dy^2 = -1$ は整数解をもたない．

次の例題は $x^2 - 5y^2 = -4$ の整数解について考えている．

例題 6.3.1 $x^2 - 5y^2 = -4$ のすべての正の整数解 (x_n, y_n) は

$$\frac{x_n + y_n\sqrt{5}}{2} = \left(\frac{1 + \sqrt{5}}{2}\right)^n \qquad (n = 1, 2, \dots)$$

から得られることを示せ．

解答 $x^2 - 5y^2 = -4$ を満たす整数解 x, y の偶奇は一致する． $\cdots\cdots(*)$

なぜならば，x が偶数のとき，$x = 2l$ $(l \in \mathbb{Z})$ とおくと，$5y^2 = x^2 + 4 = 4(l^2 + 1)$ は 4 の倍数だから，y も偶数となる．

y が偶数のとき，$y = 2m$ $(m \in \mathbb{Z})$ とおくと，$x^2 = 5y^2 + 4 = 4(5m^2 + 1)$ は 4 の倍数だから，x も偶数となる．

よって，「x が偶数 $\Longleftrightarrow$ y が偶数」が成り立つから，x, y の偶奇は一致する．

$x^2 - 5y^2 = -4$ の x が最小の正の整数解は $(x_1, y_1) = (1, 1)$ で $x_1^2 - 5y_1^2 = -4$ を

$$\frac{x_1 + y_1\sqrt{5}}{2} \cdot \frac{x_1 - y_1\sqrt{5}}{2} = -1$$

と変形し，この両辺を $2n-1$ 乗すると

$$\left(\frac{x_1+y_1\sqrt{5}}{2}\right)^{2n-1}\cdot\left(\frac{x_1-y_1\sqrt{5}}{2}\right)^{2n-1}=-1$$

すなわち

$$\left(\frac{1+\sqrt{5}}{2}\right)^{2n-1}\cdot\left(\frac{1-\sqrt{5}}{2}\right)^{2n-1}=-1$$

が成り立っている．

n に関する数学的帰納法で

$$\frac{x_n+y_n\sqrt{5}}{2}=\left(\frac{1+\sqrt{5}}{2}\right)^{2n-1} \tag{6.2}$$

$$\frac{x_n-y_n\sqrt{5}}{2}=\left(\frac{1-\sqrt{5}}{2}\right)^{2n-1} \tag{6.3}$$

を満たす正の整数 x_n, y_n が存在することを示す．

(I) $n=1$ のとき，$(x_1,y_1)=(1,1)$ で

$$\frac{x_1+y_1\sqrt{5}}{2}=\frac{1+\sqrt{5}}{2},\ \frac{x_1-y_1\sqrt{5}}{2}=\frac{1-\sqrt{5}}{2}$$

は成り立つ．

(II) $n=m$ のとき成り立つと仮定すると，

$$\frac{x_m+y_m\sqrt{5}}{2}=\left(\frac{1+\sqrt{5}}{2}\right)^{2m-1},\ \frac{x_m-y_m\sqrt{5}}{2}=\left(\frac{1-\sqrt{5}}{2}\right)^{2m-1}$$

を満たす正の整数 x_m, y_m が存在する．

$$\begin{aligned}\left(\frac{1+\sqrt{5}}{2}\right)^{2m+1}&=\left(\frac{1+\sqrt{5}}{2}\right)^{2m-1}\left(\frac{1+\sqrt{5}}{2}\right)^{2}\\&=\frac{x_m+y_m\sqrt{5}}{2}\cdot\frac{3+\sqrt{5}}{2}\\&=\frac{3x_m+5y_m+(x_m+3y_m)\sqrt{5}}{4},\\\left(\frac{1-\sqrt{5}}{2}\right)^{2m+1}&=\left(\frac{1-\sqrt{5}}{2}\right)^{2m-1}\left(\frac{1-\sqrt{5}}{2}\right)^{2}\\&=\frac{x_m-y_m\sqrt{5}}{2}\cdot\frac{3-\sqrt{5}}{2}\\&=\frac{3x_m+5y_m-(x_m+3y_m)\sqrt{5}}{4}\end{aligned}$$

となるから

$$x_{m+1} = \frac{3x_m + 5y_m}{2},\ y_{m+1} = \frac{x_m + 3y_m}{2}$$

とおくと，

$$\frac{x_{m+1} + y_{m+1}\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2}\right)^{2m+1},\ \frac{x_{m+1} - y_{m+1}\sqrt{5}}{2} = \left(\frac{1-\sqrt{5}}{2}\right)^{2m+1}$$

が成り立つ．

$(*)$ より正の整数 x_m と y_m の偶奇が一致するから，

$$x_{m+1} = \frac{3x_m + 5y_m}{2},\ y_{m+1} = \frac{x_m + 3y_m}{2}$$

は正の整数である．

よって，$n = m + 1$ のときも成り立つ．

(III) (I)，(II) からすべての正の整数 n について成り立つ．

(6.2)，(6.3) の辺々をかけると

$$x_n^2 - 5y_n^2 = -4 \tag{6.4}$$

が得られる．

◎ (u, v) を $x^2 - 5y^2 = -4$ を満たす任意の正の整数解とすると，

$$\frac{u + v\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2}\right)^{2k-1}$$

となる正の整数 k が存在することを示す．

$z = \dfrac{1+\sqrt{5}}{2}$, $r = \dfrac{u + v\sqrt{5}}{2}$ とおく．

$z > 1$ であるから，$z, z^2, \ldots, z^n, \ldots$ は増加数列で，$\lim\limits_{n\to\infty} z^n = \infty$ をみたしている．

したがって

$$z^{2k-1} \leq r < z^{2k+1}$$

を満たす正の整数 k が存在する．

$$\begin{aligned} z^{2k-1} \leq r < z^{2k+1} &\iff (2k-1)\log_{10} z \leq \log_{10} r < (2k+1)\log_{10} z \\ &\iff 2k \leq \frac{\log_{10} r}{\log_{10} z} + 1 < 2(k+1) \\ &\iff k \leq \frac{1}{2}\left(\frac{\log_{10} r}{\log_{10} z} + 1\right) < k+1 \end{aligned}$$

より，$k = \left[\dfrac{1}{2}\left(\dfrac{\log_{10} r}{\log_{10} z} + 1\right)\right]$ とすればよいことがわかる．

z^{2k-1} で割ると $1 \leq \dfrac{r}{z^{2k-1}} \leq z^2 = \dfrac{3+\sqrt{5}}{2}$.

(6.2) から $z^{2k-1} = \dfrac{x_k + y_k\sqrt{5}}{2}$ が成り立つので

$$\frac{1}{z^{2k-1}} = \frac{2}{x_k + y_k\sqrt{5}} = \frac{2\left(x_k - y_k\sqrt{5}\right)}{x_k^2 - 5y_k^2} = \frac{x_k - y_k\sqrt{5}}{-2}.$$

これから,

$$\begin{aligned}\frac{r}{z^{2k-1}} &= \frac{u+v\sqrt{5}}{2}\,\frac{-x_k+y_k\sqrt{5}}{2} \\ &= \frac{(-ux_k+5vy_k)+(-vx_k+uy_k)\sqrt{5}}{4}\end{aligned}$$

となるので，$s = \dfrac{-ux_k+5vy_k}{4}, t = \dfrac{-vx_k+uy_k}{4}$ とおくと,

$$1 \leq s+t\sqrt{5} < \frac{3+\sqrt{5}}{2} \qquad \cdots\cdots ①$$

が成り立つ.

また,

$$\begin{aligned}s^2-5t^2 &= \frac{1}{16}\left((-ux_k+5vy_k)^2 - 5(-vx_k+uy_k)^2\right) \\ &= \frac{1}{16}\left(x_k^2-5y_k^2\right)\left(u^2-5v^2\right) \\ &= \frac{1}{16}\cdot(-4)\cdot(-4) = 1\end{aligned}$$

から

$$s^2-5t^2 = 1 \qquad \cdots\cdots ②$$

が成り立つ.

- $s=1$ かつ $t=0$ を示す.

  ②から $\left(s+t\sqrt{5}\right)\left(s-t\sqrt{5}\right)=1$.

  ①から $s+t\sqrt{5}>0$ だから，上の等式より $s-t\sqrt{5}>0$ が言える.

  よって，$2s = \left(s+t\sqrt{5}\right)+\left(s-t\sqrt{5}\right) > 0$ から，$s>0$ が成り立つ.

  もしも $t<0$ だとすると，①から $s+t\sqrt{5} \geq 1$ なので

  $$1 = s^2-5t^2 = \left(s-t\sqrt{5}\right)\left(s+t\sqrt{5}\right) > \left(s+t\sqrt{5}\right)^2 \geq 1$$

  と矛盾が生じる.

  よって $t \geq 0$ である.

$t>0$ だとすると，②から $(2s)^2-5(2t)^2=4$.

また，

$$2s=\frac{-ux_k+5vy_k}{2},\ 2t=\frac{-vx_k+uy_k}{2}$$

において x_k, y_k の偶奇と u, v の偶奇は一致するから，$2s, 2t$ は整数である．

以上のことから，$(2s, 2t)$ は $x^2-5y^2=4$ の正の整数解となる．$x^2-5y^2=4$ で x が最小の正の整数解は $(3, 1)$ だから，$2s\geq 3$ でなければならない．

このとき，

$$(2t)^2=\frac{(2s)^2-4}{5}\geq\frac{3^2-4}{5}=1$$

から $2t\geq 1$ が成り立つ．

すると，$2s+2t\sqrt{5}\geq 3+\sqrt{5}=2z$ となり，①の $s+t\sqrt{5}<z$ に矛盾する．

よって，$t=0$ でなければならず，このとき②より $s=1$ となる．

$s=1$ かつ $t=0$ より，$\frac{r}{z^{2k-1}}=s+t\sqrt{D}=1$ で，$u+v\sqrt{D}=r=z^{2k-1}$ となる．　□

- 例題 6.3.1 において

$$x_{m+1}=\frac{3x_m+5y_m}{2},\ y_{m+1}=\frac{x_m+3y_m}{2}$$

が成り立っていた．これを行列を使って書き直すと

$$\begin{pmatrix}x_{m+1}\\ y_{m+1}\end{pmatrix}=\frac{1}{2}\begin{pmatrix}3 & 5\\ 1 & 3\end{pmatrix}\begin{pmatrix}x_m\\ y_m\end{pmatrix}$$

となる．これを使って $x^2-5y^2=-4$ の正の整数解を求めてみると，

$$\begin{pmatrix}x_1\\ y_1\end{pmatrix}=\begin{pmatrix}1\\ 1\end{pmatrix},$$
$$\begin{pmatrix}x_2\\ y_2\end{pmatrix}=\frac{1}{2}\begin{pmatrix}3 & 5\\ 1 & 3\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}8\\ 4\end{pmatrix}=\begin{pmatrix}4\\ 2\end{pmatrix},$$
$$\begin{pmatrix}x_3\\ y_3\end{pmatrix}=\frac{1}{2}\begin{pmatrix}3 & 5\\ 1 & 3\end{pmatrix}\begin{pmatrix}4\\ 2\end{pmatrix}=\frac{1}{2}\begin{pmatrix}22\\ 10\end{pmatrix}=\begin{pmatrix}11\\ 5\end{pmatrix},$$
$$\begin{pmatrix}x_4\\ y_4\end{pmatrix}=\frac{1}{2}\begin{pmatrix}3 & 5\\ 1 & 3\end{pmatrix}\begin{pmatrix}11\\ 5\end{pmatrix}=\frac{1}{2}\begin{pmatrix}58\\ 26\end{pmatrix}=\begin{pmatrix}29\\ 13\end{pmatrix},$$
$$\begin{pmatrix}x_5\\ y_5\end{pmatrix}=\frac{1}{2}\begin{pmatrix}3 & 5\\ 1 & 3\end{pmatrix}\begin{pmatrix}29\\ 13\end{pmatrix}=\frac{1}{2}\begin{pmatrix}152\\ 68\end{pmatrix}=\begin{pmatrix}76\\ 34\end{pmatrix},$$
$$\cdots\cdots$$

となる．

問題 6.3.1 $a \mid b^2+1$ かつ $b \mid a^2+1$ を満たすような正の整数 a, b の組 (a, b) をすべて求めよ.

問題 6.3.2 D は平方数でない正の整数で，$\gcd(D, 2)=1$ とする.
このとき，方程式 $x^2-Dy^2=4$ は正整数解 (x, y) をもつ.(注) このような正整数解のうちで x が最小のものを (x_1, y_1) とすれば，すべての解 (x_n, y_n) は

$$\frac{x_n+y_n\sqrt{D}}{2}=\left(\frac{x_1+y_1\sqrt{D}}{2}\right)^n \quad (n=1,2,\dots)$$

から得られることを示せ.

注 定理 6.2.1 から，D が平方数でない正の整数のとき，ペル方程式 $x^2-Dy^2=1$ は正の整数解をもつから，これを (s, t) とすると $s^2-Dt^2=1$.
$s^2-Dt^2=1$ の両辺に 4 をかけると，$(2s)^2-D(2t)^2=4$ となるから，$x^2-Dy^2=4$ は正の整数解 $(2s, 2t)$ をもつことがわかる.

注 ペル方程式や類似の方程式では解が存在するかどうか（存在する場合には正の最小解を求めること）が大きな問題であった.

7 世紀に，ブラーマグプタ (Brahmagupta) はペル方程式 $x^2-92y^2=1$ の正の最小解 $x=1151$, $y=120$ を求めている.

12 世紀に，Bhaskara はペル方程式 $x^2-61y^2=1$ の正の最小解 $x=226153980$, $y=1766319049$ を求めている.

1657 年に フェルマー (Fermat) は William Brouncker と John Wallis に

$$x^2-151y^2=1 \text{ と } x^2-313y^2=1$$

の整数解を求めるよう挑戦した．それに対して

Wallis は $x^2-151y^2=1$ の解として $x=1728148040$, $y=140634693$ を答え，Brouncker は $x^2-313y^2=1$ の解として $x=126862368$, $y=7170685$ を答えている.

1800 年 Carl Amthov はペル方程式 $x^2-4729494y^2=1$ の正の最小解として，y が 41 桁の数を発見している.

ペル方程式に関連する数列の問題をまとめてみた.

基本問題 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a+b\sqrt{3}$ (a, b は正の整数) と表せることを示せ.

解答 n に関する数学的帰納法で証明する.

(I) $n=1$ のときは，$a_1=2$, $b_1=1$ とおくと，$2+\sqrt{3}=a_1+b_1\sqrt{3}$ と表せる.

(II) $n=k$ のとき成り立つと仮定すると，$\left(2+\sqrt{3}\right)^k = a_k+b_k\sqrt{3}$　(a_k , b_kは正の整数) と表せる．

$$\begin{aligned}\left(2+\sqrt{3}\right)^{k+1} &= \left(2+\sqrt{3}\right)\left(2+\sqrt{3}\right)^k \\ &= \left(2+\sqrt{3}\right)\left(a_k+b_k\sqrt{3}\right) \\ &= 2a_k+3b_k+(a_k+2b_k)\sqrt{3}\end{aligned}$$

となるから，$a_{k+1}=2a_k+3b_k$，$b_{k+1}=a_k+2b_k$ とおくと，a_{k+1}, b_{k+1} は正の整数で

$$\left(2+\sqrt{3}\right)^{k+1} = a_{k+1}+b_{k+1}\sqrt{3}$$

と表せるから，$n=k+1$ のときも成り立つ．

(III) (I), (II) よりすべての正の整数に対して，$\left(2+\sqrt{3}\right)^n = a+b\sqrt{3}$　(a, b は正の整数) と表せる．　□

別解 二項定理より

$$\begin{aligned}\left(2+\sqrt{3}\right)^n &= \sum_{k=0}^{n} {}_n\mathrm{C}_k 2^{n-k}\left(\sqrt{3}\right)^k \\ &= \sum_{k:\text{偶数}}^{n} {}_n\mathrm{C}_k 2^{n-k}\left(\sqrt{3}\right)^k + \sum_{k:\text{奇数}}^{n} {}_n\mathrm{C}_k 2^{n-k}\left(\sqrt{3}\right)^k \\ &= \sum_{m=0}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m}\left(\sqrt{3}\right)^{2m} + \sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)}\left(\sqrt{3}\right)^{2m-1} \\ &= \sum_{m=0}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m}3^m + \sqrt{3}\sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)}3^{m-1}\end{aligned}$$

したがって

$$a=\sum_{m=0}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m}3^m,\ b=\sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)}3^{m-1}$$

とおくと，a, b は正の整数で，$\left(2+\sqrt{3}\right)^n = a+b\sqrt{3}$ と表せることがわかった．　□

注　解答で数列 $\{a_n\}$ を用いたのは，問題 6.3.3 等を解くために便利だからである．

- $\left(2+\sqrt{3}\right)^n = a+b\sqrt{3}$　(a, b は正の整数) と表すことができ，表し方はただ 1 通りである．

$\left(2+\sqrt{3}\right)^n = a+b\sqrt{3}$　(a, b は正の整数)，$\left(2+\sqrt{3}\right)^n = c+d\sqrt{3}$　(c, d は正の整数) と表せたとすると

$$a+b\sqrt{3}=c+d\sqrt{3}.$$

この式を変形すると

$$(b-d)\sqrt{3}=c-a. \qquad \cdots\cdots ①$$

$b \neq d$ と仮定すると

$$\sqrt{3}=\frac{c-a}{b-d}.$$

左辺は無理数，右辺は有理数であるから矛盾が生じる．

よって，$b=d$ でなければならず，①より $a=c$ となる． □

問題 6.3.3 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$ $(a_n,\, b_n$は正の整数$)$ と表すとき，$a_{n+1},\, b_{n+1}$ をそれぞれ $a_n,\, b_n$ で表せ．

問題 6.3.4 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$ $(a_n,\, b_n$は正の整数$)$ と表すとき，$\left(2-\sqrt{3}\right)^n=a_n-b_n\sqrt{3}$ と表されることを示せ．

問題 6.3.5 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$ $(a_n\,, b_n$は正の整数$)$ と表すとき，$a_n\,, b_n$ を求めよ．

問題 6.3.6 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$ $(a_n,\, b_n$は正の整数$)$ と表すとき，${a_n}^2-3{b_n}^2$ の値を求めよ．

- 問題 6.3.6 の結果から，(a_n, b_n) は双曲線 $x^2-3y^2=1$ 上にあることがわかった．

双曲線 $x^2-3y^2=1$ 上の第 1 象限における格子点は，(a_n, b_n) で尽くせるかということが問題になるが，答えを得るには京都大学や早稲田大学の本格的なペル方程式の問題を解かなければならない．

問題 6.3.7 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=\sqrt{M+1}+\sqrt{M}$ となる正の整数 M が存在することを示せ．

注 正の整数 n に対して，$\left(2-\sqrt{3}\right)^n=\sqrt{M+1}-\sqrt{M}$ となる整数 M が存在する．

問題 6.3.8 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$ $(a_n,\, b_n$は正の整数$)$ と表すとき，$\left(2+\sqrt{3}\right)^n$ の整数部分を a_n で表せ．

注 $\left(2+\sqrt{3}\right)^n$ の小数部分は $1-\left(2-\sqrt{3}\right)^n$ になる．

問題 6.3.9 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$ $(a_n,\, b_n$は正の整数$)$ と表すとき，$\lim\limits_{n\to\infty}\dfrac{a_n}{b_n}$ を求めよ．

- (a_n, b_n) は双曲線 $x^2 - 3y^2 = 1$ 上にあるから，点 (a_n, b_n) は漸近線 $x - \sqrt{3}\,y = 0$ に近づいて行くことを考えれば，$\lim_{n\to\infty} \dfrac{b_n}{a_n} = \dfrac{1}{\sqrt{3}}$ は推測できる．また，問題 6.3.10 の結果も理解できる．

問題 6.3.10 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n = a_n + b_n\sqrt{3}$ $(a_n,\, b_n$は正の整数$)$ と表すとき，不等式 $\left|\sqrt{3} - \dfrac{a_n}{b_n}\right| > \left|\sqrt{3} - \dfrac{a_{n+1}}{b_{n+1}}\right|$ が成り立つことを証明せよ．

- $\dfrac{a_{n+1}}{b_{n+1}}$ は $\dfrac{a_n}{b_n}$ よりもよい近似値であることがわかった．

問題 6.3.11 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n = a_n + b_n\sqrt{3}$ $(a_n,\, b_n$は正の整数$)$ と表すとき，すべての正の整数 n に対して a_n と b_n は互いに素であることを証明せよ．

問題 6.3.12 正の整数 n に対して，$\left(3+2\sqrt{2}\right)^n = a_n + b_n\sqrt{2}$ $(a_n,\, b_n$は正の整数$)$ と表すとき，すべての正の整数 n に対して

$$\frac{\left(17+12\sqrt{2}\right)^n - \left(17-12\sqrt{2}\right)^n}{4\sqrt{2}}$$

は整数であるが平方数にならないことを証明せよ．

大学入試等では次のように出題されている．

1 (1) $p + q\sqrt{2} = r + s\sqrt{2}$ $(p, q, r, s$ は整数$)$ が成り立つならば，$p = r$ かつ $q = s$ となることを示せ．ただし，$\sqrt{2}$ が無理数であることは使ってよい．

(2) 自然数 n に対し，$\left(3+2\sqrt{2}\right)^n = a_n + b_n\sqrt{2}$ を満たす整数 a_n, b_n が存在することを数学的帰納法により示せ．

(3) a_n, b_n を (2) のものとする．このとき，すべての自然数 n について $(x, y) = (a_n, b_n)$ は方程式 $x^2 - 2y^2 = 1$ の解であることを数学的帰納法により示せ．

(2010 三重大)

2 自然数 n, a_n, b_n を自然数とし，$\left(2+\sqrt{3}\right)^n = a_n + \sqrt{3}\,b_n$ とする．

(1) a_{n+1}, b_{n+1} を a_n, b_n で表せ．

(2) $\left(2-\sqrt{3}\right)^n = a_n - \sqrt{3}\,b_n$ となることを数学的帰納法により証明せよ．

(3) $\left(2+\sqrt{3}\right)^n$ 以下の整数のうち最大のものを $pa_n + q$ とする．p と q の値を求めよ．

(2012 京都府立大・生命環境・前期)

3 (1) $n=1,2,\dots$ に対して $\left(\sqrt{2}+1\right)^n=a_n+\sqrt{2}\,b_n$ により自然数 a_n,b_n を定義する．このとき，$\left(\sqrt{2}-1\right)^n$ を a_n,b_n を用いて表せ．また，${a_n}^2-2{b_n}^2$ の値を求めよ．

(2) 適当な自然数 k_n を用いて，$\left(\sqrt{2}-1\right)^n=\sqrt{k_n}-\sqrt{k_n-1}$ $(n=1,2,\dots)$ と表せることを示せ．（1988 慶応大・理工）

3 と同様な問題が 2013 年に静岡大学情報（情報科）・理（物理・化）・工学部 [前期] で出題されている．

3 の問題で (1) のヒントがない問題が，3’，3” である．

3’ 自然数 $n=1,2,3,\dots$ に対して，$\left(2-\sqrt{3}\right)^n$ という形の数を考える．これらの数はいずれも，それぞれ適当な自然数 m が存在して $\sqrt{m}-\sqrt{m-1}$ という表示をもつことを証明せよ．(1994　東京工大・後期)

3” n を自然数とするとき，$\left(2-\sqrt{3}\right)^n$ は $\sqrt{m}-\sqrt{m-1}$ (m は自然数) の形で表されることを示せ．(2013　静岡大・理（数学）前期)

4 n を自然数とするとき

(1) $(2+\sqrt{2}\,)^n$ は適当な自然数 a,b を用いれば $a+b\sqrt{2}$ と表されることを証明せよ．

(2) 上の a,b を用いれば，次の等式および不等式が成立することを証明せよ．

[1]　$(2-\sqrt{2}\,)^n=a-b\sqrt{2}$

[2]　$2a-1<(2+\sqrt{2}\,)^n<2a$　（1970 慶応大・医）

4 (2)[2] より $(2+\sqrt{2}\,)^n$ の整数部分は $2a-1$ であることがわかる．

5 n を自然数とするとき，$\left(3+\sqrt{7}\right)^n$ はある自然数 a_n,b_n をもちいて $\left(3+\sqrt{7}\right)^n=a_n+b_n\sqrt{7}$ と表せる．

(1)　a_n,b_n をもちいて a_{n+1},b_{n+1} それぞれ表わせ．

(2)　数学的帰納法によって，自然数 n について $\left(3-\sqrt{7}\right)^n=a_n-b_n\sqrt{7}$ となることを証明せよ．

(3)　$\left(3+\sqrt{7}\right)^n$ 以下の最大の整数は $2a_n-1$ であることを証明せよ．

（2002 慶応大・経済）

6 平面上に次の条件で定められる点列 $\mathrm{P}_0(x_0, y_0), \mathrm{P}_1(x_1, y_1), \mathrm{P}_2(x_2, y_2), \ldots, \mathrm{P}_n(x_n, y_n), \ldots$ がある．

$$\begin{cases} x_0 = 1 \\ y_0 = 0 \end{cases} \qquad \begin{cases} x_{n+1} = 2x_n + 3y_n \\ y_{n+1} = x_n + 2y_n \end{cases} \qquad (n = 0, 1, 2, \ldots)$$

(1) 適当な数 a をとると，数列 $\{x_n + ay_n\}$ が等比数列となる．このような a を定めよ．
(2) $n \to \infty$ のとき直線 OP_n (O は原点) の傾きはどんな値に近づくか．

（1969　慶応大・工）

7 正の整数 n に対して $\left(1+\sqrt{2}\right)^n = x_n + y_n\sqrt{2}$ が成り立つように整数 x_n, y_n を定める．

(1) x_{n+1}, y_{n+1} を x_n, y_n で表せ．
(2) n が偶数なら ${x_n}^2 - 2{y_n}^2 = 1$，n が奇数なら ${x_n}^2 - 2{y_n}^2 = -1$ であることを証明せよ．
(3) 任意の n に対して，$\dfrac{x_{n+1}}{y_{n+1}}$ は $\dfrac{x_n}{y_n}$ よりも $\sqrt{2}$ のよい近似値であることが証明せよ．

（1984 一橋大）

8 自然数 n に対して a_n と b_n を　$\left(3+2\sqrt{2}\right)^n = a_n + b_n\sqrt{2}$　を満たす自然数とする．このとき，以下の問いに答えよ．

(1) $n \geqq 2$ のとき，a_n および b_n を a_{n-1} と b_{n-1} を用いて表せ．
(2) $a_n^2 - 2b_n^2$ を求めよ．
(3) (2) を用いて，$\sqrt{2}$ を誤差 $\dfrac{1}{10000}$ 未満で近似する有理数を 1 つ求めよ．

（2004　名古屋大・情報文化・後期）

9 正の整数 n, p, q について，等式 $\left(\sqrt{p}+\sqrt{q}\right)^{2n-1} = a_n\sqrt{p} + b_n\sqrt{q}$ を考える．

(1) ある正の整数 a_n, b_n が上の等式を満たすことを示せ．
(2) $\sqrt{pq}$ が整数でないとき，(1) の a_n, b_n はただ 1 通りに定まることを示せ．
(3) $\sqrt{pq}$ が整数でないとき，(1) の a_n, b_n に対して $\lim\limits_{n\to\infty} \dfrac{a_n}{b_n}$ を求めよ．

（2013　滋賀医大）

10 n は正の整数とする．x^{n+1} を x^2-x-1 で割った余りを a_nx+b_n とおく．

(1) 数列 $\{a_n\},\{b_n\}$ は $\begin{cases} a_{n+1}=a_n+b_n \\ b_{n+1}=a_n \end{cases}$ を満たすことを示せ．

(2) $n=1,2,3,\ldots$ に対して，a_n,b_n はともに正の整数で，互いに素であることを証明せよ．

(2002 東京大・理・前期)

10 の類題が 2007 年に東北大学で出題されている．

11 n を自然数とし，整式 x^n を x^2-2x-1 で割った余りを $ax+b$ とする．このとき，a と b は整数であり，さらにそれらをともに割り切る素数は存在しないことを示せ．

(2013 京都大・理系・前期)

12 a と b を互いに素，すなわち 1 以外の公約数を持たない正の整数とし，さらに a は奇数とする．正の整数 n に対して整数 a_n,b_n を $\left(a+b\sqrt{2}\right)^n=a_n+b_n\sqrt{2}$ を満たすように定めるとき，次の (1)，(2) を示せ．ただし $\sqrt{2}$ が無理数であることは証明なしに用いてよい．

(1) a_2 は奇数であり，a_2 と b_2 は互いに素である．

(2) すべての n に対して a_n は奇数であり，a_n と b_n は互いに素である．

(2009 京都大・理系・前期)

解答

(1)
$$a_2+b_2\sqrt{2}=\left(a+b\sqrt{2}\right)^2=\left(a^2+2b^2\right)+2ab\sqrt{2}$$

で，$a^2+2b^2,2ab$ は整数，$\sqrt{2}$ は無理数だから

$$a_2=a^2+2b^2,\ b_2=2ab$$

が成り立つ．

a は奇数なので，a^2 は奇数，$2ab$ は偶数だから，$a_2=a^2+2ab$ は奇数である．

a_2 と b_2 の最大公約数を G とおき，$G=1$ となることを示せば，a_2 と b_2 が互いに素であることが言える．

$G>1$ と仮定して矛盾を導く．

$G>1$ より，G の素因数 p がある．$p\mid G\mid a_2$ で a_2 が奇数だから，p は奇素数である．

$p\mid b_2=2ab$ で p は奇素数だから，$p\mid a$ または $p\mid b$ となる．

$p \mid a$ のとき，$p \mid a_2 = a^2 + 2b^2$ だから，$p \mid a^2 + 2b^2 - a^2 = 2b^2$ が成り立つ．p は奇素数だから，$p \mid b$ となり，a と b は p を公約数に持つので，a と b が互いに素であることに矛盾する．

$p \mid b$ のときも同様に矛盾が生じる．

したがって，$G = 1$ でなければならないから，a_2 と b_2 が互いに素である．

(2)
$$\begin{aligned} a_{n+1} + b_{n+1}\sqrt{2} &= \left(a + b\sqrt{2}\right)^{n+1} = \left(a + b\sqrt{2}\right)\left(a + b\sqrt{2}\right)^{n} \\ &= \left(a + b\sqrt{2}\right)\left(a_n + b_n\sqrt{2}\right) \\ &= (aa_n + 2bb_n) + (ba_n + ab_n)\sqrt{2} \end{aligned}$$

で，$a_{n+1} + b_{n+1}, aa_n + 2bb_n, ba_n + ab_n$ は整数，$\sqrt{2}$ は無理数だから

$$a_{n+1} = aa_n + 2bb_n \qquad \cdots\cdots ①$$
$$b_{n+1} = ba_n + ab_n \qquad \cdots\cdots ②$$

① $\times a -$ ② $\times 2b$，② $\times a -$ ① $\times b$ から

$$\left(a - 2b^2\right) a_n = aa_{n+1} - 2bb_{n+1} \qquad \cdots\cdots ③$$
$$\left(a - 2b^2\right) b_n = -ba_{n+1} + ab_{n+1} \qquad \cdots\cdots ④$$

を得る．

n に関する数学的帰納法で証明する．

(I) $n = 1$ のとき，$a_1 = a, b_1 = b$ より a は奇数，a と b は互いに素だから，a_1 は奇数，a_1 と b_1 は互いに素となる．

$n = 2$ のとき，a_2 は奇数，a_2 と b_2 は互いに素であることは (1) で示してある．

(II) $n = k\ (\geq 2)$ のとき，a_k は奇数，a_k と b_k は互いに素であると仮定する．

①で $n = k$ とおくと

$$a_{k+1} = aa_k + 2bb_k. \qquad \cdots\cdots ⑤$$

a, a_k は奇数なので，aa_k は奇数，$2bb_k$ は偶数だから，$a_{k+1} = aa_k + 2bb_k$ は奇数である．

a_{k+1} と b_{k+1} の最大公約数を G とおき，$G = 1$ となることを示せば，a_{k+1} と b_{k+1} が互いに素であることが言える．

$G > 1$ と仮定して矛盾を導く．

$G > 1$ より，G の素因数 p がある．$p \mid G \mid a_{k+1}$ で a_{k+1} が奇数だから，p は奇素数である．

③，④で $n = k$ とおき，$p \mid a_{k+1}, p \mid b_{k+1}$ を使うと

$$p \mid aa_{k+1} - 2bb_{k+1} = \left(a - 2b^2\right) a_k \text{ すなわち } p \mid \left(a - 2b^2\right) a_k,$$

$$p \mid -ba_{k+1}+b_{k+1}=\left(a-2b^2\right)b_k \text{ すなわち } p \mid \left(a-2b^2\right)b_k.$$

$p \nmid a^2-2b^2$ とすると，p は素数なので $p \mid a_k, p \mid b_k$ となり，a_k と b_k が互いに素であることに矛盾する．したがって

$$p \mid a^2-2b^2 \qquad \cdots\cdots ⑥$$

となる．

③で $n=k-1\ (\geq 1)$ とおき，⑥を使うと

$$p \mid a^2-2b^2 \mid \left(a^2-2b^2\right)a_{k-1}=aa_k-2bb_k$$

から

$$p \mid aa_k-2bb_k. \qquad \cdots\cdots ⑦$$

⑤から

$$p \mid a_{k+1}=aa_k+2bb_k$$

すなわち

$$p \mid aa_k+2bb_k \qquad \cdots\cdots ⑧$$

を得る．⑦，⑧から

$$p \mid (aa_k+2bb_k)+(aa_k-2bb_k)=2aa_k \text{ すなわち } p \mid 2aa_k,$$

$$p \mid (aa_k+2bb_k)-(aa_k-2bb_k)=4bb_k \text{ すなわち } p \mid 4bb_k.$$

p は奇素数だから，$p \mid aa_k$, $p \mid bb_k$ となる．

ところで，⑥より $p \nmid a, p \nmid b$ が言えるから，$p \mid a_k, p \mid b_k$ となり，a_k と b_k は互いに素であることに矛盾する．

したがって，$G=1$ でなければならないから，$n=k+1$ のときも成り立つ．

(III) (I)，(II) からすべての正の整数について成り立つ．　□

(2) の別解　(1) より

（1）で $a^2+2b^2, 2ab$ は正の整数になるから，(1) より

「p, q が正の整数，p が奇数，p と q が互いに素であるとき，$P+Q\sqrt{2}=\left(p+q\sqrt{2}\right)^2$ を満たす整数 P, Q はともに正の整数で，P は奇数，P と Q は互いに素である．」

$$\begin{aligned} a_{n+1}+b_{n+1}\sqrt{2} &= \left(a+b\sqrt{2}\right)^{n+1}=\left(a+b\sqrt{2}\right)\left(a+b\sqrt{2}\right)^n \\ &= \left(a+b\sqrt{2}\right)\left(a_n+b_n\sqrt{2}\right) \\ &= (aa_n+2bb_n)+(ba_n+ab_n)\sqrt{2} \end{aligned}$$

で，$a_{n+1}+b_{n+1}, aa_n+2bb_n, ba_n+ab_n$ は整数，$\sqrt{2}$ は無理数だから

$$a_{n+1}=aa_n+2bb_n \qquad \cdots\cdots ①$$
$$b_{n+1}=ba_n+ab_n \qquad \cdots\cdots ②$$

が成り立つ．

m に関する帰納法を用いて命題（P1）が成り立つことを示す．

(P1) $n=2^m$, $(m=0,1,2,\cdots)$ のとき，a_n は奇数で，a_n と b_n は互いに素な正の整数である．

(I) $m=0$ のとき，$a_1=a, b_1=b$ で a は奇数で，a と b は互いに素な正の整数だから，a_1 は奇数で，a_1 と b_1 も互いに素な正の整数である．

(II) $m=k$ $(k\geq 0)$ のとき (P1) が成り立つとする．a_{2^k} は奇数で，a_{2^k} と b_{2^k} は互いに素な正の整数である．

$$a_{2^{k+1}}+b_{2^{k+1}}\sqrt{2}=\left(a+b\sqrt{2}\right)^{2^{k+1}}=\left(\left(a+b\sqrt{2}\right)^{2^k}\right)^2=\left(a_{2^k}+b_{2^k}\sqrt{2}\right)^2$$

だから，(1) の結果

($p=a_{2^k}, q=b_{2^k}, P=a_{2^{k+1}}, Q=b_{2^{k+1}}$として，証明の始めに述べたこと）より，$a_{2^{k+1}}$ は奇数で，$a_{2^{k+1}}$ と $b_{2^{k+1}}$ は互いに素な正の整数である．

よって，$m=k+1$ のときも (P1) は成り立つ．

(III) (I)，(II) より，非負の整数 m に対して (P1) は成り立つ．

次に

(P2) n が正の整数のとき，

$$a_{n+1}\text{は奇数で}, a_{n+1}\text{と } b_{n+1}\text{が互いに素} \Longrightarrow a_n\text{は奇数で}, a_n\text{と } b_n\text{も互いに素}$$

であることを示す．

a_n が偶数だとすると，①から，a_{n+1} が偶数となり仮定に矛盾する．よって，a_n は奇数である．

a_n と b_n は互いに素であることを示すために，対偶をとり

$$\gcd(a_n,b_n)>1 \Longrightarrow \gcd(a_{n+1},b_{n+1})>1$$

が成り立つことを示せばよい．

$g=\gcd(a_n,b_n)>1$ とおくと，$g\mid a_n,\ g\mid b_n$.

①，②を使うと

$$g\mid aa_n+2bb_n=a_{n+1},\ g\mid ba_n+ab_n=b_{n+1}$$

が成り立つから，$\gcd(a_n,b_n)\geq g>1$.

対偶が成り立つから，元の命題 (P2) も成り立つ.

(P1)，(P2) よりすべての正の整数 n について，a_n は奇数であり，a_n と b_n が互いに素であることが言える. □

13 $\left[\left(5\sqrt{2}+7\right)^{2011}\right]$ を 14, 49, 50 で割ったときの余りをそれぞれ求めよ.

(数検 1 級)

解答　正の整数 n に対して，$\left(7+5\sqrt{2}\right)^n=a_n+b_n\sqrt{2}$, $\left(7-5\sqrt{2}\right)^n=a_n-b_n\sqrt{2}$ (a_n,b_nは正の整数) と表すと，$\left(7+5\sqrt{2}\right)^n+\left(7-5\sqrt{2}\right)^n=2a_n$ より

$$\left(7+5\sqrt{2}\right)^n=2a_n-\left(7-5\sqrt{2}\right)^n.$$

n が奇数のとき

$$\left(7+5\sqrt{2}\right)^n=2a_n+\left(5\sqrt{2}-7\right)^n.$$

$0<5\sqrt{2}-7<1$ から $0<\left(5\sqrt{2}-7\right)^n<1$ となるので

$$\left[\left(5\sqrt{2}+7\right)^n\right]=2a_n. \quad \cdots\cdots ①$$

よって，$\left[\left(5\sqrt{2}+7\right)^{2011}\right]=2a_{2011}$.

n が偶数のときは，$\left(7+5\sqrt{2}\right)^n=2a_n-\left(5\sqrt{2}-7\right)^n$.

$0<5\sqrt{2}-7<1$ から $0<\left(5\sqrt{2}-7\right)^n<1$ となるので

$$\left[\left(5\sqrt{2}+7\right)^n\right]=2a_n-1.$$

二項定理より

$$\begin{aligned}
\left(7+5\sqrt{2}\right)^n&=\sum_{k=0}^{n}{}_n\mathrm{C}_k7^{n-k}\left(5\sqrt{2}\right)^k\\
&=\sum_{k:\text{偶数}}^{n}{}_n\mathrm{C}_k7^{n-k}\left(5\sqrt{2}\right)^k+\sum_{k:\text{奇数}}^{n}{}_n\mathrm{C}_k7^{n-k}\left(5\sqrt{2}\right)^k\\
&=\sum_{r=0}^{\left[\frac{n}{2}\right]}{}_n\mathrm{C}_{2r}7^{n-2r}\left(5\sqrt{2}\right)^{2r}+\sum_{r=1}^{\left[\frac{n+1}{2}\right]}{}_n\mathrm{C}_{2r-1}7^{n-(2r-1)}\left(5\sqrt{2}\right)^{2r-1}\\
&=\sum_{r=0}^{\left[\frac{n}{2}\right]}{}_n\mathrm{C}_{2r}7^{n-2r}50^r+\sqrt{2}\sum_{r=1}^{\left[\frac{n+1}{2}\right]}{}_n\mathrm{C}_{2r-1}7^{n-(2r-1)}\cdot5\cdot50^{r-1}
\end{aligned}$$

となるから

$$a_n=\sum_{r=0}^{\left[\frac{n}{2}\right]}{}_n\mathrm{C}_{2r}7^{n-2r}50^r \qquad 2a_n=\sum_{r=0}^{\left[\frac{n}{2}\right]}{}_n\mathrm{C}_{2r}2\cdot 7^{n-2r}50^r$$

よって

$$\begin{aligned}&2a_{2011}\\&=\sum_{r=0}^{1005}{}_{2011}\mathrm{C}_{2r}2\cdot 7^{2011-2r}50^r\\&=\underline{2\cdot 7^{2011}+{}_{2011}\mathrm{C}_2 2\cdot 7^{2009}\cdot 50+\cdots+{}_{2011}\mathrm{C}_{2008}2\cdot 7^3 50^{1004}+{}_{2011}\mathrm{C}_{2010}2\cdot 7\cdot 50^{1005}}\end{aligned}$$

$2a_{2011}$ を 14 で割った余りは 0.

mod 49 で考えると，下線部の最後の項 ${}_{2011}\mathrm{C}_{2010}2\cdot 7\cdot 50^{1005}$ を除いた項はすべて 49 で割り切れるから

$$\begin{aligned}2a_{2011}&\equiv {}_{2011}\mathrm{C}_{2010}2\cdot 7\cdot 50^{1005}\\&\equiv 2011\cdot 2\cdot 7\cdot 50^{1005}\\&\equiv 2\cdot 2\cdot 7\cdot 1^{1005} \qquad\qquad 2011\equiv 2 \pmod{49}\\&\equiv 28 \pmod{49}.\end{aligned}$$

mod 50 で考えると，下線部の最初の項 $2\cdot 7^{2011}$ を除いた項はすべて 50 で割り切れるから

$$\begin{aligned}2a_{2011}\equiv 2\cdot 7^{2011}&\equiv 2\cdot 7\cdot\left(7^2\right)^{1005}\\&\equiv 2\cdot 7\cdot(-1)^{1005}\\&\equiv -14\\&\equiv 36 \pmod{50}.\end{aligned}$$

$\left[\left(5\sqrt{2}+7\right)^{2011}\right]$ を 14, 49, 50 で割った余りはそれぞれ 0 28,36 となる．　□

割った余りを漸化式から求める方法もある．

別解　$a_{n+1}+b_{n+1}\sqrt{2}=\left(7+5\sqrt{2}\right)^{n+1}=\left(7+5\sqrt{2}\right)\left(7+5\sqrt{2}\right)^n$

$$\begin{aligned}&=\left(7+5\sqrt{2}\right)\left(a_n+b_n\sqrt{2}\right)\\&=(7a_n+10b_n)+(5a_n+7b_n)\sqrt{2}\end{aligned}$$

から

$$a_{n+1}=7a_n+10b_n,\ b_{n+1}=5a_n+7b_n.$$

$A_n=2a_n, B_n=2b_n$ とおくと，$A_1=2a_1=14, B_1=2b_1=10$ で

$$A_{n+1}=7A_n+10B_n, \qquad \cdots\cdots①$$

$$B_{n+1}=5A_n+7B_n. \qquad \cdots\cdots ②$$

①，②から $\{A_n\}$ の漸化式をつくる．

$B_n=\dfrac{A_{n+1}-7A_n}{10}, B_{n+1}=\dfrac{A_{n+2}-7A_{n+1}}{10}$ を②に代入すると

$$\frac{A_{n+2}-7A_{n+1}}{10}=5A_n+7\cdot\frac{A_{n+1}-7A_n}{10}$$

から，$A_{n+2}=14A_{n+1}+A_n$ を得る．A_2 を求めると，$A_2=7A_1+10B_1=198$. よって

$$A_1=14,\ A_2=198,\ A_{n+2}=14A_{n+1}+A_n. \qquad \cdots\cdots ③$$

(1)　mod 14 で考えると，$A_1\equiv 0 \pmod{14}, A_2\equiv 2 \pmod{14}$.

$$A_{n+2}=14A_{n+1}+A_n\equiv A_n \pmod{14}$$

より，A_n を 14 で割った余りは周期 2 で繰り返すから，$A_{2011}\equiv A_1\equiv 0 \pmod{14}$.

(2)　mod 49 で考えると，$A_1\equiv 14 \pmod{49}, A_2\equiv 2 \pmod{49}$.

$$\begin{aligned}
A_3&=14A_2+A_1\equiv 14\cdot 2+14\equiv 42\equiv -7\\
A_4&=14A_3+A_2\equiv 14\cdot(-7)+2\equiv 0+2\equiv 2\\
A_5&=14A_4+A_3\equiv 14\cdot 2-7\equiv 21\\
A_6&=14A_5+A_4\equiv 14\cdot 21+2\equiv 0+2\equiv 2\\
A_7&=14A_6+A_5\equiv 14\cdot 2+21\equiv 49\equiv 0\\
A_8&=14A_7+A_6\equiv 14\cdot 0+2\equiv 2\\
A_9&=14A_8+A_7\equiv 14\cdot 2+0\equiv 28\\
A_{10}&=14A_9+A_8\equiv 14\cdot 28+2\equiv 0+2\equiv 2\\
A_{11}&=14A_{10}+A_9\equiv 14\cdot 2+28\equiv 56\equiv 7\\
A_{12}&=14A_{11}+A_{10}\equiv 14\cdot 7+2\equiv 0+2\equiv 2\\
A_{13}&=14A_{12}+A_{11}\equiv 14\cdot 2+7\equiv 35\\
A_{14}&=14A_{13}+A_{12}\equiv 14\cdot 35+2\equiv 0+2\equiv 2\\
A_{15}&=14A_{14}+A_{13}\equiv 14\cdot 2+35\equiv 63\equiv 14\\
A_{16}&=14A_{15}+A_{14}\equiv 14\cdot 14+2\equiv 0+2\equiv 2.
\end{aligned}$$

$A_{15}\equiv A_1 \pmod{49}, A_{16}\equiv A_2 \pmod{49}$ だから，A_n を 49 で割った余りは周期 14 で繰り返す．よって，$A_{2011}=A_{14\times 143+9}\equiv A_9\equiv 28 \pmod{49}$.

(3)　mod 50 で考えると，$A_1\equiv 14 \pmod{50}, A_2\equiv 198\equiv -2 \pmod{50}$.

$$\begin{aligned}
A_3&=14A_2+A_1\equiv 14\cdot(-2)+14\equiv -14\\
A_4&=14A_3+A_2\equiv 14\cdot(-14)-2\equiv -198\equiv 2\\
A_5&=14A_4+A_3\equiv 14\cdot 2-14\equiv 14
\end{aligned}$$

$$A_6 = 14A_5 + A_4 \equiv 14 \cdot 14 + 2 \equiv 198 \equiv -2.$$

$A_5 \equiv A_1 \pmod{50}, A_6 \equiv A_2 \pmod{50}$ だから，A_n を 50 で割った余りは周期 4 で繰り返す．よって，$A_{2011} = A_{4\times 502+3} \equiv A_3 \equiv 36 \pmod{50}$.

$\left[\left(5\sqrt{2}+7\right)^{2011}\right]$ を 14, 49, 50 で割った余りはそれぞれ 0 28,36 となる．　□

次の問題 14 のように，13 の別解の方法で解かなければならないものもある．

14　0 以上の整数 a_1, a_2 があたえられたとき，数列 $\{a_n\}$ を $a_{n+2} = a_{n+1} + 6a_n$ により定める．

(1) $a_1 = 1, a_2 = 2$ のとき，a_{2010} を 10 で割った余りを求めよ．
(2) $a_2 = 3a_1$ のとき，$a_{n+4} - a_n$ は 10 の倍数であることを示せ．

（2010 一橋大・前期）

※ (1) で a_n を 10 で割った余りは周期 20 で繰り返す．

類題　整数からなる数列 $\{a_n\}$ を漸化式 $a_1 = 1$, $a_2 = 3$, $a_{n+2} = 3a_{n+1} - 7a_n$ $(n = 1, 2, \dots)$ によって定める．

(1) a_n が偶数となることと，n が 3 の倍数となることは同値であることを示せ．
(2) a_n が 10 の倍数となるための条件を (1) と同様の形式で求めよ．

（1993 東京大・理系・前期）

最後は，問題 6.2.1(2015 早稲田大学) の類題である．

15　2 つの条件

(イ) $a^2 - 2b^2 = 1$ または $a^2 - 2b^2 = -1$　　(ロ) $a + \sqrt{2}\,b > 0$

を満たす任意の整数 a, b から得られる実数 $g = a + \sqrt{2}\,b$ 全体の集合を G とする．
1 より大きい G の元のうち最小のものを u とする．

(1) u を求めよ．
(2) 整数 n と G の元 g に対し，gu^n は G の元であることを示せ．
(3) G の任意の元 g は適当な整数 m によって，$g = u^m$ と書かれることを示せ．

（1985 東京工大）

第7章

Lifting The ExPonent Lemma(LTE)

7.1　補助定理

整数 x を割りきる素数 p の最大のべきが p^α のとき，$v_p(x)=\alpha$ と定義した．すなわち

$$v_p(x)=\alpha \Longleftrightarrow p^\alpha \| x.$$

注 すべての素数 p に対して，$v_p(0)=\infty$.
すると，次のことが成り立つ．

$$v_p(xy)=v_p(x)+v_p(y),\ v_p\left(\frac{x}{y}\right)=v_p(x)-v_p(y),\ v_p(x+y)\geq \min\{v_p(x),v_p(y)\}.$$

LTE の定理を証明するために，補助定理を二つ用意しておく．

補助定理 7.1.1　n : 正の整数，x,y : 整数，
p : 素数，$\gcd(n,p)=1$, $p \mid x-y$, $p \nmid x$, $p \nmid y$ とする．このとき

$$v_p\left(x^n-y^n\right)=v_p(x-y)$$

が成り立つ．

証明　$n=1$ のときは明らかに成り立つから，$n\geq 2$ とする．
$p \mid x-y$ より $x=y+kp\ (k\in\mathbb{Z})$ とおくと

$$\begin{aligned}
&x^n-y^n\\
&=(y+kp)^n-y^n\\
&=\binom{n}{1}y^{n-1}\cdot kp+\binom{n}{2}y^{n-2}\cdot (kp)^2+\cdots+\binom{n}{n-1}y\cdot (kp)^{n-1}+\binom{n}{n}\cdot (kp)^n\\
&=kp\left(ny^{n-1}+\binom{n}{2}y^{n-2}\cdot kp+\cdots+\binom{n}{n-1}y\cdot (kp)^{n-2}+(kp)^{n-1}\right)
\end{aligned}$$

$$= (x-y)\left(ny^{n-1} + \underbrace{\binom{n}{2}y^{n-2}\cdot kp + \cdots + \binom{n}{n-1}y\cdot(kp)^{n-2} + (kp)^{n-1}}_{p\text{ で割り切れる}} \right)$$

$p \nmid y, p \nmid n$ だから $p \nmid ny^{n-1}$.
よって $p \nmid ny^{n-1} + \binom{n}{2}y^{n-2}\cdot kp + \cdots + \binom{n}{n-1}y\cdot(kp)^{n-2} + (kp)^{n-1}$ となり

$$p^{\alpha} \,||\, x^n - y^n \Longleftrightarrow p^{\alpha} \,||\, x - y$$

が成り立つ. □

別証明　$x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}\right)$ を使う.

$$\begin{aligned} v_p\left(x^n - y^n\right) &= v_p\left((x-y)\left(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}\right)\right) \\ &= v_p(x-y) + v_p\left(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}\right). \end{aligned}$$

さて，$p \nmid x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}$ を示せば証明は終わる.
これを示すために，$p \mid x-y$ を使う．$y \equiv x \pmod{p}$ が成り立つから

$$\begin{aligned} & x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1} \\ \equiv\ & x^{n-1} + x^{n-2}\cdot x + x^{n-3}\cdot x^2 + \cdots + x\cdot x^{n-2} + x^{n-1} \\ \equiv\ & nx^{n-1} \pmod{p}. \end{aligned}$$

仮定から $\gcd(n,p) = 1$, $p \nmid x$ なので，$nx^{n-1} \not\equiv 0 \pmod{p}$.
したがって，$p \nmid x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}$ が成り立つ. □

注　補助定理 7.1.1 の (別証明ではない) 証明は p が素数でなくても通用するので，次の系を得る.

系 7.1.1　n, p : 正の整数，x, y : 整数，
$p \nmid n$, $p \mid x-y$, $p \nmid x$, $p \nmid y$ とする．このとき

$$p^{\alpha} \,||\, x^n - y^n \Longleftrightarrow p^{\alpha} \,||\, x - y$$

が成り立つ.

補助定理 7.1.2　n : 正の奇数，x, y : 整数，
p : 素数，$\gcd(n,p) = 1$, $p \mid x+y$, $p \nmid x$, $p \nmid y$ とする．このとき

$$v_p\left(x^n + y^n\right) = v_p(x+y)$$

が成り立つ.

証明　n : 正の奇数，x, y : 整数，p : 素数，$\gcd(n, p) = 1$, $p \mid x-(-y)$, $p \nmid x$, $p \nmid -y$ であるから，補助定理 7.1.1 より

$$v_p\left(x^n + y^n\right) = v_p\left(x^n - (-y)^n\right) = v_p(x-(-y)) = v_p(x+y). \qquad \square$$

系 7.1.2　n : 正の奇数，p : 正の整数，x, y : 整数，
$p \nmid n$, $p \mid x+$, $p \nmid x$, $p \nmid y$ とする．このとき

$$p^\alpha \,||\, x^n + y^n \Longleftrightarrow p^\alpha \,||\, x+y$$

が成り立つ．

証明　n : 正の奇数，x, y : 整数，p : 正の整数，$p \nmid n$, $p \mid x-(-y)$, $p \nmid x$, $p \nmid -y$ であるから，系 7.1.1 より

$$p^\alpha \,||\, x^n + y^n \Longleftrightarrow p^\alpha \,||\, x^n - (-y)^n \Longleftrightarrow p^\alpha \,||\, x-(-y) \Longleftrightarrow p^\alpha \,||\, x+y. \qquad \square$$

7.2 Lifting The ExPonent Lemma(LTE)

定理 7.2.1　n : 正の整数，x, y : 整数，
p : 奇素数，$p \mid x-y$, $p \nmid x$, $p \nmid y$ とする．このとき

$$v_p\left(x^n - y^n\right) = v_p(x-y) + v_p(n) \tag{7.1}$$

が成り立つ．

証明　$n = p^\alpha b$, $\gcd(p, b) = 1, \alpha \in \mathbb{N}_0, b \in \mathbb{N}$ とおくと，補助定理 7.1.1 より

$$v_p\left(x^n - y^n\right) = v_p\left(x^{p^\alpha b} - y^{p^\alpha b}\right) = v_p\left(\left(x^{p^\alpha}\right)^b - \left(y^{p^\alpha}\right)^b\right) = v_p\left(x^{p^\alpha} - y^{p^\alpha}\right)$$

となるから，

$$v_p\left(x^{p^\alpha} - y^{p^\alpha}\right) = v_p(x-y) + \alpha \qquad \cdots\cdots ①$$

を示せばよいことがわかる．

まず

$$v_p\left(x^p - y^p\right) = v_p(x-y) + 1 \qquad \cdots\cdots ②$$

を示す．$p \mid x-y$ より $x = y + kp$ $(k \in \mathbb{Z})$ とおくと

$$x^p - y^p$$

$$
\begin{aligned}
&= (y+kp)^p - y^p \\
&= \binom{p}{1} y^{p-1} \cdot kp + \binom{p}{2} y^{p-2} \cdot (kp)^2 + \cdots + \binom{p}{p-1} y \cdot (kp)^{p-1} + \binom{p}{p} \cdot (kp)^p \\
&= kp \left(py^{p-1} + \binom{p}{2} y^{p-2} \cdot kp + \cdots + \binom{p}{p-1} y \cdot (kp)^{p-2} + (kp)^{p-1} \right) \\
&= (x-y) \left(py^{p-1} + \binom{p}{2} y^{p-2} \cdot kp + \cdots + \binom{p}{p-1} y \cdot (kp)^{p-2} + (kp)^{p-1} \right)
\end{aligned}
$$

ところで，$1 \leq i \leq p-1$ のとき

$$\binom{p}{i} = \frac{p!}{(p-i)!i!} = \frac{p}{i} \cdot \frac{(p-1)!}{(p-i)!(i-1)!} = \frac{p}{i} \binom{p-1}{i-1}$$

から

$$\binom{p}{i} = \frac{p}{i} \binom{p-1}{i-1} \qquad \cdots\cdots (*)$$

を得る．

p は素数で，p と $i\,(1 \leq i \leq p-1)$ は互いに素なので，$(*)$ より $\binom{p}{i}$ は p の倍数になる．

$p \geq 3$ だから，$\binom{p}{2} y^{p-2} \cdot kp + \cdots + \binom{p}{p-1} y \cdot (kp)^{p-2} + (kp)^{p-1}$ は p^2 で割り切れる．しかし，$p \nmid y$ だから，$p \,||\, py^{y-1}$ なので

$$p \,||\, py^{p-1} + \binom{p}{2} y^{p-2} \cdot kp + \cdots + \binom{p}{p-1} y \cdot (kp)^{p-2} + (kp)^{p-1}.$$

よって②が成り立つ．

以上で②が証明できたので，②を用いて①を示す．

$$
\begin{aligned}
v_p \left(x^{p^\alpha} - y^{p^\alpha} \right) &= v_p \left(\left(x^{p^{\alpha-1}} \right)^p - \left(y^{p^{\alpha-1}} \right)^p \right) \\
&= v_p \left(x^{p^{\alpha-1}} - y^{p^{\alpha-1}} \right) + 1 \\
&= v_p \left(\left(x^{p^{\alpha-2}} \right)^p - \left(y^{p^{\alpha-2}} \right)^p \right) + 1 \\
&= v_p \left(x^{p^{\alpha-2}} - y^{p^{\alpha-2}} \right) + 2 \\
&= \cdots\cdots \\
&= v_p \left(x^p - y^p \right) + \alpha - 1 \\
&= v_p (x-y) + \alpha.
\end{aligned}
$$

したがって，①は成り立つ．　□

次の事実はよく使われる．（フェルマーの小定理のところでも扱った．）

> p は素数で，$1 \leq i \leq p-1$ のとき $\binom{p}{i}$ は p の倍数になる．

別証明　$n = p^\alpha b,\ \gcd(p,b) = 1, \alpha \in \mathbb{N}_0, b \in \mathbb{N}$ とおくと，補助定理 7.1.1 より

$$v_p\left(x^n - y^n\right) = v_p\left(x^{p^\alpha b} - y^{p^\alpha b}\right) = v_p\left(\left(x^{p^\alpha}\right)^b - \left(y^{p^\alpha}\right)^b\right) = v_p\left(x^{p^\alpha} - y^{p^\alpha}\right)$$

となるから，

$$v_p\left(x^{p^\alpha} - y^{p^\alpha}\right) = v_p(x-y) + \alpha \qquad \cdots\cdots ①$$

を示せばよいことがわかる．

まず

$$v_p\left(x^p - y^p\right) = v_p(x-y) + 1 \qquad \cdots\cdots ②$$

を示す．

$x^p - y^p = (x-y)\left(x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \cdots + xy^{p-2} + y^{p-1}\right)$ を使うと

$$v_p\left(x^p - y^p\right) = v_p(x-y) + v_p\left(x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \cdots + xy^{p-2} + y^{p-1}\right)$$

が成り立つから，$v_p\left(x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \cdots + xy^{p-2} + y^{p-1}\right) = 1$ すなわち

$$p \mid x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \cdots + xy^{p-2} + y^{p-1}$$

かつ

$$p^2 \nmid x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \cdots + xy^{p-2} + y^{p-1}$$

を示せばよい．

$p \mid x - y$ から $y \equiv x \pmod p$ が成り立つから

$$x^{p-1} + x^{p-2}y + \cdots + y^{p-1} \equiv x^{p-1} + x^{p-2}\cdot x + \cdots + x^{p-1} \equiv px^{p-1} \equiv 0 \pmod p$$

すなわち

$$p \mid x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \cdots + xy^{p-2} + y^{p-1}.$$

次に，$y = x + kp\ (k \in \mathbb{Z})$ とおき，$1 \le t \le p-1$ となる整数 t に対して，$x^{p-1-t}y^t$ を $\bmod p^2$ で考えると

$$\begin{aligned}
&x^{p-1-t}y^t \\
&= x^{p-1-t}(x+kp)^t \\
&= x^{p-1-t}\left(x^t + t(kp)x^{t-1} + \underbrace{\binom{t}{2}(kp)^2x^{t-2} + \binom{t}{3}(kp)^3x^{t-3} + \cdots + (kp)^t}_{t\ge 2 \text{ のとき } p^2 \text{で割り切れる}}\right) \\
&\equiv x^{p-1-t}\left(x^t + t(kp)x^{t-1}\right) \\
&\equiv x^{p-1} + tkpx^{p-2} \pmod{p^2}
\end{aligned}$$

から，$x^{p-1-t}y^t \equiv x^{p-1} + tkpx^{p-2} \pmod{p^2}$.
このことを使うと

$$\begin{aligned}
&x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \cdots + xy^{p-2} + y^{p-1} \\
&\equiv x^{p-1} + \left(x^{p-1} + kpx^{p-2}\right) + \left(x^{p-1} + 2kpx^{p-2}\right) \\
&\qquad + \cdots + \left(x^{p-1} + (p-2)kpx^{p-2}\right) + \left(x^{p-1} + (p-1)kpx^{p-2}\right) \\
&\equiv px^{p-1} + (1 + 2 + \cdots + (p-1))\, kpx^{p-2} \\
&\equiv px^{p-1} + \frac{p(p-1)}{2} kpx^{p-2} \\
&\equiv px^{p-1} + \frac{p-1}{2} kp^2x^{p-2} \\
&\equiv px^{p-1} \pmod{p^2}.
\end{aligned}$$

$p \nmid x$ より $px^{p-1} \not\equiv 0 \pmod{p^2}$ となるから，$p^2 \nmid x^{p-1} + x^{p-2}y + \cdots + y^{p-1}$ である．

以上で②が証明できたので，②を用いて①を示す．

$$\begin{aligned}
v_p\left(x^{p^\alpha} - y^{p^\alpha}\right) &= v_p\left(\left(x^{p^{\alpha-1}}\right)^p - \left(y^{p^{\alpha-1}}\right)^p\right) \\
&= v_p\left(x^{p^{\alpha-1}} - y^{p^{\alpha-1}}\right) + 1 \\
&= v_p\left(\left(x^{p^{\alpha-2}}\right)^p - \left(y^{p^{\alpha-2}}\right)^p\right) + 1 \\
&= v_p\left(x^{p^{\alpha-2}} - y^{p^{\alpha-2}}\right) + 2 \\
&= \cdots\cdots \\
&= v_p\left(x^p - y^p\right) + \alpha - 1 \\
&= v_p(x-y) + \alpha.
\end{aligned}$$

したがって，①は成り立つ．　□

定理 7.2.2　n : 正の奇数，x, y : 整数，
p : 奇素数，$p \mid x+y$, $p \nmid x$, $p \nmid y$ とする．このとき

$$v_p\left(x^n + y^n\right) = v_p(x+y) + v_p(n) \tag{7.2}$$

が成り立つ．

証明　n : 正の奇数，x, y : 整数，p : 奇素数，$p \mid x-(-y)$, $p \nmid x$, $p \nmid -y$ であるから，定理 7.2.1 より

$$v_p\left(x^n + y^n\right) = v_p\left(x^n - (-y)^n\right) = v_p(x-(-y)) + v_p(n) = v_p(x+y) + v_p(n). \quad \square$$

例題 7.2.1　自然数に対し，$\dfrac{10^n-1}{9}=\overbrace{111\cdots111}^{n\text{ 個}}$ を$\boxed{n}$で表す．例えば $\boxed{1}=1$，$\boxed{2}=11$，$\boxed{3}=111$ である．

(1)　m を 0 以上の整数とする．$\boxed{3^m}$ は 3^m で割り切れるが，3^{m+1} では割り切れないことを示せ．

(2)　n が 27 で割り切れることが，$\boxed{n}$ が 27 で割り切れるための必要十分条件であることを示せ．　(2008 東京大・理)

解答 入試問題の解答としてはふさわしくないかもしれない．

(1) $3^m \parallel \boxed{3^m}$ すなわち，$3^{m+2} \parallel 10^{3^m}-1$ を示せばよい．

$3 \mid 10-1, 3 \nmid 10, 3 \nmid 1$ だから，LTE より

$$v_3\left(10^{3^m}-1\right)=v_3\left(10^{3^m}-1^{3^m}\right)=v_3(10-1)+v_3\left(3^m\right)=2+m.$$

よって，$3^{m+2} \parallel 10^{3^m}-1$ が成り立つ．

(2) $27 \mid \boxed{n} \iff 3^{3+2} \mid 10^n-1$ が成り立つ．

$3 \mid 10-1, 3 \nmid 10, 3 \nmid 1$ だから，定理 7.2.1 より

$$v_3\left(10^n-1\right)=v_3(10-1)+v_3(n)=2+v_3(n).$$

よって，

$$\begin{aligned} 27 \mid \boxed{n} &\iff 3^{3+2} \mid 10^n-1 \\ &\iff v_3\left(10^n-1\right) \geq 5 \\ &\iff 2+v_3(n) \geq 5 \\ &\iff v_3(n) \geq 3 \\ &\iff 27 \mid n \end{aligned}$$

から，n が 27 で割り切れることが，$\boxed{n}$ が 27 で割り切れるための必要十分条件である．　□

例題 7.2.2　m, p を 3 以上の奇数とし，m は p で割り切れないとする．

(1)　$(x-1)^{101}$ をの展開式における x^2 の項の係数を求めよ．

(2)　$(p-1)^m+1$ は p で割り切れることを示せ．

(3)　$(p-1)^m+1$ は p^2 で割り切れないことを示せ．

(4)　r を正の整数とし，$s=3^{r-1}m$ とする．2^s+1 は 3^r で割り切れることを示せ．

(2012 名古屋大)

(4) は次のように示すことができる．

$3 \mid 2+1, 3 \nmid 2, 3 \nmid 1$ で，3 は奇素数，s は奇数だから，定理 7.2.2 より

$$v_3\left(2^s+1\right) = v_3(2+1) + v_3(s) = 1 + v_3\left(3^{r-1}\right) + v_3(m) \geq 1 + (r-1) = r.$$

よって，$3^r \mid 2^s + 1$.

(2)，(3) は p が素数ではないので LTE よりも系 7.1.2 を使うとよい．

$x = p-1, y = 1$ とおくと，m は正の奇数で，$p \nmid m$, $p \,||\, x+y = p$, $p \nmid x$, $p \nmid 1$ だから系 7.1.2 より

$$p^\alpha \,||\, x^m + y^m \Longleftrightarrow p^\alpha \,||\, x+y$$

が成り立つ．

$p \,||\, x+y = p$ から $\alpha = 1$ となり，$p \,||\, x^m + y^m$ すなわち，$p \mid (p-1)^m + 1$ かつ $p^2 \nmid (p-1)^m + 1$ が成り立つ．

7.3　$p = 2$ のときの LTE

定理 7.3.1　n : 正の整数，x, y : 奇数，$4 \mid x-y$ とする．このとき

$$v_2\left(x^n - y^n\right) = v_2(x-y) + v_2(n) \tag{7.3}$$

が成り立つ．

証明　n が奇数のとき，$\gcd(n, 2) = 1$, $2 \mid x-y$, $2 \nmid x$, $2 \nmid y$ が成り立つから，補助定理 7.1.1 より

$$v_2\left(x^n - y^n\right) = v_2(x-y) = v_2(x-y) + 0 = v_2(x-y) + v_2(n)$$

が成り立つ．

n が偶数のとき，$n = 2^a b$, ($a \in \mathbb{N}$, b は奇数) とおくと，補助定理 7.1.1 より

$$v_2\left(x^n - y^n\right) = v_2\left(x^{2^a b} - y^{2^a b}\right) = v_2\left(\left(x^{2^a}\right)^b - \left(y^{2^a}\right)^b\right) = v_2\left(x^{2^a} - y^{2^a}\right)$$

となるから，

$$v_2\left(x^{2^a} - y^{2^a}\right) = v_2(x-y) + a \qquad \cdots\cdots ①$$

を示せばよいことがわかる．

$$x^{2^a} - y^{2^a} = \left(x^{2^{a-1}} + y^{2^{a-1}}\right)\left(x^{2^{a-2}} + y^{2^{a-2}}\right)\cdots\left(x^2+y^2\right)(x+y)(x-y)$$

を利用する．

x,y : 奇数で，$4 \mid x-y$ だから，$x \equiv 1, y \equiv 1 \pmod 4$ または $x \equiv -1, y \equiv -1 \pmod 4$ となる．

これから，$k=1,2,\ldots,a-1$ のとき，$x^{2^k} \equiv y^{2^k} \equiv 1 \pmod 4$ となるので，$x^{2^k}+y^{2^k} \equiv 2 \pmod 4$.

よって，$x^{2^{a-1}}+y^{2^{a-1}}, x^{2^{a-2}}+y^{2^{a-2}}, \ldots, x^2+y^2$ は 2 で割り切れるが 4 では割り切れない．また，$x+y \equiv 2 \pmod 4$ なので，$x+y$ は 2 で割り切れるが 4 では割り切れないので

$$\begin{aligned}
&v_2\left(x^{2^a}-y^{2^a}\right)\\
&=v_2\left(\left(x^{2^{a-1}}+y^{2^{a-1}}\right)\left(x^{2^{a-2}}+y^{2^{a-2}}\right)\cdots\left(x^2+y^2\right)(x+y)(x-y)\right)\\
&=v_2\left(x^{2^{a-1}}+y^{2^{a-1}}\right)+v_2\left(x^{2^{a-2}}+y^{2^{a-2}}\right)+\cdots+v_2\left(x^2+y^2\right)+v_2(x+y)+v_2(x-y)\\
&=a+v_2(x-y).
\end{aligned}$$

したがって，①は成り立つ． □

定理 7.3.2　n : 正の偶数，x,y : 奇数とする．このとき

$$v_2\left(x^n-y^n\right)=v_2(x-y)+v_2(x+y)+v_2(n)-1 \tag{7.4}$$

が成り立つ．

証明 奇数 $z=2l+1$ ($l \in \mathbb{Z}$) の平方は $z^2=4\left(l^2+l\right)+1 \equiv 1 \pmod 4$ となる．x,y は奇数だから，$x^2 \equiv 1 \pmod 4, y^2 \equiv 1 \pmod 4$ となり，$4 \mid x^2-y^2$ を満たす．

定理 7.3.1 より

$$\begin{aligned}
v_2\left(x^n-y^n\right)&=v_2\left(\left(x^2\right)^{\frac{n}{2}}-\left(y^2\right)^{\frac{n}{2}}\right)\\
&=v_2\left(x^2-y^2\right)+v_2\left(\frac{n}{2}\right)\\
&=v_2(x-y)+v_2(x+y)+v_2(n)-1.
\end{aligned}$$

したがって，①は成り立つ． □

例題 7.3.1　次の問いに答えよ．

(1)　n を正の整数，$a=2^n$ とする． 3^a-1 は 2^{n+2} で割り切れるが 2^{n+3} では割り切れないことを示せ．

(2)　m を正の偶数とする． 3^m-1 が 2^m で割り切れるならば $m=2$ または $m=4$ であることを示せ． (2010 京都大学・理系乙)

解答

(1) 定理 7.3.2 を使うと

$$v_2(3^a-1^a)=v_2(3-1)+v_2(3+1)+v_2(a)-1$$

$$\begin{aligned} &= 2 + v_2(a) \\ &= n + 2 \end{aligned}$$

より成り立つ.

(2) $m = 2^n k$ (k は正の奇数) とおける．定理 7.3.2 を使うと

$$\begin{aligned} v_2(3^m - 1^m) &= v_2(3-1) + v_2(3+1) + v_2(m) - 1 \\ &= 2 + v_2(m) \\ &= n + 2. \end{aligned}$$

$3^m - 1$ が 2^m で割り切れるので

$$n + 2 \geq m = 2^n k \geq 2^n.$$

すなわち $n + 2 \geq 2^n$ が成り立つ.

$n \geq 3$ のとき $2^n > n + 2$ が成り立つことを数学的帰納法で示せるから $n = 1$ または $n = 2$ を得る．$(n, k) = (1, 1), (2, 1)$ から $m = 2$ または $m = 4$ である． □

注　$n \geq 3$ のとき $2^n > n + 2$ が成り立つことを n に関する数学的帰納法で示す.

(I) $n = 3$ のとき $2^n = 2^3 = 8 > 5 = n + 2$ より，不等式は成り立つ.

(II) $n = k$ (≥ 3) のとき成り立つと仮定すると，$2^k > k + 2$.

この不等式の両辺に 2 をかけると

$$2^{k+1} > 2(k + 2) = 2k + 4 > k + 3$$

となり，$n = k + 1$ のときも不等式は成り立つ.

(III) (I)，(II) より，すべての正の整数 $n \geq 3$ に対して，$2^n > n + 2$ が成り立つ.

7.4 例題と問題

例題 7.4.1 (Russia 1996)

Find all positive integers n for which there exist positive integers x, y and k such that $\gcd(x,y)=1$, $k>1$, and $3^n = x^k + y^k$.

解答 k は奇数である．

もしも，k が偶数だとすると，x^k, y^k は平方数である．

整数 a, b について，$3 \mid a^2+b^2 \iff 3 \mid a$ かつ $3 \mid b$ が成り立つ．

このことを使うと，$3 \mid 3^n = x^k + y^k = \left(x^{\frac{k}{2}}\right)^2 + \left(y^{\frac{k}{2}}\right)^2$ だから，$3 \mid x^{\frac{k}{2}}$ かつ $3 \mid y^{\frac{k}{2}}$ から $3 \mid x$ かつ $3 \mid y$ となり，$\gcd(x,y)=1$ に矛盾する．

k は奇数なので

$$x^k + y^k = (x+y)\left(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}\right)$$

が成り立つから，

$$3^n = (x+y)\left(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}\right). \qquad \cdots\cdots ①$$

$x+y \geq 2$ だから，①から

$$x + y = 3^m \quad (m \in \mathbb{N}) \qquad \cdots\cdots ②$$

と表せる．②から，$3 \mid x+y$ で，$\gcd(x,y)=1$ なので，$3 \nmid x, 3 \nmid y$ である．定理 7.2.2 より

$$v_3\left(3^n\right) = v_3\left(x^k + y^k\right) = v_3(x+y) + v_3(k)$$

から

$$n = m + v_3(k). \qquad \cdots\cdots ③$$

$v_3(k) = 0$ とすると，$n = m$ で $x^k + y^k = x + y = 3^n$ となる．

$k \geq 3$, $x, y \geq 1$ より $x^k \geq x, y^k \geq y$ から $x^k + y^k \geq x + y$ で等号は $x = y = 1$ のときのみ成立する．このとき，$x + y = 2$ は 3 で割り切れないから矛盾が生じる．

したがって

$$v_3(k) \geq 1 \qquad \cdots\cdots ④$$

が成り立つ．

m の値で場合分けする．

- $m \geq 2$ の場合

  $\alpha = v_3(k) \geq 1$ とおくと，$3^\alpha \mid k$ より $3^\alpha \leq k$.

すべての正の整数 a に対して，$a+2 \leq 3^a$ が成り立つことを数学的帰納法で示すことができるから，この不等式を使うと，$\alpha+2 \leq 3^\alpha$.
よって，$\alpha+2 \leq 3^\alpha \leq k$ から $\alpha+2 \leq k$ すなわち，

$$v_3(k) \leq k-2. \qquad \cdots\cdots ⑤$$

$k \geq 3$ だから，$\dfrac{x^k+y^k}{2} \geq \left(\dfrac{x+y}{2}\right)^k = \left(\dfrac{3^m}{2}\right)^k$ が成り立つので

$$\begin{aligned} x^k+y^k &\geq 2\cdot\left(\frac{3^m}{2}\right)^k = 3^m\left(\frac{3^m}{2}\right)^{k-1} \\ &> 3^m(3^{m-1})^{k-1} \\ &\geq 3^m\cdot 3^{k-1} \qquad (\because\ m \geq 2) \\ &> 3^m\cdot 3^{k-2} \\ &\geq 3^m\cdot 3^{v_3(k)} \\ &= 3^n. \end{aligned}$$

これは，$x^k+y^k=3^n$ に矛盾する．

- $m=1$ の場合

$x+y=3$ から $(x,y)=(1,2),(2,1)$
③から，$n=1+v_3(k)$ で $3^n=x^n+y^k$ は

$$3^{1+v_3(k)} = 1+2^k$$

となる．
$\alpha = v_3(k) \geq 1$ とおくと，$3^\alpha \mid k$ より $3^\alpha \leq k$.
$3^{v_3(k)} \leq k$ であるから，

$$1+2^k = 3^{1+v_3(k)} = 3\cdot 3^{v_3(k)} \leq 3k$$

から

$$1+2^k \leq 3k. \qquad \cdots\cdots ⑥$$

すべての正の整数 $a \geq 4$ に対して，$2^a+1 > 3a$ が成り立つことを数学的帰納法で示すことができるから，⑥を満たす k は $k=3$ のみである．このとき，$n=1+v_3(k)=2$.
よって，$(x,y,n,k)=(1,2,2,3),(2,1,2,3)$.

以上のことから，$n=2$.

例題 7.4.2 (Balkan 1993)

Let p be a prime number and $m > 1$ be a positive integer.

Show that if for some positive integers $x > 1, y > 1$ we have $\dfrac{x^p + y^p}{2} = \left(\dfrac{x+y}{2}\right)^m$, then $m = p$.

解答 すべての正の整数 n に対して，$\dfrac{x^n + y^n}{2} \geq \left(\dfrac{x+y}{2}\right)^n$ が成り立つことを数学的帰納法で示すことができる．

さて，この不等式を使うと，$\dfrac{x^p + y^p}{2} = \left(\dfrac{x+y}{2}\right)^m \leq \dfrac{x^m + y^m}{2}$ から

$$\frac{x^p + y^p}{2} \leq \frac{x^m + y^m}{2}.$$

$p > m$ だとすると，$x, y > 1$ だから，$x^p > x^m, y^p > y^m$ より $\dfrac{x^p + y^p}{2} > \dfrac{x^m + y^m}{2}$ となり，$\dfrac{x^p + y^p}{2} \leq \dfrac{x^m + y^m}{2}$ に矛盾する，

よって，

$$p \leq m \qquad \cdots\cdots ①$$

でなければならない．

$d = \gcd(x, y)$ とおくと，$x = dx_1$, $y = dy_1$, $\gcd(x_1, y_1) = 1$ を満たす正の整数 x_1, y_1 が存在する．

これらを，$\dfrac{x^p + y^p}{2} = \left(\dfrac{x+y}{2}\right)^m$ に代入すると，$\dfrac{d^p x_1^p + d^p y_1^p}{2} = \dfrac{d^m (x_1 + y_1)^m}{2^m}$ から

$$2^{m-1}\left(x_1^p + y_1^p\right) = d^{m-p}(x_1 + y_1)^m. \qquad \cdots\cdots ②$$

p の偶奇で 2 つの場合に分ける．

(i) p が奇数の場合

$q \mid x_1 + y_1$ を満たす素数 q をとる．$\gcd(x_1, y_1) = 1$ だから，$q \nmid x_1, q \nmid y_1$ である．

$v = v_q(x_1 + y_1) \geq 1$ とおく．

q が奇数ならば，

$$v_q\left(2^{m-1}\left(x_1^p + y_1^p\right)\right) = v_q\left(x_1^p + y_1^p\right) = v_q(x_1 + y_1) + v_q(p) = v + v_q(p),$$

p, q はともに奇素数だから $v_q(p) \in \Big\{0,\ 1\Big\}$.

$$v_q\left(d^{m-p}(x_1 + y_1)^m\right) = v_q\left(d^{m-p}\right) + m v_q(x_1 + y_1) \geq mv.$$

$v_q\left(2^{m-1}\left(x_1^p + y_1^p\right)\right) = v_q\left(d^{m-p}(x_1 + y_1)^m\right)$ だから

$$v + v_q(p) \geq mv \qquad 1 \geq v_q(p) \geq (m-1)v \geq m - 1.$$

$1 \geq m-1$ から $m \leq 2$ となるが $m > 1$ であったから，$m = 2$．①から $p \leq 2$ となり，p が奇素数であることに矛盾する．
したがって，q は偶数でなければならない．q は素数だから，$q = 2$ となる．

$$v_2\left(2^{m-1}\left(x_1^p + y_1^p\right)\right) = v_2\left(2^{m-1}\right) + v_2\left(x_1^p + y_1^p\right) = m - 1 + v_2\left(x_1^p + y_1^p\right).$$

$2 \mid x_1 + y_1, \gcd(x_1, y_1) = 1$ から $2 \nmid x_1, 2 \nmid y_1$ が成り立つ．また，$\gcd(p, 2) = 1$ だから，補助定理 7.1.2 より，$v_2\left(x_1^p + y_1^p\right) = v_2\left(x_1 + y_1\right) = v$ が成り立つから，

$$v_2\left(2^{m-1}\left(x_1^p + y_1^p\right)\right) = m - 1 + v_2\left(x_1^p + y_1^p\right) = m - 1 + v.$$

また，

$$v_2\left(d^{m-p}(x_1 + y_1)^m\right) = v_2\left(d^{m-p}\right) + mv_2(x_1 + y_1) \geq mv$$

が成り立ち，$v_2\left(2^{m-1}\left(x_1^p + y_1^p\right)\right) = v_2\left(d^{m-p}(x_1 + y_1)^m\right)$ だから

$$m - 1 + v \geq mv \quad \text{すなわち} \quad (m-1)(v-1) \leq 0.$$

$m \geq 2$ だから，$v \leq 1$．ところが，$v \geq 1$ であったから，$v = 1$ となる．
よって，$2 \parallel x_1 + y_1$.
$q \mid x_1 + y_1$ となる奇素数 q はないから，$x_1 + y_1 = 2$ が成り立つ．
結局 $x_1 = y_1 = 1$ となり $x = y$ で，$\dfrac{x^p + y^p}{2} = \left(\dfrac{x+y}{2}\right)^m$ から，$m = p$.

(ii) p が偶数の場合，$p = 2$.
$x \geq 2, y \geq 2$ より $x + y \geq 4$ だから

$$\left(\frac{x+y}{2}\right)^3 \geq 2\left(\frac{x+y}{2}\right)^2 > \frac{x^2 + y^2}{2}$$

が成り立つ．
$m \geq 3$ だと

$$\left(\frac{x+y}{2}\right)^m \geq \left(\frac{x+y}{2}\right)^3 > \frac{x^2 + y^2}{2}$$

となり，$\dfrac{x^2 + y^2}{2} = \left(\dfrac{x+y}{2}\right)^m$ に矛盾する．
よって，$m \leq 2$．ところが $m \geq 2$ であったから，$m = 2$ となり，$m = p$.　□

例題 7.4.3 Find all positive integers a, b that are greater than 1 and satisfy $b^a \mid a^b - 1$.

解答 $b > 1$ だから，$p \mid b$ を満たす最小の素数 p をとる．$p \mid b \mid b^a \mid a^b - 1$ から $p \mid a^b - 1$ となるので，$\mathrm{ord}_p(a)$ が存在するから，$m = \mathrm{ord}_p(a)$ とおくと，$m \mid b$.

$p \mid a^b - 1$ から $p \nmid a$ なので，フェルマーの小定理より，$a^{p-1} - 1 \equiv 0 \pmod{p}$.
よって $m \mid p - 1$.

$m > 1$ だとすると，$p_1 \mid m$ となる素数 p_1 が存在し，$p_1 \mid m \mid p - 1$ から $p_1 \leq m \leq p - 1 < p$ となり p の最小性に矛盾する．

したがって，$m = 1$ でなければならない．このとき，

$$p \mid a - 1. \qquad \cdots\cdots ①$$

p の偶奇で 2 つの場合に分ける．

(i) p が奇数の場合

①から $p \mid a - 1, p \nmid a, p \nmid 1$ なので，定理 7.2.1 より

$$v_p\left(a^b - 1\right) = v_p\left(a - 1\right) + v_p\left(b\right).$$

また，$b^a \mid a^b - 1$ より

$$v_p\left(a^b - 1\right) \geq v_p\left(b^a\right) = a\, v_p\left(b\right)$$

が成り立つから

$$v_p\left(a - 1\right) + v_p\left(b\right) \geq a\, v_p\left(b\right).$$

この不等式を変形すると

$$v_p\left(a - 1\right) \geq (a - 1) v_p\left(b\right) \geq a - 1.$$

$p^{a-1} \mid a - 1$ が成り立つから，

$$p^{a-1} \leq a - 1. \qquad \cdots\cdots ②$$

ところが，$A, q \geq 2$ が正の整数のとき，$q^A > A$ が成り立つから，$p^{a-1} > a - 1$ となり，②に矛盾する．

(ii) p が偶数の場合，$p = 2$.

$2 \mid a - 1$ から a は奇数で，$2 \mid a + 1$.

$2 \mid b$ より b は偶数である．

$2 \mid a - 1, 2 \nmid a, 2 \nmid 1$ なので，定理 7.3.2 より

$$v_2\left(a^b - 1\right) = v_2\left(a - 1\right) + v_2\left(a + 1\right) + v_2\left(b\right) - 1.$$

また，$b^a \mid a^b - 1$ より

$$v_2\left(a^b-1\right) \geq v_2\left(b^a\right) = a\, v_2\left(b\right)$$

が成り立つから

$$v_2\left(a-1\right) + v_2\left(a+1\right) + v_2\left(b\right) - 1 \geq a\, v_2\left(b\right).$$

この不等式を変形すると

$$v_2\left(a-1\right) + v_2\left(a+1\right) \geq (a-1)v_2\left(b\right) + 1 \geq (a-1)\cdot 1 + 1 = a$$

から

$$v_2\left(a-1\right) + v_2\left(a+1\right) \geq a. \qquad \cdots\cdots ③$$

$2 \mid a-1, 2 \mid a+1$ から

$$a-1 = 2^l p_1,\ l \geq 1,\ \gcd(2, p_1) = 1, \quad a+1 = 2^m p_2,\ m \geq 1,\ \gcd(2, p_2) = 1$$

とおくと

$$2 = (a+1) - (a-1) = 2^m p_2 - 2^l p_1 \qquad 1 = 2^{m-1} p_2 - 2^{l-1} p_1$$

この式から，$\min\left(2^{m-1}, 2^{l-1}\right) = 1$ がわかり，$l = 1$ または $m = 1$　となる．

$l = 1$ の場合

③より，$v_2\left(a+1\right) \geq a-1$ となるので，$2^{a-1} \mid a+1$. よって，

$$2^{a-1} \leq a+1. \qquad \cdots\cdots ④$$

$A \geq 4$ のとき，$2^{A-1} > A+1$ が成り立つから，$a \leq 3$.

$a > 1$ は奇数なので $a = 3$ である．

このとき，$v_2(a-1) = v_2(2) = 1, v_2(a+1) = v_2(4) = 2$ で，③で等号が成り立つから，$v_2(b) = 1$ となる．

$b = 2B$　(B は奇数) とおくと，$b^a \mid a^b - 1$ は

$$8B^3 \mid 3^{2B} - 1 \qquad \cdots\cdots ⑤$$

となる．

[1] $B > 1$ の場合

$B > 1$ だから，$q \mid B$ を満たす最小の素数 q をとると，q は奇素数である．

$q \mid B \mid 8B^3 \mid 3^{2B} - 1$ から $q \mid 3^{2B} - 1$ となるので，$\mathrm{ord}_q(3)$ が存在するから，$n = \mathrm{ord}_q(3)$ とおくと，$n \mid 2B$.

$q \mid 3^{2B}-1$ から $q \nmid 3$ なので，フェルマーの小定理より，$3^{q-1}-1 \equiv 0 \pmod{q}$.
よって $n \mid q-1$ も成り立つから，

$$n \mid 2B, \quad n \mid q-1. \qquad \cdots\cdots ⑥$$

n が偶数のとき，$n=2n_1$ $(n_1 \in \mathbb{N})$ とおくと，$n_1 \mid B$, $n_1 \mid \dfrac{q-1}{2}$.
$n_1 > 1$ だとすると，$q_1 \mid n_1$ となる素数 q_1 が存在し，
$q_1 \mid n_1 \mid B$ かつ $q_1 \leq n_1 \leq \dfrac{q-1}{2} < q-1$ となり q の最小性に矛盾する．
したがって，$n_1=1$ でなければならない．このとき，$n=2$.
ところが，$q \mid 3^n-1=3^2-1=8$ となり，q が奇素数であることに矛盾する．
n が奇数のとき，⑥から

$$n \mid B, \ n \mid q-1.$$

$n > 1$ だとすると，$q_1 \mid n$ となる素数 q_1 が存在し，
$q_1 \mid n \mid B$ かつ $q_1 \leq n \leq q-1 (< q)$ となり q の最小性に矛盾する．
したがって，$n=1$ でなければならない．
ところが，$q \mid 3^n-1=3^1-1=2$ となり，q が奇素数であることに矛盾する．
[2] $B=1$ の場合，⑤は成り立つ．
$b=2B$ から $b=2$ となるから，$\boldsymbol{a=3, b=2}$.
$m=1$ の場合
　③より，$v_2(a-1) \geq a-1$ となるので，$2^{a-1} \mid a-1$. よって，

$$2^{a-1} \leq a-1. \qquad \cdots\cdots ⑦$$

A が正の整数のとき，$2^A > A$ が成り立つから，⑦を満たす a は存在しない．

以上のことから，求める正の整数 a, b は $a=3, b=2$ □

例題 7.4.4　Find all positive integer solutions of the equation $x^{2009}+y^{2009}=7^z$.

解答　$2009=7^2\cdot 41$.

$x+y\geq 2$ で

$$7^z=x^{2009}+y^{2009}=(x+y)\left(x^{2008}-x^{2007}y+\cdots-xy^{2007}+y^{2008}\right)$$

から，$7\mid x+y$ である．

$7\nmid x, 7\nmid y$ でないと，LTE が使えないから，

$$x=7^px_1, y=7^py_1,\ p\in\mathbb{N}_0,\ x_1,y_1\in\mathbb{N},\ \gcd(7,x_1)=1 \text{ または } \gcd(7,y_1)=1$$

とおき，$x^{2009}+y^{2009}=7^z$ に代入すると，$\left(7^px_1\right)^{2009}+\left(7^py_1\right)^{2009}=7^z$.

$z_1=z-2009p$ とおくと

$$x_1^{2009}+y_1^{2009}=7^{z_1} \qquad \cdots\cdots ①$$

となる．$x_1,y_1\in\mathbb{N}$，①から，$z_1\in\mathbb{N}$ となる．

①から，$7\mid x_1+y_1$ が成り立つ．$\gcd(7,x_1)=1$ または $\gcd(7,y_1)=1$ であるから，$7\nmid x_1, 7\nmid y_1$ となる．

定理 7.2.2 より，

$$v_7\left(x_1^{2009}+y_1^{2009}\right)=v_7\left(x_1+y_1\right)+v_7\left(2009\right)=v_p\left(x_1+y_1\right)+2$$

が成り立つ．よって，

$$x_1^{2009}+y_1^{2009}=7^2\cdot k\cdot(x_1+y_1)\quad(7\nmid k)$$

とおける．$x_1^{2009}+y_1^{2009}=7^{z_1}$ だから，$k=1$ で

$$x_1^{2009}+y_1^{2009}=49\cdot(x_1+y_1). \qquad \cdots\cdots ②$$

②を変形すると

$$x_1\left(x_1^{2008}-49\right)+y_1\left(y_1^{2008}-49\right)=0. \qquad \cdots\cdots ③$$

$x_1\geq 2, y_1\geq 2$ だとすると，$x_1^{2008}-49\geq 2^{2008}-49>0, y_1^{2008}-49\geq 2^{2008}-49>0$ となり，③は成り立たない．

したがって，$x_1=1$ または $y_1=1$ である．対称性から $x_1=1$ としても一般性を失わない．$x_1=1$ のとき，③から

$$y_1\left(y_1^{2008}-49\right)=48 \qquad \cdots\cdots ④$$

$y_1\geq 2$ のとき，$y_1^{2008}-49\geq 2^{2008}-49>48$ となり，④は成り立たない．$y_1=1$ のときも④は成り立たない．

ゆえに，解は存在しない．　□

問題 7.4.1 Let k be a positive integer. Find all positive integers n such that $3^k \mid 2^n - 1$.

問題 7.4.2 (UNESCO Competition 1995)

Let a, n be two positive integers and let p be an odd prime number such that

$$a^p \equiv 1 \pmod{p^n}.$$

Prove that

$$a \equiv 1 \pmod{p^{n-1}}.$$

問題 7.4.3 (Iran Second Round 2008)

Show that the only positive integer value of a for which $4\,(a^n + 1)$ is a perfect cube for all positive integers n, is 1.

問題 7.4.4 (Ireland 1996)

Let p be a prime number, and a and n positive integers. Prove that if

$$2^p + 3^p = a^n$$

then $n = 1$.

問題 7.4.5 (Russia 1996)

Let x, y, p, n, k be positive integers such that n is odd and p is an odd prime. Prove that if $x^n + y^n = p^k$ then n is a power of p.

類題 (Hungary-Israel Binational 2006)

If natuaral numbers x, y, p, n, k with $n > 1$ odd and p an odd prime satisfy $x^n + y^n = p^k$, prove that n is a power of p.

問題 7.4.6 Find the sum of all the divisors d of $N = 19^{88} - 1$ which are of the form $d = 2^a 3^b$ with $a, b \in \mathbb{N}_0$.

問題 7.4.7 Let p be a prime number. Solve the equation $a^p - 1 = p^k$ in the set of positive integers.

問題 7.4.8 For some positive integer n , the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.

問題 7.4.9 (IMO Shortlist 1991)

Find the higest degree k of 1991 for which 1991^k devides the number

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

問題 7.4.10 (China Western Mathematical Olympiad 2010)

Suppose that m and k are non-negative integers, and $p = 2^{2^m} + 1$ is a prime number. Prove that

(1) $2^{2^{m+1}p^k} \equiv 1 \pmod{p^{k+1}}$;

(2) $2^{m+1}p^k$ is the smallest positive integer n satisfying the congruence equation $2^n \equiv 1 \pmod{p^{k+1}}$.

問題 7.4.11 Let $p \geq 5$ be a prime. Find the maximum value of positive integer k such that

$$p^k \mid (p-2)^{2(p-1)} - (p-4)^{p-1}.$$

問題 7.4.12 (China TST 2009)

Let $a > b > 1$ be positive integers and b be an odd number, let n be a positive integer. If $b^n \mid a^n - 1$, then show that $a^b > \dfrac{3^n}{n}$.

問題 7.4.13 (Romanian Junior Balkan TST 2008)

Let p be a prime number, $p \neq 3$, and integers a, b such that $p \mid a+b$ and $p^2 \mid a^3+b^3$. Prove that $p^2 \mid a+b$ or $p^3 \mid a^3+b^3$.

問題 7.4.14 (IMO 1990)

Determine all integers $n > 1$ such that

$$\frac{2^n + 1}{n^2}$$

is an integer.

問題 7.4.15 Find all pairs of prime p, q such that $pq \mid (5^p - 2^p)(5^q - 2^q)$.

問題 7.4.16 For some natural number n let a be the greatest natural number for which $5^n - 3^n$ is divisible by 2^a. Also let b be the greatest natural number such that $2^b \leq n$. Prove that $a \leq b + 3$.

問題 7.4.17 (Romania TST 1994)

Let n be an odd positive integer. Prove that $((n-1)^n + 1)^2$ divides $n(n-1)^{(n-1)^n+1} + n$.

問題 7.4.18 Find all positive integers n such that $3^n - 1$ is divisible by 2^n.

問題 7.4.19 (Romania TST 2009)

Let $a, n \geq 2$ be two integers, which have the following property:

there exists an integer $k \geq 2$, such that n divides $(a-1)^k$.

Prove that n also divides $a^{n-1} + a^{n-2} + \cdots + a + 1$.

問題 7.4.20 Find all the positive integers a sucn that $\dfrac{5^a + 1}{3^a}$ is a positive integer.

問題 7.4.21 Let $k > 1$ be an integer. Show that there exists infinitely many positive integers n such that

$$n \mid 1^n + 2^n + 3^n + \cdots + k^n.$$

問題 7.4.22 (IMO shortlist 2010)

Find all pairs (m, n) of nonnegative integers for which

$$m^2 + 2 \cdot 3^n = m\left(2^{n+1} - 1\right).$$

類題 (Vietmam Team Selection Test 2011)

Find all positive integers n such that $A = 2^{n+2}\left(2^n - 1\right) - 8 \cdot 3^n + 1$ is a perfect square.

答えは $n = 3, 5$.

問題 7.4.23 (Gabriel Dospinescu, Mathlinks Contest)

Let a, b two different positive rational numbers such that for infinitely many numbers n, $a^n - b^n$ is integer. Then prove that a, b are also integers.

第8章

円分多項式

8.1　1の原始n乗根

nを正の整数とするとき，方程式$z^n = 1$の根を1のn乗根という．1のn乗根はn個あって，それらは

$$w_k = \cos\left(\frac{2\pi}{n} \times k\right) + i\sin\left(\frac{2\pi}{n} \times k\right) \quad (k = 0, 1, \ldots, n-1) \tag{8.1}$$

で与えられる．

$w_0 = w_n = 1$であるから，1のn乗根は

$$w_k = \cos\left(\frac{2\pi}{n} \times k\right) + i\sin\left(\frac{2\pi}{n} \times k\right) \quad (k = 1, 2, \ldots, n) \tag{8.2}$$

でも得られる．

(8.1) の証明 $z = r(\cos\theta + i\sin\theta) \quad (r > 0, 0 \leq \theta < 2\pi)$とおくと，$z^n = 1$より

$$r^n(\cos n\theta + i\sin n\theta) = \cos 0 + i\sin 0.$$

両辺の絶対値と偏角を比較して

$$r^n = 1, \quad n\theta = 0 + 2k\pi \ (k \in \mathbb{Z}).$$

$r > 0$より $r = 1$.
また，$n\theta = 2k\pi$, $0 \leq \theta < 2\pi$より $\theta = \dfrac{2k\pi}{n}$ $(k = 0, 1, \ldots, n-1)$.
よって，1のn乗根は，(8.1) のようになる．　□

例 8.1.1　1の6乗根は

$$w_0 = 1, w_1 = \frac{1+\sqrt{3}i}{2}, w_2 = \frac{-1+\sqrt{3}i}{2}, w_3 = -1, w_4 = \frac{-1-\sqrt{3}i}{2}, w_5 = \frac{1-\sqrt{3}i}{2}$$

で，

$$w_0^1 = 1, w_3^2 = 1, w_2^3 = w_4^3 = 1, w_1^6 = w_5^6 = 1$$

となっている．

n を正の整数，ζ を 1 の n 乗根とする．

$\zeta^m = 1$ を満たす最小の正の整数 m のことを ζ の**位数** (order of ζ) といい，$\boldsymbol{ord(\zeta)}$ で表すことにする．

補助定理 8.1.1　n を正の整数，ζ を 1 の n 乗根とする．

任意の正の整数 m に対して

$$\zeta^m = 1 \iff ord(\zeta) \mid m.$$

特に，$ord(\zeta) \mid n$ が成り立つ．

証明　$d = ord(\zeta)$ とおく．

$\zeta^m = 1$ とする．m を d で割った商を q，余りを r とおくと $m = dq + r,\ 0 \leq r < d$ を満たす整数 q, r が存在する．

$$1 = \zeta^m = \zeta^{dq+r} = \left(\zeta^d\right)^q \zeta^r = 1^q \cdot \zeta^r = \zeta^r$$

が成り立つ．$r \neq 0$ だと，$\zeta^r = 1,\ 0 < r < d$ となり，d の最小性に矛盾する．
よって，$r = 0$ で $d \mid m$ が成り立つ．

$d \mid m$ とする．$m = dm_1\ (m_1 \in \mathbb{N})$ とおけるから

$$\zeta^m = \zeta^{dm_1} = \left(\zeta^d\right)^{m_1} = 1^{m_1} = 1.$$ □

系 8.1.1　n を正の整数，ζ を 1 の n 乗根とする．

任意の正の整数 k, l に対して

$$\zeta^k = \zeta^l \iff k \equiv l \pmod{ord(\zeta)}.$$

特に，$1 \leq k, l \leq ord(\zeta)$ のときには $\zeta^k = \zeta^l \iff k = l$ が成り立つ．

証明　$d = ord(\zeta)$ とおく．

$\zeta^k = \zeta^l,\ k \geq l$ とする．$\zeta^k = \zeta^l$ の両辺を ζ^l で割ると，$\zeta^{k-l} = 1$.
補助定理 8.1.1 より $d \mid k - l$ が成り立つから，$k \equiv l \pmod{d}$.

$k \equiv l \pmod{d},\ k \geq l$ とする．$k = l + dm,\ m \in \mathbb{N}_0$ とおける．このとき

$$\zeta^k = \zeta^{l+dm} = \zeta^l \left(\zeta^d\right)^m = \zeta^l \cdot 1^m = \zeta^l.$$

$1 \leq k, l \leq d$ のときには，$-d+1 \leq k-l \leq d-1$ より，$k-l$ がで d 割り切れるのは $k=l$ のときしかないことから，$\zeta^k = \zeta^l \iff k=l$ が成り立つことがわかる．　□

n を正の整数，ζ を 1 の n 乗根とする．$ord(\zeta) = n$ が成り立つとき，ζ を 1 **の原始 n 乗根**という．(n 乗して初めて 1 になる，1 の n 乗根 ζ を 1 の原始 n 乗根という．)

命題 8.1.1　n を正の整数とする．

$$w_k = \cos\left(\frac{2\pi}{n} \times k\right) + i\sin\left(\frac{2\pi}{n} \times k\right) \quad (k = 0, 1, \ldots, n-1)$$

とおくと，1 の原始 n 乗根の集合は $\left\{w_k : k \in \mathbb{N},\ \gcd(k,\, n) = 1\right\}$ である．

証明　$\gcd(k,n) = 1$ のとき，$\dfrac{2k\pi}{n}$ は n 倍して初めて，2π の整数倍になるから，w_k は n 乗して初めて 1 になり，1 の原始 n 乗根である．

$\gcd(k,n) = d > 1$ のときは，$k = dk_1, n = dn_1, k_1, n_1 \in \mathbb{N}, \gcd(k_1, n_1) = 1$ とかける から，

$$\frac{2k\pi}{n} = \frac{2k_1\pi}{n_1}, \quad w_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = \cos\frac{2k_1\pi}{n_1} + i\sin\frac{2k_1\pi}{n_1}.$$

w_k は n_1 乗して初めて 1 になるから．1 の原始 n_1 乗根である．

したがって，1 の原始 n 乗根の集合は $\left\{w_k : k \in \mathbb{N},\ \gcd(k,\, n) = 1\right\}$ である．　□

- 命題 (8.1.1) より，1 の原始 n 乗根は $\varphi(n)$ 個あることがわかる．

8.2　円分多項式 (Cyclotomic Polynomials)

正の整数 n に対して，**円分多項式 $\boldsymbol{\Phi_n(x)}$** (nth cyclotomic polynomial) は 1 の原始 n 乗根 $z_1, z_2, \ldots, z_s$ $(s = \varphi(n))$ のみを根とする，最高次の係数が 1 の多項式

$$\Phi_n(x) = (x - z_1)(x - z_2)\cdots(x - z_s)$$

で定義される．$\Phi_n(x)$ は次のようにかくこともできる．

$$\Phi_n(x) = \prod_{\substack{\zeta^n=1 \\ ord(\zeta)=n}} (x - \zeta) = \prod_{\substack{1\le k\le n \\ \gcd(k,n)=1}} (x - w_k)$$

ただし，$w_k = \cos\dfrac{2k\pi}{n} + i\sin\dfrac{2k\pi}{n}$ とする．

1 の原始 n 乗根は $\varphi(n)$ 個あるから $\Phi_n(x)$ の次数は $\varphi(n)$ である．

定理 8.2.1　n が正の整数のとき

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{8.3}$$

が成り立つ．

証明 1 の n 乗根 $w_k = \cos\dfrac{2k\pi}{n} + i\sin\dfrac{2k\pi}{n}$ $(k = 1, 2, \ldots, n)$ を分類していく．

$\gcd(k, n) = 1$ のとき，$\dfrac{2k\pi}{n}$ は n 倍して初めて，2π の整数倍になるから，w_k は n 乗して初めて 1 になり，1 の原始 n 乗根である．

$\gcd(k, n) = 1$ となる k は $1, 2, \ldots n$ の中で $\varphi(n)$ 個あり，命題 (8.1.1) より，1 の原始 n 乗根は $\varphi(n)$ 個あるので，$\left\{w_k : \gcd(k,\, n) = 1,\, k \in \left\{1,\, 2,\, \ldots,\, n\right\}\right\}$ は $\Phi_n(x) = 0$ の根の集合と等しい．

$\gcd(k, n) = d > 1$ のときは，$k = dk_1, n = dn_1, k_1, n_1 \in \mathbb{N}, \gcd(k_1, n_1) = 1$ とかけるから，

$$\frac{2k\pi}{n} = \frac{2k_1\pi}{n_1}, \quad w_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = \cos\frac{2k_1\pi}{n_1} + i\sin\frac{2k_1\pi}{n_1}.$$

w_k は n_1 乗して初めて 1 になるから．1 の原始 n_1 乗根である．

$\gcd(k_1, n_1) = 1$ となる k_1 は $1, 2, \ldots n_1$ の中で $\varphi(n_1)$ 個あり，1 の原始 n_1 乗根は $\varphi(n_1)$ 個あるので，$\left\{w_k : \gcd(k,\, n) = d,\, k \in \left\{1,\, 2,\, \ldots,\, n\right\}\right\}$ は $\Phi_{n_1}(x) = 0$ の根の集合と等しい．

以上のことから

$$x^n - 1 = \prod_{\substack{d|n \\ dn_1=n}} \Phi_{n_1}(x)$$

が成り立つ．$\left\{n_1 : d \mid n,\ dn_1 = n\right\} = \left\{e : e \mid n\right\}$ であるから

$$x^n - 1 = \prod_{\substack{d|n \\ dn_1=n}} \Phi_{n_1}(x) = \prod_{e|n} \Phi_e(x). \qquad \square$$

定理 8.2.2　n が正の整数のとき

$$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)} \tag{8.4}$$

が成り立つ．

証明 (8.3) より

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

が成り立つので，メビウスの反転公式より

$$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$$

が成り立つ． $\square$

例 8.2.1　(8.4) を用いて $\Phi_n(x)$ $(1 \leq n \leq 8)$ を求めてみる．

$$\begin{aligned}
\Phi_1(x) &= (x-1)^{\mu(1)} = x - 1 \\
\Phi_2(x) &= \left(x^2-1\right)^{\mu(1)} (x-1)^{\mu(2)} = \left(x^2-1\right)(x-1)^{-1} = x + 1 \\
\Phi_3(x) &= \left(x^3-1\right)^{\mu(1)} (x-1)^{\mu(3)} = \left(x^3-1\right)(x-1)^{-1} = x^2 + x + 1 \\
\Phi_4(x) &= \left(x^4-1\right)^{\mu(1)} \left(x^2-1\right)^{\mu(2)} (x-1)^{\mu(4)} \\
&= \left(x^4-1\right)\left(x^2-1\right)^{-1} (x-1)^0 = x^2 + 1 \\
\Phi_5(x) &= \left(x^5-1\right)^{\mu(1)} (x-1)^{\mu(5)} = \left(x^5-1\right)(x-1)^{-1} = x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= \left(x^6-1\right)^{\mu(1)} \left(x^3-1\right)^{\mu(2)} \left(x^2-1\right)^{\mu(3)} (x-1)^{\mu(6)} \\
&= \left(x^6-1\right)^1 \left(x^3-1\right)^{-1} \left(x^2-1\right)^{-1} (x-1)^1 = x^2 - x + 1 \\
\Phi_7(x) &= \left(x^7-1\right)^{\mu(1)} (x-1)^{\mu(7)} = \left(x^7-1\right)(x-1)^{-1} \\
&= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= \left(x^8-1\right)^{\mu(1)} \left(x^4-1\right)^{\mu(2)} \left(x^2-1\right)^{\mu(4)} (x-1)^{\mu(8)} \\
&= \left(x^8-1\right)\left(x^4-1\right)^{-1} \left(x^2-1\right)^0 (x-1)^0 = x^4 + 1
\end{aligned}$$

今後，多項式を扱うので，記号等を確認しておきたい．$\mathbb{Z}[x]$ で整数係数の多項式全体の集合を表す．

$\mathbb{Q}[x]$ で有理数係数の多項式全体の集合を表す．

$\mathbb{R}[x]$ で実数係数の多項式全体の集合を表す．

定理 8.2.3　多項式 $A(x), B(x) \in \mathbb{Q}[x]$ に対して

$$A(x) = B(x)Q(x) + R(x), \quad \deg R(x) < \deg B(x) \text{ または } R(x) = 0$$

となる多項式 $Q(x), R(x) \in \mathbb{Q}[x]$ がただ一つ存在する．

$Q(x)$，$R(x)$ については，整数の場合と同様に，$A(x)$ を $B(x)$ で割った商を $Q(x)$，余りを $R(x)$ と呼ぶ．

(証明省略)

命題 8.2.1　m, n は正の整数とする．

多項式

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$$
$$g(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in \mathbb{Z}[x],\ b_n \neq 0$$

に対して，$g(x)$ を $f(x)$ で割った商を $q(x)$，余り $r(x)$ をとすると，$q(x), r(x) \in \mathbb{Z}[x]$ が成り立つ．

実際に割り算をすることを考えれば，割り算は最高次の係数を 1 で割るだけで，あとは係数の整数間における加法，減法，乗法だけなので，$q(x), r(x) \in \mathbb{Z}[x]$ は明らかに成り立つが……

証明　$n < m$ のときは，

$$g(x) = f(x) \cdot 0 + g(x), \quad \deg g(x) < \deg f(x)$$

より $q(x) = 0 \in \mathbb{Z}[x],\ r(x) = g(x) \in \mathbb{Z}[x]$ となるので成り立つ．

$n \geq m$ のときは，n に関する数学的帰納法で示す．

(I) $n = m$ のとき

$$g(x) - b_mf(x) = (b_{m-1} - b_ma_{m-1})x^{m-1} + (b_{m-2} - b_ma_{m-2})x^{m-1} + \cdots + (b_0 - b_ma_0)$$

より $q(x) = b_m \in \mathbb{Z}[x],\ r(x) = (b_{m-1} - b_ma_{m-1})x^{m-1} + (b_{m-2} - b_ma_{m-2})x^{m-1} + \cdots + (b_0 - b_ma_0) \in \mathbb{Z}[x]$ となるので成り立つ．

(II) $k \geq m$ とし，$n \leq k$ を満たすすべての n に対して成り立つと仮定する．
$g(x) = b_{k+1}x^{k+1} + b_k x^k + \cdots + b_1 x + b_0 \in \mathbb{Z}[x],\ b_{k+1} \neq 0$
に対して

$$\begin{aligned} & g(x) - b_{k+1}x^{k-m+1}f(x) \\ = & (b_k - b_{k+1}a_{m-1})x^k + (b_{k-1} - b_{k+1}a_{m-2})x^{k-1} + \cdots \\ & + (b_{k-m+1} - b_{k+1}a_0)x^{k-m+1} + b_{k-m}x^{k-m} + \cdots + b_1 x + b_0 \end{aligned}$$

は k 次以下の整数係数の多項式であるから，仮定より

$$g(x) - b_{k+1}x^{k-m+1}f(x) = f(x)q_1(x) + r_1(x), \quad \deg r_1(x) < \deg f(x) \text{ または } r_1(x) = 0.$$

となる $q_1(x), r_1(x) \in \mathbb{Z}[x]$ が存在する．この等式を変形すると

$$\begin{aligned} g(x) &= b_{k+1}x^{k-m+1}f(x) + f(x)q_1(x) + r_1(x) \\ &= f(x)\left(b_{k+1}x^{k-m+1} + q_1(x)\right) + r_1(x). \end{aligned}$$

$q(x) = b_{k+1}x^{k-m+1} + q_1(x) \in \mathbb{Z}[x], r(x) = r_1(x) \in \mathbb{Z}[x]$ とおくと

$$g(x) = f(x)q(x) + r(x), \quad \deg r(x) < \deg f(x) \text{ または } r(x) = 0.$$

となる $q(x), r(x) \in \mathbb{Z}[x]$ が存在することが言えた．

(III) (I)，(II) よりすべての正の数 $n \geq m$ について成り立つ． □

定理 8.2.4 n は正の整数とするとき，次のことが成り立つ．
$\Phi_n(x) \in \mathbb{Z}[x]$ で，$\Phi_n(x)$ の最高次の係数は 1 である．

証明 n に関する数学的帰納法で証明する．

(I) $n = 1$ のとき， $\Phi_1(x) = x - 1$ であるから成り立つ．

(II) $k \geq 2$ として，$n < k$ を満たすすべての n に対して成り立つと仮定する．

$$x^k - 1 = \prod_{d|k} \Phi_d(x) = \Phi_k(x) \prod_{\substack{d|k \\ d<k}} \Phi_d(x)$$

より

$$f(x) = \prod_{\substack{d|k \\ d<k}} \Phi_d(x)$$

とおく．仮定より，すべての $1 \leq d < k$ について，$\Phi_d(x)$ は整数係数の多項式で，最高次の係数は 1 となるので，$f(x)$ も整数係数の多項式で，最高次の係数は 1 となる．

$g(x) = x^k - 1 \in \mathbb{Z}[x]$ を $f(x)$ で割った商を $q(x)$，余りを $r(x)$ とすると

$$g(x) = f(x)q(x) + r(x), \quad r(x) = 0 \text{ または } \deg r(x) < \deg f(x)$$

とかけて，命題 8.2.1 より $q(x), r(x) \in \mathbb{Z}[x]$ となる．

また，

$$g(x) = x^k - 1 = \prod_{d|k} \Phi_d(x) = \Phi_k(x) \prod_{\substack{d|k \\ d<k}} \Phi_d(x) = \Phi_k(x) f(x)$$

を使うと，$\Phi_k(x)f(x) = f(x)q(x) + r(x)$ すなわち

$$r(x) = f(x)\left(\Phi_k(x) - q(x)\right)$$

が成り立つ．$\Phi_k(x) \neq q(x)$ だと，

$$\deg r(x) = \deg f(x) + \deg\left(\Phi_k(x) - q(x)\right) \geq \deg f(x)$$

となり，$r(x) = 0$ または $\deg r(x) < \deg f(x)$ に矛盾する．

したがって，$\Phi_k(x) = q(x)$, $r(x) = 0$ となり，$\Phi_k(x) \in \mathbb{Z}[x]$.

$f(x)$ の最高次の係数は 1 で $x^k - 1 = f(x)q(x) = f(x)\Phi_k(x)$ より $\Phi_k(x)$ の最高次の係数は 1 である．

以上のことから，$n = k$ のときも成り立つ．

(III) (I)，(II) よりすべての正の数 n について成り立つ． □

命題 8.2.2　n, a は正の整数で $n \geq 2, a \geq 2$ とする．

r が $r \mid n$, $r < n$ を満たす正の整数ならば

$$\Phi_n(a) \,\Big|\, \frac{a^n - 1}{a^r - 1}$$

が成り立つ．

証明　$a^n - 1 = \prod_{d|n} \Phi_d(a)$, $a^r - 1 = \prod_{d_1|r} \Phi_{d_1}(a)$ で，定理 8.2.4 より $\Phi_d(a) \in \mathbb{Z}$, $\Phi_{d_1}(a) \in \mathbb{Z}$.

$$\frac{a^n - 1}{a^r - 1} = \frac{\displaystyle\prod_{d|n} \Phi_d(a)}{\displaystyle\prod_{d_1|r} \Phi_{d_1}(a)} = \frac{\Phi_n(a) \displaystyle\prod_{\substack{d|n \\ d<n}} \Phi_d(a)}{\displaystyle\prod_{d_1|r} \Phi_{d_1}(a)}. \qquad \cdots\cdots ①$$

$d_1 \mid r$ ならば，$r \mid n, r < n$ でもあるから，$d_1 \mid n, d_1 < n$ が成り立つから

$$\left\{d_1 : d_1 \mid r,\, d_1 \in \mathbb{N}\right\} \subseteq \left\{d : d \mid n,\, d < n,\, d \in \mathbb{N}\right\}$$

となる．このことから，

$$\frac{\displaystyle\prod_{\substack{d|n\\ d<n}} \Phi_d(a)}{\displaystyle\prod_{d_1|r} \Phi_{d_1}(a)} \in \mathbb{Z}$$

がわかる．よって，①から $\Phi_n(a) \,\Big|\, \dfrac{a^n-1}{a^r-1}$. □

命題 8.2.3 (1) p が素数ならば，次のことが成り立つ．

$$\Phi_p(x) = x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1.$$

(2) p が奇素数ならば，次のことが成り立つ．

$$\Phi_{2p}(x) = x^{p-1} - x^{p-2} + x^{p-3} - \cdots + x^2 - x + 1.$$

証明

(1) p が素数のとき

$$x^p - 1 = \prod_{d|p} \Phi_d(x) = \Phi_1(x)\Phi_p(x)$$

が成り立つから

$$\Phi_p(x) = \frac{x^p-1}{\Phi_1(x)} = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1.$$

(2) p が奇素数のとき

$$x^{2p} - 1 = \prod_{d|2p} \Phi_d(x) = \Phi_{2p}(x)\Phi_p(x)\Phi_2(x)\Phi_1(x)$$

が成り立つから

$$\begin{aligned}
\Phi_{2p}(x) &= \frac{x^{2p}-1}{\Phi_p(x)\Phi_2(x)\Phi_1(x)} \\
&= \frac{x^{2p}-1}{\left(x^{p-1} + x^{p-2} + \cdots + x + 1\right)(x+1)(x-1)} \\
&= \frac{(x^p-1)(x^p+1)}{(x^p-1)(x+1)} = \frac{x^p+1}{x+1} \\
&= x^{p-1} - x^{p-2} + x^{p-3} - \cdots + x^2 - x + 1.
\end{aligned}$$ □

補助定理 8.2.1 p は素数， n は正の整数とするとき，次のことが成り立つ．

$$\Phi_{pn}(x) = \begin{cases} \Phi_n\left(x^p\right) & (p \mid n) \\ \dfrac{\Phi_n\left(x^p\right)}{\Phi_n\left(x\right)} & (p \nmid n). \end{cases} \tag{8.5}$$

証明

(1) $p \mid n$ の場合

$$\begin{aligned}\Phi_{pn}(x) &= \prod_{d \mid pn} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)} \\ &= \left(\prod_{d \mid n} \left((x^p)^{\frac{n}{d}} - 1\right)^{\mu(d)}\right) \left(\prod_{\substack{d \mid pn \\ d \nmid n}} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \\ &= \Phi_n(x^p) \prod_{\substack{d \mid pn \\ d \nmid n}} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)} \qquad \cdots\cdots ①\end{aligned}$$

と変形できる．

$d \mid pn, p \mid n, d \nmid n$ のときは，$pn = dn_1, n = pn_2$ $(n_1, n_2 \in \mathbb{N})$ とかける．これらの式から n を消去すると，

$$p^2 n_2 = dn_1.$$

$p \mid n_1$ だと，$pn = dn_1$ から $\dfrac{n}{d} = \dfrac{n_1}{p} \in \mathbb{N}$ となり，$d \mid n$. これは $d \nmid n$ に矛盾する．

したがって，$p \nmid n_1$ で，$p^2 n_2 = dn_1$ より $p^2 \mid d$ となるので，

$d \mid pn, p \mid n, d \nmid n$ のとき，$\mu(d) = 0$.

このことから

$$\prod_{\substack{d \mid pn \\ d \nmid n}} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)} = \prod_{\substack{d \mid pn \\ d \nmid n}} \left(x^{\frac{pn}{d}} - 1\right)^{0} = 1$$

となるので，①より

$$\Phi_{pn}(x) = \Phi_n(x^p).$$

(2) $p \nmid n$ の場合

$$\Phi_{pn}(x) = \prod_{d \mid pn} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)}.$$

$p \nmid n$ だから，$D_1 = \left\{d : d \mid n,\, d \in \mathbb{N}\right\}$, $D_2 = \left\{pd_1 : d_1 \mid n,\, d_1 \in \mathbb{N}\right\}$ とおくと $D_1 \cap D_2 = \emptyset$ で，pn の正の約数全体の集合は，$D_1 \cup D_2$ となるから

$$\begin{aligned}\prod_{d \mid pn} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)} &= \prod_{d \mid n} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)} \prod_{d_1 \mid n} \left(x^{\frac{pn}{pd_1}} - 1\right)^{\mu(pd_1)} \\ &= \prod_{d \mid n} \left((x^p)^{\frac{n}{d}} - 1\right)^{\mu(d)} \prod_{d_1 \mid n} \left(x^{\frac{n}{d_1}} - 1\right)^{\mu(p)\mu(d_1)}\end{aligned}$$

$$= \prod_{d|n} \left((x^p)^{\frac{n}{d}} - 1 \right)^{\mu(d)} \prod_{d_1|n} \left(x^{\frac{n}{d_1}} - 1 \right)^{-\mu(d_1)}$$
$$= \frac{\Phi_n(x^p)}{\Phi_n(x)}.$$ □

系 8.2.1 p は素数，n, k は正の整数とするとき，次のことが成り立つ．

$$\Phi_{p^k n}(x) = \begin{cases} \Phi_n\left(x^{p^k}\right) & (p \mid n) \\ \dfrac{\Phi_n\left(x^{p^k}\right)}{\Phi_n\left(x^{p^{k-1}}\right)} & (p \nmid n). \end{cases} \tag{8.6}$$

特に $a \in \mathbb{Z}$ のとき，$\Phi_{p^k n}(a) \mid \Phi_n\left(a^{p^k}\right)$.

証明 補助定理 8.2.1 より

$$\begin{aligned} \Phi_{p^k n}(x) &= \Phi_{p \cdot p^{k-1} n}(x) = \Phi_{p^{k-1} n}(x^p) \\ &= \Phi_{p \cdot p^{k-2} n}(x^p) = \Phi_{p^{k-2} n}((x^p)^p) = \Phi_{p^{k-2} n}\left(x^{p^2}\right) \\ &= \cdots\cdots \\ &= \Phi_{pn}\left(x^{p^{k-1}}\right) \\ &= \begin{cases} \Phi_n\left(\left(x^{p^{k-1}}\right)^p\right) & (p \mid n) \\ \dfrac{\Phi_n\left(\left(x^{p^{k-1}}\right)^p\right)}{\Phi_n\left(x^{p^{k-1}}\right)} & (p \nmid n). \end{cases} \\ &= \begin{cases} \Phi_n\left(x^{p^k}\right) & (p \mid n) \\ \dfrac{\Phi_n\left(x^{p^k}\right)}{\Phi_n\left(x^{p^{k-1}}\right)} & (p \nmid n). \end{cases} \end{aligned}$$ □

補助定理 8.2.2 $n \geq 2$ を正の整数で，n の素因数分解を $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ $(\alpha_1, \ldots, \alpha_r \in \mathbb{N})$ として，$N = p_1 \cdots p_r$ とおくと

$$\Phi_n(x) = \Phi_N\left(x^{\frac{n}{N}}\right)$$

が成り立つ．

証明 $d \mid n$ かつ $d \nmid N$ が成り立つとき，$\mu(d) = 0$ となることを示す．

$$d = p_1^{\beta_1} \cdots p_r^{\beta_r},\ \beta_i \in \mathbb{N}_0,\ 0 \leq \beta_i \leq \alpha_i\ (1 \leq i \leq r)$$

とおくと

$$\frac{N}{d} = p_1^{1-\beta_1} \cdots p_r^{1-\beta_r}.$$

$d \nmid N$ となるのは $1-\beta_i \leq -1$ すなわち $\beta_i \geq 2$ となる $i \in \left\{1, \ldots, r\right\}$ が存在する場合であるから，d は平方数 p_i^2 で割り切れて，$\mu(d) = 0$ となる．
ゆえに

$$\begin{aligned}
\Phi_n(x) &= \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)} \\
&= \prod_{d|N} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)} \prod_{\substack{d|n \\ d\nmid N}} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)} \\
&= \prod_{d|N} \left(\left(x^{\frac{n}{N}}\right)^{\frac{N}{d}} - 1\right)^{\mu(d)} \prod_{\substack{d|n \\ d\nmid N}} \left(x^{\frac{n}{d}} - 1\right)^{0} \\
&= \Phi_N\left(x^{\frac{n}{N}}\right).
\end{aligned}$$

□

8.3　多項式の合同

整数係数の多項式

$$\begin{aligned}
f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \\
g(x) &= b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0
\end{aligned}$$

において，$a_0 \equiv b_0, a_1 \equiv b_1, \ldots, a_n \equiv b_n \pmod{m}$ が成り立つとき，これらの多項式は互いに合同であるといい，

$$f(x) \equiv g(x) \pmod{m}$$

と表す．
特に $f(x) \equiv 0 \pmod{m}$ となるのは，$f(x)$ の各係数が m で割り切れるときである．

命題 8.3.1　$f_1(x) \equiv g_1(x) \pmod{m}$, $f_2(x) \equiv g_2(x) \pmod{m}$ のとき，次のことが成り立つ．

$$\begin{aligned}
f_1(x) + f_2(x) &\equiv g_1(x) + g_2(x) \pmod{m}, \\
f_1(x) - f_2(x) &\equiv g_1(x) - g_2(x) \pmod{m}, \\
f_1(x) f_2(x) &\equiv g_1(x) g_2(x) \pmod{m}.
\end{aligned}$$

証明　$f_1(x) \equiv g_1(x) \pmod{m}$, $f_2(x) \equiv g_2(x) \pmod{m}$ から

$$f_1(x) = g_1(x) + m h_1(x), \ f_2(x) = g_2(x) + m h_2(x)$$

を満たす $h_1(x), h_2(x) \in \mathbb{Z}[x]$ が存在する．このとき

$$\begin{aligned}
f_1(x) + f_2(x) &= g_1(x) + g_2(x) + m\left(h_1(x) + h_2(x)\right) \equiv g_1(x) + g_2(x) \pmod{m},\\
f_1(x) - f_2(x) &= g_1(x) - g_2(x) + m\left(h_1(x) - h_2(x)\right) \equiv g_1(x) - g_2(x) \pmod{m},\\
f_1(x)f_2(x) &= \left(f_1(x) - g_1(x)\right) f_2(x) + \left(f_2(x) - g_2(x)\right) g_1(x) + g_1(x)g_2(x)\\
&= mh_1(x)f_2(x) + mh_2(x)g_1(x) + g_1(x)g_2(x)\\
&= g_1(x)g_2(x) + m\left(h_1(x)f_2(x) + h_2(x)g_1(x)\right)\\
&\equiv g_1(x)g_2(x) \pmod{m}.
\end{aligned}$$

□

次に素数 p を法とする場合を考える．

$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ において，$a_n \not\equiv 0 \pmod{p}$ が成り立つとき，法 p に関して $f(x)$ は n 次式であるという．

$f(x), g(x)$ がそれぞれ法 p に関して n 次式，m 次式ならば

$$\begin{aligned}
f(x) &= a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad a_n \not\equiv 0 \pmod{p}\\
g(x) &= b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0, \ b_m \not\equiv 0 \pmod{p}
\end{aligned}$$

とおける．

$a_nb_m \equiv 0 \pmod{p}$ だと仮定すると $p \mid a_nb_m$ で，p は素数だから，$p \mid a_n$ または $p \mid b_m$ が成り立つ．よって，$a_n \equiv 0 \pmod{p}$ または $b_m \equiv 0 \pmod{p}$ となり，$a_n \not\equiv 0 \pmod{p}$ かつ $b_m \not\equiv 0 \pmod{p}$ に矛盾する．

したがって，$a_nb_m \not\equiv 0 \pmod{p}$ であるから，積 $f(x)g(x) \in \mathbb{Z}[x]$ は法 p に関して $n+m$ 次式である．

命題 8.3.2　p は素数で，$f(x), g(x) \in \mathbb{Z}[x]$ のとき，次のことが成り立つ．

$$f(x)g(x) \equiv 0 \pmod{p} \Longrightarrow f(x) \equiv 0 \pmod{p} \text{ または } g(x) \equiv 0 \pmod{p}.$$

証明　$f(x) \not\equiv 0 \pmod{p}$ かつ $g(x) \not\equiv 0 \pmod{p}$ と仮定する．

$f(x), g(x)$ がそれぞれ法 p に関して n 次式，m 次式とすると

$$\begin{aligned}
f(x) &= a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad a_n \not\equiv 0 \pmod{p}\\
g(x) &= b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0, \ b_m \not\equiv 0 \pmod{p}
\end{aligned}$$

とおけて，x^{n+m} 次の係数は a_nb_m で，$f(x)g(x) \equiv 0 \pmod{p}$ から $a_nb_m \equiv 0 \pmod{p}$. これから $a_n \equiv 0 \pmod{p}$ または $b_m \equiv 0 \pmod{p}$ となり，$a_n \not\equiv 0 \pmod{p}, b_m \not\equiv 0 \pmod{p}$ に矛盾する．□

命題 8.3.3　p は素数で，a は整数とする．$f(x) \in \mathbb{Z}[x]$ のとき，次のことが成り立つ．$f(a) \equiv 0 \pmod{p}$ ならば，$f(x) \equiv (x-a)q(x) \pmod{p}$ となる $q(x) \in \mathbb{Z}[x]$ が存在する．

証明　$f(x)$ を $x-a$ で割った商を $q(x)$，余りを r とすると，$r=f(a)$ で

$$f(x)=(x-a)q(x)+f(a),\quad q(x)\in\mathbb{Z}[x]$$

が成り立つ．p を法として考えると，$f(a)\equiv 0 \pmod p$ だから

$$f(x)=(x-a)q(x)+f(a)\equiv(x-a)q(x)\pmod p. \qquad \square$$

フェルマーの小定理の証明の中で

$$\binom{n}{i}=\frac{n}{i}\binom{n-1}{i-1} \qquad \cdots\cdots(*)$$

を使い，次のことを示した．

> n は素数のとき，$\binom{n}{i}$ $(1\le i\le n-1)$ は p の倍数になる．

これをさらに一般化したものも成り立つ．

> p は素数で $n=p^k$ $(k\in\mathbb{N})$ のとき，$\binom{n}{i}$ $(1\le i\le n-1)$ は p の倍数になる．

証明 $(*)$ から，$1\le i\le n-1$ のとき

$$i\binom{n}{i}=n\binom{n-1}{i-1} \qquad \cdots\cdots(**)$$

が成り立つ．$p^k=n\,\Big|\,n\binom{n-1}{i-1}$ より，$(**)$ の右辺は p^k で割り切れるから，$(**)$ の左辺は p^k で割り切れる．よって，

$$p^k\,\Big|\,i\binom{n}{i}.$$

$1\le i\le n-1=p^k-1$ だから，i は p を素因数として高々 $k-1$ 個しか持たないから，$\binom{n}{i}$ は p を素因数に持たなければならない．したがって，$\binom{n}{i}$ は p の倍数である．　$\square$

次の例題 8.3.1 の (4) から次のことがわかる．

> p を素数とし，n を 2 以上の正整数とする．$n-1$ 個の二項係数 $\binom{n}{i}$ $(1\le i\le n-1)$ がすべて p の倍数であるための必要十分条件は，整数 n が適当な正整数 k を用いて $n=p^k$ と表せることである．

例題 8.3.1 整数 m が与えられたとき，x に関する整数係数の 2 つの整式 $f(x), g(x)$ が関係式

$$f(x) \equiv g(x) \pmod{m}$$

を満たすとは，等式 $f(x) - g(x) = mh(x)$ を満たすような整数係数の整式 $h(x)$ が存在することである．

(1) $f(x), g(x), F(x), G(x)$ を整数係数の整式とする．もし，ある整数 m について関係式 $f(x) \equiv g(x) \pmod{m}$，かつ $F(x) \equiv G(x) \pmod{m}$ が満たされるならば，関係式 $f(x) + F(x) \equiv g(x) + G(x) \pmod{m}$，かつ $f(x)F(x) \equiv g(x)G(x) \pmod{m}$ が満たされることを証明せよ．

(2) 正整数 $p\,(> 1)$ を素数とする． p より小さい任意の正整数 i に対して二項係数 ${}_p\mathrm{C}_i$ は p の倍数であることを証明せよ．

(3) 正整数 $p\,(> 1)$ を素数とする．任意の正整数 n について，関係式
$(1 + x)^{p^n} \equiv 1 + x^{p^n} \pmod{p}$ が満たされることを証明せよ．

(4) 正整数 $p\,(> 1)$ を素数とし，n を 2 以上の正整数とする．$n - 1$ 個の二項係数 ${}_n\mathrm{C}_i\ (1 \leqq i \leqq n - 1)$ がすべて p の倍数であるための必要十分条件は，整数 n が素数 p の正べきである（すなわち，適当な正整数 k を用いて $n = p^k$ と表せる）ことを証明せよ． (2012 奈良県立医大・医)

解答 ${}_n\mathrm{C}_i$ は $\binom{n}{i}$ と書き直すことにする．

(1) 命題 8.3.1 で証明済みであるが，もう一度書いておく．
$f(x) \equiv g(x) \pmod{m},\ F(x) \equiv G(x) \pmod{m}$ から

$$f(x) - g(x) = mh(x),\ F(x) - G(x) = mH(x)$$

を満たす整数係数の多項式 $h(x), H(x)$ が存在する．このとき

$$\begin{aligned} f(x) + F(x) - \big(g(x) + G(x)\big) &= f(x) - g(x) + F(x) - G(x) \\ &= mh(x) + mH(x) \\ &= m\big(h(x) + H(x)\big) \end{aligned}$$

で，$h(x) + H(x)$ は整数係数の多項式だから，$f(x) + F(x) \equiv g(x) + G(x) \pmod{m}$.

$$\begin{aligned} f(x)F(x) - g(x)G(x) &= \big(f(x) - g(x)\big)F(x) + \big(F(x) - G(x)\big)g(x) \\ &= mh(x)F(x) + mH(x)g(x) \\ &= m\big(h(x)F(x) + H(x)g(x)\big) \end{aligned}$$

で，$h(x)F(x) + H(x)g(x)$ は整数係数の多項式だから，$f(x)F(x) \equiv g(x)G(x) \pmod{m}$.

(2) $1 \leq i \leq p-1$ のとき

$$\binom{p}{i} = \frac{p!}{(p-i)!i!} = \frac{p}{i} \cdot \frac{(p-1)!}{(p-i)!(i-1)!} = \frac{p}{i}\binom{p-1}{i-1}$$

から

$$\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1} \qquad \cdots\cdots(*)$$

を得る.

p は素数で，p と $i\,(1 \leq i \leq p-1)$ は互いに素なので，$(*)$ より $\binom{p}{i}$ は p の倍数になる.

(3) (1) から，l が正整数のとき，x に関する整数係数の多項式 $f_i(x), g_i(x)\ (1 \leq i \leq l)$ が $f_i(x) \equiv g_i(x) \pmod{m}\ (1 \leq i \leq l)$ を満たすならば, $f_1(x)\cdots f_l(x) \equiv g_1(x)\cdots g_l(x) \pmod{m}$ が成り立つことがわかる.

このことから，2 つの整式 $f(x), g(x)$ が関係式 $f(x) \equiv g(x) \pmod{m}$ を満たすとき，$f_1(x) = \cdots = f_l(x) = f(x)$, $g_1(x) = \cdots = g_l(x) = g(x)$ とおくことにより，

$$\big(f(x)\big)^l \equiv \big(g(x)\big)^l \pmod{m}$$

が成り立つことが言える.

n に関する帰納法で

$$(1+x)^{p^n} \equiv 1 + x^{p^n} \pmod{p} \qquad \cdots\cdots①$$

が成り立つことを示す.

(I) $n = 1$ のとき

$$\begin{aligned}(1+x)^p - (1+x^p) &= 1 + \binom{p}{1}x + \binom{p}{2}x^2 + \cdots + \binom{p}{p}x^p - (1+x^p) \\ &= \binom{p}{1}x + \binom{p}{2}x^2 + \cdots + \binom{p}{p-1}x^{p-1}.\end{aligned}$$

(2) より，$\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ は p の倍数だから，

$$\binom{p}{i} = pa_i\ a_i \in \mathbb{N} \quad (1 \leq i \leq p-1)$$

とおくと

$$\binom{p}{1}x + \binom{p}{2}x^2 + \cdots + \binom{p}{p-1}x^{p-1} = p\left(a_1x + a_2x^2 + \cdots + a_{p-1}x^{p-1}\right).$$

$h(x)=a_1x+a_2x^2+\cdots+a_{p-1}x^{p-1}$ とおくと，$h(x)$ は x に関する整数係数の多項式で，

$$\binom{p}{1}x+\binom{p}{2}x^2+\cdots+\binom{p}{p-1}x^{p-1}=ph(x)$$

と書けるから

$$(1+x)^p\equiv 1+x^p \pmod p \qquad \cdots\cdots ②$$

が成り立つ．

よって，$n=1$ のとき，①は成り立つ．

(II) $k\geq 1$ として，$n\leq k$ のとき①が成り立つと仮定すると，

$$(1+x)^{p^k}\equiv 1+x^{p^k} \pmod p.$$

この両辺を p 乗すると

$$\left((1+x)^{p^k}\right)^p\equiv\left(1+x^{p^k}\right)^p \pmod p$$

から

$$(1+x)^{p^{k+1}}\equiv\left(1+x^{p^k}\right)^p \pmod p. \qquad \cdots\cdots ③$$

また，$n=1$ のときも①は成り立つから，②で x のところに x^{p^k} を代入すると

$$\left(1+x^{p^k}\right)^p\equiv 1+\left(x^{p^k}\right)^p\equiv 1+x^{p^{k+1}} \pmod p.$$

このことを使うと，③は

$$(1+x)^{p^{k+1}}\equiv 1+x^{p^{k+1}} \pmod p$$

となる．

よって，$n=k+1$ のときも①は成り立つ．

(III) (I)，(II) より，すべての正の整数 n について①は成り立つ．

(4) p を素数として，$n=p^k$ $(k\in\mathbb{N})$ とかけると仮定する．

(3) より，$(1+x)^{p^k}\equiv 1+x^{p^k} \pmod p$ が成り立つので，整数係数の多項式 $h(x)$ が存在して $(1+x)^{p^k}-\left(1+x^{p^k}\right)=ph(x)$ とおける．

$$\begin{aligned}(1+x)^{p^k}-\left(1+x^{p^k}\right)&=(1+x)^n-(1+x^n)\\&=\binom{n}{1}x+\binom{n}{2}x^2+\cdots\binom{n}{n-1}x^{n-1}\end{aligned}$$

だから

$$\binom{n}{1}x+\binom{n}{2}x^2+\cdots\binom{n}{n-1}x^{n-1}=ph(x)$$

は恒等式なので，$\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ はすべて p の倍数である．

逆に，$\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ がすべて p の倍数であると仮定する．

$\binom{n}{1} = n$ は p の倍数となるから，n は p の倍数である．

よって，$n = p^k m$ $(k, m \in \mathbb{N}, \gcd(p, m) = 1)$ とおける．

$m \geq 2$ とすると矛盾が生じることを示す．（ここでは，$v_p()$ を使ってみる．）

$$
\begin{aligned}
v_p\left(\binom{n}{p^k}\right) &= v_p\left(\frac{(p^k m)!}{(p^k)!\,(p^k(m-1))!}\right) \\
&= v_p\left((p^k m)!\right) - v_p\left((p^k)!\right) - v_p\left((p^k(m-1))!\right) \\
&= \left[\frac{p^k m}{p}\right] + \left[\frac{p^k m}{p^2}\right] + \cdots + \left[\frac{p^k m}{p^k}\right] + \cdots \\
&\quad - \left(\left[\frac{p^k}{p}\right] + \left[\frac{p^k}{p^2}\right] + \cdots + \left[\frac{p^k}{p^k}\right]\right) \\
&\quad\quad - \left(\left[\frac{p^k(m-1)}{p}\right] + \left[\frac{p^k(m-1)}{p^2}\right] + \cdots + \left[\frac{p^k(m-1)}{p^k}\right] + \cdots\right) \\
&= p^{k-1}m + p^{k-2}m + \cdots + m + \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \cdots \\
&\quad - \left(p^{k-1} + p^{k-2} + \cdots + p + 1\right) \\
&\quad\quad - \left(p^{k-1}(m-1) + p^{k-2}(m-1) + \cdots + (m-1)\right. \\
&\quad\quad\quad \left. + \left[\frac{m-1}{p}\right] + \left[\frac{m-1}{p^2}\right] + \cdots\right) \\
&= \left(\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \cdots\right) - \left(\left[\frac{m-1}{p}\right] + \left[\frac{m-1}{p^2}\right] + \cdots\right) \\
&= v_p(m!) - v_p((m-1)!) \\
&= v_p\left(\frac{m!}{(m-1)!}\right) \\
&= v_p(m) = 0 \qquad\qquad (\gcd(p, m) = 1)
\end{aligned}
$$

となり，$\binom{n}{p^k}$ は p の倍数とならない．

これは，$\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ がすべて p の倍数であることに矛盾する．

したがって，$m = 1$ でなければならないから，$n = p^k$ となる．　□

(3) の別解　$q = p^n$ とおくと

$$(1+x)^{p^n} - \left(1 + x^{p^n}\right) = (1+x)^q - (1+x)^q$$

$$= \binom{q}{1}x + \binom{q}{2}x^2 + \cdots \binom{q}{q-1}x^{n-1}$$

だから，$\binom{q}{1}, \binom{q}{2}, \ldots, \binom{q}{q-1}$ がすべて p の倍数であることを示せばよい．

（2）で用いた等式 $(*)$ から，$1 \leq i \leq q-1$ のとき

$$i\binom{q}{i} = q\binom{q-1}{i-1} \qquad \cdots\cdots(\star)$$

が成り立つ．$p^n = q \,\Big|\, q\binom{q-1}{i-1}$ より，$(\star)$ の右辺は p^n で割り切れるから，$(\star)$ の左辺は p^n で割り切れる．よって，

$$p^n \,\Big|\, i\binom{q}{i}.$$

$1 \leq i \leq q-1 = p^n - 1$ だから，i は p を素因数として高々 $n-1$ 個しか持たないから，$\binom{q}{i}$ は p を素因数に持たなければならない．したがって，$\binom{q}{i}$ は p の倍数である．　□

• (3) の別解のように (3) を解いてしまうと，(4) の前半は証明済みになってしまう．すなわち，(3) までの結果を使用しないことになってしまう．

(4) **後半の別解**

$\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ がすべて p の倍数であると仮定する．

$\binom{n}{1} = n$ は p の倍数となるから，n は p の倍数である．

よって，$n = p^k m$ $(k, m \in \mathbb{N},\ \gcd(p, m) = 1)$ とおける．

$m \geq 2$ とすると矛盾が生じることを示す．

$$\begin{aligned}\binom{n}{p^k} &= \frac{(p^k m)!}{(p^k)!\,(p^k(m-1))!} \\ &= \frac{\left(p^k(m-1)+p^k\right)\left(p^k(m-1)+p^k-1\right)\cdots\left(p^k(m-1)+2\right)\left(p^k(m-1)+1\right)}{p^k\cdot\left(p^k-1\right)\cdot\cdots\cdot 2\cdot 1}.\end{aligned}$$

$$\cdots\cdots(\star\star)$$

分子の因数 $p^k(m-1)+l$ $(1 \leq l \leq p^k)$ を考えると，$p^k(m-1)$ は p^k で割り切れるから，$r = 1, 2, \ldots, k$ として

「$p^k(m-1)+l$ が p^r で割り切れる　$\Longleftrightarrow$ l が p^r で割り切れる」

が成り立つから，分子に含まれる素因数 p の個数は，$p^k\cdot\left(p^k-1\right)\cdot\cdots\cdot 2\cdot 1 = \left(p^k\right)!$ に含まれる素因数 p の個数に等しい．したがって，$(\star\star)$ の分母と分子に含まれる素因数 p の個数は等しいから，$\binom{n}{p^k}$ は p の倍数とならない．

これは，$\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ がすべて p の倍数であることに矛盾する．
したがって，$m = 1$ でなければならないから，$n = p^k$ となる．　□

問題 8.3.1　n が相異なる素数 p, q の積，$n = pq$，であるとき，$n-1$ 個の数
${}_n\mathrm{C}_k$ $(1 \leqq k \leqq n-1)$ の最大公約数は 1 であることを示せ．　(1997 京都大・理系・前期)

8.4　円分多項式の性質

補助定理 8.4.1　p は素数，n は正の整数とする．
多項式 $x^n - 1$ が p を法として二重根をもつ．すなわち，

$$x^n - 1 \equiv (x-a)^2 f(x) \pmod{p}$$

を満たす整数 a と，整数係数の多項式 $f(x)$ が存在するならば，$p \mid n$ が成り立つ．

証明　◎ $p \nmid a$ であることを示す．
$p \mid a$ だと仮定すると，$(x-a)^2 = x^2 - 2ax + a^2 \equiv x^2 \pmod{p}$ だから，$x^n - 1 \equiv (x-a)^2 f(x) \pmod{p}$ は

$$x^n - 1 \equiv x^2 f(x) \pmod{p}$$

となる．定数項を比較すると，$-1 \equiv 0 \pmod{p}$ となり矛盾が生じる．
よって，$p \nmid a$ である．
$y = x - a$ とおき，$x^n - 1 \equiv (x-a)^2 f(x) \pmod{p}$ を y の式にすると

$$(y+a)^n - 1 \equiv y^2 f(y+a) \pmod{p}.$$

左辺の y の 1 次の係数は $\binom{n}{n-1} \cdot a^{n-1} = na^{n-1}$ で，右辺の 1 次の係数は 0 であるから，

$$na^{n-1} \equiv 0 \pmod{p}$$

が成り立つ．
$p \nmid a$ であったから，$p \nmid a^{n-1}$ なので $p \mid n$ でなければならない．　□

系 8.4.1　n は正の整数，d は $d \mid n, d < n$ を満たす正の整数，a は整数とする．
p は素数で $p \mid \Phi_n(a), p \mid \Phi_d(a)$ を満たすならば，$p \mid n$ が成り立つ．

証明　$p \mid \Phi_n(a), p \mid \Phi_d(a)$ だから，$\Phi_n(a) \equiv 0 \pmod{p}, \Phi_d(a) \equiv 0 \pmod{p}$.
命題 8.3.3 より

$$\Phi_n(x) \equiv (x-a)q_1(x) \pmod{p},\ \Phi_d(x) \equiv (x-a)q_2(x) \pmod{p}$$

となる $q_1(x), q_2(x) \in \mathbb{Z}[x]$ が存在する．このとき

$$\Phi_n(x)\Phi_d(x) \equiv (x-a)^2 q_1(x)q_2(x) \pmod{p}.$$

$d \mid n, d < n,\ x^n - 1 = \prod_{t \mid n} \Phi_t(x)$ より $x^n - 1$ は $\Phi_n(x)\Phi_d(x)$ で割り切れる．

$x^n - 1 = \Phi_n(x)\Phi_d(x)q_3(x),\ q_3(x) \in \mathbb{Z}[x]$ とおくと，

$$x^n - 1 = \Phi_n(x)\Phi_d(x)q_3(x) \equiv (x-a)^2 q_1(x)q_2(x)q_3(x) \pmod{p},\ q_1(x)q_2(x)q_3(x) \in \mathbb{Z}[x]$$

となり，多項式 $x^n - 1$ が p を法として a を二重根にもつから，補助定理 8.4.1 より，$p \mid n$ である． □

定理 8.4.1 n は正の整数，a は整数とする．

素数 p が $p \mid \Phi_n(a)$ を満たすならば，$p \equiv 1 \pmod{n}$ または $p \mid n$ が成り立つ．

証明 $p \mid \Phi_n(a) \mid a^n - 1$ から $p \mid a^n - 1$ となるので，$p \nmid a$ であることがわかる．
$k = ord_p(a)$ とおくと，$a^n \equiv 1 \pmod{p}$ より $k \mid n$ である．

(1) $k = n$ の場合

フェルマーの小定理より，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つから，$n = k \mid p - 1$ すなわち $p \equiv 1 \pmod{n}$ である．

(2) $k < n$ の場合

$0 \equiv a^k - 1 = \prod_{d \mid k} \Phi_d(a) \pmod{p}$ より，k の約数 d で，$p \mid \Phi_d(a)$ となる $d \in \mathbb{N}$ が存在する．

$d \mid k \mid n, k < n$ より $d \mid n, d < n$．また，$p \mid \Phi_n(a), p \mid \Phi_d(a)$ でもあるので，系 8.4.1 より，$p \mid n$ である． □

系 8.4.2 p は素数，a は整数とする．

素数 q が $q \mid 1 + a + \cdots + a^{p-1}$ を満たすならば，$q \equiv 1 \pmod{p}$ または $q = p$ が成り立つ．

証明 p は素数だから，$1 + a + \cdots + a^{p-1} = \Phi_p(a)$ なので，仮定から $q \mid \Phi_p(a)$ が成り立つ．
定理 8.4.1 より，$q \equiv 1 \pmod{p}$ または $q \mid p$ となる．
p, q は素数なので，$q \mid p$ となるのは，$p = q$ のときしかない．
したがって，$q \equiv 1 \pmod{p}$ または $q = p$ が成り立つことが言えた． □

補助定理 8.4.2 p は素数，n は $n = p^\alpha q\ (\alpha \in \mathbb{N}_0, q \in \mathbb{N}, p \nmid q)$ の形の正の整数とする．

整数 a が $p \mid \Phi_n(a)$ を満たすならば，$\mathrm{ord}_p(a) = q$ が成り立つ．

証明　$p \mid \Phi_n(a) \mid a^n - 1$ から $p \mid a^n - 1$ となるので，$p \nmid a$ であることがわかる．

$p \nmid a$ なので，フェルマーの小定理より，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ．

$p^\alpha - 1$ は $p-1$ で割り切れるから，$a^{p^\alpha - 1} - 1 \equiv 0 \pmod{p}$ すなわち $a^{p^\alpha} \equiv a \pmod{p}$ が成り立つ．これを使うと

$$1 \equiv a^n \equiv a^{p^\alpha q} \equiv \left(a^{p^\alpha}\right)^q \equiv a^q \pmod{p}.$$

$\mathrm{ord}_p(a)$ が存在することがわかるから，$k = \mathrm{ord}_p(a)$ とおくと，$a^q \equiv 1 \pmod{p}$ より $k \mid q$ である．

系 8.2.1 より

$$\Phi_n(a) = \Phi_{p^k q}(a) \mid \underbrace{\Phi_q\left(a^{p^k}\right) \equiv \Phi_q(a)}_{a^{p^\alpha} \equiv a \pmod{p}} \pmod{p}$$

が成り立つ．$p \mid \Phi_n(a)$ なので，$\Phi_n(a) \equiv \Phi_q(a) \pmod{p}$ より $p \mid \Phi_q(a)$ が成り立つ．

$k \mid q$ より，$k \leq q$ である．もしも，$k < q$ だとすると，$p \mid a^k - 1 = \prod_{d \mid k} \Phi_d(a)$ より $d \mid k$ で $p \mid \Phi_d(a)$ となる正の整数 d が存在する．

$d \mid k \mid q$ かつ $k < q$ から $d \mid q, d < q$ となり，$p \mid \Phi_q(a)$ かつ $p \mid \Phi_d(a)$ が成り立つ．系 8.4.1 より $p \mid q$ となるが，これは $p \nmid q$ に矛盾する．

したがって，$k = q$ でなければならず，$\mathrm{ord}_p(a) = q$ が成り立つ．　□

系 8.4.3　p は素数，$n \geq 2$ は正の整数，a は整数とする．

$p \mid \Phi_n(a),\ d \mid n,\ d < n,\ a^d \equiv 1 \pmod{p}$ ならば，$p \mid \dfrac{n}{d}$ が成り立つ．

証明　$0 \equiv a^d - 1 \equiv \prod_{d_1 \mid d} \Phi_{d_1}(a) \pmod{p}$ より，$p \mid \Phi_{d_1}(a)$ を満たす $d_1 \mid d, d_1 \in \mathbb{N}$ が存在する．$d_1 \mid d \mid n, d < n$ より $d_1 \mid n, d_1 < n$ である．また，$p \mid \Phi_n(a), p \mid \Phi_{d_1}(a)$ であるから，系 8.4.1 より，$p \mid n$ である．

$n = p^\alpha q$ $(\alpha \in \mathbb{N}, q \in \mathbb{N}, p \nmid q)$ とおくと，補助定理 8.4.2 より，$\mathrm{ord}_p(a) = q$ が成り立つ．

$a^d \equiv 1 \pmod{p}$ なので $q \mid d$ が成り立つ．

$q \mid d,\ d \mid n, d < n,\ n = p^\alpha q$ より $d = p^{\alpha_1} q$ $(0 \leq \alpha_1 \leq \alpha - 1, \alpha_1 \in \mathbb{N}_0)$ とおける．このとき

$$\frac{n}{d} = p^{\alpha - \alpha_1} \quad (\alpha - \alpha_1 \geq 1)$$

から，$p \mid \dfrac{n}{d}$ が言える．　□

補助定理 8.4.3 n は正の整数，$x>1$ は実数とする．このとき，不等式

$$(x-1)^{\varphi(n)} \leq \Phi_n(x) \leq (x+1)^{\varphi(n)}$$

が成り立つ．

ここで，左側の等号は $n=1$ のとき，右側の等号は $n=2$ のときのみ成り立つ．

証明 複素数に対する三角不等式

$$|z_1|-|z_2| \leq |z_1+z_2| \leq |z_1|+|z_2|$$

が成り立つ．$x>1, \zeta^n=1$ のとき

$$|x|-|\zeta| \leq |x-\zeta| \leq |x|+|\zeta|$$

から

$$x-1 \leq |x-\zeta| \leq x+1.$$

左側の等号は $\zeta=1$ のとき，右側の等号は $\zeta=-1$ のときのみ成り立つ．

$\Phi_1(x)=x-1, \Phi_2(x)=x+1$ であったことを思い出しておこう．

$ord(\zeta)=n$ となる ζ は $\varphi(n)$ 個あるから，この不等式を使うと

$$(x-1)^{\varphi(n)} \leq \prod_{\substack{\zeta^n=1 \\ ord(\zeta)=n}} |x-\zeta| \leq (x+1)^{\varphi(n)}. \qquad \cdots\cdots ①$$

$\Phi_n(x) = \displaystyle\prod_{\substack{\zeta^n=1 \\ ord(\zeta)=n}} (x-\zeta)$ を使うと

$$|\Phi_n(x)| = \left| \prod_{\substack{\zeta^n=1 \\ ord(\zeta)=n}} (x-\zeta) \right| = \prod_{\substack{\zeta^n=1 \\ ord(\zeta)=n}} |x-\zeta|$$

が成り立つので，①は

$$(x-1)^{\varphi(n)} \leq |\Phi_n(x)| \leq (x+1)^{\varphi(n)} \qquad \cdots\cdots ②$$

と書き直せる．

$x>1$ のとき，$x^{\frac{n}{d}}-1>0$ であるから、$\Phi_n(x) = \displaystyle\prod_{d|n} \left(x^{\frac{n}{d}}-1\right)^{\mu(d)} > 0$ が成り立つので，②は

$$(x-1)^{\varphi(n)} \leq \Phi_n(x) \leq (x+1)^{\varphi(n)}$$

となる．左側の等号は $n=1$ のとき，右側の等号は $n=2$ のときのみ成り立つ． □

補助定理 8.4.4　$n \geq 2,\ a \geq 3$ は正の整数とする．

p が素数で，$p \mid n$ ならば，$\Phi_n(a) > p$ が成り立つ．

証明　$n = p^\alpha q\ (\alpha,\ q \in \mathbb{N},\ p \nmid q)$ とおくと

$$\varphi(n) = \varphi\left(p^\alpha q\right) = \varphi\left(p^\alpha\right)\varphi(q) = \left(p^\alpha - p^{\alpha-1}\right)\varphi(q) = p^{\alpha-1}(p-1)\varphi(q) > p-1.$$

補助定理 8.4.3 より

$$\Phi_n(a) > (a-1)^{\varphi(n)} \geq 2^{\varphi(n)} > 2^{p-1}.$$

$p \geq 2$ なので

$$\begin{aligned} 2^{p-1} &= (1+1)^{p-1} \\ &= \binom{p-1}{0} + \binom{p-1}{1} + \cdots + \binom{p-1}{p-1} \\ &\geq \binom{p-1}{0} + \binom{p-1}{1} = 1 + (p-1) \\ &= p \end{aligned}$$

が成り立つ．

よって $\Phi_n(a) > 2^{p-1} \geq p$ より，$\Phi_n(a) > p$ となる．　□

補助定理 8.4.5　a, b は正の整数，$x \neq 1$ は整数とする．このとき

$$\gcd\left(x^a - 1, x^b - 1\right) = \left|x^{\gcd(a,b)} - 1\right|$$

が成り立つ．

例題 2.3.2 で，$a,\ m,\ n$ が正の整数で，$a > 1$ のとき

$$\gcd\left(a^m - 1,\ a^n - 1\right) = a^{\gcd(m,\ n)} - 1$$

が成り立つことを示してある．

証明　$g = \gcd(a,b), G = \gcd\left(x^a - 1, x^b - 1\right)$ とおく．

$g \mid a, g \mid b$ より $x^g - 1 \mid x^a - 1, x^g - 1 \mid x^b - 1$ であるから $x^g - 1 \mid \gcd\left(x^a - 1, x^b - 1\right)$ すなわち $x^g - 1 \mid G$ が成り立つ．この式から，$\gcd(x, G) = 1$ であることがわかる．

$x^g - 1 \mid G$ より，$\mathrm{ord}_G(x)$ が存在するから，$d = \mathrm{ord}_G(x)$ とおく．

$x^a \equiv 1 \pmod{G}, x^b \equiv 1 \pmod{G}$ であるから，$d \mid a, d \mid b$ が成り立つ．よって，$d \mid \gcd(a,b) = g$ が言えて，$x^d - 1 \mid x^g - 1$ が成り立つ．

$d = \mathrm{ord}_G(x)$ より，$G \mid x^d - 1$ であるから，$x^d - 1 \mid x^g - 1$ を使うと，$G \mid x^g - 1$ が言える．

また，$x^g - 1 \mid G$ なので，$G = |x^g - 1|$ すなわち $\gcd\left(x^a - 1, x^b - 1\right) = \left|x^{\gcd(a,b)} - 1\right|$ が成り立つ．　□

定理 8.4.2 a, b は正の整数とする．

ある整数 x に対して $\gcd(\Phi_a(x), \Phi_b(x)) > 1$ ならば，$\dfrac{a}{b}$ はある素数 p と整数 k を用いて

$$\frac{a}{b} = p^k$$

とかける．

証明 $p \mid \gcd(\Phi_a(x), \Phi_b(x))$ となる素数 p をとると，

$$a = p^\alpha A, b = p^\beta B \quad (\alpha, \beta \in \mathbb{N}_0,\ A, B \in \mathbb{N},\ p \nmid A, p \nmid B)$$

とかけるから，$A = B$ となることを示す．

◎ 最初に $p \mid \Phi_A(x)$ であることを示す．

$p \mid \Phi_a(x) \mid x^a - 1$ であるから明らかに $p \nmid x$ である．

$\alpha = 0$ のときは，$A = a$ より $p \mid \Phi_a(x) = \Phi_A(x)$.

$\alpha > 1$ のときは，系 8.2.1 より

$$0 \equiv \Phi_a(x) \equiv \Phi_{p^\alpha A}(x) \equiv \frac{\Phi_A\left(x^{p^\alpha}\right)}{\Phi_A\left(x^{p^{\alpha-1}}\right)} \pmod{p}$$

が成り立つから

$$\Phi_A\left(x^{p^\alpha}\right) \equiv 0 \pmod{p}.$$

$p \nmid x$ であるから，フェルマーの小定理より，$x^{p-1} - 1 \equiv 0 \pmod{p}$.

$p^\alpha - 1$ は $p - 1$ で割り切れるから，$p \mid x^{p-1} - 1 \mid x^{p^\alpha - 1} - 1$ すなわち $x^{p^\alpha - 1} \equiv 1 \pmod{p}$ が成り立つ．よって，$x^{p^\alpha} \equiv x \pmod{p}$ を得る．

このことを使うと，$\Phi_A\left(x^{p^\alpha}\right) \equiv 0 \pmod{p}$ は $\Phi_A(x) \equiv 0 \pmod{p}$ となり，$p \mid \Phi_A(x)$ が成り立つことがわかった．

同様にして，$p \mid \Phi_B(x)$ が成り立つ．ここで $A \geq B$ と仮定しても一般性を失わない．

もしも $A > B$ だと仮定する．$G = \gcd(A, B)$ とおくと，$G < A$.

$x \neq 1$ のときは，$p \mid \Phi_A(x) \mid x^A - 1, p \mid \Phi_B(x) \mid x^B - 1$ が成り立つので，

$$p \mid \gcd\left(x^A - 1, x^B - 1\right).$$

補助定理 8.4.5 より

$$\gcd\left(x^A - 1, x^B - 1\right) = \left|x^{\gcd(A,B)} - 1\right| = \left|x^G - 1\right|$$

が成り立つので，$p \mid x^G - 1$ を得る．

$x = 1$ のとき，明らかに $p \mid x^G - 1$ は成り立つ．

これから，$0 \equiv x^G - 1 \equiv \prod_{d|G} \Phi_d(x) \pmod{p}$ となるので，G の約数 d で $p \mid \Phi_d(x)$ となる正の整数 d が存在する．

$d \mid G \mid A, G < A$ より $d \mid A, d < A$ で，$p \mid \Phi_A(x), p \mid \Phi_d(x)$ が成り立つので，系 8.4.1 より $p \mid A$ となる．これは $p \nmid A$ に矛盾する．

したがって，$A = B$ でなければならない．このとき，$a = p^\alpha A, b = p^\beta B = p^\beta A$ から

$$\frac{a}{b} = p^{\alpha-\beta}\ ,\ \alpha - \beta \in \mathbb{Z}$$

となる．$k = \alpha - \beta$ とおくと，素数 p と整数 k を用いて，$\frac{a}{b} = p^k$ と表せる．　□

第9章

Zsigmondy の定理の特別な場合

9.1 Zsigmondy の定理の特別な場合の証明

定理 9.1.1 $a \geq 2, n \geq 2$ は正の整数とする．このとき，$a^n - 1$ の素数の約数 p で $p \nmid a^k - 1$ $(k = 1, 2, \ldots, n-1)$ を満たすものが存在する．ただし，次の場合を除く．

(a) $2^6 - 1^6$
(b) $n = 2$ で $a + 1 = 2^l$ を満たす正の整数 l が存在する

定理 9.1.1 を証明するために，次の補助定理を用意する．

補助定理 9.1.1 $a \geq 2, n \geq 2$ は正の整数とする．
p を $\Phi_n(a)$ の素数の約数とし，$f = \mathrm{ord}_p(a)$ とおくと， $n = fp^\alpha$, $\alpha \in \mathbb{N}_0$ とかける．
もしも，$\alpha \geq 1$ ならば，p は n を割り切る最大の素数である．
さらに，$\alpha \geq 1$, $p^2 \mid \Phi_n(a)$ ならば，$n = p = 2$ である．

証明 p は $\Phi_n(a)$ の素数の約数だから，$p \mid \Phi_n(a) \mid a^n - 1$ より $a^n \equiv 1 \pmod{p}$.
$f = \mathrm{ord}_p(a)$ だから，$f \mid n$ が成り立つ．よって，

$$n = fp^\alpha w\,,\ \alpha \in \mathbb{N}_0, w \in \mathbb{N}, \gcd(p, w) = 1$$

とおける．

◎ $w = 1$ であることを示す．
$w \neq 1$ だと仮定して，$r = fp^\alpha$ とおく．$(n = rw)$
$f = \mathrm{ord}_p(a)$ より $a^f \equiv 1 \mod p$ が成り立つから

$$a^r = a^{fp^\alpha} = \left(a^f\right)^{p^\alpha} \equiv 1^{p^\alpha} \equiv 1 \pmod{p}.$$

よって，$p \mid a^r - 1$ で

$$\begin{aligned}\frac{a^n-1}{a^r-1} &= \frac{(1+(a^r-1))^w-1}{a^r-1}\\ &= \frac{\sum_{i=1}^{w}\binom{w}{i}(a^r-1)^i}{a^r-1}\\ &= w+\sum_{i=2}^{w}\binom{w}{i}(a^r-1)^{i-1}\\ &\equiv w+\sum_{i=2}^{w}\binom{w}{i}(0)^{i-1}\\ &\equiv w \not\equiv 0 \pmod{p}.\end{aligned}$$

$r \mid n, w \neq 1$ より $r < n$ であるから，命題 8.2.2 より，$\Phi_n(a) \left| \dfrac{a^n-1}{a^r-1} \right.$ が成り立つ．

$p \mid \Phi_n(a)$ だから，$p \left| \dfrac{a^n-1}{a^r-1} \right.$ が成り立つ．これは，$\dfrac{a^n-1}{a^r-1} \equiv w \not\equiv 0 \pmod{p}$ に矛盾する．

したがって，$w = 1$ で，$n = fp^\alpha$, $\alpha \in \mathbb{N}_0$ とかける．

◎ $\alpha \geq 1$ ならば，p は n を割り切る最大の素数であることを示す．

$p \mid a^n - 1$ なので明らかに $p \nmid a$ である．

フェルマーの小定理より，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つので，$f \mid p-1$ である．

もしも，$q \mid n = fp^\alpha$ が p と異なる素数だとすると，$q \mid f$ であるから $q \leq f \leq p-1$ となる．よって，p は n を割り切る最大の素数である．

◎ $\alpha \geq 1$ かつ $p^2 \mid \Phi_n(a)$ ならば，$n = p = 2$ であることを示す．

もしも $p > 2$ だとすると，

$$\begin{aligned}\frac{a^n-1}{a^{\frac{n}{p}}-1} &= \frac{\left(1+\left(a^{\frac{n}{p}}-1\right)\right)^p-1}{a^{\frac{n}{p}}-1}\\ &= \frac{\sum_{i=1}^{p}\binom{p}{i}\left(a^{\frac{n}{p}}-1\right)^i}{a^{\frac{n}{p}}-1}\\ &= p+\sum_{i=2}^{p}\binom{p}{i}\left(a^{\frac{n}{p}}-1\right)^{i-1}\\ &= p+\underline{\binom{p}{2}\left(a^{\frac{n}{p}}-1\right)+\sum_{i=3}^{p}\binom{p}{i}\left(a^{\frac{n}{p}}-1\right)^{i-1}}.\end{aligned}$$

$$a^{\frac{n}{p}}-1 = a^{fp^{\alpha-1}}-1 = \left(a^f\right)^{p^{\alpha-1}}-1 \equiv 1^{p^{\alpha-1}}-1 \equiv 0 \pmod{p}.$$

また，$p>2$ は奇素数で，$\binom{p}{2}=p\cdot\dfrac{p-1}{2}\equiv 0 \pmod p$ となり，下線を引いた部分

$$\binom{p}{2}\left(a^{\frac{n}{p}}-1\right)+\sum_{i=3}^{p}\binom{p}{i}\left(a^{\frac{n}{p}}-1\right)^{i-1}$$

は p^2 の倍数である．よって

$$\frac{a^n-1}{a^{\frac{n}{p}}-1}\equiv p\not\equiv 0 \pmod{p^2}. \qquad \cdots\cdots ①$$

$\dfrac{n}{p}\,\Big|\,n$, $\dfrac{n}{p}<n$ であるから，命題 8.2.2 より，$\Phi_n(a)\,\Big|\,\dfrac{a^n-1}{a^{\frac{n}{p}}-1}$ が成り立つ．
これから，$p^2\mid\Phi_n(a)\,\Big|\,\dfrac{a^n-1}{a^{\frac{n}{p}}-1}$ となり，①に矛盾する．
したがって，$p=2$ でなければならない．
$n=f\cdot 2^\alpha$ で $p\,(=2)$ は n を割り切る最大の素数であったから，$f=1$ でなければならない．よって，$n=2^\alpha$ となる．
このとき

$$\begin{aligned}\Phi_n(a)&=\Phi_{2^\alpha}(a)\\&=\prod_{d\mid 2^\alpha}\left(a^{\frac{2^\alpha}{d}}-1\right)^{\mu(d)}\\&=\left(a^{2^\alpha}-1\right)^{\mu(1)}\left(a^{2^{\alpha-1}}-1\right)^{\mu(2)}\\&=\frac{a^{2^\alpha}-1}{a^{2^{\alpha-1}}-1}\\&=a^{2^{\alpha-1}}+1.\end{aligned}$$

$\alpha\geq 2$ だとすると，$2=p\nmid a$ であったから，a は奇数なので，$a^2\equiv 1 \pmod 4$ が成り立つ．これを使うと

$$\Phi_n(a)=a^{2^{\alpha-1}}+1\equiv 1+1\equiv 2 \pmod 4$$

となり，$4=p^2\mid\Phi_n(a)$ に矛盾する．
したがって，$\alpha=1$ でなければならない．このとき，$n=2^\alpha=2$ となる． □

定理 9.1.1 の証明

$n=2$ の場合　$a+1=2^l$ $(l\in\mathbb{N})$ の形ではないとすると

$$a+1=2^s t,\ s\in\mathbb{N}_0,\ t\in\mathbb{N},\ t(\geq 3)\text{ は奇数}$$

とおける．t は奇数で $t\geq 3$ であるから，$p\mid t$ となる奇数の素数 p が存在する．

$p\mid t\mid 2^s t=a+1$ より $p\mid a+1$．この p が $p\nmid a-1$ を満たすことを示す．

$p\mid a-1$ だとすると，$p\mid (a+1)-(a-1)=2$．ところが，p は奇数であるから，$p\nmid 2$ となり，$p\mid 2$ に矛盾する．

したがって，$p\nmid a-1$ でなければならない．また，$p\mid a+1\mid (a+1)(a-1)=a^2-1$ より $p\mid a^2-1$ であるから，定理は成り立つ．

以下，$n\geq 3$ とする．

（対偶を考えて）

$p\mid a^n-1$ を満たすどのような素数 p も $\mathrm{ord}_p(a)\neq n$ を満たすならば，$n=6,a=2$ となることを示す．

$n\geq 3,a\geq 2$ であるから，補助定理 8.4.3 より

$$1\leq (a-1)^{\varphi(n)}<\Phi_n(a)<(a+1)^{\varphi(n)}$$

が成り立つ．

$1<\Phi_n(a)$ だから，$p\mid \Phi_n(a)$ を満たす素数 p をとると，$p\mid \Phi_n(a)\mid a^n-1$ より $p\mid a^n-1$ である．$p\mid a^n-1$ より，$a^n\equiv 1\pmod p$ だから，$\mathrm{ord}_p(a)$ が存在して，$f=\mathrm{ord}_p(a)$ とおくと $f\mid n$.

$p\mid a^n-1$ だから，仮定より $f=\mathrm{ord}_p(a)\neq n$ が成り立つ．よって，$f<n$

補助定理 9.1.1 より $n=fp^\alpha,\ \alpha\in\mathbb{N}_0$ とかける．

$\alpha=0$ だと，$n=f$ となり，$f<n$ に矛盾するので，$\alpha\geq 1$ である．補助定理 9.1.1 より，p は n を割り切る最大の素数であることがわかる．

$p\mid \Phi_n(a)$ から $\Phi_n(a)=pq$ $(q\in\mathbb{N})$ とおける．

もしも，$q>1$ だとすると，$q_1\mid q$ となる素数 q_1 が存在する．

$q_1\mid q\mid \Phi_n(a)$ より $q_1\mid \Phi_n(a)$ となるので，$f_1=\mathrm{ord}_{q_1}(a)$ とおくと，上の p に対する議論と同様にして，q_1 は n を割り切る最大の素数となる．したがって，$q_1=p$ でなければならない．すると，$p^2\mid \Phi_n(a)$ となり，補助定理 9.1.1 より，$n=p=2$ である．これは，$n\geq 3$ に矛盾する．

したがって，$q=1$ で $\Phi_n(a)=p$ が成り立つ．

今までのことを整理すると，

$n\geq 3,a\geq 2,f=\mathrm{ord}_p(a)<n,n=fp^\alpha,\alpha\in\mathbb{N},\Phi_n(a)=p$，$p$ は n を割り切る最大の素数である．

$a \geq 3$ ならば，補助定理 8.4.4 より，$\Phi_n(a) > p$ となり，$\Phi_n(a) = p$ に矛盾する．ゆえに，$a = 2$ で $\Phi_n(2) = p$.

$p = \Phi_n(2) \mid a^n - 1 = 2^n - 1$ から $p \mid 2^n - 1$．よって，p は奇数とわかり，p は 3 以上の素数である．

$\alpha \geq 2$ だとすると，系 8.2.1 より

$$p = \Phi_n(2) = \Phi_{fp^\alpha}(2) = \Phi_{fp}\left(2^{p^{\alpha-1}}\right)$$

が成り立つ．

$fp \geq 3, p \mid fp, 2^{p^{\alpha-1}} \geq 2^{3^1} = 8 > 3$ だから，補助定理 8.4.4 より，$\Phi_{fp}\left(2^{p^{\alpha-1}}\right) > p$ となる．よって，$p = \Phi_{fp}\left(2^{p^{\alpha-1}}\right)$ に矛盾する．

よって，$\alpha = 1$ でなければならない．このとき，$n = fp$ となる．

$p \mid 2^n - 1$ より，$p \nmid 2$ なので，フェルマーの小定理より，$2^{p-1} \equiv 1 \pmod{p}$ が成り立つ．$f = \mathrm{ord}_p(2)$ なので，$f \mid p - 1$．これから $p \nmid f$ が成り立つ．

系 8.2.1 と補助定理 8.4.3 より

$$p = \Phi_{fp}(2) = \frac{\Phi_f(2^p)}{\Phi_f(2)} > \frac{(2^p-1)^{\varphi(n)}}{(2+1)^{\varphi(n)}} = \left(\frac{2^p-1}{3}\right)^{\varphi(n)} \geq \frac{2^p-1}{3}$$

から，$p > \dfrac{2^p-1}{3}$ すなわち

$$3p + 1 > 2^p. \qquad \cdots\cdots ①$$

◎ $l \geq 4$ のとき，$2^l > 3l + 1$ が成り立つことを l に関する数学的帰納法で示す．

(I) $l = 4$ のとき，$2^4 = 16 > 13 = 3 \cdot 4 + 1$ だから，不等式は成り立つ．

(II) $l = k\,(\geq 4)$ のとき成り立つと仮定すると，$2^k > 3k + 1$.

この不等式の両辺に 2 をかけると

$$2^{k+1} > 2(3k + 1).$$

$$2(3k + 1) - (3(k + 1) + 1) = 3k - 2 \geq 3 \cdot 4 - 2 = 10 > 0$$

より，$2(3k + 1) > 3(k + 1) + 1$.

よって，$2^{k+1} > 2(3k + 1) > 3(k + 1) + 1$ となるから，$2^{k+1} > 3(k + 1) + 1$.

$l = k + 1$ のときも不等式は成り立つ．

(III) (I)，(II) より，すべての正の整数 $l \geq 4$ について成り立つ．

$p > 3$ のとき，$2^p > 3p + 1$ だから，①は成り立たない．したがって，$p = 3$ でなければならない．

$n = 3f$, $f = \mathrm{ord}_3(2)$ より $f = 2$ で，$n = 3f = 6$ となる．

以上のことから，$n = 6, a = 2$ が示せた． □

第10章

Zsigmondy の定理

10.1 Zsigmondy の定理

定理 10.1.1 (Zsigmondy's theorem)
$n \geq 2$ は正の整数，a と b は互いに素な正の整数で $a \neq b$ とする．
このとき，$a^n - b^n$ の素数の約数 p で，$p \nmid a^k - b^k$ $(k = 1, 2, \ldots, n-1)$ を満たすものが存在する．
ただし，次の場合を除く．

(a) $2^6 - 1^6$
(b) $n = 2$ で $a + b = 2^l$ を満たす正の整数 l が存在する

$a^n - b^n$ の素数の約数 p で，$p \nmid a^k - b^k$ $(k = 1, 2, \ldots, n-1)$ を満たすものを，**primitive prime divisor** of $a^n - b^n$ と呼ぶことにする．

まず，(a)，(b) の場合に定理が成り立たないことを確認しておこう．

(a) $2^6 - 1^6$ の場合
$2^6 - 1^6 = 3^2 \cdot 7$ であるから，$p \mid 2^6 - 1^6$ を満たす素数 p は $p = 3$ または $p = 7$ となる．
$p = 3$ のときは，$p \mid 2^2 - 1^2$，$p = 7$ のときは，$p \mid 2^3 - 1^3$ となり，定理は成り立たない．

(b) $n = 2$ で $a + b = 2^l$ を満たす正の整数 l が存在する場合

$$a^n - b^n = a^2 - b^2 = (a+b)(a-b) = 2^l(a-b).$$

$p \mid a^2 - b^2 = 2^l(a-b)$ を満たす素数 p は，$p = 2$ または $p \mid a - b$ である．
$p \mid a - b$ のとき定理は成り立たない．

$p = 2$ のときは，$a + b = 2^l$ $(l \geq 1)$ より，a と b の偶奇が一致する．よって，$p = 2 \mid a - b$ すなわち $p \mid a - b$ となり，定理は成り立たない．

$n = 2$ の場合の証明　$a^2 - b^2 = (a + b)(a - b)$ を利用する．

$a + b$ は $a + b = 2^l$ $(l \in \mathbb{N})$ の形ではないから，$a + b$ を割り切る奇数の素数を p をとる．$p \mid a + b$ だから，$p \mid (a + b)(a - b) = a^2 - b^2$ である．

もしも，$p \mid a - b$ だとすると，$p \mid (a + b) + (a - b) = 2a$, $p \mid (a + b) - (a - b) = 2b$ から $p \mid 2a$, $p \mid 2b$ が成り立つ．p は奇数の素数だから，$p \mid a$, $p \mid b$ となり，a と b が互いに素であることに矛盾する．

したがって，$p \nmid a - b$ でなければならない．ゆえに，この p は，$p \mid a^2 - b^2$, $p \nmid a - b$ を満たす．　□

以下，$n \geq 3$ とする．

補助定理 10.1.1　$n \geq 3$ は正の整数，a と b は互いに素な正の整数で $a > b$ とする．

このとき，$a^n - b^n$ の素数の約数 p で，すべての k $(k \mid n, k \in \mathbb{N})$ に対して $p \nmid a^k - b^k$ を満たすならば，$a - b, a^2 - b^2, \ldots, a^{n-1} - b^{n-1}$ の中に p で割り切れるものが存在しない．

証明　$p \mid a^n - b^n$, $p \nmid a^k - b^k$ for all $k \mid n$, $(k \in \mathbb{N})$ を満たす素数 p をとる．

もしも，$a - b, a^2 - b^2, \ldots, a^{n-1} - b^{n-1}$ の中に p で割り切れるものが存在したとして，指数が最小のものを $a^m - b^m$ $(1 \leq m \leq n - 1)$ とする．

$\gcd(p, b) = 1$ であるから，$bc \equiv 1 \pmod{p}$ となる p を法とする b の逆数 $c \in \mathbb{N}$ が存在する．

◎ $\mathrm{ord}_p(ac)$ が存在し，$m_1 = \mathrm{ord}_p(ac)$ とおくと，$m_1 = m$ が成り立つことを示す．

$p \mid a^m - b^m$ から $a^m \equiv b^m \pmod{p}$ が成り立つ．両辺に c^m をかけると

$$(ac)^m \equiv (bc)^m \equiv 1 \pmod{p}.$$

これから，$\mathrm{ord}_p(ac)$ が存在し，$m_1 = \mathrm{ord}_p(ac)$ とおくと，$m_1 \mid m$ が成り立つ．よって，$m_1 \leq m$.

$m_1 < m$ だとすると，$(ac)^{m_1} \equiv 1 \pmod{p}$ の両辺に b^{m_1} をかけると，

$$a^{m_1}(bc)^{m_1} \equiv b^{m_1} \pmod{p} \text{ から } a^{m_1} \equiv b^{m_1} \pmod{p}.$$

これは m の最小性に反する．したがって，$m_1 = m$ でなければならない．

$a^n \equiv b^n \pmod{p}$ であったから，両辺に c^n をかけることにより，$(ac)^n \equiv 1 \pmod{p}$ が示せるから，$m_1 = \mathrm{ord}_p(ac) \mid n$ となる．$m_1 = m$ だから，$m \mid n$ が言える．

よって，$p \nmid a^m - b^m$ が成り立つので，$p \mid a^m - b^m$ に矛盾する．
したがって，$a-b, a^2-b^2, \ldots, a^{n-1}-b^{n-1}$ の中に p で割り切れるものが存在しない． □

定理 10.1.1 を証明するために必要な命題をいくつか準備しておく．

円分多項式 $\Phi_n(x)$ について，次のことが成り立つ．

$m \in \mathbb{N}$ のとき

$$x^m - 1 = \prod_{d|m} \Phi_d(x) \tag{10.1}$$

$$\Phi_n(x) = \prod_{d|m} \left(x^{\frac{m}{d}} - 1\right)^{\mu(d)} \tag{10.2}$$

命題 10.1.1 $m, a, b \in \mathbb{N},\ a > b$ のとき

$$\left.\begin{aligned} z_m &= a^m - b^m \\ \psi_m &= \prod_{d|m} z_{\frac{m}{d}}{}^{\mu(d)} = \prod_{d|m} \left(a^{\frac{m}{d}} - b^{\frac{m}{d}}\right)^{\mu(d)} \end{aligned}\right\} \tag{10.3}$$

と定めると

$$\psi_m = b^{\varphi(m)} \Phi_m\left(\frac{a}{b}\right) \tag{10.4}$$

$$z_m = \prod_{d|m} \psi_d \tag{10.5}$$

$$\psi_m \in \mathbb{Z} \tag{10.6}$$

が成り立つ．

証明 $z_m = a^m - b^m = b^m \left(\left(\frac{a}{b}\right)^m - 1\right)$ であるから，(10.1) と (10.2) を使うと

$$\begin{aligned} \psi_m = \prod_{d|m} z_{\frac{m}{d}}{}^{\mu(d)} &= \prod_{d|m} \left(a^{\frac{m}{d}} - b^{\frac{m}{d}}\right)^{\mu(d)} \\ &= \prod_{d|m} \left(b^{\frac{m}{d}}\right)^{\mu(d)} \left(\left(\frac{a}{b}\right)^{\frac{m}{d}} - 1\right)^{\mu(d)} \\ &= b^{\sum\limits_{d|m} \frac{m}{d}\mu(d)} \prod_{d|m} \left(\left(\frac{a}{b}\right)^{\frac{m}{d}} - 1\right)^{\mu(d)}. \end{aligned}$$

$\sum\limits_{d|m} \frac{m}{d}\mu(d) = \varphi(m)$ であるから

$$\psi_m = b^{\sum\limits_{d|m} \frac{m}{d}\mu(d)} \prod_{d|m} \left(\left(\frac{a}{b}\right)^{\frac{m}{d}} - 1\right)^{\mu(d)} = b^{\varphi(n)} \Phi_m\left(\frac{a}{b}\right).$$

よって，(10.4) は成り立つ．

(10.1) で $x = \dfrac{a}{b}$ とおいた等式の両辺に b^m をかけると

$$a^m - b^m = b^m \prod_{d|m} \Phi_d\left(\frac{a}{b}\right).$$

(10.4) を使うと

$$a^m - b^m = b^m \prod_{d|m} \frac{\psi_d}{b^{\varphi(d)}} = b^m \cdot \frac{1}{b^{\sum\limits_{d|m} \varphi(d)}} \cdot \prod_{d|m} \psi_d.$$

$\sum\limits_{d|m} \varphi(d) = m$ であるから

$$\begin{aligned} a^m - b^m &= b^m \cdot \frac{1}{b^{\sum\limits_{d|m} \varphi(d)}} \cdot \prod_{d|m} \psi_d \\ &= b^m \cdot \frac{1}{b^m} \cdot \prod_{d|m} \psi_d \\ &= \prod_{d|m} \psi_d. \end{aligned}$$

よって，(10.5) は成り立つ．

$\Phi_m(x) \in \mathbb{Z}[x]$ で

$$\Phi_m(x) = x^l + a_{l-1}x^{l-1} + \cdots + a_1 x + a_0 \quad (a_0, a_1, \ldots, a_{l-1} \in \mathbb{Z},\ l = \varphi(m))$$

とおくと，

$$\begin{aligned} \psi_m &= b^l \Phi_m\left(\frac{a}{b}\right) \\ &= b^l \left(\left(\frac{a}{b}\right)^l + a_{l-1}\left(\frac{a}{b}\right)^{l-1} + \cdots + a_1\left(\frac{a}{b}\right) + a_0\right) \\ &= a^l + a_{l-1}a^{l-1}b + \cdots + a_1 a b^{l-1} + a_0 b^l \in \mathbb{Z}. \end{aligned}$$

よって，(10.6) は成り立つ．　□

命題 10.1.2　$n \geq 2$ は正の整数，a と b は互いに素な正の整数で $a > b$ とする．

素数 p が $p \mid \psi_n$ を満たすならば，$p \equiv 1 \pmod{n}$ または $p \mid n$ が成り立つ．

証明　$p \mid \psi_n \mid \prod\limits_{d|n} \psi_d = z_n = a^n - b^n$ より $p \mid a^n - b^n$.

この式と $\gcd(a, b) = 1$ から $p \nmid a, p \nmid b$ がわかる．

$\gcd(p,b)=1$ であるから，$bc\equiv 1 \pmod p$ を満たす p を法とする b の逆数 $c\in\mathbb{N}$ が存在する．

$$\Phi_n(x)=x^l+a_{l-1}x^{l-1}+\cdots+a_1x+a_0 \quad (a_0,a_1,\ldots,a_{l-1}\in\mathbb{Z},\ l=\varphi(n))$$

とおくと，$p\mid\psi_n=b^{\varphi(n)}\Phi_n\left(\dfrac{a}{b}\right)$ より

$$\begin{aligned}\psi_n&=b^l\Phi_n\left(\frac{a}{b}\right)\\&=b^l\left(\left(\frac{a}{b}\right)^l+a_{l-1}\left(\frac{a}{b}\right)^{l-1}+\cdots+a_1\left(\frac{a}{b}\right)+a_0\right)\\&=a^l+a_{l-1}a^{l-1}b+\cdots+a_1ab^{l-1}+a_0b^l\equiv 0 \pmod p.\end{aligned}$$

よって

$$a^l+a_{l-1}a^{l-1}b+\cdots+a_1ab^{l-1}+a_0b^l\equiv 0 \pmod p.$$

両辺に c^l をかけると

$$(ac)^l+a_{l-1}(ac)^{l-1}\cdot bc+\cdots+a_1(ac)(bc)^{l-1}+a_0(bc)^l\equiv 0 \pmod p.$$

$bc\equiv 1 \pmod p$ を用いると

$$(ac)^l+a_{l-1}(ac)^{l-1}+\cdots+a_1(ac)+a_0\equiv 0 \pmod p$$

すなわち，$p\mid\Phi_n(ac)$ を得る．

定理 8.4.1 より，$p\equiv 1 \pmod n$ または $p\mid n$ が成り立つ． □

命題 10.1.3 $n\geq 2$ は正の整数とする．

$1\leq d<n$ を満たす n の約数 d に対して，$\psi_n\left|\dfrac{z_n}{z_d}\right.$ が成り立つ．

証明 命題 10.1.1 の (10.5) より

$$z_n=\prod_{d_1\mid n}\psi_{d_1}=\psi_n\prod_{\substack{d_1\mid n\\ d_1<n}}\psi_{d_1},\ z_d=\prod_{d_2\mid d}\psi_{d_2}.$$

$d_2\mid d, d\mid n, 1\leq d<n$ のとき，$d_2\mid n, 1\leq d_2<n$ であるから，

$$\left\{d_2 : d_2\mid d\right\}\subseteq\left\{d_1 : d_1\mid n,\ 1\leq d_1<n\right\}.$$

よって，$\displaystyle\prod_{d_2\mid d}\psi_{d_2}\left|\prod_{\substack{d_1\mid n\\ d_1<n}}\psi_{d_1}\right.$ となるから，$\displaystyle N=\prod_{\substack{d_1\mid n\\ d_1<n}}\psi_{d_1}\Big/\prod_{d_2\mid d}\psi_{d_2}\in\mathbb{Z}$ とおくと

$$\frac{z_n}{z_d}=\psi_n\left(\prod_{\substack{d_1\mid n\\ d_1<n}}\psi_{d_1}\Big/\prod_{d_2\mid d}\psi_{d_2}\right)=\psi_nN.$$

命題 10.1.1 の (10.6) より $\psi_n \in \mathbb{Z}$ だから $\dfrac{z_n}{z_d} = \psi_n N \in \mathbb{Z}$. したがって，$\psi_n \Big| \dfrac{z_n}{z_d}$ が成り立つ．　□

10.2　定理 10.1.1 の証明

定理 10.1.1　　($n \geq 3$ の場合)

$n \geq 3$ は正の整数，a と b は互いに素な正の整数で $a > b$ とする．

このとき，$a^n - b^n$ の素数の約数 p で，すべての k $(k = 1, \ldots, n-1)$ に対して $p \nmid a^k - b^k$ であるものが存在する．

ただし，次の場合を除く．

(a) $2^6 - 1^6$

証明　　$z_n = a^n - b^n$ を素因数分解して

$$z_n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad (p_1, \ldots, p_r \text{ は異なる素数 }, \ \alpha_1, \ldots, \alpha_r \in \mathbb{N})$$

とおいたとき，$p_{s_1}, \ldots, p_{s_t}$ が $z_n = a^n - b^n$ の primitive prime divisor すべてとする．すなわち，$p_1, \ldots, p_r$ のなかで，

$$p \mid a^n - b^n, \ p \nmid a^k - b^k \quad (k = 1, \ldots, n-1)$$

を満たすものすべてとして，

$$P_n = p_{s_1}^{\alpha_{s_1}} \cdots p_{s_t}^{\alpha_{s_t}} \qquad \cdots\cdots ①$$

とおく．定理 10.1.1 で除外した場合以外では，$P_n > 1$ が示せれば定理 10.1.1 の証明は終わる．

- $P_n \mid \psi_n$ $\cdots\cdots ②$

  が成り立つことを示す．

  $P_n = 1$ のとき，明らかに②は成り立つ．

  以下，$P_n > 1$ とする．

  $p_{s_1}, \ldots, p_{s_t}$ の選び方から，$\gcd(P_n, z_k) > 1$ となる z_k は z_n のみである．

  $P_n \mid z_n = z_{\frac{n}{1}}{}^{\mu(1)}$, $\gcd(P_n, z_k) = 1 \ \ (k = 1, 2, \ldots, n-1)$ であるから

$$\psi_n = \prod_{d \mid n} z_{\frac{n}{d}}{}^{\mu(d)} = z_n \prod_{\substack{d \mid n, d > 1 \\ \mu(d) = 1}} z_{\frac{n}{d}}{}^{\mu(d)} \Big/ \prod_{\substack{d \mid n \\ \mu(d) = -1}} z_{\frac{n}{d}}{}^{\mu(d)} = \frac{z_n M}{N}$$

  とおくと，$\gcd(P_n, M) = 1, \gcd(P_n, N) = 1$ が成り立ち，(10.6) より，$\psi_n = \dfrac{z_n M}{N}$ は整数である．

$\psi_n = \dfrac{z_n M}{N}$ を変形すると，

$$\frac{z_n M}{P_n} = \frac{\psi_n N}{P_n}.$$

$P_n \mid z_n$ より左辺は整数なので，右辺 $\dfrac{\psi_n N}{P_n}$ も整数となる．P_n と N は互いに素であるから，P_n は ψ_n の約数である．よって，$P_n \mid \psi_n$ は成り立つ．

$P_n \mid \psi_n$ より

$$\psi_n = \lambda_n P_n \quad (\lambda_n \in \mathbb{N}) \qquad \cdots\cdots ③$$

とおく．

$\lambda_n = 1$ の場合は，③より，$P_n = \psi_n$.

$n \geq 3$ だから

$$P_n = \psi_n = b^{\varphi(n)} \Phi_n \left(\frac{a}{b}\right) > b^{\varphi(n)} \left(\frac{a}{b} - 1\right)^{\varphi(n)} = (a-b)^{\varphi(n)} \geq 1.$$

よって，$P_n > 1$ が成り立つ．

以下，$\lambda_n > 1$ とする．

- $\gcd(\lambda_n, P_n) = 1$ が成り立つことを示す．
  $P_n = 1$ のときは明らかに $\gcd(\lambda_n, P_n) = 1$ なので，以下 $P_n > 1$ とする．
  $\lambda_n P_n = \psi_n \mid z_n$ より，λ_n は $z_n = a^n - b^n$ の約数であるが，P_n の定義より，P_n は z_n の primitive prime divisor すべての積であるから，λ_n は P_n を割り切る素数を因数に含んでいない．このことから，

  $$\gcd(\lambda_n, P_n) = 1 \qquad \cdots\cdots ④$$

  が成り立つ．
- $p \mid \lambda_n$ となる素数 p をとる．
  この p に対して，$p \nmid a, p \nmid b$ が成り立つことを示す．
  $p \mid \lambda_n$ から p は z_n の primitive prime divisor ではないので，$d < n$ で $p \mid z_d$ となる最小の $d \in \mathbb{N}$ が存在する．
  $a^d \equiv b^d \pmod{p}$ で，この式と $\gcd(a, b) = 1$ から $p \nmid a, p \nmid b$ がわかる．
- $p \mid n$ $\qquad \cdots\cdots ⑤$
  が成り立つことを示す．
  $p = 2$ のときは，$2 \mid \psi_n$ で，命題 10.1.2 より $2 \mid n$ が成り立つ．
  以下 $p \geq 3$ とすると p は奇素数である．
  $\gcd(p, b) = 1$ であるから，$bc \equiv 1 \pmod{p}$ を満たす，p を法とする b の逆数 $c \in \mathbb{N}$ が存在する．

$p \mid \lambda_n$ から p は z_n の primitive prime divisor ではないので，$d < n$ で $p \mid z_d$ となる最小の $d \in \mathbb{N}$ が存在する．
$a^d \equiv b^d \pmod p$ の両辺に c^d をかけると

$$(ac)^d \equiv (bc)^d \equiv 1 \pmod p.$$

これから，$\mathrm{ord}_p(ac)$ が存在し，$d_1 = \mathrm{ord}_p(ac)$ とおくと，$d_1 \mid d$ が成り立つ．
よって，$d_1 \leq d$.
$d_1 < d$ だとすると，$(ac)^{d_1} \equiv 1 \pmod p$ の両辺に b^{d_1} をかけると，

$$a^{d_1}(bc)^{d_1} \equiv b^{d_1} \pmod p \text{ から } a^{d_1} \equiv b^{d_1} \pmod p.$$

これは d の最小性に反する．したがって，$d_1 = d$ でなければならない．
$a^n \equiv b^n \pmod p$ であったから，両辺に c^n をかけることにより，$(ac)^n \equiv 1 \pmod p$ が示せるから，$d_1 = \mathrm{ord}_p(ac) \mid n$ となる．$d_1 = d$ だから，$d \mid n$ が言える．

$p \nmid n$ だとすると，$d \mid n$ なので，$p \nmid d$. また，$p \mid a^d - b^d$, $p \nmid a^d$, $p \nmid b^d$ が成り立つから，LTE より

$$\begin{aligned} v_p(z_n) = v_p\left(a^n - b^n\right) &= v_p\left(\left(a^d\right)^{\frac{n}{d}} - \left(b^d\right)^{\frac{n}{d}}\right) \\ &= v_p\left(a^d - b^d\right) + v_p\left(\frac{n}{d}\right) \\ &= v_p\left(a^d - b^d\right) + v_p(n) - v_p(d) \\ &= v_p\left(a^d - b^d\right) + 0 - 0 \\ &= v_p(z_d). \end{aligned}$$

これから，$p \nmid \dfrac{z_n}{z_d}$ が言える．
ところで，$p \mid \lambda_n \mid \psi_n \left| \dfrac{z_n}{z_d} \right.$ から，$p \left| \dfrac{z_n}{z_d} \right.$ となり，$p \nmid \dfrac{z_n}{z_d}$ に矛盾する．
したがって，$p \mid n$ でなければならない．

- $p \mid \lambda_n$ を満たす素数 p に対して，$p \mid n$ が成り立つから，

$$n = p^\alpha q \quad (\alpha, q \in \mathbb{N},\ p \nmid q) \qquad \cdots\cdots ⑥$$

とおくと

$$p \mid \psi_n \mid \psi_q\left(a^{p^\alpha}, b^{p^\alpha}\right) \equiv \psi_q \pmod p$$

が成り立つことを示す．

ここで，$m \in \mathbb{N}$ のとき

$$\boldsymbol{\psi_m(x,y) = y^{\varphi(m)}\Phi_m\left(\frac{x}{y}\right)}$$

とする．

まず，$p \mid \lambda_n$ だから，$p \mid \lambda_n \mid \lambda_n P_n = \psi_n$ から $p \mid \psi_n$ が成り立つ．

$p \nmid q$ だから系 8.2.1 より

$$\begin{aligned}\psi_n = b^{\varphi(n)}\Phi_n\left(\frac{a}{b}\right) &= b^{\varphi(p^\alpha q)}\Phi_{p^\alpha q}\left(\frac{a}{b}\right)\\ &= b^{\varphi(p^\alpha q)}\frac{\Phi_q\left(\left(\frac{a}{b}\right)^{p^\alpha}\right)}{\Phi_q\left(\left(\frac{a}{b}\right)^{p^{\alpha-1}}\right)}.\end{aligned}$$

$p \nmid q$ より $\gcd(p^\alpha, q) = 1$ なので

$$\varphi(p^\alpha q) = \varphi(p^\alpha)\varphi(q) = \left(p^\alpha - p^{\alpha-1}\right)\varphi(q) = p^\alpha\varphi(q) - p^{\alpha-1}\varphi(q)$$

が成り立つので

$$\begin{aligned}\psi_n &= b^{\varphi(p^\alpha q)}\frac{\Phi_q\left(\left(\frac{a}{b}\right)^{p^\alpha}\right)}{\Phi_q\left(\left(\frac{a}{b}\right)^{p^{\alpha-1}}\right)}\\ &= \frac{b^{p^\alpha\varphi(q)}\Phi_q\left(\left(\frac{a}{b}\right)^{p^\alpha}\right)}{b^{p^{\alpha-1}\varphi(q)}\Phi_q\left(\left(\frac{a}{b}\right)^{p^{\alpha-1}}\right)}\\ &= \frac{\psi_q\left(a^{p^\alpha}, b^{p^\alpha}\right)}{\psi_q\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right)}\end{aligned}$$

となる．よって

$$\psi_n = \frac{\psi_q\left(a^{p^\alpha}, b^{p^\alpha}\right)}{\psi_q\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right)}. \qquad \cdots\cdots ⑦$$

(10.4) と (10.5) から，$\psi_n \in \mathbb{Z}$，$\psi_q\left(a^{p^\alpha}, b^{p^\alpha}\right) = b^{p^\alpha\varphi(q)}\Phi_q\left(\left(\frac{a}{b}\right)^{p^\alpha}\right) \in \mathbb{Z}$,

$\psi_q\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right) = b^{p^{\alpha-1}\varphi(q)}\Phi_q\left(\left(\frac{a}{b}\right)^{p^{\alpha-1}}\right) \in \mathbb{Z}$.

これと⑦から，$\psi_n \mid \psi_q\left(a^{p^\alpha}, b^{p^\alpha}\right)$ が成り立つ．

次に，

$$\Phi_q(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \quad (a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z},\ m = \varphi(q))$$

とおくと，

$$\begin{aligned}
&\psi_q\left(a^{p^\alpha},\, b^{p^\alpha}\right)\\
&= (b^{p^\alpha})^{\varphi(q)}\Phi_q\left(\frac{a^{p^\alpha}}{b^{p^\alpha}}\right)\\
&= (b^{p^\alpha})^m\left(\left(\frac{a^{p^\alpha}}{b^{p^\alpha}}\right)^m + a_{m-1}\left(\frac{a^{p^\alpha}}{b^{p^\alpha}}\right)^{m-1} + \cdots + a_1\cdot\frac{a^{p^\alpha}}{b^{p^\alpha}} + a_0\right)\\
&= \left(a^{p^\alpha}\right)^m + a_{m-1}\left(a^{p^\alpha}\right)^{m-1} b^{p^\alpha} + \cdots + a_1 a^{p^\alpha}\left(b^{p^\alpha}\right)^{m-1} + a_0\left(b^{p^\alpha}\right)^m.
\end{aligned}$$

$\gcd(a,p)=1$ なので，フェルマーの小定理より，$a^{p-1}\equiv 1 \pmod p$ が成り立つから，$a^p \equiv a \pmod p$ である．同様にして，$b^p \equiv b \pmod p$ も成り立つので

$$\begin{aligned}
&\psi_q\left(a^{p^\alpha},\, b^{p^\alpha}\right)\\
&= \left(a^{p^\alpha}\right)^m + a_{m-1}\left(a^{p^\alpha}\right)^{m-1} b^{p^\alpha} + \cdots + a_1 a^{p^\alpha}\left(b^{p^\alpha}\right)^{m-1} + a_0\left(b^{p^\alpha}\right)^m\\
&\equiv a^m + a_{m-1}\cdot a^{m-1}\cdot b + \cdots + a_1\cdot a\cdot b^{m-1} + a_0\cdot b^m\\
&\equiv b^{\varphi(q)}\Phi_q\left(\frac{a}{b}\right)\\
&\equiv \psi_q \pmod p.
\end{aligned}$$

以上のことから

$$p \mid \psi_n \mid \psi_q\left(a^{p^\alpha}, b^{p^\alpha}\right) \equiv \psi_q \pmod p$$

が成り立つ．

- 次のことを示す．

  p は n を割り切る最大の素数である．　……⑧

  p は $p \mid \lambda_n$ を満たす素数だから，$p \mid \psi_q$ が成り立つので，命題 10.1.2 より，$p \equiv 1 \pmod q$ または $p \mid q$ が成り立つ．$p \nmid q$ であったから，$p \equiv 1 \pmod q$.

  これから，$q < p$ が言える．

  もしも，$r \mid n$ が p と異なる素数ならば，$n = p^\alpha q$ より $r \mid q$ であるから $r \le q < p$ となる．

  したがって，p は n を割り切る最大の素数である．

- $\lambda_n = p^\beta \quad (\beta \in \mathbb{N})$　……⑨

  とかけることを示す．

  p_1 が $p_1 \mid \lambda_n$ となる p と異なる素数だとすると，上と同じ議論で，$p_1 \mid n$ が成り立ち

  $$n = p_1^{\alpha_1} q_1 \quad (\alpha_1, q_1 \in \mathbb{N},\, p_1 \nmid q_1)$$

とおけて，p_1 は n を割り切る最大の素数であることになり，$p_1 = p$ でなければならない．これは $p_1 \neq p$ であることに矛盾する．
したがって，$p_1 \mid \lambda_n$ となる p と異なる素数 p_1 は存在しないから，

$$\lambda_n = p^\beta \quad (\beta \in \mathbb{N})$$

とおくことができる．

- 次のことを示す．
  $\beta = 1$ すなわち $\lambda_n = p$.　……⑩

[1] $p = 2$ の場合　$n = 2^\alpha q$　$(\alpha \geq 1, q \geq 1, p \nmid q)$
$p\,(= 2)$ は n を割り切る最大の素数であったから，$q = 1$ となり，$n = 2^\alpha$ である．
$n \geq 3$ より $\alpha \geq 2$, $n \geq 4$ となる．
また，$p \nmid a, p \nmid b$ から $2 \nmid a, 2 \nmid b$ なので，a と b は奇数である．

$$\begin{aligned}
\psi_n &= \prod_{d \mid 2^\alpha} z_{\frac{2^\alpha}{d}}{}^{\mu(d)} \\
&= z_{\frac{2^\alpha}{1}}{}^{\mu(1)} z_{\frac{2^\alpha}{2}}{}^{\mu(2)} \\
&= \frac{z_{2^\alpha}}{z_{2^{\alpha-1}}} = \frac{a^{2^\alpha} - b^{2^\alpha}}{a^{2^{\alpha-1}} - b^{2^{\alpha-1}}} \\
&= a^{2^{\alpha-1}} + b^{2^{\alpha-1}} \\
&= \left(a^2\right)^{2^{\alpha-2}} + \left(b^2\right)^{2^{\alpha-2}}.
\end{aligned}$$

a と b は奇数なので，$a^2 \equiv 1 \pmod 4$, $b^2 \equiv 1 \pmod 4$ を使うと

$$\psi_n = \left(a^2\right)^{2^{\alpha-2}} + \left(b^2\right)^{2^{\alpha-2}} \equiv 1 + 1 \equiv 2 \pmod 4.$$

$\beta \geq 2$ だとすると，$\psi_n = \lambda_n P_n = 2^\beta P_n$ は 4 で割り切れ，$\psi_n \equiv 0 \pmod 4$ となるが，$\psi_n \equiv 2 \pmod 4$ に矛盾する．
したがって，$\beta = 1$ でなければならない．

[2] $p > 2$ の場合
$\gcd(p, b) = 1$ であるから，$bc \equiv 1 \pmod p$ を満たす，p を法とする b の逆数 $c \in \mathbb{N}$ が存在する．
$p \mid \lambda_n \mid \lambda_n P_n = \psi_n$ より $p \mid \psi_n$ となるから，命題 10.1.2 のところで示したように，$p \mid \Phi_n(ac)$ が言える．
補助定理 8.4.2 より，$\mathrm{ord}_p(ac) = q$ が成り立つ．
$p \mid \lambda_n$ から p は z_n の primitive prime divisor ではないので，$d < n$ で $p \mid z_d$ となる $d < n$, $d \in \mathbb{N}$ が存在する．補助定理 10.1.1 より，

「$p \mid a^n - b^n$, $p \nmid a^k - b^k$ for all $k \mid n$, ($k \in \mathbb{N}$) を満たす素数 p に対して，
$a-b, a^2-b^2, \ldots, a^{n-1}-b^{n-1}$ の中に p で割り切れるものが存在しない」
ことがわかるので，d は $d \mid n$ としてよい．（d が n の約数の中に存在しなければ，p は primitive prime devisor になってしまう．）
$p \mid z_d = a^d - b^d$ から $a^d \equiv b^d \pmod{p}$．両辺に c^d をかけると，$(ac)^d \equiv (bc)^d \equiv 1 \pmod{p}$ から

$$(ac)^d \equiv 1 \pmod{p}.$$

$\mathrm{ord}_p(ac) = q$ であったから，$q \mid d$.
以上のことから，$p \mid z_d$ となる可能性がある d ($d \mid n$, $d < n$) は $q \mid d$ でなければならない．

$$\psi_n = \prod_{d_1 \mid n} {z_n}^{\mu(d)}.$$

$n = p^\alpha q$ の約数の中で q の倍数になるものを調べると

$\frac{n}{d_1}$:	$1\cdot q$	$p\cdot q$	$p^2\cdot q$	$\ldots$	$p^{\alpha-2}q$	$p^{\alpha-1}q$	$p^\alpha q$
d_1 :	p^α	$p^{\alpha-1}$	$p^{\alpha-2}$	$\ldots$	p^2	p	1
$\mu(d_1)$:	0	0	0	$\ldots$	0	-1	1

のようになるから

$$v_p(\psi_n) = v_p\left(z_{p^\alpha q}\right) - v_p\left(z_{p^{\alpha-1}q}\right) = v_p(z_n) - v_p(z_{\frac{n}{p}}).$$

$p \mid z_d = a^d - b^d$, $p \nmid a^d$, $p \nmid b^d$ であるから，LTE より

$$v_p(z_n) = v_p\left(a^n - b^n\right) = v_p\left(\left(a^d\right)^{\frac{n}{d}} - \left(b^d\right)^{\frac{n}{d}}\right) = v_p\left(a^d - b^d\right) + v_p\left(\frac{n}{d}\right),$$

$$v_p(z_{\frac{n}{p}}) = v_p\left(a^{\frac{n}{p}} - b^{\frac{n}{p}}\right) = v_p\left(\left(a^d\right)^{\frac{n}{dp}} - \left(b^d\right)^{\frac{n}{dp}}\right) = v_p\left(a^d - b^d\right) + v_p\left(\frac{n}{dp}\right),$$

$$v_p\left(\frac{n}{d}\right) = v_p\left(\frac{n}{dp}\cdot p\right) = v_p\left(\frac{n}{dp}\right) + v_p(p) = v_p\left(\frac{n}{dp}\right) + 1$$

であることを用いると

$$v_p(\psi_n) = v_p(z_n) - v_p(z_{\frac{n}{p}}) = v_p\left(\frac{n}{d}\right) - v_p\left(\frac{n}{dp}\right) = 1.$$

$\psi_n = \lambda_n P_n$ から

$$v_p(\psi_n) = v_p(\lambda_n P_n) = v_p(\lambda_n) + v_p(P_n) = v_p\left(p^\beta\right) + 0 = \beta.$$

$v_p(\psi_n) = 1$ であったから，$\beta = 1$ を得る．

- $\beta = 1$ すなわち $\lambda_n = p$ であるが，$a - b$ と 1 との大小で 2 つの場合に分けて，$P_n > 1$ を示す．

  (a) $\lambda_n = p,\ a - b > 1$ の場合

  $P_n = \dfrac{\psi_n}{\lambda_n} = \dfrac{\psi_n}{p}$.

  ここで，補助定理 8.4.3 より

$$\psi_n = b^{\varphi(n)}\Phi_n\left(\frac{a}{b}\right) > b^{\varphi(n)}\left(\frac{a}{b} - 1\right)^{\varphi(n)} = (a-b)^{\varphi(n)}$$

  $p \nmid q$ より $\gcd(p^\alpha, q) = 1$ なので

$$\varphi(n) = \varphi(p^\alpha q) = \varphi(p^\alpha)\,\varphi(q) = \left(p^\alpha - p^{\alpha-1}\right)\varphi(q) = p^{\alpha-1}(p-1)\varphi(q) \geq p - 1$$

  が成り立つから，

$$P_n = \frac{\psi_n}{p} > \frac{(a-b)^{\varphi(n)}}{p} \geq \frac{2^{\varphi(n)}}{p} \geq \frac{2^{p-1}}{p}.$$

  よって，

$$P_n > \frac{2^{p-1}}{p}.$$

  $m \geq 2, m \in \mathbb{N}$ のとき，

$$\begin{aligned} 2^{m-1} &= (1+1)^{m-1} \\ &= 1 + \binom{m-1}{1} + \binom{m-1}{2} + \cdots + \binom{m-1}{m-1} \\ &\geq 1 + \binom{m-1}{1} = 1 + (m-1) \\ &= m \end{aligned}$$

  から，$2^{m-1} \geq m$ が成り立つ．

  $p \geq 2$ だから，$2^{p-1} \geq p$ すなわち，$\dfrac{2^{p-1}}{p} \geq 1$ が成り立つから，

$$P_n > \frac{2^{p-1}}{p} \geq 1.$$

  ゆえに，$P_n > 1$ が成り立つ．

  (b) $\lambda_n = p,\ a - b = 1$ の場合

  $P_n > 1$ でないと仮定すると，$P_n = 1, \psi_n = \lambda_n P_n = p$.

  $n = p^\alpha q \quad (\alpha, q \in \mathbb{N},\ p \nmid q\,)$ であったが

  ◎ $\alpha = 1$ であることを示す．

  もしも，$\alpha \geq 2$ が成り立つと仮定する．

$$\varphi(p^\alpha q) = \varphi(p^\alpha)\,\varphi(q) = \left(p^\alpha - p^{\alpha-1}\right)\varphi(q)$$

$$= p^{\alpha-1}(p-1)\varphi(q) = p^{\alpha-1}\varphi(p)\varphi(q)$$
$$= p^{\alpha-1}\varphi(pq)$$

を用いると

$$\begin{aligned} p = \psi_n &= b^{\varphi(n)}\Phi_n\left(\frac{a}{b}\right) = b^{\varphi(p^\alpha q)}\Phi_{p^\alpha q}\left(\frac{a}{b}\right) \\ &= b^{p^{\alpha-1}\varphi(pq)}\Phi_{pq}\left(\left(\frac{a}{b}\right)^{p^{\alpha-1}}\right) \\ &= \left(b^{p^{\alpha-1}}\right)^{\varphi(pq)}\Phi_{pq}\left(\left(\frac{a}{b}\right)^{p^{\alpha-1}}\right) \\ &= \psi_{pq}\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right). \end{aligned}$$

しかし，

$$\begin{aligned} \psi_{pq}\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right) &= \left(b^{p^{\alpha-1}}\right)^{\varphi(pq)}\Phi_{pq}\left(\left(\frac{a}{b}\right)^{p^{\alpha-1}}\right) \\ &\geq \left(b^{p^{\alpha-1}}\right)^{\varphi(pq)}\left(\left(\frac{a}{b}\right)^{p^{\alpha-1}} - 1\right)^{\varphi(pq)} \\ &= \left(a^{p^{\alpha-1}} - b^{p^{\alpha-1}}\right)^{\varphi(pq)} \\ &\geq a^{p^{\alpha-1}} - b^{p^{\alpha-1}} \\ &= b^{p^{\alpha-1}}\left(\left(\frac{a}{b}\right)^{p^{\alpha-1}} - 1\right) \\ &\geq b^p\left(\left(\frac{a}{b}\right)^p - 1\right) \qquad (\because\ \alpha \geq 2) \\ &= a^p - b^p = (b+1)^p - b^p \\ &= \binom{p}{1}b^{p-1} + \binom{p}{2}b^{p-2} + \cdots + \binom{p}{p} \\ &> \binom{p}{1}b^{p-1} \geq \binom{p}{1} = p \end{aligned}$$

が成り立つから

$$p = \psi_n = \psi_{pq}\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right) > p$$

と，矛盾が生じる．

したがって，$\alpha = 1$ でなければならない．このとき

$$n = pq \quad (p \nmid q). \qquad \cdots\cdots ⑪$$

$p = 2$ のとき $n = 2q$, $2 \nmid q$ で $p = 2$ は n を割り切る最大の素数だから $q = 1$ でなければならず $n = 2$ となる．これは $n \geq 3$ に矛盾する．したがって，以下 $p \geq 3$ とする．

◎ $p=\psi_n=\dfrac{\psi_q\left(a^p,b^p\right)}{\psi_q}\geq\left(\dfrac{a^p-b^p}{a+b}\right)^{\varphi q}\geq\dfrac{a^p-b^p}{a+b}$　……⑫

が成り立つことを示す.

$p\nmid q$ だから

$$p=\psi_n=\psi_{pq}=b^{\varphi(pq)}\Phi_{pq}\left(\frac{a}{b}\right)=b^{\varphi(pq)}\frac{\Phi_q\left(\left(\dfrac{a}{b}\right)^p\right)}{\Phi_q\left(\dfrac{a}{b}\right)}$$

において，$\varphi(pq)=\varphi(p)\varphi(q)=(p-1)\varphi(q)=p\varphi(q)-\varphi(q)$ を使うと

$$\begin{aligned}p&=b^{\varphi(pq)}\frac{\Phi_q\left(\left(\dfrac{a}{b}\right)^p\right)}{\Phi_q\left(\dfrac{a}{b}\right)}\\&=\frac{b^{p\varphi(q)}}{b^{\varphi(q)}}\cdot\frac{\Phi_q\left(\left(\dfrac{a}{b}\right)^p\right)}{\Phi_q\left(\dfrac{a}{b}\right)}\\&=\frac{\left(b^p\right)^{\varphi(q)}\Phi_q\left(\left(\dfrac{a}{b}\right)^p\right)}{b^{\varphi(q)}\Phi_q\left(\dfrac{a}{b}\right)}\\&=\frac{\psi_q\left(a^p,b^p\right)}{\psi_q}.\end{aligned}$$

ここで,

$$\psi_q\left(a^p,b^p\right)=\left(b^p\right)^{\varphi(q)}\Phi_q\left(\left(\frac{a}{b}\right)^p\right)\geq\left(b^p\right)^{\varphi(q)}\left(\left(\frac{a}{b}\right)^p-1\right)^{\varphi(q)}=\left(a^p-b^p\right)^{\varphi(q)},$$

$$\psi_q=b^{\varphi(q)}\Phi_q\left(\frac{a}{b}\right)\leq b^{\varphi(q)}\left(\left(\frac{a}{b}\right)+1\right)^{\varphi(q)}=(a+b)^{\varphi(q)}$$

が成り立つから

$$\frac{\psi_q\left(a^p,b^p\right)}{\psi_q}\geq\frac{\left(a^p-b^p\right)^{\varphi(q)}}{(a+b)^{\varphi(q)}}=\left(\frac{a^p-b^p}{a+b}\right)^{\varphi q}\geq\frac{a^p-b^p}{a+b}$$

が成り立つ.

◎ $\dfrac{a^p-b^p}{a+b}\geq\dfrac{2^p-1}{3}$　……⑬

が成り立つことを示す.

まず，$m\in\mathbb{N},m\geq3,x\in\mathbb{R},x\geq1$ のとき，$(x+1)^m-x^m\geq\left(2^m-1\right)x$ が成り立つことを示す.

$f(x)=(x+1)^m-x^m-\left(2^m-1\right)x\quad(x\geq1)$ とおくと,

$$f'(x)=m(x+1)^{m-1}-mx^{m-1}-\left(2^m-1\right),$$

$$\begin{aligned} f''(x) &= m(m-1)(x+1)^{m-2} - m(m-1)x^{m-2} \\ &= m(m-1)\left((x+1)^{m-2} - x^{m-2}\right) > 0. \end{aligned}$$

$f'(x)$ は $[1,\infty)$ で増加関数で，
$x \geq 1$ のとき，

$$\begin{aligned} f'(x) \geq f'(1) &= m2^{m-1} - 2^m - m + 1 \\ &= (m-2)\left(2^{m-1} - 1\right) - 1 \\ &\geq (3-2)\left(2^{3-1} - 1\right) - 1 = 2 > 0. \end{aligned}$$

$f(x)$ は $[1,\infty)$ で増加関数で，
$x \geq 1$ のとき，$f(x) \geq f(1) = 0$.
よって，$x \geq 1$ のとき，$(x+1)^m - x^m \geq (2^m - 1)\,x$ が成り立つ．

$p \geq 3, b \geq 1$ であるから，$(b+1)^p - b^p \geq (2^p - 1)\,b$ が成り立つ．この不等式を使うと，

$$\frac{a^p - b^p}{a+b} = \frac{(b+1)^p - b^p}{2b+1} \geq \frac{(2^p-1)\,b}{2b+1} = \frac{2^p - 1}{2 + \dfrac{1}{b}} \geq \frac{2^p - 1}{3}.$$

◎ ⑫，⑬から

$$p \geq \frac{2^p - 1}{3} \qquad \cdots\cdots ⑭$$

が成り立つ．この不等式を利用して，$n = 6, a = 2, b = 1$ であることを示す．

まず，$m \in \mathbb{N}, m \geq 4$ のとき，$2^m > 3m + 1$ が成り立つことを m に関する数学的帰納法で示す．

(I) $m = 4$ のとき，$2^4 = 16 > 13 = 3 \cdot 4 + 1$ から，不等式は成り立つ．

(II) $m = k$ $(k \geq 4)$ のとき不等式が成り立つと仮定すると，$2^k > 3k + 1$.
この不等式の両辺に 2 をかけると，$2^{k+1} > 6k + 2$.
$6k + 2 - \left(3(k+1) + 1\right) = 3k - 2 \geq 3 \cdot 4 - 2 = 10 > 0$ から $6k + 2 > 3(k+1) + 1$.
よって，$2^{k+1} > 6k + 2 > 3(k+1) + 1$ から $2^{k+1} > 3(k+1) + 1$.
すなわち，$m = k + 1$ のときも不等式は成り立つ．

(III) (I)，(II) から，すべての正の整数 $m \geq 4$ に対して，不等式は成り立つ．
$p > 3$ のとき，$2^p > 3p + 1$ すなわち，$\dfrac{2^p - 1}{3} > p$ が成り立ち，これは⑭に矛盾する．
したがって，$p = 3$ でなければならない．このとき，⑪から，$n = 3q,\ 3 \nmid q$.
$p\,(= 3)$ は n を割り切る最大の素数であるから，$q = 1$ または $q = 2$ となる．

$q=1$ のとき，$n=3$.
このとき，$a^3-b^3=(b+1)^3-b^3=3b^2+3b+1\equiv 1 \pmod 3$ となり，
$p=3\mid a^3-b^3$ に矛盾する．
$q=2$ のとき，$n=6$．$\psi_n=p$ から $\psi_6=3$.

$$\begin{aligned}\psi_6&=\prod_{d|6} {z_{\frac{6}{d}}}^{\mu(d)}\\&={z_6}^{\mu(1)}{z_3}^{\mu(2)}{z_2}^{\mu(3)}{z_1}^{\mu(6)}\\&=z_6z_3^{-1}z_2^{-1}z_1\\&=\frac{\left(a^6-b^6\right)(a-b)}{\left(a^3-b^3\right)\left(a^2-b^2\right)}\\&=a^2-ab+b^2=(b+1)^2-(b+1)b+b^2\\&=b^2+b+1.\end{aligned}$$

$\psi_6=3$ であるから，$b^2+b+1=3\qquad b^2+b-2=0\qquad (b-1)(b+2)=0.$
$b\geq 1$ なので，$b=1$．よって，$a=2$.
したがって，この場合は，$a^n-b^n=2^6-1^6$ となり，例外の場合になっている，
$P_n>1$ でないならば，$n=6, a=2, b=1$ が示せたので，対偶をとると，
2^6-1^6 の場合でなければ，$P_n>1$ が成り立つことが言えた．　□

10.3　和に対する Zsigmondy の定理

定理 10.3.1　(Zsigmondy's theorem for sums)
$n \geq 2$ は正の整数，a と b は互いに素な正の整数で $a \neq b$ とする．
このとき，$a^n + b^n$ の素数の約数 p で，$p \nmid a^k + b^k$ $(k = 1, 2, \ldots, n-1)$ を満たすものが存在する．
ただし，次の場合を除く．

(a)　$2^3 + 1^3$

証明　$a > b$ と仮定しても一般性を失わない．$2n\,(\geq 4)$ に対して Zsigmondy の定理を適用すると，$a^{2n} - b^{2n}$ は primitive prime divisor p をもつ．
よって，$p \mid a^{2n} - b^{2n} = (a^n + b^n)(a^n - b^n)$,

$$p \nmid a - b,\ p \nmid a^2 - b^2,\ \ldots,\ p \nmid a^n - b^n,\ p \nmid a^{n+1} - b^{n+1},\ \ldots,\ p \nmid a^{2n-1} - b^{2n-1}$$

が成り立つ．

$p \nmid a^n - b^n$, $p \mid a^{2n} - b^{2n} = (a^n + b^n)(a^n - b^n)$ から，$p \mid a^n - +^n$.

$k \in \left\{1, 2, \ldots, n-1\right\}$ に対して，$p \nmid a^{2k} - b^{2k} = \left(a^k + b^k\right)\left(a^k - b^k\right)$ から $p \nmid a^k + b^k$ がでる．

$2n \neq 2$ であるから，例外は，$2^6 - 1^6 = \left(2^3 + 1\right)\left(2^3 - 1\right)$ から $2^3 + 1^3$ の場合である．　□

10.4 例題と問題

例題 10.4.1 (Japanese MO 2011)

Find all quintuples of positive integers (a, n, p, q, r) such that

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1).$$

解答 $a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1).$ …… ①

対称性から $p \geqq q \geqq r$ と仮定する.

$a = 1$ のとき①は常に成り立つから，$a = 1$, n, p, q, r は任意の正の整数.

以下，$a \geqq 2$ とする.

$a \geqq 3$ かつ $n \geqq 3$ とする.

$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1) > a^p - 1$ から $n > p$ すなわち $n > p \geqq q \geqq r$ が成り立つ.

Zsigmondy の定理により $a^n - 1$ は $a^p - 1$, $a^q - 1$, $a^r - 1$ を割り切らない素数の因数をもつから，①を満たす解はない.

したがって，$a < 3$ または $n < 3$ となる.

(i) $a = 2$ の場合

①は

$2^n - 1 = (2^p - 1)(2^q - 1)(2^r - 1)$ …… ②

となる.

$2^n - 1 = (2^p - 1)(2^q - 1)(2^r - 1) \geqq 2^p - 1$ から $n \geqq p$ となるので，$n > p$ と $n = p$ の場合に分けて考える.

(1) $n > p$ のとき

Zsigmondy の定理により $n \neq 6$ ならば $2^n - 1$ は $2^p - 1$, $2^q - 1$, $2^r - 1$ を割り切らない素数の因数をもつから，②を満たす解はない.

よって $n = 6$ で

$(2^p-1)(2^q-1)(2^r-1) = 2^6-1 = 7\cdot 3^2$ となるから $2^p-1 = 7, 2^q-1 = 2^r-1 = 3$

すなわち $(a, n, p, q, r) = (2, 6, 3, 2, 2)$ となる.

(2) $n = p$ のとき

②は

$1 = (2^q - 1)(2^r - 1)$ となり $(a, n, p, q, r) = (2, n, n, 1, 1)$ を得る.

(ii) $n < 3$ の場合

(3) $n = 1$ のとき

①は

$a-1=(a^p-1)(a^q-1)(a^r-1)$ …… ③

となる．$a \geqq 2$ なので

$(a-1)^3 \geq a-1=(a^p-1)(a^q-1)(a^r-1) \geqq (a-1)^3$ が成り立つから，

$p=q=r=1$, $a-1=(a-1)^3$ から $(a,\, n,\, p,\, q,\, r)=(2,\, 1,\, 1,\, 1,\, 1)$ を得る．

(4) $n=2$ のとき

①は

$a^2-1=(a^p-1)(a^q-1)(a^r-1)$ …… ④

となる．

$a=2$ ならば，④は $3=(2^p-1)(2^q-1)(2^r-1)$ となるので，

$$2^p-1=3,\ 2^q-1=2^r-1=1$$

すなわち $(a,\, n,\, p,\, q,\, r)=(2,\, 2,\, 2,\, 1,\, 1)$ となる．

$a \geqq 3$ ならば，

$a^2-1=(a^p-1)(a^q-1)(a^r-1) \geqq (a-1)^3$ から $a^2-1 \geqq (a-1)^3$ が成り立つ．$a \geqq 3$ なので $a+1 \geqq (a-1)^2$ を解くと $a=3$ を得る．

よって $(a,\, n,\, p,\, q,\, r)=(3,\, 2,\, 1,\, 1,\, 1)$

以上のことから，求める解は

- $a=1$, n, p, q, r は任意の正の整数
- $(a,\, n,\, p,\, q,\, r)=(2,\, 6,\, 3,\, 2,\, 2)$, と，$p,\, q,\, r$ とを並べ替えたもの
- $(a,\, n,\, p,\, q,\, r)=(2,\, n,\, n,\, 1,\, 1)$, n は任意の正の整数と，$p,\, q,\, r$ とを並べ替えたもの
- $(a,\, n,\, p,\, q,\, r)=(3,\, 2,\, 1,\, 1,\, 1)$ □

例題 10.4.2　(Math Olmpiad Summer Program 2001)

Find all quadruples of positive integers $(x,\, r,\, p,\, n)$ such that p is a prime, $n, r>1$ and $x^r-1=p^n$.

解答 明らかに $x \geq 2$ である．

(i) $x=2$ の場合

$x^r-1=p^n$ から

$$2^r=p^n+1. \qquad \cdots\cdots ①$$

$p=2$ のときは，①を満たす r, n は存在しないから，$p \geq 3$ となり，p は奇素数である．

n が偶数だと $p^2 \equiv 1 \pmod 4$ より $p^n \equiv 1 \pmod 4$.

よって，$p^n+1 \equiv 2 \pmod 4$ となり，$2^2 \mid p^n+1$ に矛盾する．
したがって，n は奇数でなければならない．
Zsigmondy の定理より，p^n+1 は

$$q_1 \mid p^n+1, \quad q_1 \nmid p^k+1 \ (k=1,2,\ldots,n-1)$$

を満たす素数の因数 q_1 をもつ．
q_1 は素数で，$q_1 \mid p^n+1=2^r$ だから $q_1=2$ となる．

$$2^r = p^n+1 = (p+1)\left(p^{n-1}-p^{n-2}+\cdots-p+1\right)$$

$p+1 \geq 4$ だから．$2 \mid p+1$ となるが，これは $2=q_1 \nmid p^1+1$ に矛盾する．

(ii) $x \geq 3$ の場合

$$p^n = x^r-1 = (x-1)\left(x^{r-1}+x^{r-1}+\cdots+x+1\right)$$

で，$x-1 \geq 2$ だから，$p \mid x-1$ が成り立つ．
（a） $r=2$ かつ $x+1$ が 2 のべき乗になる
場合を除くと，Zsigmondy の定理より，x^r-1 は

$$q_2 \mid x^r-1, \quad q_2 \nmid x^k-1 \ (k=1,2,\ldots,r-1)$$

を満たす素数の因数 q_2 をもつ．
q_2 は素数で，$q_2 \mid x^r-1=p^n$ だから $q_2=p$ となる．
よって， $p=q_2 \nmid x^1-1$ となるが，これは $p \mid x-1$ に矛盾する．
したがって，(a) を除くと解がないから，(a) の場合を考える．
$r=2, x+1=2^y \ (y \geq 2, y \in \mathbb{N})$ とおける．$x^r-1=p^n$ は

$$x^2-1=p^n \qquad (x+1)(x-1)=p^n$$

と変形できるから，$x+1=2^y$ を使うと

$$2^y\left(2^y-2\right)=p^n \qquad 2^{y+1}\left(2^{y-1}-1\right)=p^n.$$

p は素数だから，$p=2$ で $2^{y+1}\left(2^{y-1}-1\right)=2^n$ から

$$2^{y-1}-1=2^{n-y-1}.$$

$y-1=1, n-y-1=0$ となるから $y=2, n=3$.
よって，求める解は，$(x,r,p,n)=(3,2,2,3)$. □

例題 10.4.3　(Balkan MO 2009)

Find all triples of positive integers (x, y, z) such that $5^x - 3^y = z^2$.

解答　mod 3 で考えると，

$$z^2 = 5^x - 3^y \equiv (-1)^x - 0 \equiv (-1)^x \pmod 3.$$

ところで $z^2 \equiv 0 \pmod 3$ または $z^2 \equiv 1 \pmod 3$ であるから，x は偶数である．
$x = 2w$ $(w \in \mathbb{N})$ とおき，$5^x - z^2 = 3^y$ に代入すると，$5^{2w} - z^2 = 3^y$ から

$$(5^w - z)(5^w + z) = 3^y \qquad \cdots\cdots ①$$

$$\gcd(5^w - z, 5^w + z) = \gcd(5^w - z, (5^w + z) - (5^w - z)) = \gcd(5^w - z, 2z).$$

①から，$5^w - z$ は 2 で割り切れないことがわかるので

$$\gcd(5^w - z, 2z) = \gcd(5^w - z, z) = \gcd(5^w - z + z, z) = \gcd(5^w, z).$$

①から，z は 5 で割り切れないことがわかるので，$\gcd(5^w, z) = 1$.
よって，$\gcd(5^w - z, 5^w + z) = 1$.
$5^w + z$ と $5^w - z$ は互いに素で，$5^w + z > 5^w - z$ だから，①より

$$5^w + z = 3^y \qquad \cdots\cdots ② \qquad 5^w - z = 1 \qquad \cdots\cdots ③$$

②+③から

$$2 \cdot 5^w = 3^y + 1.. \qquad \cdots\cdots ④$$

$y \geq 3$ のとき，Zsigmondy の定理より，$3^y + 1$ は

$$p \mid 3^y + 1,\ p \nmid 3^k + 1\ (k = 1, 2, \ldots, y-1)$$

を満たす素数の因数 p をもつ．$p \nmid 3^2 + 1 = 10 = 2 \cdot 5$ より，$p \neq 2, p \neq 5$．ところが，
$p \mid 3^y + 1 = 2 \cdot 5^w$ より，$p \in \Big\{2, 5\Big\}$．これは，$p \neq 2, p \neq 5$ に矛盾する．
したがって，$y \leq 2$.
$y = 1$ のとき，④から $5^w = 2$．これを満たす正の整数はない．
$y = 2$ のとき，$5^w = 1$ から $w = 1$.
よって，求める解は，$(x, y, z) = (2, 2, 4)$. □

例題 10.4.4　Find all positive integral solutions to

$$(a+1)\left(a^2 + a + 1\right) \cdots \left(a^n + a^{n-1} + \cdots + 1\right) = a^m + a^{m-1} + \cdots + 1.$$

解答

$$(a+1)\left(a^2 + a + 1\right) \cdots \left(a^n + a^{n-1} + \cdots + 1\right) = a^m + a^{m-1} + \cdots + 1. \qquad \cdots\cdots ①$$

とおく．

$m=1$ のとき，$n=1$ でなければならず，このとき，①は，$a+1=a+1$ となり常に成り立つ．

$a=1$ のとき，①は $2\cdot 3\cdots(n+1)=m+1$ から $m=(n+1)!-1$ となる．

以下，$a\geq 2,\ m\geq 2$ とする．

$$\begin{aligned} a^m+a^{m-1}+\cdots+1&=(a+1)\left(a^2+a+1\right)\cdots\left(a^n+a^{n-1}+\cdots+1\right)\\ &>a^n+a^{n-1}+\cdots+1. \end{aligned}$$

この不等式を変形すると，$\dfrac{a^{m+1}-1}{a-1}>\dfrac{a^{n+1}-1}{a-1}$ すなわち $a^{m+1}>a^{n+1}$ となるから，$m>n$ を得る．

①を変形する．

$$\frac{a^2-1}{a-1}\cdot\frac{a^3-1}{a-1}\cdots\frac{a^{n+1}-1}{a-1}=\frac{a^{m+1}-1}{a-1}$$

から

$$\left(a^2-1\right)\left(a^3-1\right)\cdots\left(a^{n+1}-1\right)=\left(a^{m+1}-1\right)(a-1)^{n-1}. \qquad \cdots\cdots ②$$

$m+1\geq 3$ なので，

（a）$a=2,\ m+1=6$ でなければ，

Zsigmondy の定理より，$a^{m+1}-1$ は $a^2-1, a^3-1,\ldots,a^{n+1}-1$ を割り切らない素数の因数 p をもつ．$p\mid a^{m+1}-1,\ p\nmid\left(a^2-1\right)\left(a^3-1\right)\cdots\left(a^{n+1}-1\right)$ であるから，これは，②に矛盾する．

したがって，$a=2,\ m+1=6$ となる．$m>n$ から $n\leq 4$.

このとき②は

$$\left(2^2-1\right)\left(2^3-1\right)\cdots\left(2^{n+1}-1\right)=2^6-1. \qquad \cdots\cdots ③$$

$n+1=2$ のとき，③は成り立たない．

$n+1=3$ のとき，③は成り立たない．

$n+1\geq 4$ のとき，③の両辺を $\left(2^2-1\right)\left(2^3-1\right)$ で割ると

$$\left(2^4-1\right)\cdots\left(2^{n+1}-1\right)=3$$

となる．$2^4-1>3$ であるから，この等式を満たす n は存在しない．

以上のことから，求める解は次のようになる．

- $m=n=1$，a は任意の正の整数
- $a=1$，m,n は $m=(n+1)!-1$ を満たす正の整数

□

例題 10.4.5　(Czech-Slovak Match 1996)

Find all positive integral solutions to $p^x - y^p = 1$, where p is a prime.

解答

$$y^p + 1 = p^x \qquad \cdots\cdots ①$$

とおく，

(i) $y = 1$ のとき，①は，$2 = p^x$ となり，$p = 2, x = 1$．よって $(p, x, y) = (2, 1, 1)$.

(ii) $p = 2$ のとき，①は

$$y^2 + 1 = 2^x \qquad \cdots\cdots ②$$

となる．②から，y は奇数であることがわかる．②の両辺から 2 を引くと

$$(y + 1)(y - 1) = 2\left(2^{x-1} - 1\right) \qquad \cdots\cdots ③$$

y が奇数のとき，③の左辺は 4 の倍数になるが，③の右辺は，$x = 1$ のときのみ，4 の倍数になる．よって $(p, x, y) = (2, 1, 1)$ となる．

(iii) $y \geq 2, p \geq 3$ の場合

$(y, p) \neq (2, 3)$ のとき，Zsigmondy の定理より，$y^p + 1$ は $y + 1$ を割り切らない素数の因数 q_1 をもつ．$q_1 \mid y^p + 1 = p^x$ から $q_1 \mid p^x$ で，p, q_1 は素数だから，$p = q_1$ となる．

$y + 1 \geq 3$ より $y + 1$ は素数の因数を持つから，これを q_2 とすると，$q_1 \nmid y + 1$ だから $q_1 \neq q_2$.

$$y^p + 1 = (y + 1)\left(y^{p-1} - y^{p-2} + \cdots - y + 1\right)$$

から，$y + 1 \mid y^p + 1$ が成り立つ．

$q_2 \mid y + 1 \mid y^p + 1 = p^x$ から $q_2 \mid p^x$ で，p, q_2 は素数だから，$p = q_2$ となる．$p = q_1$ であったから，$q_1 = q_2$ となり $q_1 \neq q_2$ に矛盾する．

したがって，$y = 2, p = 3$．このとき，①は，$2^3 + 1 = 3^x$ となり，$x = 2$ を得る．

よって $(p, x, y) = (3, 2, 2)$.

以上のことから，求める解は，$(p, x, y) = (2, 1, 1), (3, 2, 2)$ となる．　□

例題 10.4.6　(IMO Shortlist 2000)

Find all triples of positive integers (a, m, n) such that $a^m + 1$ divides $(a + 1)^n$.

解答

$$a^m + 1 \mid (a + 1)^n \qquad \cdots\cdots ①$$

とする．

(i) $a=1$ のとき，①は常に成り立つ．

(ii) $m=1$ のとき，①は常に成り立つ．

(iii) $a\geq 2, m\geq 2$ の場合

$(a,m)\neq(2,3)$ のとき，Zsigmondy の定理より，a^m+1 は $a+1$ を割り切らない素数の因数 p をもつ．

$p\mid a^m+1$ であるが，$p\nmid a+1$ から $p\nmid(a+1)^n$ なので，$a^m+1\mid(a+1)^n$ に矛盾する．

したがって，$(a,m)=(2,3)$ でなければならない．このとき，①は $9\mid 3^n$ となるので，$n\geq 2$ を得る．

以上から，求める解は

- $a=1,\quad m,n$ は任意の正の整数
- $m=1,\quad a,n$ は任意の正の整数
- $(a,m)=(2,3),\quad n$ は 2 以上の正の整数

となる． □

例題 10.4.7 (Polish MO 2010 Round 1)

Let p and q be prime numbers with $q>p>2$. Prove that $2^{pq}-1$ has at least three distinct prime factors.

解答 $pq>q>p>2$ で $2^p-1\mid 2^{pq}-1,\ 2^q-1\mid 2^{pq}-1$ が成り立つ．

Zsigmondy の定理より，$2^{pq}-1$ は 2^q-1 も 2^p-1 も割り切らない素数の因数 p_1 をもつ．さらに，2^q-1 は 2^p-1 を割り切らない素数の因数 p_2 をもつ．最期に $2^p-1\ (\geq 7)$ は素数の因数 p_3 をもつ．

よって，$2^{pq}-1$ は少なくとも 3 個の異なる素数 p_1,p_2,p_3 をもつ． □

例題 10.4.8 (1^{ST} European Mathematical Cup 2012)

Find all positive integers a,b,n and prime numbers p that satisfy $a^{2013}+b^{2013}=p^n$.

解 1 $2013=3\cdot 11\cdot 61$.

$d=\gcd(a,b), a=dx, b=dy, \gcd(x,y)=1, x,y\in\mathbb{N}$ とおき，$a^{2013}+b^{2013}=p^n$ に代入すると

$$d^{2013}\left(x^{2013}+y^{2013}\right)=p^n.$$

p は素数だから，$d=p^k, k\in\mathbb{N}_0$ とおけるから，上の式に代入して

$$x^{2013}+y^{2013}=p^{n-2013k}$$

と変形できる．$x^{2013}+y^{2013}\geq 2$ だから，$n-2013k\geq 1$ で，$m=n-2013k\in\mathbb{N}$ とお

くと

$$x^{2013}+y^{2013}=p^m \qquad \cdots\cdots ①$$

となる．①の左辺を因数分解した式

$$(x+y)\left(x^{2012}-x^{2011}y+x^{2010}y^2-\cdots-xy^{2011}+y^{2012}\right)=p^m$$

と，$x+y\geq 2$ より

$$p \mid x+y$$

がわかる．

$x\neq y$ と仮定すると，Zsigmondy の定理より，$p_1 \mid x^{2013}+y^{2013}$ かつ $p_1 \nmid x+y$ となる素数 p_1 が存在する．

$p_1 \mid x^{2013}+y^{2013}=p^m$ で p_1, p は素数だから，$p_1=p$ となる．このとき，$p=p_1 \nmid x+y$ であるが，これは $p \mid x+y$ に矛盾する．

したがって，$x=y$ でなければならない．$\gcd(x,y)=1$ であったから，$x=y=1$ である．①は $2=p^m$ となるので，$p=2, m=1$ を得る．

ゆえに，求める解は

$a=b=2^k,\ n=2013k+1,\ p=2,\ k\in\mathbb{N}_0.$ □

解 2　　$2013=3\cdot 11\cdot 61.$

対称性から，$x\geq y$ と仮定しても一般性を失わない．

$d=\gcd(a,b), a=dx, b=dy, \gcd(x,y)=1, x,y\in\mathbb{N}$ とおき，$a^{2013}+b^{2013}=p^n$ に代入すると

$$d^{2013}\left(x^{2013}+y^{2013}\right)=p^n.$$

p は素数だから，$d=p^k, k\in\mathbb{N}_0$ とおけるから，上の式に代入して

$$x^{2013}+y^{2013}=p^{n-2013k}$$

と変形できる．$x^{2013}+y^{2013}\geq 2$ だから，$n-2013k\geq 1$ で，$m=n-2013k\in\mathbb{N}$ とおくと

$$x^{2013}+y^{2013}=p^m \qquad \cdots\cdots ①$$

となる．①の左辺を因数分解した式

$$(x+y)\left(x^{2012}-x^{2011}y+x^{2010}y^2-\cdots-xy^{2011}+y^{2012}\right)=p^m$$

と，$x+y\geq 2$ より

$$p \mid x+y$$

がわかる．また，

$$A=x^{2012}-x^{2011}y+x^{2010}y^2-\cdots-xy^{2011}+y^{2012}$$

とおくと

$$A(x+y)=p^m \qquad \cdots\cdots ②$$

となる.

(1) $\gcd(2013,p)=1$ の場合

$p \mid x+y$ と $\gcd(x,y)=1$ より $p \nmid x, p \nmid y$ である.

LTE の補助定理より，$v_p\left(x^{2013}+y^{2013}\right)=v_p(x+y)$ が成り立つ.

ところで，$v_p\left(x^{2013}+y^{2013}\right)=v_p((x+y)A)=v_p(x+y)+v_p(A)$ であるから，$v_p(A)=0$ となる.

$x>y$ だとすると，

$$A=x^{2011}(x-y)+x^{2009}y^2(x-y)+\cdots+xy^{2010}(x-y)+y^{2012}>1$$

で，$A(x+y)=x^{2013}+y^{2013}=p^m$ であったから，$p \mid A$ すなわち $v_p(A)\geq 1$ となり，$v_p(A)=0$ に矛盾する.

したがって，$x=y$ でなければならない.

$\gcd(x,y)=1$ であったから，$x=y=1$ である．①は $2=p^m$ となるので，$p=2, m=1$ を得る.

ゆえに，求める解は，$a=b=2^k$, $n=2013k+1$, $p=2$, $k\in\mathbb{N}_0$.

(2) $\gcd(2013,p)=\gcd(3\cdot 11\cdot 61,p)>1$ の場合　$p\in\left\{3,\ 11,\ 61\right\}$

$p \mid x+y$ と $\gcd(x,y)=1$ より $p \nmid x, p \nmid y$ である.

LTE から

$$v_p\left(x^{2013}+y^{2013}\right)=v_p(x+y)+v_p(2013)$$

が成り立つ.

$v_p\left(x^{2013}+y^{2013}\right)=v_p\left(p^m\right)=m$, $v_p(x+y)+v_p(2013)=v_p(x+y)+v_p(3\cdot 11\cdot 61)=v_p(x+y)+1$ だから，$m=v_p(x+y)+1$ より，$v_p(x+y)=m-1$.

$p \mid x+y$ であったから，$m\geq 2$.

ところで，$m=v_p\left(x^{2013}+y^{2013}\right)=v_p((x+y)A)=v_p(x+y)+v_p(A)=m-1+v_p(A)$ であるから，$v_p(A)=1$ となる.

$v_p(x+y)=m-1, v_p(A)=1$ と②から

$$x+y=p^{m-1},\ A=p \quad (m\geq 2)$$

である.

$x>y$ だとすると，

$$p=A=x^{2011}(x-y)+x^{2009}y^2(x-y)+\cdots+xy^{2010}(x-y)+y^{2012}$$

$$\begin{aligned}
&\geq x^{2011} + x^{2009}y^2 + \cdots + xy^{2010} + y^{2012} \\
&> x^{2011} + y^{2012} \\
&> x + y = p^{m-1}
\end{aligned}$$

から $p > p^{m-1}$ となり $p \leq p^{m-1}$ に矛盾する．

したがって，$x = y$ でなければならないが，$x^{2013} + y^{2013} = p^m$ から $2x^{2013} = p^m$．

$p = 2$ となるが，$p \in \left\{3,\, 11,\, 61\right\}$ であることに矛盾する． □

問題 10.4.1 (例題 7.4.4 と同じ問題)

Find all solutions of the equation $x^{2009} + y^{2009} = 7^z$ for x, y, z positive integers.

問題 10.4.2 (IMO Shortlist 1997)

Let $b, m, n \in \mathbb{N}$ with $b > 1$ and $m \neq n$.

Suppose that $b^m - 1$ and $b^n - 1$ have the same set of prime divisors. Show that $b + 1$ must be a power of 2.

問題 10.4.3 Determine all positive integer m, n, l, k with $l > 1$ such that :

$$(1 + m^n)^l = 1 + m^k.$$

問題 10.4.4 (Romania TST 1994)

Prove that the sequence $a_n = 3^n - 2^n$ contains no three terms in geometric progression.

問題 10.4.5 (Italy TST 2003)

Find all triples of positive integers (a, b, p) with a, b positive integers and p a prime number such that $2^a + p^b = 19^a$.

問題 10.4.6 Find all nonnegative integers m, n such that $3^m - 5^n$ is perfect square.

問題 10.4.7 Find all positive integers $a, n > 1$ and k for which $3^k - 1 = a^n$.

問題 10.4.8 Find all positive integers a, b and $c \geq 2$ such that : $a^b + 1 = (a + 1)^c$.

問題 10.4.9 (British Math Olympiad 1996)

Determine all sets of non-negative integers x, y and z which satisfy the equation $2^x + 3^y = z^2$.

問題 10.4.10 Fermat's last theorem asserts that for a positive integer $n \geq 3$, the equation $x^n + y^n = z^n$ has no integral solution with $xyz \neq 0$. Prove this statement when z is a prime.

問題 10.4.11 (Russia 1996) (例題 7.4.1 と同じ問題)

Find all positive integers n for which there exist positive integers x, y and k such that $\gcd(x, y) = 1$, $k > 1$ and $3^n = x^k + y^k$.

問題 10.4.12 Find all quadruples of positive integers (x, y, z, m) such that m is a odd number , $m \geq 3$ and $3^x 7^y + 1 = z^m$.

第11章

問題の解答

問題 1.1.1　n を正の整数とするとき，次の等式を組合せ論を用いて証明せよ．

$$\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}, \qquad (1\leq k\leq n).$$

解答　$n+1$ 個の $a_1, a_2, \ldots, a_{n+1}$ から k 個とって作った $\binom{n+1}{k}$ 個の組合せは，次の 2 種類に分けられる．

- a_1 を含まない組合せ
  a_1 以外の n 個から k 個を選んで得られるから，組合せの数は $\binom{n}{k}$.
- a_1 を含む組合せ
  a_1 以外の n 個から $k-1$ 個を選んで，それに a_1 を付け加えて得られるから，組合せの数は $\binom{n}{k-1}$.

したがって，

$$\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k} \qquad (1\leq k\leq n). \qquad \square$$

注　問題 1.1.2 と同様に解くこともできる．
等式 $(1+x)^{n+1}=(1+x)^n(1+x)$ を利用する．
左辺 $(1+x)^{n+1}$ の展開式における x^k の係数は $\binom{n+1}{n}$ である．
右辺

$$(1+x)^n(1+x)=\left[\binom{n}{0}+\binom{n}{1}x+\cdots+\binom{n}{n}x^n\right](1+x)$$

の展開式における x^k を含む項は $\binom{n}{k}x^k\cdot 1+\binom{n}{k-1}x^{k-1}\cdot x$ だから，x^k の係数は

$\binom{n}{k}+\binom{n}{k-1}$ となるので，

$$\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k} \qquad (1\leq k\leq n). \qquad \square$$

問題 1.1.2　n を正の整数とするとき，等式 $(1+x)^{2n}=(1+x)^n(1+x)^n$ の両辺の展開式を利用して，次の等式が成り立つことを証明せよ．

$$\binom{2n}{n}=\binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n}^2. \qquad \cdots\cdots(*)$$

解答 左辺 $(1+x)^{2n}$ の展開式における x^n の係数は $\binom{2n}{n}$ で，右辺

$$(1+x)^n(1+x)^n=\left[\binom{n}{0}+\binom{n}{1}x+\cdots+\binom{n}{n}x^n\right]\left[\binom{n}{0}+\binom{n}{1}x+\cdots+\binom{n}{n}x^n\right]$$

の展開式における x^n の係数は $\binom{n}{0}\cdot\binom{n}{n}+\binom{n}{1}\cdot\binom{n}{n-1}+\cdots+\binom{n}{n}\cdot\binom{n}{0}$ で，$\binom{n}{r}=\binom{n}{n-r}$ を使うと

$$\begin{aligned}&\binom{n}{0}\cdot\binom{n}{n}+\binom{n}{1}\cdot\binom{n}{n-1}+\cdots+\binom{n}{n}\cdot\binom{n}{0}\\ =&\binom{n}{0}\cdot\binom{n}{0}+\binom{n}{1}\cdot\binom{n}{1}+\cdots+\binom{n}{n}\cdot\binom{n}{n}\\ =&\binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n}^2\end{aligned}$$

となるから

$$\binom{2n}{n}=\binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n}^2.$$

が成り立つ． $\square$

注　組合せ論を用いて，$(*)$ を示すこともできる．

1 から n までの番号のついた赤札および青札がそれぞれ n ずつある．これら $2n$ 枚の札の中から，n 枚の札を取り出すことを考える．

$2n$ 枚の札の中から，n 枚の札の取り出し方は $\binom{2n}{n}$ 通りある．

赤札をちょうど r 枚取り出すのは，赤札を r 枚，青札を $n-r$ 枚取り出すときだから，赤札がちょうど r 枚ふくまれる取り出し方は $\binom{n}{r}\cdot\binom{n}{n-r}$ 通りあるから，$2n$ 枚の札の

中から，n 枚の札の取り出し方の総数は

$$\binom{n}{0}\cdot\binom{n}{n}+\binom{n}{1}\cdot\binom{n}{n-1}+\cdots+\binom{n}{n}\cdot\binom{n}{0}$$

で，$\binom{n}{r}=\binom{n}{n-r}$ を使うと

$$\begin{aligned}&\binom{n}{0}\cdot\binom{n}{n}+\binom{n}{1}\cdot\binom{n}{n-1}+\cdots+\binom{n}{n}\cdot\binom{n}{0}\\ =&\binom{n}{0}\cdot\binom{n}{0}+\binom{n}{1}\cdot\binom{n}{1}+\cdots+\binom{n}{n}\cdot\binom{n}{n}\\ =&\binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n}^2\end{aligned}$$

となるから

$$\binom{2n}{n}=\binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n}^2.$$

が成り立つ．□

※ 母関数については，[101] 第 2 章　母関数　参照.

※ 二項係数を含む大学入試問題については，[102]，[103]，[104] 参照.

問題 1.1.3　p は素数，r は正の整数とする．以下の問いに答えよ．

(1) $x_1,x_2,\ldots,x_r$ についての式 $(x_1+x_2+\cdots+x_r)^p$ を展開したときの単項式 $x_1^{p_1}x_2^{p_2}\cdots x_r^{p_r}$ の係数を求めよ．ここで，$p_1,p_2,\ldots,p_r$ は 0 または正の整数で，$p_1+p_2+\cdots+p_r=p$ を満たすとする．

(2) $x_1,x_2,\ldots,x_r$ が正の整数のとき，$(x_1+x_2+\cdots+x_r)^p-(x_1^p+x_2^p+\cdots+x_r^p)$ は，p で割り切れることを示せ．

(3) r は p で割り切れないとする．このとき，$r^{p-1}-1$ は p で割り切れることを示せ．　(2010 大阪大)

解答 (1) $(x_1+x_2+\cdots+x_r)^p=(x_1+x_2+\cdots+x_r)(x_1+x_2+\cdots+x_r)\cdots(x_1+x_2+\cdots+x_r)$ を展開したとき，等式の第 1 項から x_{i_1}，第 2 項から x_{i_2}，…，第 p 項から x_{i_p} を選んだとき，$x_{i_1}x_{i_2}\cdots x_{i_p}$ と表すことにすると，$x_1^{p_1}x_2^{p_2}\cdots x_r^{p_r}$ の係数は，$x_1,x_2,\ldots,x_r$ の r 個の中から，x_1 を p 個，x_2 を p_2 個，… ，x_r を p_r 個並べる (同じものを含む) 順列の総数と等しいから，

$$\frac{p!}{p_1!p_2!\cdots p_r!}$$

となる.

(2) $(x_1+x_2+\cdots+x_r)^p-(x_1^p+x_2^p+\cdots+x_r^p)$ を展開したときに現れる項は，

$$0\leq p_1\leq p-1, 0\leq p_2\leq p-1,\ldots, 0\leq p_r\leq p-1, p_1+p_2+\cdots+p_r=p \quad \cdots\cdots ①$$

を満たす整数の組 $(p_1,p_2,\ldots,p_r)$ に対する単項式 $x_1^{p_1}x_2^{p_2}\cdots x_r^{p_r}$ であるから，この係数を P とおくと，P は正整数である．①で，$p_1,p_2,\ldots,p_r$ の中で 0 でないものを $p_{j_1},p_{j_2},\ldots,p_{j_s}$ とすると，$1\leq j_k\leq p-1\ (1\leq k\leq s)$ のとき，

$$\begin{aligned}P&=\frac{p!}{p_1!p_2!\cdots p_r!}\\&=\frac{p!}{p_{j_1}!p_{j_2}!\cdots p_{j_s}!}\\&=\frac{p(p-1)\cdots 2\cdot 1}{p_{j_1}(p_{j_1}-1)\cdots 1\cdot p_{j_2}(p_{j_2}-1)\cdots 1\cdot\cdots\cdot p_{j_s}(p_{j_s}-1)\cdots 1}\end{aligned}$$

において，p は素数であり，分母の $p_{j_k},p_{j_k}-1,\ldots,1\ (1\leq k\leq s)$ はすべて p より小さい正整数だから，分子の p は約分されないで残る．ゆえに，P は p の倍数である．$(x_1+x_2+\cdots+x_r)^p-(x_1^p+x_2^p+\cdots+x_r^p)$ を展開したときに現れるすべての項の係数は p で割り切れるから，$x_1,x_2,\ldots,x_r$ が正の整数のとき，

$$(x_1+x_2+\cdots+x_r)^p-(x_1^p+x_2^p+\cdots+x_r^p)$$

は，p で割り切れる．

(3) (2) で $x_1=x_2=\cdots=x_r=1$ とおくと，$r^p-r=r\left(r^{p-1}-1\right)$ は p で割り切れる．r は p で割り切れないから，$r^{p-1}-1$ は p で割り切れる．　□

問題 1.1.4　7^{9999} の下 3 桁（しもみけた）を求めよ．

解答 $7^4=2401$, $9999=4\times 2499+3$ であるから，$n=2499$ とおくと

$$7^{4n}=2401^n=(1+2400)^n=1+n\cdot 2400+\underbrace{\binom{n}{2}\cdot 2400^2+\binom{n}{3}\cdot 2400^3+\cdots+2400^n}_{\text{下 4 桁は 0}}.$$

7^{4n} の下 3 桁は $1+n\cdot 2400$ の下 3 桁を求めればよい．

$$1+2499\cdot 2400=5997601$$

より，$1+n\cdot 2400$ の下 3 桁は 601 となる．

したがって，

$$7^{9999}=7^{9999}\cdot 7^3=(\cdots 601)(343)=\cdots 143$$

となり，7^{9999} の下 3 桁は 143.　□

問題 1.1.5　$\left(x^3+\sqrt{2}\,x^2+\sqrt[3]{3}\,x+1\right)^{100}$ を展開したときの，x^{296} の係数を求めよ．
(1974 京都大・文)

解答　$\left(x^3+\sqrt{2}\,x^2+\sqrt[3]{3}\,x+1\right)^{100}$ を展開したときの一般項は

$$\frac{100!}{p!q!r!s!}\left(x^3\right)^p\left(\sqrt{2}\,x^2\right)^q\left(\sqrt[3]{3}\,x\right)^r 1^s=\frac{100!}{p!q!r!s!}\left(\sqrt{2}\right)^q\left(\sqrt[3]{3}\right)^r x^{3p+2q+r}$$

である．ただし，$p,q,r,s\in\mathbb{N}_0$, $p+q+r+s=100$　……①とする．

x^{296} の係数を求めるのであるから，$3p+2q+r=296$　……②とする．

②を $p+2(p+q+r)-r=296$ と変形して，①を使うと，$p+2(100-s)-r=296$ から

$$p=96+2s+r\geq 96.$$

また，$3p\leq 3p+2q+r=296$ から $p\leq\dfrac{296}{3}=98\dfrac{2}{3}$.

したがって，$p\in\left\{96,\,97,\,98\right\}$ となるから

$$(p,q,r,s)=(96,4,0,0),(97,2,1,0),(98,1,0,1),(98,0,2,0).$$

ゆえに，求める x^{296} の係数は

$$\begin{aligned}&\frac{100!}{96!4!}\left(\sqrt{2}\right)^4+\frac{100!}{97!2!}\left(\sqrt{2}\right)^2\sqrt[3]{3}+\frac{100!}{98!}\left(\sqrt{2}\right)+\frac{100!}{98!2!}\left(\sqrt[3]{3}\right)^2\\&=15684900+9900\sqrt{2}+970200\sqrt[3]{3}+4950\sqrt[3]{9}\end{aligned}$$

□

注　$\left(x^3+\sqrt{2}\,x^2+\sqrt[3]{3}\,x+1\right)^{100}=a_0x^{300}+a_1x^{299}+a_2x^{298}+a_3x^{297}+a_4x^{296}+\cdots$ とおき，両辺を x^{300} で割り，$t=\dfrac{1}{x}$ とおくと

$$\left(1+\sqrt{2}\,t+\sqrt[3]{3}\,t^2+t^3\right)^{100}=a_0+a_1t+a_2t^2+a_3t^3+a_4t^4+\cdots$$

となり，$f(t)=\left(1+\sqrt{2}\,t+\sqrt[3]{3}\,t^2+t^3\right)^{100}$ とおき $a_4=\dfrac{f^{(4)}(0)}{4!}$ を求めればよいが文系向きではないかもしれない．

問題 1.1.6　n を 4 以上の自然数とする．$\left(1+x+x^2+x^3+x^4\right)^n$ を展開したときの x^4 の係数を求めよ．
(1993 京都大・文・後期)

解答　$\left(1+x+x^2+x^3+x^4\right)^n$ を展開したときの一般項は

$$\frac{n!}{p!q!r!s!t!}1^p x^q\left(x^2\right)^r\left(x^3\right)^s\left(x^4\right)^t=\frac{n!}{p!q!r!s!t!}x^{q+2r+3s+4t}$$

である．ただし，$p,q,r,s,t \in \mathbb{N}_0, p+q+r+s=n$ とする．

x^4 の係数を求めるのであるから，$q+2r+3s+4t=4$ とする．t の値で場合分けをする．

$t=1$ のとき，$q=r=s=0, p=n-1$.

$t=0$ のとき，$q+2r+3s=4$.

$(s,r,q,p)=(1,0,1,n-2),(0,2,0,n-2),(0,1,2,n-3),(0,0,4,n-4)$

すなわち

$$(p,q,r,s)=(n-1,0,0,0,1),(n-2,1,0,1,0),(n-2,0,2,0,0),(n-3,2,1,0,0),(n-4,4,0,0,0).$$

ゆえに，求める x^4 の係数は

$$\begin{aligned}
&\frac{n!}{(n-1)!}+\frac{n!}{(n-2)!}+\frac{n!}{(n-2)!2!}+\frac{n!}{(n-3)!2!}+\frac{n!}{(n-4)!4!}\\
&=\frac{n}{4!}\left(24+24(n-1)+12(n-1)+12(n-1)(n-2)+(n-1)(n-2)(n-3)\right)\\
&=\frac{n\left(n^3+6n^2+11n+6\right)}{24}\\
&=\frac{n(n+1)(n+2)(n+3)}{24}
\end{aligned}$$

……(答)

別解　$\left(1+x+x^2+x^3+x^4\right)^n$

$$=\underbrace{\left(1+x+x^2+x^3+x^4\right)\left(1+x+x^2+x^3+x^4\right)\cdots\left(1+x+x^2+x^3+x^4\right)}_{n}$$

の第 1 の ( ) から x^{a_1} を，第 2 の ( ) から x^{a_2} を，…，第 n の ( ) から x^{a_n} を取り出すとすると，$\left(1+x+x^2+x^3+x^4\right)^n$ を展開したときの x^4 の係数は，

$$a_1+a_2+\cdots+a_n=4,\ a_i\geq 0\ (1\leq i\leq n)$$

を満たす $a_1,a_2,\ldots,a_n$ の組 $(a_1,a_2,\ldots,a_n)$ の個数に等しい．よって，

$${}_n\mathrm{H}_4={}_{n+4-1}\mathrm{C}_4={}_{n+3}\mathrm{C}_4=\frac{(n+3)(n+2)(n+1)n}{4!}=\frac{n(n+1)(n+2)(n+3)}{24}$$

……(答)

問題 1.1.7 数列 $\{a_n\}$ を次のように定義する．

$$\begin{cases} a_1=1, \\ a_{n+1}=\dfrac{1}{2}a_n+\dfrac{1}{n+1}\ (n=1,2,\ldots\ldots) \end{cases}$$

このとき，各自然数 n に対して不等式 $a_n \leqq \dfrac{4}{n}$ が成り立つことを証明せよ．

(1993 京都大・文・後期)

数学帰納法で証明することになるが，形式的な（解答の書き方の）理解だけでは証明できないことに注意したい．第 2 段の部分で，$k=1$ のときはうまくいかない．第 1 段で，$n=2$ を含めた $n=1,2$ のときをすませておく必要がある．（第 2 段の部分で $k \geq 2$ でないと証明できないと気づいた段階で，第 1 段の部分の解答を修正すればよい．）

解答 n に関する数学的帰納法で

$$a_n \leq \frac{4}{n} \qquad \cdots\cdots ①$$

が成り立つことを証明する．

(I) $n=1$ のとき，$a_1 = 1 \leq \dfrac{4}{1}$ となり，①は成り立つ．

$n=2$ のとき，$a_2 = \dfrac{1}{2}a_1 + \dfrac{1}{2} = 1 \leq \dfrac{4}{2}$ となり，①は成り立つ．

(II) $n=k\ (\geq 2)$ のとき，①が成り立つと仮定すると，$a_k \leq \dfrac{4}{k}$.

漸化式から

$$a_{k+1} = \frac{1}{2}a_k + \frac{1}{k+1} \leq \frac{1}{2}\cdot\frac{4}{k} + \frac{1}{k+1} = \frac{2}{k} + \frac{1}{k+1}$$

すなわち

$$a_{k+1} = \frac{1}{2}a_k + \frac{1}{k+1} \leq \frac{2}{k} + \frac{1}{k+1}. \qquad \cdots\cdots ②$$

$k \geq 2$ だから

$$\frac{4}{k+1} - \left(\frac{2}{k} + \frac{1}{k+1}\right) = \frac{3}{k+1} - \frac{2}{k} = \frac{k-2}{k(k+1)} \geq 0.$$

よって

$$\frac{2}{k} + \frac{1}{k+1} \leq \frac{4}{k+1}. \qquad \cdots\cdots ③$$

②，③より $a_{k+1} \leq \dfrac{4}{k+1}$ となり，$n=k+1$ のときも①は成り立つ．

(III) (I)，(II) より，すべての正の整数 n に対して，$a_n \leq \dfrac{4}{n}$ が成り立つ． □

問題 1.1.8 (2013 PUMaC)

数列 $\{a_n\}, \{b_n\}$ を次のように定義する．

$$a_1 = 2013,\ a_{n+1} = 2013^{a_n}\ (n = 1, 2, \dots)$$

$$b_1 = 1,\ b_{n+1} = 2013^{2012b_n}\ (n = 1, 2, \dots)$$

このとき，すべての正の整数 n に対して不等式 $a_n > b_n$ が成り立つことを証明せよ．

数学帰納法で証明することになるが，$a_n > b_n$ のままでは証明できないことに注意したい．

解答　n に関する数学的帰納法で

$$a_n \geq 2013b_n \qquad \cdots\cdots ①$$

が成り立つことを証明する．

(I) $n=1$ のとき，$a_1 = 2013 = 2013b_1$ となり，①は成り立つ．

(II) $n=k$ のとき①が成り立つと仮定すると，$a_k \geq 2013b_k$.

$$a_{k+1} = 2013^{a_k} \geq 2013^{2013b_k} = 2013^{b_k}2013^{2012b_k} \geq 2013^{1}2013^{2012b_k} = 2013b_{k+1}$$

となり，$n=k+1$ のときも①は成り立つ．

(III) (I)，(II) より，すべての正の整数 n に対して，$a_n \geq 2013b_n$ が成り立つ．

$a_n \geq 2013b_n$ が成り立つから，$a_n \geq 2013b_n > b_n$ すなわち $a_n > b_n$ は成り立つ．　□

注　帰納法で証明すべき命題をを工夫する例として問題 4.7.6 も参照．

問題 1.2.1

(1) a,b,c,d が有理数のとき，$\sqrt{3} = \dfrac{a+b\sqrt{2}}{c+d\sqrt{2}}$ となることがあるか．

(2) a,b,c,d が有理数で $a+\sqrt{2}\,b+\sqrt{3}\,c+\sqrt{6}\,d=0$ となるのは，$a=b=c=d=0$ のときに限ることを証明せよ．((2) のみ 1969 一橋大)

解答　$\sqrt{3} = \dfrac{a+b\sqrt{2}}{c+d\sqrt{2}}$ となることがあると仮定する．

右辺の分母を有理化すると

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{\left(a+b\sqrt{2}\right)\left(c-d\sqrt{2}\right)}{\left(c+d\sqrt{2}\right)\left(c-d\sqrt{2}\right)} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2}$$

となるから，

$$e = \frac{ac-2bd}{c^2-2d^2},\ f = \frac{bc-ad}{c^2-2d^2}$$

とおくと，e,f は有理数で $\dfrac{a+b\sqrt{2}}{c+d\sqrt{2}} = e+f\sqrt{2}$ となるから

$$\sqrt{3} = e+f\sqrt{2} \qquad \cdots\cdots (*)$$

が成り立つ．両辺を平方した $3 = e^2+2f^2+2ef\sqrt{2}$ から

$$2ef\sqrt{2} = 3-e^2-2f^2.$$

$ef \neq 0$ だとすると，$\sqrt{2} = \dfrac{3 - e^2 - 2f^2}{2ef}$ は有理数となり，$\sqrt{2}$ が無理数であることに矛盾する．

したがって，$ef = 0$ でなければならない．

$e = 0$ のとき，$(*)$ より $\sqrt{3} = f\sqrt{2}$．両辺にをかけると，$\sqrt{6} = 2f$ は有理数となり，$\sqrt{6}$ が無理数であることに矛盾する．

$f = 0$ のとき，$(*)$ より $\sqrt{3} = e$ は有理数となり，$\sqrt{3}$ が無理数であることに矛盾する．

以上のことから，$\sqrt{3} = \dfrac{a + b\sqrt{2}}{c + d\sqrt{2}}$ となることはない．

(2) $a + \sqrt{2}\,b + \sqrt{3}\,c + \sqrt{6}\,d = 0$ を

$$a + b\sqrt{2} + \left(c + d\sqrt{2}\right)\sqrt{3} = 0 \qquad \cdots\cdots (**)$$

と変形する．

p, q が有理数のとき

$$p + q\sqrt{2} = 0 \Longleftrightarrow p = q = 0$$

が成り立つ．

$c \neq 0$ または $d \neq 0$ と仮定すると，$c + d\sqrt{2} \neq 0$ だから，$(**)$ の両辺を $c + d\sqrt{2}$ で割ることにより

$$\sqrt{3} = -\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(-a) + (-b)\sqrt{2}}{c + d\sqrt{2}}.$$

(1) より，$\sqrt{3}$ がこのように表されることはないから，矛盾が生じた．

したがって，$c = 0$ かつ $d = 0$ でなければならない．

このとき，$a + \sqrt{2}\,b + \sqrt{3}\,c + \sqrt{6}\,d = 0$ から，$a + b\sqrt{2} = 0$.

よって，$a = b = 0$ が言えて，結局 $a = b = c = d = 0$ が得られた．

$a = b = c = d = 0$ のとき，明らかに，$a + \sqrt{2}\,b + \sqrt{3}\,c + \sqrt{6}\,d = 0$ は成り立つ． □

- $a + \sqrt{2}\,b + \sqrt{3}\,c + \sqrt{6}\,d = 0$ を $(**)$ のように変形しないのであれば，次のように解くこともできる．

  $$a + d\sqrt{6} = -\left(b\sqrt{2} + c\sqrt{3}\right)$$

  と変形し，両辺を平方すると

  $$a^2 + 6d^2 + 2ad\sqrt{6} = 2b^2 + 3c^2 + 2bc\sqrt{6}.$$

  a, b, c, d は有理数で，$\sqrt{6}$ は無理数だから

  $$a^2 + 6d^2 = 2b^2 + 3c^2 \qquad \cdots\cdots ①$$
  $$ad = bc \qquad \cdots\cdots ②$$
  $$\cdots\cdots$$

問題 1.2.2 自然数 n に対して，関数 $f_n(x) = x^n e^{1-x}$ と，その定積分 $a_n = \displaystyle\int_0^1 f_n(x)\,dx$ を考える．ただし，e は自然対数の底である．次の問いに答えよ．

(1) 区間 $0 \leqq x \leqq 1$ 上で $0 \leqq f_n(x) \leqq 1$ であることを示し，さらに $0 < a_n < 1$ が成り立つことを示せ．

(2) a_1 を求めよ．$n > 1$ に対して a_n と a_{n-1} の間の漸化式を求めよ．

(3) 自然数 n に対して，等式 $\dfrac{a_n}{n!} = e - \left(1 + \dfrac{1}{1!} + \dfrac{1}{2!} + \cdots + \dfrac{1}{n!}\right)$ が成り立つことを証明せよ．

(4) いかなる自然数 n に対しても，$n!e$ は整数とならないことを示せ．

(1997 大阪大・理・工・基礎工・後期)

- (1) の結果を使うと，$0 < \dfrac{a_n}{n!} < \dfrac{1}{n!}$ だから，$\lim\limits_{n\to\infty} \dfrac{a_n}{n!} = 0.$

  次に，(3) の結果において $n \to \infty$ とすると

  $$\lim_{n\to\infty} \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}\right) = \lim_{n\to\infty} \left(e - \frac{a_n}{n!}\right) = e$$

  だから

  $$\boldsymbol{e = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \cdots}$$

  が得られる．

- (4) から，**e は無理数である**ことがわかる．

  e が有理数だと仮定して $e = \dfrac{a}{b}$, $a, b \in \mathbb{N}$ とおくと，$b!e$ は整数となるが，(4) の結果に矛盾する．

解答　$f_n(x) = x^n e^{1-x}$, $a_n = \displaystyle\int_0^1 f_n(x)\,dx.$

(1) $0 < x < 1$ では $f_n{}'(x) = x^{n-1}e^{1-x}(n-x) > 0$ だから，$f_n(x)$ は $[0,1]$ で増加関数である．

$0 \leqq x \leqq 1$ のとき $f_n(0) \leqq f_n(x) \leqq f_n(1)$ だから，$0 \leqq f_n(x) \leqq 1$ である．

また，$0 < x < 1$ では $0 < f_n(x) < 1$ であるから，

$$0 = \int_0^1 0\,dx < \int_0^1 f_n(x)\,dx < \int_0^1 1\,dx = 1.$$

よって，$0 < a_n < 1$ が成り立つ．

(2)

$$a_1 = \int_0^1 xe^{1-x}\,dx = \int_0^1 x\left(-e^{1-x}\right)'\,dx$$

$$
\begin{aligned}
&= \left[x\left(-e^{1-x}\right)\right]_0^1 + \int_0^1 e^{1-x}\,dx \\
&= -1 + \left[-e^{1-x}\right]_0^1 \\
&= e - 2
\end{aligned}
$$

から

$$a_1 = e - 2 \qquad \cdots\cdots \text{(答)}$$

$$
\begin{aligned}
a_n &= \int_0^1 x^n e^{1-x}\,dx = \int_0^1 x^n \left(-e^{1-x}\right)'\,dx \\
&= \left[x^n\left(-e^{1-x}\right)\right]_0^1 + n\int_0^1 x^{n-1}e^{1-x}\,dx \\
&= -1 + na_{n-1}
\end{aligned}
$$

から

$$a_n = na_{n-1} - 1 \qquad \cdots\cdots \text{(答)}$$

(3) (2) より $a_n = na_{n-1} - 1$ $\cdots\cdots$①

①から得られる等式 $a_k = ka_{k-1} - 1$ の両辺を $k!$ で割ると

$$\frac{a_k}{k!} - \frac{a_{k-1}}{k-1!} = -\frac{1}{k!}.$$

ゆえに

$$\frac{a_{k+1}}{(k+1)!} - \frac{a_k}{k!} = -\frac{1}{(k+1)!}.$$

$n \geqq 2$ のとき

$$
\begin{aligned}
\frac{a_n}{n!} &= \frac{a_1}{1!} + \sum_{k=1}^{n-1}\left(\frac{a_{k+1}}{(k+1)!} - \frac{a_k}{k!}\right) \\
&= e - 2 - \sum_{k=1}^{n-1}\frac{1}{(k+1)!} \\
&= e - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots\cdots + \frac{1}{n!}\right).
\end{aligned}
$$

この式は $n = 1$ のときも成り立つ.

(4) (3) の結果の等式に $n!$ をかけると

$$n!e = a_n + \left(n! + \frac{n!}{1!} + \frac{n!}{2!} + \cdots\cdots + \frac{n!}{n!}\right).$$

$1 \leqq k \leqq n-1$ のとき, $\dfrac{n!}{k!} = n(n-1)\cdots(k+1)$ は整数となる.

また $k = n$ のときも, $\dfrac{n!}{k!} = \dfrac{n!}{n!} = 1$ は整数となる.

よって，右辺の（　）内の各項は整数である．

また，(1) より $0 < a_n < 1$ であるから，$n!e$ は整数にならない． □

- (3) は n に関する数学的帰納法で証明してもよい．

  (2) より $a_n = na_{n-1} - 1$ ……①

$$\frac{a_n}{n!} = e - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}\right) \quad \cdots\cdots(*)$$

とおく．

(I) $n = 1$ のとき，(2) より $a_1 = e - 2$ だから，$(*)$ は成り立つ．

(II) $n = k$ のとき $(*)$ が成り立つと仮定すると

$$\frac{a_k}{k!} = e - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{k!}\right).$$

①で $n = k + 1$ とおくと，$a_{k+1} = (k+1)a_k - 1$.

これを使うと

$$\begin{aligned}
\frac{a_{k+1}}{(k+1)!} &= \frac{(k+1)a_k - 1}{(k+1)!} = \frac{(k+1)a_k}{(k+1)!} - \frac{1}{(k+1)!} \\
&= \frac{a_k}{k!} - \frac{1}{(k+1)!} \\
&= e - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{k!}\right) - \frac{1}{(k+1)!} \\
&= e - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{k!} + \frac{1}{(k+1)!}\right)
\end{aligned}$$

となり，$n = k + 1$ のときも成り立つ．

(III) (I)，(II) よりすべての正の整数 n について $(*)$ は成り立つ． □

問題 1.2.3

(1) $\log_5 3$ は無理数であることを示せ.
(2) $\log_{10} r$ が有理数となる有理数 r は $r = 10^q$ $(q = 0, \pm 1, \pm 2, \dots)$ に限ることを示せ.

(3) 任意の正の整数 n に対して,

$$\log_{10}\left(1 + 3 + 3^2 + \cdots + 3^n\right)$$

は無理数であることを示せ.

(1998 一橋大・商・経済・社会・後期)

(1) $\log_5 3$ が有理数だと仮定すると，$\log_5 3 = \dfrac{m}{n}$ $(m, n \in \mathbb{N})$ とかける．これから $3 = 5^{\frac{m}{n}}$ と書き直して，等式の両辺を n 乗すると，$3^n = 5^m$．この式を $3^n = 5 \cdot 5^{m-1}$ と変形すると，3^n は 5 の倍数でなければならない．これは不可能である．
したがって，$\log_5 3$ が有理数ではない．ゆえに，$\log_5 3$ は無理数である．

(2) (i) $\log_{10} r > 0$ の場合
$\log_{10} r = \dfrac{m}{n}$, $(m, n \in \mathbb{N},\ \gcd(m, n) = 1)$ とかける．これを $r = 10^{\frac{m}{n}}$ と書き直して，両辺を乗すると，

$$r^n = 10^m. \qquad \cdots\cdots ①$$

$r(> 1)$ は正の有理数だから，$r = \dfrac{p}{q}$, $(p, q \in \mathbb{N},\ \gcd(p, q) = 1)$ と書ける．これを①に代入した $\left(\dfrac{p}{q}\right)^n = 10^m$ を

$$\frac{p^n}{q} = q^{n-1} 10^m \qquad \cdots\cdots ②$$

と変形する．②の右辺は整数だから，左辺の $\dfrac{p^n}{q}$ も整数となる．p と q は互いに素だから，$q = 1$ となる．
このとき，②は

$$p^n = 10^m = 2^m 5^m \qquad \cdots\cdots ③$$

となる．明らかに $p \neq 1$ だから，p を素因数分解して考えると，③より，$p = 2^\alpha 5^\beta$, $(\alpha, \beta \in \mathbb{N})$ と書けて，$p^n = 2^{n\alpha} 5^{n\beta} = 2^m 5^m$ より

$$n\alpha = m,\ n\beta = m.$$

これから $\alpha = \beta = \dfrac{m}{n}$ が整数で，m と n は互いに素だから，$n = 1$ となる．

よって，③より，$p = 10^m$ すなわち，$r = \dfrac{p}{q} = p = 10^m$ $(m = 1, 2, \dots)$ となる．

(ii) $\log_{10} r < 0$ の場合

$\log_{10} \dfrac{1}{r} = -\log_{10} r > 0$ が有理数になるから，(i) より，

$\dfrac{1}{r} = 10^m$ $(m = 1, 2, \dots)$ すなわち，$r = 10^{-m}$ $(m = 1, 2, \dots)$

となる．

(iii) $\log_{10} r = 0$ の場合

$r = 1 = 10^0$.

(i)，(ii)，(iii) より，$\log_{10} r$ が有理数となる有理数 r は $r = 10^q$ $(q = 0, \pm 1, \pm 2, \dots)$ に限る．

(3) $\log_{10}\left(1 + 3 + 3^2 + \cdots + 3^n\right)$ が有理数だとする．

n が正の整数のとき，$1+3+3^2+\cdots+3^n > 1$ だから，$\log_{10}\left(1 + 3 + 3^2 + \cdots + 3^n\right) > 0$ となるので，(2) より

$$1 + 3 + 3^2 + \cdots + 3^n = 10^m \qquad \cdots\cdots ④$$

を満たす正の整数 m が存在する．④より，$\dfrac{3^{n+1} - 1}{3 - 1} = 10^m$ すなわち

$$3^{n+1} = 2 \cdot 10^m + 1. \qquad \cdots\cdots ⑤$$

mod 9 で考えると，

$2 \cdot 10^m + 1 \equiv 2 \cdot 1^m + 1 \equiv 3 \pmod 9$.

$n \geq 1$ より，$3^{n+1} \equiv 0 \pmod 9$.

⑤を用いると

$$0 \equiv 3^{n+1} \equiv 2 \cdot 10^m + 1 \equiv 3 \pmod 9$$

となり，矛盾が生じる．

よって，任意の正の整数 n に対して，

$$\log_{10}\left(1 + 3 + 3^2 + \cdots + 3^n\right)$$

は無理数である．　□

注 (3) の⑤以降は次のように解くこともできる．

(3) の⑤を $3^{n+1} - 3 = 2\left(10^m - 1\right)$ すなわち

$$3\left(3^n - 1\right) = 2\left(10^m - 1\right) \qquad \cdots\cdots ⑥$$

と変形すると，⑥の左辺 $3\left(3^n - 1\right)$ は 3 の倍数であるが，9 の倍数ではない．

$10^m-1=(10-1)\left(10^{m-1}+10^{m-2}+\cdots+10+1\right)=9\left(10^{m-1}+10^{m-2}+\cdots+10+1\right)$ は 9 の倍数だから，⑥の右辺は，9 の倍数となり矛盾が生じる．

蛇足 ⑥のように変形するのだったら，等比数列の和の公式など使わず，④を

$$3+3^2+\cdots+3^n=10^m-1, \qquad 3\left(1+3+\cdots+3^{n-1}\right)=10^m-1$$

と変形したほうがわかりやすかったかもしれない．

問題 1.2.4 次の問いに答えよ．

(1) 正の整数 n に対して，関数 $f(x)=\dfrac{x^n(1-x)^n}{n!}$ を考える．

(a) $f(x)$ は

$$f(x)=\frac{1}{n!}\left(a_nx^n+a_{n+1}x^{n+1}+\cdots+a_{2n}x^{2n}\right) \quad (a_n,a_{n+1},\ldots,a_{2n}\in\mathbb{Z}) \qquad \cdots\cdots ①$$

という形の多項式であることを示せ．

(b) $0<x<1$ で $0<f(x)<\dfrac{1}{n!}$ であることを示し，さらに

$$0<\int_0^1 f(x)\sin(\pi x)\,dx<\frac{1}{n!}$$

が成り立つことを示せ．

(c) 非負の整数 m に対して，$\dfrac{d^mf(0)}{dx^m}$, $\dfrac{d^mf(1)}{dx^m}$ はともに整数であることを示せ．

(2) n,q を正の整数として，

$$F(x)=q^n\left(\pi^{2n}f(x)-\pi^{2n-2}f^{(2)}(x)+\pi^{2n-4}f^{(4)}(x)-\cdots+(-1)^nf^{(2n)}(x)\right)$$

とおく．ただし，$f(x)=\dfrac{x^n(1-x)^n}{n!}$ とする．

(d) $\dfrac{d}{dx}\left(F'(x)\sin(\pi x)-\pi F(x)\cos(\pi x)\right)$ を考えることにより，

$$F''(x)+\pi^2F(x)=q^n\pi^{2n+2}f(x)$$

が成り立つことを示せ．

(e) $q^n\pi^{2n+1}\displaystyle\int_0^1 f(x)\sin(\pi x)\,dx=F(0)+F(1)$ が成り立つことを示せ．

(f) π^2 は無理数であることを証明せよ．ただし，必要があれば，t が実数のとき $\displaystyle\lim_{n\to\infty}\frac{t^n}{n!}=0$ であることを用いてもよい．

(g) π は無理数であることを証明せよ．

解答

(1) (a) 二項定理より

$$(1-x)^n = 1 - \binom{n}{1}x + \binom{n}{2}x^2 - \cdots + \binom{n}{n-1}x^{n-1} + (-1)^n x^n$$

となるから，

$$\begin{aligned} f(x) &= \frac{x^n(1-x)^n}{n!} \\ &= \frac{1}{n!}\left(x^n - \binom{n}{1}x^{n+1} + \binom{n}{2}x^{n+2} - \cdots + \binom{n}{n-1}x^{2n-1} + (-1)^n x^{2n}\right). \end{aligned}$$

よって，$f(x)$ は

$$f(x) = \frac{1}{n!}\left(a_n x^n + a_{n+1}x^{n+1} + \cdots + a_{2n}x^{2n}\right) \quad (a_n, a_{n+1}, \ldots, a_{2n} \in \mathbb{Z})$$

という形の多項式である．

(b) $0 < x < 1$ だから，$0 < x(1-x) < 1$ が成り立つから，$0 < x^n(1-x)^n < 1$．

ゆえに $0 < x < 1$ で $0 < f(x) < \dfrac{1}{n!}$．

$0 < x < 1$ で $0 < f(x) < \dfrac{1}{n!}$, $0 < \sin(\pi x) < 1$ より，$0 < f(x)\sin(\pi x) < 1$．

$f(x)\sin(\pi x)$ は $[0,1]$ において，連続関数だから

$$\int_0^1 0\,dx < \int_0^1 f(x)\sin(\pi x)\,dx < \frac{1}{n!}\int_0^1 1\,dx$$

すなわち

$$0 < \int_0^1 f(x)\sin(\pi x)\,dx < \frac{1}{n!}. \qquad \cdots\cdots ②$$

(c) $f(1-x) = f(x)$ が成り立つ．等式の両辺を x で $m\,(\geq 0)$ 回微分すると

$$(-1)^m \frac{d^m f(1-x)}{dx^m} = \frac{d^m f(x)}{dx^m}.$$

この式で，$x = 1$ とおくと

$$(-1)^m \frac{d^m f(0)}{dx^m} = \frac{d^m f(1)}{dx^m}$$

①から，$m < n$ または $2n < m$ のときは，$\dfrac{d^m f(0)}{dx^m} = 0$．

$n \leq m \leq 2n$ のときは

$$f^{(m)}(x) = \frac{1}{n!}\sum_{k=m}^{2n} a_k k(k-1)\cdots(k-m+1)x^{k-m}$$

だから，

$$f^m(0) = \frac{1}{n!}a_m m! = m(m-1)\cdots(m-n+1)a_m \in \mathbb{Z}$$

よって，$\dfrac{d^m f(0)}{dx^m} \in \mathbb{Z}$ が言える．

$(-1)^m \dfrac{d^m f(0)}{dx^m} = \dfrac{d^m f(1)}{dx^m}$ から $\dfrac{d^m f(1)}{dx^m} \in \mathbb{Z}$ も言える．

(2) (d) $\dfrac{d}{dx}\left(F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)\right)$

$= F''(x)\sin(\pi x) + F'(x)\cdot\pi\cos(\pi x) - \pi F'(x)\cos(\pi x) - \pi F(x)\cdot\pi\left(-\sin(\pi x)\right)$
$= \left(F''(x) + \pi^2 F(x)\right)\sin(\pi x)$

より

$$\frac{d}{dx}\left(F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)\right) = \left(F''(x) + \pi^2 F(x)\right)\sin(\pi x). \quad \cdots\cdots ③$$

ここで

$$F''(x) = q^n\left(\pi^{2n} f^{(2)}(x) - \pi^{2n-2} f^{(4)}(x) + \pi^{2n-4} f^{(6)}(x) - \cdots + (-1)^n f^{(2n+2)}(x)\right),$$

$$\pi^2 F(x) = q^n\left(\pi^{2n+2} f(x) - \pi^{2n} f^{(2)}(x) + \pi^{2n-2} f^{(4)}(x) - \cdots + (-1)^n \pi^2 f^{(2n)}(x)\right)$$

これらの等式の辺々を加えると

$$F''(x) + \pi^2 F(x) = q^n\left(\pi^{2n+2} f(x) + (-1)^n f^{(2n+2)}(x)\right)$$

となる．①より，$f^{(2n+2)}(x) = 0$ だから，この等式は

$$F''(x) + \pi^2 F(x) = q^n \pi^{2n+2} f(x) \qquad \cdots\cdots ④$$

となる．

(e) ③と④から

$$\frac{d}{dx}\left(F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)\right) = q^n \pi^{2n+2} f(x)\sin(\pi x)$$

となるから，両辺の式を 0 から 1 まで積分すると

$$\Big[F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)\Big]_0^1 = q^n \pi^{2n+2}\int_0^1 f(x)\sin(\pi x)\,dx$$

$$\pi\left(F(0) + F(1)\right) = q^n \pi^{2n+2}\int_0^1 f(x)\sin(\pi x)\,dx.$$

ゆえに

$$q^n\pi^{2n+1}\int_0^1 f(x)\sin(\pi x)\,dx = F(0)+F(1) \qquad \cdots\cdots ⑤$$

が成り立つ．

(f) π^2 が有理数だと仮定すると，$\pi^2 = \dfrac{p}{q}$ $(p, q \in \mathbb{N})$ とおける．

$$\begin{aligned}
F(x) &= q^n\left(\pi^{2n}f(x) - \pi^{2n-2}f^{(2)}(x) + \pi^{2n-4}f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x)\right) \\
&= q^n\left(\left(\frac{p}{q}\right)^n f(x) - \left(\frac{p}{q}\right)^{n-1} f^{(2)}(x)\right. \\
&\qquad\qquad \left. + \left(\frac{p}{q}\right)^{n-2} f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x)\right) \\
&= p^n f(x) - p^{n-1}qf^{(2)}(x) + p^{n-2}q^2 f^{(4)}(x) - \cdots + (-1)^n q^n f^{(2n)}
\end{aligned}$$

と変形し，(c) を使うと，$F(0), F(1)$ は整数であることがわかる．

$I_n = q^n\pi^{2n+1}\displaystyle\int_0^1 f(x)\sin(\pi x)\,dx$ とおくと，$F(0), F(1)$ は整数だから，⑤より I_n は整数となる．②より

$$0 < I_n = \pi^{2n+1}q^n\int_0^1 f(x)\sin(\pi x)\,dx < \frac{\pi^{2n+1}q^n}{n!}.$$

$\displaystyle\lim_{n\to\infty}\frac{\pi^{2n+1}q^n}{n!} = 0$ だから，はさみうちの原理より

$$\lim_{n\to\infty} I_n = 0$$

となるが，I_n は整数なのでこれは不可能である．

したがって，矛盾が生じたので，π^2 は無理数である．

(g) π が有理数だと仮定すると，$\pi = \dfrac{a}{b}$ $(a, b \in \mathbb{N})$ とおける．

このとき，$\pi^2 = \dfrac{a^2}{b^2} \in \mathbb{Q}$ となり，π^2 が無理数であることに矛盾する．

したがって，π は無理数である．　□

問題 1.2.5　π を円周率とする．次の積分について考える．

$$I_0=\pi\int_0^1 \sin\pi t\,dt,\ I_n=\frac{\pi^{n+1}}{n!}\int_0^1 t^n(1-t)^n\sin\pi t\,dt\ (n=1,2,\dots)$$

(1) n が自然数であるとき，不等式

$$1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}<e^x\ (x>0)$$

が成立することを数学的帰納法により示せ．これを用いて，不等式

$$I_0+uI_1+u^2I_2+\cdots+u^nI_n<\pi e^{\pi u}\ (u>0)$$

が成立することを示せ．

(2) I_0, I_1 の値を求めよ．また，漸化式

$$I_{n+1}=\frac{4n+2}{\pi}I_n-I_{n-1}$$

が成立することを示せ．

(3) π が無理数であることを背理法により証明しよう．π が無理数でないとし，正の整数 p,q によって $\pi=\dfrac{p}{q}$ として表されると仮定する．$A_0=I_0, A_n=p^nI_n$ とおくとき，$A_0, A_1, A_2, \dots$ は正の整数になることを示せ．さらに，これから矛盾を導け．　(2003 大阪大・理・工・基礎工・後期)

解答　$f_n(x)=e^x-\left(1+\dfrac{x}{1!}+\dfrac{x^2}{2!}+\cdots+\dfrac{x^n}{n!}\right)$ とおく．

(1) n が正の整数であるとき，不等式

$$1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}<e^x\ (x>0)\qquad\cdots\cdots(*)$$

が成立することを n に関する数学的帰納法により示す．

(I) $n=1$ のとき，$f_1(x)=e^x-(1+x),\ f_1'(x)=e^x-1$.

$x>0$ のとき，$f_1'(x)=e^x-1>0$ であるから，$x\geq 0$ で $f_1(x)$ は増加関数である．

よって，$x>0$ ならば，$f_1(x)>f_1(0)=0$ となり，$(*)$ は成り立つ．

(II) $n=k\,(\geq 1)$ のとき，$(*)$ が成り立つと仮定すると，$x>0$ のとき $f_k(x)>0$.

$f_{k+1}(x)=e^x-\left(1+\dfrac{x}{1!}+\dfrac{x^2}{2!}+\cdots+\dfrac{x^{k+1}}{(k+1)!}\right)$ で

$f_{k+1}'(x)=e^x-\left(1+\dfrac{x}{1!}+\dfrac{x^2}{2!}+\cdots+\dfrac{x^k}{k!}\right)=f_k(x)$ となる．

帰納法の仮定より，$x>0$ のとき，$f'_{k+1}(x)=f_k(x)>0$ であるから，$x\geq 0$ で $f_{k+1}(x)$ は増加関数である．

よって，$x>0$ ならば，$f_{k+1}(x)>f_{k+1}(0)=0$ となり，$(*)$ は成り立つ．

$n=k+1$ のときも $(*)$ は成り立つ．

(III) (I)，(II) より，すべての正の整数 n に対して $(*)$ は成り立つ．

$$\begin{aligned} I_0+uI_1+u^2I_2+\cdots+u^nI_n &= \sum_{k=0}^{n} u^kI_k \\ &= \sum_{k=0}^{n} u^k\cdot\frac{\pi^{k+1}}{k!}\int_0^1 t^k(1-t)^k\sin\pi t\,dt \\ &= \sum_{k=0}^{n} \pi\cdot\frac{(\pi u)^k}{k!}\int_0^1 t^k(1-t)^k\sin\pi t\,dt. \end{aligned}$$

ここで，$\displaystyle\sum_{k=0}^{n}\frac{x^k}{k!}<e^x$ において，$x=\pi u$ とおくと，$\displaystyle\sum_{k=0}^{n}\frac{(\pi u)^k}{k!}<e^{\pi u}$.

両辺に π をかけて

$$\sum_{k=0}^{n}\pi\cdot\frac{(\pi u)^k}{k!}<\pi e^{\pi u}.$$

したがって，あとは

$$\int_0^1 t^k(1-t)^k\sin\pi t\,dt<1$$

を示せばよい．$0<t<1$ では $0<t^k(1-t)^k\sin\pi t<1$ が成り立つので，この両辺を 0 から 1 まで積分すると，$\displaystyle\int_0^1 0\,dt<\int_0^1 t^k(1-t)^k\sin\pi t\,dt<\int_0^1 1\,dt$ すなわち $\displaystyle 0<\int_0^1 t^k(1-t)^k\sin\pi t\,dt<1$ が得られる．

よって，

$$\begin{aligned} I_0+uI_1+u^2I_2+\cdots+u^nI_n &= \sum_{k=0}^{n}\pi\cdot\frac{(\pi u)^k}{k!}\int_0^1 t^k(1-t)^k\sin\pi t\,dt \\ &< \sum_{k=0}^{n}\pi\cdot\frac{(\pi u)^k}{k!} \\ &< \pi e^{\pi u} \end{aligned}$$

から，$u>0$ のとき

$$I_0+uI_1+u^2I_2+\cdots+u^nI_n<\pi e^{\pi u} \qquad \cdots\cdots ①$$

が成り立つ．

(2) $I_0 = \pi\displaystyle\int_0^1 \sin\pi t\,dt = \big[-\cos\pi t\big]_0^1 = 2.$

$$
\begin{aligned}
I_1 &= \frac{\pi^2}{1!}\int_0^1 t(1-t)\sin\pi t\,dt = \pi\int_0^1 t(1-t)(-\cos\pi t)'\,dt \\
&= \pi\big[-t(1-t)\cos\pi t\big]_0^1 - \pi\int_0^1 (2t-1)\cos\pi t\,dt \\
&= 0 - \big[(2t-1)\sin\pi t\big]_0^1 + \int_0^1 2\sin\pi t\,dt \\
&= 2\left[-\frac{\cos\pi t}{\pi}\right]_0^1 \\
&= \frac{4}{\pi}
\end{aligned}
$$

$$
\begin{aligned}
I_{n+1} &= \frac{\pi^{n+2}}{(n+1)!}\int_0^1 t^{n+1}(1-t)^{n+1}\sin\pi t\,dt = \frac{\pi^{n+1}}{(n+1)!}\int_0^1 t^{n+1}(1-t)^{n+1}(-\cos\pi t)'\,dt \\
&= \frac{\pi^{n+1}}{(n+1)!}\big[-t^{n+1}(1-t)^{n+1}\cos\pi t\big]_0^1 \\
&\quad + \frac{\pi^{n+1}}{n!}\int_0^1 \big\{t^n(1-t)^{n+1} - t^{n+1}(1-t)^n\big\}\cos\pi t\,dt \\
&= 0 + \frac{\pi^n}{n!}\big[\big\{t^n(1-t)^{n+1} - t^{n+1}(1-t)^n\big\}\sin\pi t\big]_0^1 \\
&\quad - \frac{\pi^n}{n!}\int_0^1 \big\{nt^{n-1}(1-t)^{n+1} - 2(n+1)t^n(1-t)^n + nt^{n+1}(1-t)^{n-1}\big\}\sin\pi t\,dt \\
&= 2(n+1)\cdot\frac{\pi^n}{n!}\int_0^1 t^n(1-t)^n\sin\pi t\,dt \\
&\quad - \frac{\pi^n}{n!}\int_0^1 nt^{n-1}(1-t)^{n-1}\{1-2t(1-t)\}\sin\pi t\,dt \\
&= \frac{2(n+1)}{\pi}\cdot\frac{\pi^{n+1}}{n!}\int_0^1 t^n(1-t)^n\sin\pi t\,dt \\
&\quad - \frac{\pi^n}{(n-1)!}\int_0^1 t^{n-1}(1-t)^{n-1}\sin\pi t\,dt + \frac{2n}{\pi}\cdot\frac{\pi^{n+1}}{n!}\int_0^1 t^n(1-t)^n\sin\pi t\,dt \\
&= \frac{2(n+1)}{\pi}I_n - I_{n-1} + \frac{2n}{\pi}I_n \\
&= \frac{4n+2}{\pi}I_n - I_{n-1}.
\end{aligned}
$$

よって，$I_{n+1} = \dfrac{4n+2}{\pi}I_n - I_{n-1}$ が成り立つ．

(3) π が無理数でないとし，正の整数 p, q によって $\pi = \dfrac{p}{q}$ として表されると仮定する．

(2) の漸化式より

$$A_{n+1} = p^{n+1}I_{n+1} = p^{n+1}\left(\frac{4n+2}{\pi}I_n - I_{n-1}\right)$$

$$= p^{n+1}\left(\frac{q(4n+2)}{p}I_n - I_{n-1}\right)$$
$$= q(4n+2)p^n I_n - p^2 \cdot p^{n-1} I_{n-1}$$
$$= q(4n+2)A_n - p^2 A_{n-1}$$

から

$$A_{n+1} = q(4n+2)A_n - p^2 A_{n-1}. \qquad \cdots\cdots ②$$

$A_0 = I_0 = 2, A_1 = pI_1 = p \cdot \dfrac{4}{\pi} = p \cdot \dfrac{4q}{p} = 4q$ は整数で，A_n と A_{n-1} が整数だと仮定すると，②より A_{n+1} も整数となるから，数学的帰納法により $A_0, A_1, A_2, \ldots$ は整数になる．

$0 < \displaystyle\int_0^1 t^n(1-t)^n \sin \pi t \, dt < 1$ を (1) で示したから，$I_n > 0$ $(n \geq 1)$ は明らかに成り立つので，$A_n = p^n I_n > 0$ $(n \geq 1)$ となる．$A_0 = 2 > 0$ とあわせて，$A_n > 0$ $(n = 0, 1, 2, \ldots)$ が言える．

よって，$A_0, A_1, A_2, \ldots$ は正の整数になる．

①で $u = p$ とおくと，$I_0 + pI_1 + p^2 I_2 + \cdots + p^n I_n < \pi e^{\pi p}$ から

$$A_0 + A_1 + A_2 + \cdots + A_n < \pi e^{\pi p}. \qquad \cdots\cdots ③$$

A_n $(n = 0, 1, 2, \ldots)$ は正の整数だから，$n \to \infty$ とすると，③の左辺は ∞ に発散し，③の右辺は定数であるから矛盾が生じる．

よって，π は無理数である．　□

問題 2.1.1 (APMO 2002)

$\dfrac{a^2+b}{b^2-a}, \dfrac{b^2+a}{a^2-b}$ がともに整数となるような正の整数の組 (a, b) をすべて求めよ．

解答　$\dfrac{a^2+b}{b^2-a}$ が整数だから，$\left|\dfrac{a^2+b}{b^2-a}\right| \geq 1$ すなわち

$$a^2 + b \geq \left|b^2 - a\right| \geq b^2 - a$$

が成り立つ．$a^2 + b \geq b^2 - a$ から

$$(a+b)(a-b+1) \geq 0 \qquad a - b + 1 \geq 0 \qquad a \geq b - 1.$$

ゆえに，$a \geq b - 1$ が成り立つ．同様にして，$\dfrac{b^2+a}{a^2-b}$ が整数であることより，$b \geq a - 1$ すなわち，$a \leq b + 1$ が成り立つ．

2 つの不等式から，$b - 1 \leq a \leq b + 1$ となり，$a \in \left\{b-1, b, b+1\right\}$.

(i) $a=b-1$ の場合　$b\geq 2$.

$$\frac{a^2+b}{b^2-a}=\frac{(b-1)^2+b}{b^2-(b-1)}=\frac{b^2-b+1}{b^2-b+1}=1.$$

$$\frac{b^2+a}{a^2-b}=\frac{b^2+b-1}{(b-1)^2-b}=\frac{b^2+b-1}{b^2-3b+1}=1+\frac{4b-2}{b^2-3b+1}$$

が整数だから，$\dfrac{4b-2}{b^2-3b+1}$ が整数となる．

$b=2$ のとき $\dfrac{4b-2}{b^2-3b+1}=-6$ となる．

$b\geq 3$ のときは，$\dfrac{4b-2}{b^2-3b+1}>0$ だから，$\dfrac{4b-2}{b^2-3b+1}\geq 1$ から $b^2-7b+3\leq 0$ が成り立たなければならない．

$b\geq 7$ のとき，$b(b-7)+3\geq 3>0$ なので，$b^2-7b+3\leq 0$ は成り立たない．

ゆえに，$b\in\left\{3,\,4,\,5,\,6\right\}$ でなければならない．このうち，$\dfrac{4b-2}{b^2-3b+1}$ が整数となるのは $b=3$ のときだけである．よって，解は $(a,b)=(1,2),\,(2,3)$.

(ii) $a=b$ の場合

$$\frac{a^2+b}{b^2-a}=\frac{b^2+a}{a^2-b}=\frac{b^2+b}{b^2-b}=\frac{b+1}{b-1}=1+\frac{2}{b-1}$$

が整数だから，$b\geq 2$ で $b-1$ は 2 の約数となり，$b-1\in\left\{1,\,2\right\}$ すなわち $b\in\left\{2,\,3\right\}$ となる．よって，解は $(a,b)=(2,2),\,(3,3)$.

(iii) $a=b+1$ の場合　$b=a-1,\ a\geq 2$

$$\frac{b^2+a}{a^2-b}=\frac{(a-1)^2+a}{a^2-(a-1)}=\frac{a^2-a+1}{a^2-a+1}=1.$$

$$\frac{a^2+b}{b^2-a}=\frac{a^2+a-1}{(a-1)^2-a}=\frac{a^2+a-1}{a^2-3a+1}=1+\frac{4a-2}{a^2-3a+1}.$$

(i) の場合と同様にして，解は $(b,a)=(1,2),\,(2,3)$ すなわち $(a,b)=(2,1),\,(3,2)$.

(i)，(ii)，(iii) より解は，$(a,b)=(2,2),\,(3,3),\,(1,2),\,(2,3),\,(2,1),\,(3,2)$　□

問題 2.1.2 (IMO 1992)

a,b,c は $1<a<b<c$ を満たす整数とする．このとき，$(a-1)(b-1)(c-1)$ が $abc-1$ を割り切るような整数 a,b,c をすべて求めよ．

解答　$x=a-1, y=b-1, z=c-1$ とおくと，$1\leq x<y<z$ で

$$xyz\mid(x+1)(y+1)(z+1)-1=xyz+xy+yz+zx+x+y+z$$

から

$$xyz\mid xy+yz+zx+x+y+z$$

が言える.

$$k = \frac{xy+yz+zx+x+y+z}{xyz} \in \mathbb{N}$$

とおくと，$x \geq 1, y \geq 2, z \geq 3$ だから

$$\begin{aligned} k &= \frac{xy+yz+zx+x+y+z}{xyz} \\ &= \frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{xy}+\frac{1}{yz}+\frac{1}{zx} \\ &\leq 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 1} \\ &= \frac{17}{6} = 2\frac{5}{6} \end{aligned}$$

から，$k \leq 2$ で $k \in \left\{1,\, 2\right\}$.

$x \geq 3$ のとき $y \geq 4, z \geq 5$ だから

$$\begin{aligned} k &= \frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{xy}+\frac{1}{yz}+\frac{1}{zx} \\ &\leq \frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{3\cdot 4}+\frac{1}{4\cdot 5}+\frac{1}{5\cdot 3} \\ &= \frac{59}{60} < 1 \end{aligned}$$

となり，$k \in \left\{1,\, 2\right\}$ をみたさないから，$x < 3$ すなわち $x \in \left\{1,\, 2\right\}$ である.

(i) $x = 1$ の場合　$2 \leq y < z$

$$k = \frac{yz+2y+2z+1}{yz} = 1+\frac{2y+2z+1}{yz} > 1$$

より，$k = 2$ となるから，

$$\frac{2y+2z+1}{yz} = 1 \qquad yz-2y-2z = 1 \qquad (y-2)(z-2) = 5.$$

$0 \leq y-2 < z-2$ だから，$y-2 = 1, z-2 = 5$ すなわち $y = 3, z = 7$.

よって，$(x, y, z) = (1, 3, 7)$.

(ii) $x = 2$ の場合　$3 \leq y < z$

$$k = \frac{yz+3y+3z+2}{2yz}.$$

$k = 1$ のとき

$$\frac{yz+3y+3z+2}{2yz} = 1 \qquad yz-3y-3z = 2 \qquad (y-3)(z-3) = 11.$$

$0 \leq y-3 < z-3$ だから，$y-3 = 1, z-3 = 11$ すなわち $y = 4, z = 14$.

よって，$(x, y, z) = (2, 4, 14)$.

$k = 2$ のとき

$$\frac{yz+3y+3z+2}{2yz} = 2 \qquad 3yz-3y-3z = 2 \qquad 3(yz-y-z) = 2.$$

2 は 3 の倍数ではないから，$3(yz-y-z) = 2$ を満たす整数 y, z は存在しない.

(i)，(ii)，(iii) より解は，$(x,y,z)=(1,3,7),(2,4,14)$ すなわち
$(a,b,c)=(2,4,8),(3,5,15)$. □

別解　$k=\dfrac{abc-1}{(a-1)(b-1)(c-1)}\in\mathbb{N}$ とおくと

$$k=\frac{abc-1}{(a-1)(b-1)(c-1)}<\frac{abc}{(a-1)(b-1)(c-1)}=\frac{a}{a-1}\cdot\frac{b}{b-1}\cdot\frac{c}{c-1}.$$

$a\geq 2,b\geq 3,c\geq 3$ だから

$$\begin{aligned}\frac{a}{a-1}&=1+\frac{1}{a-1}\leq 1+\frac{1}{2-1}=2,\\ \frac{b}{b-1}&=1+\frac{1}{b-1}\leq 1+\frac{1}{3-1}=\frac{3}{2},\\ \frac{c}{c-1}&=1+\frac{1}{c-1}\leq 1+\frac{1}{4-1}=\frac{4}{3}\end{aligned}$$

が成り立つので，$k<2\cdot\dfrac{3}{2}\cdot\dfrac{4}{3}=4$. また

$$(a-1)(b-1)(c-1)<(a-1)bc=abc-bc<abc-1$$

より

$$k=\frac{abc-1}{(a-1)(b-1)(c-1)}>\frac{abc-1}{(a-1)bc}>\frac{abc-1}{abc-1}=1.$$

したがって，$k\in\left\{2,\,3\right\}$.

$a\geq 4$ のとき $b\geq 5,c\geq 6$ だから

$$\begin{aligned}\frac{a}{a-1}&=1+\frac{1}{a-1}\leq 1+\frac{1}{4-1}=\frac{4}{3},\\ \frac{b}{b-1}&=1+\frac{1}{b-1}\leq 1+\frac{1}{5-1}=\frac{5}{4},\\ \frac{c}{c-1}&=1+\frac{1}{c-1}\leq 1+\frac{1}{6-1}=\frac{6}{5}\end{aligned}$$

が成り立つので，$k<\dfrac{4}{3}\cdot\dfrac{5}{4}\cdot\dfrac{6}{5}=2$ となり，$k\in\left\{2,\,3\right\}$ に矛盾する．
したがって，$2\leq a\leq 3$.

(i) $a=2$ のとき，$k=\dfrac{2bc-1}{(b-1)(c-1)}$，　$3\leq b<c$

$k=2$ のとき

$$\frac{2bc-1}{(b-1)(c-1)}=2\qquad 2(b+c)=3.$$

3 は 2 の倍数ではないから，$2(b+c)=3$ を満たす整数 b,c は存在しない．

$k=3$ のとき

$$\frac{2bc-1}{(b-1)(c-1)}=3\qquad bc-3b-3c=-4\qquad (b-3)(c-3)=5.$$

$0\leq b-3<c-3$ だから，$b-3=1,c-3=5$ すなわち $b=4,c=8$.

よって，$(a,b,c)=(2,4,8)$.

(ii) $a=3$ のとき，$k=\dfrac{3bc-1}{2(b-1)(c-1)}$，$4\leq b<c$

$k=2$ のとき

$$\frac{3bc-1}{2(b-1)(c-1)}=2 \qquad bc-4b-4c=-5 \qquad (b-4)(c-4)=11.$$

$0\leq b-4<c-4$ だから，$b-4=1, c-4=11$ すなわち $b=5, c=15$.

よって，$(a,b,c)=(3,5,15)$.

$k=3$ のとき

$$\frac{3bc-1}{2(b-1)(c-1)}=3 \qquad 3bc-6b-6c=-7 \qquad 3(bc-2b-2c)=-7.$$

-7 は 3 の倍数ではないから，$3(bc-2b-2c)=-7$ を満たす整数 b,c は存在しない．

(i)，(ii) より解は，$(a,b,c)=(2,4,8),(3,5,15)$. □

注 $f(x)=\dfrac{x}{x-1}$ $(x>1)$ は減少関数である．

問題 2.1.3 整数を係数とする多項式 $f(x)$ について，次のことを証明しなさい．

(1) 任意の整数 m,n に対し $f(n+m)-f(n)$ は m の倍数である．
(2) 任意の整数 k,n に対し $f(n+f(n)k)$ は $f(n)$ の倍数である．
(3) 任意の自然数 n に対し $f(n)$ が素数であるならば，$f(x)$ は定数である．

(2002 慶応大・理工)

解答　$l\in\mathbb{N}_0$ として，$f(x)=a_lx^l+a_{l-1}x^{l-1}+\cdots+a_1x+a_0$ とおく．ただし，$a_l,a_{l-1},\ldots,a_0$ は整数とする．

(1) $f(x)$ が定数のときは，明らかに成り立つから，$l\geq 1$ とする．

$$f(n+m)-f(n)=a_l\left[(n+m)^l-n^l\right]+a_{l-1}\left[(n+m)^{l-1}-n^{l-1}\right]$$
$$+\cdots+a_1\left[(n+m)-n\right] \qquad \cdots\cdots①$$

$1\leq j\leq l$ のとき

$$(n+m)^j-n^j=\binom{j}{1}n^{j-1}\cdot m+\binom{j}{2}n^{j-2}\cdot m^2+\cdots+\binom{j}{j-1}n\cdot m^{j-1}+\binom{j}{j}m^j$$
$$=m\left[\binom{j}{1}n^{j-1}+\binom{j}{2}n^{j-2}\cdot m+\cdots+\binom{j}{j-1}n\cdot m^{j-2}+\binom{j}{j}m^{j-1}\right]$$

は m の倍数である．

よって，①より，$f(n+m)-f(n)$ は m の倍数である．

(2) $p = f(n)$ とおくと，p は整数である．$m = pk$ とおくと，(1) より $f(n+m) - f(n) = f(n + pk) - p$ は $m = pk$ の倍数である．$f(n + pk) - p = pkq,\ q \in \mathbb{Z}$ とおくと，$f(n + pk) = p(1 + kq),\ 1 + kq \in \mathbb{Z}$ より，$f(n + f(n)k)$ は p=$f(n)$ の倍数である．

(3) 任意の正の整数 n に対し $f(n)$ が素数であるとする．$f(x)$ が定数でないと仮定して矛盾が生じることを示す．

$p = f(n)$ とおくと，(2) より，$f(n + pk)$ は p の倍数である．

また，p は素数だから，$p > 1$ で，$k = 0, 1, \ldots$ に対し，$n + pk$ は正の整数となるから，$f(n + pk)$ は素数である．

したがって，$k = 0, 1, \ldots$ に対して $f(n + pk) = p$ が成り立つ．$f(x)$ の次数は $l \geq 1$ だから，$f(x) = p$ は高々 l 個の解しかもたないから，無限個の解 $x = p + nk$ $(k = 0, 1, \ldots)$ をもつことはできない．

よって，$f(x)$ は定数である． □

問題 2.2.1　a, b, c は整数で，a と b の少なくとも一方は 0 ではないものとする．このとき，次のことが成り立つことを示せ．

$$a \mid c,\ b \mid c,\ \gcd(a, b) = 1 \quad \Longrightarrow \quad ab \mid c.$$

解答　a と b は互いに素であるから，系 2.2.1 より $ax + by = 1$ を満たす整数 x, y が存在する．このとき

$$c = c \cdot 1 = c(ax + by) = acx + bcy.$$

$b \mid c$ から $ab \mid ac$，$a \mid c$ から $ab \mid bc$ が言えるから，$ab \mid ac \mid acx,\ ab \mid bc \mid bcy$.

よって，$ab \mid acx + bcy = c$ から $ab \mid c$. □

問題 2.3.1

(1) $25m + 17n = 1623$ を満たす正の整数の組 $(m,\, n)$ を 1 つ求めなさい.
(2) $25m + 17n = 1623$ を満たす正の整数の組 $(m,\, n)$ をすべて求めなさい.

$1623 = 25 \times 64 + 23,\ 1623 = 17 \times 95 + 8$ のうち余りが小さい方を利用するとよい.

解答　$1623 = 17 \times 95 + 8$ を利用して，$25m + 17n = 1623$ を

$$25m + 17(n - 95) = 8 \qquad \cdots\cdots ①$$

と変形する.

(1) $m = 1, n - 95 = -1$ は①の解であるから，$(m, n) = (1, 94)$ は正の整数解の 1 つである.
(2) (1) より

$$25 \times 1 + 17 \times (-1) = 8. \qquad \cdots\cdots ②$$

① − ② より

$$25(m - 1) + 17(n - 94) = 0 \qquad 25(m - 1) = -17(n - 94).$$

25 と 17 は互いに素であるから，k を整数として

$$m - 1 = 17k,\ n - 94 = -25k$$

とかける.
$m = 17k + 1,\ n = -25k + 94$ は正の整数だから，$17k + 1 \geq 1, -25k + 94 \geq 1$ より

$$0 \leq k \leq \frac{93}{25}.$$

整数 k のとり得る値は，$k = 0, 1, 2, 3$ で

$$(m, n) = (1, 94), (18, 69), (35, 44), (52, 19) \qquad \square$$

(2) の別解　$25m + 17n = 1623$ を mod 17 で考えると

$$25m + 17n \equiv 25m \equiv 8m \pmod{17},\ 1623 \equiv 17 \cdot 95 + 8 \equiv 8 \pmod{17}$$

だから，$8m \equiv 8 \pmod{17}$. 8 と 17 は互いに素だから，$m \equiv 1 \pmod{17}$ を得る.
これから，$m = 17k + 1, k \in \mathbb{Z}$ と書ける．これを，$25m + 17n = 17 \cdot 95 + 8$ に代入すると，

$$25(17k + 1) + 17n = 17 \cdot 95 + 8 \qquad 17(n + 25k) = 17 \cdot 95 - 17$$

より，$n+25k=95-1=94$ すなわち $n=-25k+94$ を得る．

$m=17k+1$, $n=-25k+94$ は正の整数だから，$17k+1\geq 1, -25k+94\geq 1$ より

$$0\leq k\leq \frac{93}{25}.$$

整数 k のとり得る値は，$k=0,1,2,3$ で

$$(m,n)=(1,94),(18,69),(35,44),(52,19) \qquad \square$$

問題 2.3.2　p, q を互いに素な正整数とする．

(1) 任意の整数 x に対して，p 個の整数 $x-q$, $x-2q$, …, $x-pq$ を p で割った余りはすべて相異なることを証明せよ．

(2) $x>pq$ なる任意の整数 x は，適当な正整数 a, b を用いて $x=pa+qb$ と表せることを示せ．

(2008 奈良県立医大)

- 例題 4.1.1，問題 4.1.2 も参照．

解答 (1) 背理法で証明する．

$x-q$, $x-2q$, …, $x-pq$ を p で割った余りの中に等しいものがあったと仮定する．i,j を $1\leq i<j\leq p$ を満たす正の整数として，$x-iq$ と $x-jq$ を p で割った余りが r に等しいものとする．$x-iq$ を p で割った商を q_i, 余りを r，$x-jq$ を p で割った商を q_j, 余りを r とすると，

$$x-iq=pq_i+r \quad \cdots\cdots ①, \quad x-jq=pq_j+r \quad \cdots\cdots ②$$

ただし，$0\leq r<p$ である．

① − ② より

$$(j-i)q=p(q_i-q_j) \qquad \cdots\cdots ③$$

p と q は互いに素だから，③より，$j-i$ は p で割り切れる．

ところが，$1\leq j-i\leq p-1<p$ であるから，$j-i$ は p で割り切れないので，$j-i$ が p で割り切れることに矛盾する．

したがって，$x-q$, $x-2q$, …, $x-pq$ を p で割った余りはすべて相異なる．

(2) 任意の整数を p で割った余りは，p 個の 0, $1,\ldots,p-1$ のいずれかである．

(1) の結果より，$x>pq$ なる任意の整数 x に対して，p 個の整数 $x-q$, $x-2q$, …, $x-pq$ を p で割った余りはすべて相異なるので，これらの中に，p で割った余りが 0 となるものが存在する．それを，$x-bq$ とおき，$x-bq$ を p で割った商を a とおくと

$$x-qb=pa \qquad \cdots\cdots ④$$

が成り立つ．

$1 \leq b \leq p$ と $x > pq$ より $x - bq \geq x - pq > 0$ で，正整数 $x - bq$ を p で割った商が a であるから，a は正整数である．

④から，正整数 a, b を用いて $x = pa + qb$ と表せることがわかる．　□

問題 2.3.3 以下の問いに答えよ．

(1) 方程式 $65x + 31y = 1$ の整数解をすべて求めよ．

(2) $65x + 31y = 2016$ を満たす正の整数の組 (x, y) を求めよ．

(3) 2016 以上の整数 m は，正の整数 x, y を用いて $m = 65x + 31y$ と表せることを示せ．　(2016 福井大・教育地域科学)

解 1 (3) の解答は，上の奈良県立医科大の問題の解答を参考にした．

(1)　$65x + 31y = 1$　……①

とおく．

$65 = 31 \cdot 2 + 3,\ 31 = 3 \cdot 10 + 1$ が成り立つから

$$\begin{aligned} 1 &= 31 - 3 \cdot 10 \\ &= 31 - (65 - 31 \cdot 2) \cdot 10 \\ &= 65 \cdot (-10) + 31 \cdot 21. \end{aligned}$$

よって，

$$65 \cdot (-10) + 31 \cdot 21 = 1. \quad \cdots\cdots ②$$

① − ② から，$65(x + 10) + 31(y - 21) = 0$ すなわち

$$65(x + 10) = 31(-y + 21).$$

65 と 31 は互いに素だから，整数 k を用いて，$x + 10 = 31k, -y + 21 = 65k$ と表される．よって，求める整数解は，

$$x = 31k - 10, y = -65k + 21 \ (k \text{ は整数}).$$

(2) $2016 = 65 \cdot 31 + 1$ だから，$65x + 31y = 2016$ は $65x + 31y = 65 \cdot 31 + 1$ すなわち

$$65(x - 31) + 31y = 1$$

と変形できる．(1) より，k を整数として，$x - 31 = 31k - 10, y = -65k + 21$ すなわち $x = 31k + 21, y = -65k + 21$.

$x \geq 1, y \geq 1$ から，$-\dfrac{20}{31} \leq k \leq \dfrac{4}{13}$.

k は整数だから，$k = 0$．ゆえに，$(x, y) = (21, 21)$.

(3) 65 個の数,

$$m-1\cdot 31, m-2\cdot 31, \cdots, m-65\cdot 31 \qquad \cdots\cdots (*)$$

を考える．$m \geq 2016 > 2015 = 65\cdot 31$ だから，$(*)$ の数はすべて正の整数で，65 で割った余りはすべて異なることを示す．

もしも，$(*)$ の中に，65 で割った余りが等しいものがあったと仮定する．i, j を $1 \leq i < j \leq 65$ を満たす正の整数として，$m-i\cdot 31$ と $m-j\cdot 31$ を 65 で割った余りが等しいものとすると，$m-i\cdot 31 \equiv m-j\cdot 31 \pmod{65}$．これから，$31(j-i) \equiv 0 \pmod{65}$．65 と 31 は互いに素であるから，$j-i \equiv 0 \pmod{65}$ すなわち $j-i$ は 65 で割り切れることになる．しかし，$0 < j-i < 65$ だから，65 で割り切れることはなく，$j-i$ が 65 で割り切れることに矛盾する．

したがって，$(*)$ の数を 65 で割った余りはすべて異なる．

任意の整数を 65 で割った余りは，65 個の $0, 1, \ldots, 64$ のいずれかである．

上の結果より，$m \geq 2016$ なる任意の整数 m に対して，65 個の正の整数

$$m-1\cdot 31, m-2\cdot 31, \cdots, m-65\cdot 31$$

を 65 で割った余りはすべて相異なるので，これらの中に，65 で割った余りが 0 となるものが存在する．それを，$m-b\cdot 31$ $(1 \leq b \leq 65)$ とおき，$m-b\cdot 31$ を 65 で割った商を $a(>0)$ とおくと

$$m-b\cdot 31 = 65a \qquad m = 65a+31b$$

が成り立つ．$x=a, y=b$ とおくと，2016 以上の整数 m は正の整数 x, y を用いて $m=65x+31y$ と表せる． □

注　(2) の別解　$65x+31y=2016$ を mod 31 で考えると

$$65x+31y \equiv 65x \equiv 3x \pmod{31},\ 2016 \equiv 31\cdot 65+1 \equiv 1 \pmod{31}$$

だから，$3x \equiv 1 \equiv -30 \pmod{31}$．3 と 31 は互いに素だから，$x \equiv -10 \equiv 21 \pmod{31}$ を得る．

これから，$x = 31k+21, k \in \mathbb{Z}$ と書ける．これを，$65x+31y = 31\cdot 65+1$ に代入すると，

$$65(31k+21)+31y = 31\cdot 65+1 \qquad 31(y+65k) = 65\cdot(31-21)+1 = 651 = 31\cdot 21$$

より，$y+65k=21$ すなわち $n=-65k+21$ を得る．

$m=31k+21$, $n=-65k+21$ は正の整数だから，$31k+21 \geq 1, -65k+21 \geq 1$ より

$$-\frac{20}{31} \leq k \leq \frac{4}{13}.$$

k は整数だから，$k = 0$ で

$$(x, y) = (21, 21).$$ □

注 (3) を合同式を使うと次のようになる．

$65x + 31y = m$ を mod 31 で考えると

$$65x + 31y \equiv 65x \equiv 3x \pmod{31}$$

だから，

$$3x \equiv m \pmod{31}.$$

3 と 31 は互いに素だから，31 を法として 3 の逆数 $3^{-1} \equiv -10 \pmod{31}$ が存在する．
よって，$x \equiv 3^{-1}m \equiv -10m \pmod{31}$ を得る．
これから，$x = 31k - 10m, k \in \mathbb{Z}$ と書ける．これを，$65x + 31y = m$ に代入すると，

$$65(31k - 10m) + 31y = m \qquad 31(y + 65k) = 651m$$

より，$y + 65k = 21m$ すなわち $n = -65k + 21m$ を得る．

$m = 31k - 10m$, $n = -65k + 21m$ は正の整数だから，$31k - 10m > 0, -65k + 21m > 0$ より

$$\frac{10m}{31} < k < \frac{21m}{65}. \quad \cdots (*)$$

$m \geq 2016$ だから

$$\frac{21m}{65} - \frac{10m}{31} = \frac{m}{2015} > 1.$$

よって，$(*)$ を満たす整数 k が存在する． □

解 2 (1)　$65x + 31y = 1$ ……①

とおく．

$65 = 31 \cdot 2 + 3$, $31 = 3 \cdot 10 + 1$ が成り立つから

$$\begin{aligned} 1 &= 31 - 3 \cdot 10 \\ &= 31 - (65 - 31 \cdot 2) \cdot 10 \\ &= 65 \cdot (-10) + 31 \cdot 21. \end{aligned}$$

よって，

$$65 \cdot (-10) + 31 \cdot 21 = 1.$$ ……②

① − ② から，$65(x + 10) + 31(y - 21) = 0$ すなわち

$$65(x + 10) = -31(y - 21).$$

65 と 31 は互いに素だから，整数 k を用いて，$x + 10 = 31k, y - 21 = -65k$ と表される．よって，求める整数解は，

$$x = 31k - 10, y = -65k + 21 \ (k \text{ は整数}).$$

(2)　$65x+31y=2016$ ……③

とおく．②の両辺に 2016 をかけると

$$65\cdot(-20160)+31\cdot 42336=2016. \quad \cdots\cdots④$$

③ − ④ から，$65(x+20160)+31(y-42336)=0$ すなわち

$$65(x+20160)=-31(y-42336).$$

65 と 31 は互いに素だから，整数 k を用いて，$x+20160=31k, y-42336=-65k$ と表される．よって，求める整数解は，

$$x=31k-20160, y=-65k+42336\ (k\text{ は整数}).$$

$x>0, y>$ から，$650\dfrac{10}{31}=\dfrac{20160}{31}<k<\dfrac{42336}{65}=651\dfrac{21}{65}$.

k は整数だから，$k=651$.

ゆえに，$(x,y)=(31\cdot 651-20160, -65\cdot 651+42336)=(21,21)$.

(3)　$65x+31y=m$ ……⑤

とおく．ただし，$m\geq 2016$.

②の両辺に m をかけると

$$65\cdot(-10m)+31\cdot 21m=m. \quad \cdots\cdots⑥$$

⑤ − ⑥ から，$65(x+10m)+31(y-21m)=0$ すなわち

$$65(x+10m)=-31(y-21m).$$

65 と 31 は互いに素だから，整数 k を用いて，$x+10m=31k, y-21m=-65k$ と表される．よって，求める整数解は，

$$x=31k-10m, y=-65k+21m\ (k\text{ は整数}).$$

$x>0, y>0$ から，

$$\frac{10m}{31}<k<\frac{21m}{65}. \quad \cdots\cdots⑦$$

$m\geq 2016$ だから

$$\frac{21m}{65}-\frac{10m}{31}=\frac{m}{2015}>1.$$

よって，⑦を満たす整数 k が存在する． □

注 解 2 の（3）で $x\geq 1, y\geq 1$ から k の値の範囲を求めると，少し面倒になる．

$65x+31y=m$ ……⑤

とおく．ただし，$m \geq 2016$.

②の両辺に m をかけると

$$65 \cdot (-10m) + 31 \cdot 21m = m. \qquad \cdots\cdots ⑥$$

⑤ − ⑥ から，$65(x + 10m) + 31(y - 20m) = 0$ すなわち

$$65(x + 10m) = -31(y - 20m).$$

65 と 31 は互いに素だから，整数 k を用いて，$x + 10m = 31k, y - 20m = -65k$ と表される．よって，求める整数解は，

$$x = 31k - 10m, y = -65k + 20m \ (k \text{ は整数}).$$

$x \geq 1, y \geq 1$ から，

$$\frac{10m+1}{31} \leq k \leq \frac{21m-1}{65}. \qquad \cdots\cdots ⑦$$

$$\frac{21m-1}{65} - \frac{10m+1}{31} = \frac{m-96}{2015} > 1$$

がいえないから，場合分けをする．

$\dfrac{10m+1}{31}$ または $\dfrac{21m-1}{65}$ が整数のときには，⑦を満たす整数 k が存在する．

$\dfrac{10m+1}{31}$ と $\dfrac{21m-1}{65}$ がともに整数でないときには，

$$\frac{10m}{31} < k < \frac{21m}{65} \qquad \cdots\cdots ⑧$$

を満たす整数 k が存在することを示せばよい．

$m \geq 2016$ だから

$$\frac{21m}{65} - \frac{10m}{31} = \frac{m}{2015} > 1.$$

よって，⑧を満たす整数 k が存在する．

ちなみに，(2) は次のような解になる．

$65x + 31y = 2016$ $\qquad \cdots\cdots ③$

とおく．②の両辺に 2016 をかけると

$$65 \cdot (-20160) + 31 \cdot 42336 = 2016. \qquad \cdots\cdots ④$$

③ − ④ から，$65(x + 20160) + 31(y - 42336) = 0$ すなわち

$$65(x + 20160) = -31(y - 42336).$$

65 と 31 は互いに素だから，整数 k を用いて，$x+20160=31k, y-42336=-65k$ と表される．よって，求める整数解は，

$$x=31k-20160, y=-65k+42336\ (k \text{ は整数}).$$

$x \geq 1, y \geq 1$ から，$650\frac{11}{31}=\frac{20161}{31} \leq k \leq \frac{8467}{13}=651\frac{4}{13}$.

k は整数だから，$k=651$.

ゆえに，$(x,y)=(31\cdot 651-20160, -65\cdot 651+42336)=(21,21)$.

注 (3) において，具体的に調べてみる．

$65\cdot 21+31\cdot 21=2016(*)$　　$65\cdot(-10)+31\cdot 21=1(*1)$　　$65\cdot 21+31\cdot(-44)=1(*2)$

が成り立つ．

$65\cdot 21+31\cdot(-44)=1$ は $65\cdot(-10)+31\cdot 21=1$ で $-10+31=21, 21-65=-44$ から求まる．

m が $65x+31y=m$, $x,y \in \mathbb{N}$ と表されるとき，$<x,y,m>$ と書くことにする．まず次のことがわかる．

• $<x,y,m>$ のとき，すべての非負の整数 k に対して，$<x+k,y+k,m+96k>$.

$65x+31y=m$ に $65k+31k=96k$ を加えると，$65(x+k)+31(y+k)=m+96k$ となることから言える．

• m が $2016, 2016+1, \ldots, 2016+95$ のとき，$65x+31y=m$, $x,y \in \mathbb{N}$ と表されることを示せばよい．

このことが成り立てば，$<x,y,m>$ のとき，すべての非負の整数 k に対して，$<x+k,y+k,m+96k>$ であることを使えば，$m \geq 2016$ のとき，$65x+31y=m$, $x,y \in \mathbb{N}$ と表されれるからである．

• m が $2016, 2016+1, \ldots, 2016+95$ のとき，$65x+31y=m$, $x,y \in \mathbb{N}$ と表されることを示す．

$(*)+(*1), (*)+2(*1), (*)+2(*1)+(*2)$ から

$$65\cdot 11+31\cdot 42=2017, 65\cdot 1+31\cdot 63=2018, 65\cdot 22+31\cdot 19=2019.$$

ゆえに，$<21,21,2016> \to <11,42,201> \to <1,63,2018> \to <22,19,2019>$ となった．

$65\cdot 22+31\cdot 19=2019$ を $(*)$ として，同様な操作を行うと，$<22,19,2019> \to <12,40,2020> \to <2,61,2021> \to <23,17,2022>$ となる．2 回の操作の結果を簡単に表すと，$<21,21,2016> \Longrightarrow <22,19,2019> \Longrightarrow <23,17,2022>$ となる．

このことを繰り返すと

$$<21,21,2016> \Longrightarrow <22,19,2019> \Longrightarrow \ldots \Longrightarrow <30,3,2043> \Longrightarrow <31,1,2046>.$$

$65\cdot31+31\cdot1=2046$ に $(*1)$ を加えた $65\cdot21+31\cdot22=2047$ すなわち $<21,22,2047>$ から始めると

$$<21,22,2047>\Longrightarrow<22,20,2050>\Longrightarrow\ldots\Longrightarrow<30,4,2044>\Longrightarrow<31,2,2077>.$$

$65\cdot31+31\cdot2=2077$ に $(*1)$ を加えた $65\cdot21+31\cdot23=2078$ すなわち $<21,23,2078>$ から始めると

$$<21,23,2078>\Longrightarrow<22,21,2081>\Longrightarrow\ldots\Longrightarrow<30,5,2105>\Longrightarrow<31,3,2108>.$$

$65\cdot31+31\cdot3=2108$ に $(*1)$ を加えた $65\cdot21+31\cdot24=2109$ すなわち $<21,24,2109>$ から始めると

$$<21,24,2109>\Longrightarrow<22,22,2110>\Longrightarrow\ldots\Longrightarrow<30,6,2136>\Longrightarrow<31,4,2139>.$$

よって，m が $2016, 2016+1, \ldots, 2016+95$ のとき，$65x+31y=m$, $x,y\in\mathbb{N}$ と表されることがわかった．　□

問題 2.3.4　xy 平面上の点で x 座標，y 座標がともに整数である点を格子点という．
a,k は整数で $a\geq2$ とし，直線 $L: ax+\left(a^2+1\right)y=k$ を考える．

(1) 直線 L 上の格子点を 1 つ求めよ．
(2) $k=a\left(a^2+1\right)$ のとき，$x>0$, $y>0$ の領域に直線 L 上の格子点は存在しないことを示せ．
(3) $k>a\left(a^2+1\right)$ ならば，$x>0$, $y>0$ の領域に直線 L 上の格子点が存在することを示せ．　(2000　京都大・理・医・薬・工・農・後期)

解答　$ax+\left(a^2+1\right)y=k$　……①
とおく．

(1) $a^2+1=a\cdot a+1$ より $\gcd\left(a,a^2+1\right)=1$ で $a\cdot(-a)+\left(a^2+1\right)\cdot1=1$.
この等式の両辺に k をかけると

$$a\cdot(-ak)+\left(a^2+1\right)\cdot k=k.\qquad\cdots\cdots②$$

よって，格子点の 1 つは $(-ak,k)$.

(2) 不定方程式①の整数解を求める．
① − ② から，$a(x+ak)+\left(a^2+1\right)(y-k)=0$ すなわち

$$a(x+ak)=\left(a^2+1\right)(-y+k)$$

a と a^2+1 は互いに素であるから，m を整数として，

$$x+ak=\left(a^2+1\right)m,\ -y+k=am$$

すなわち

$$x=-ak+\left(a^2+1\right)m,\ y=k-am$$

と表される．

$x>0, y>0$ より $-ak+\left(a^2+1\right)m>0,\ k-am>0$ だから，この不等式を解くと

$$\frac{ak}{a^2+1}<m<\frac{k}{a}. \qquad \cdots\cdots ③$$

$k=a\left(a^2+1\right)$ のとき，③は $a^2<m<a^2+1$ となる．$a\geq 2$ は整数だから，$a^2<m<a^2+1$ を満たす整数 m は存在しない．

したがって，$k=a\left(a^2+1\right)$ のとき，$x>0,\ y>0$ の領域に直線 L 上の格子点は存在しない．

(3) $k>a\left(a^2+1\right)$ のとき，$\dfrac{k}{a}-\dfrac{ak}{a^2+1}=\dfrac{k}{a\left(a^2+1\right)}>1$ が成り立ち，③を満たす整数 m が存在するから，$x>0,\ y>0$ の領域に直線 L 上の格子点が存在することがわかる． □

問題 2.3.5 (Putnam 2000)

$n\geq m\geq 1$ を満たすすべての正の整数の組 $(m,\ n)$ に対して

$$\frac{\gcd(m,n)}{n}\binom{n}{m}$$

は整数であることを証明せよ．

解答　$\gcd(m,n)=am+bn$ を満たす整数 a, b が存在する．

$$\frac{\gcd(m,n)}{n}\binom{n}{m}=\frac{am+bn}{n}\binom{n}{m}=\frac{am}{n}\binom{n}{m}+b\binom{n}{m}$$

であるから，$\dfrac{m}{n}\binom{n}{m}$ が整数となることを示せばよい．

$$\frac{m}{n}\binom{n}{m}=\frac{m}{n}\cdot\frac{n!}{m!(n-m)!}=\frac{(n-1)!}{(m-1)!(n-m)!}=\binom{n-1}{m-1}$$

は整数である． □

問題 2.3.6 (PUMAC 2013)
$2^{30^{10}}-2$ と $2^{30^{45}}-2$ の最大公約数が 2^x-2 の形に表されるとき，x を求めよ．

解答　a, m, n は正の整数で $a>1$ のとき

$$\gcd\left(a^m-1,\, a^n-1\right)=a^{\gcd(m,\,n)}-1$$

が成り立つことを利用する．

$$\begin{aligned}\gcd\left(2^{30^{10}}-1, 2^{30^{45}}-1\right)&=\gcd\left[2\left(2^{30^{10}-1}-1\right), 2\left(2^{30^{45}-1}-1\right)\right]\\&=2\gcd\left(2^{30^{10}-1}-1, 2^{30^{45}-1}-1\right)\\&=2\left(2^{\gcd\left(30^{10}-1,\,30^{45}-1\right)}-1\right)\end{aligned}$$

となり，

$$\gcd\left(30^{10}-1, 30^{45}-1\right)=30^{\gcd(10,45)}-1=30^5-1$$

であることを利用すると，

$$\gcd\left(2^{30^{10}}-1, 2^{30^{45}}-1\right)=2\left(2^{\gcd\left(30^{10}-1,\,30^{45}-1\right)}-1\right)=2\left(2^{30^5-1}-1\right)=2^{30^5}-2.$$

ゆえに，$x=30^5$. □

問題 2.3.7 a, m, n は正の整数で，$m\neq n$ のとき次のことを証明せよ．

$$\gcd\left(a^{2^m}+1, a^{2^n}+1\right)=\begin{cases}1 & (a\text{ は偶数})\\ 2 & (a\text{ は奇数})\end{cases}.$$

解答　$m>n$ と仮定しても一般性を失わない．
$a^{2^n}+1 \,\middle|\, \left(a^{2^n}+1\right)\left(a^{2^n}-1\right)=a^{2^{n+1}}-1 \,\middle|\, a^{2^m}-1$ であるから，

$$a^{2^m}-1=\left(a^{2^n}+1\right)q\quad(q\in\mathbb{N})$$

とおける．これを，$a^{2^m}+1=\left(a^{2^n}+1\right)q+2$ と変形する．

$$\gcd\left(a^{2^m}+1, a^{2^n}+1\right)=\gcd\left(a^{2^m}+1-q\left(a^{2^n}+1\right), a^{2^n}+1\right)=\gcd\left(2, a^{2^n}+1\right).$$

a が偶数のとき，$2\nmid a^{2^n}+1$ より $\gcd\left(2, a^{2^n}+1\right)=1$.
よって，$\gcd\left(a^{2^m}+1, a^{2^n}+1\right)=1$.
a が奇数のとき，$2\mid a^{2^n}+1$ より $\gcd\left(2, a^{2^n}+1\right)=2$.
よって，$\gcd\left(a^{2^m}+1, a^{2^n}+1\right)=2$. □

問題 2.3.8　a, b, m, n が正の整数で $a > b$, $\gcd(a, b) = 1$ のとき

$$\gcd\left(a^m - b^m,\, a^n - b^n\right) = a^{\gcd(m,\,n)} - b^{\gcd(m,\,n)} \tag{11.1}$$

が成り立つことを証明せよ.

解答　$m = n$ のとき (11.1) は成り立つから，$m > n$ と仮定する.

$r_0 = m$, $r_1 = n$ とおき，r_0 を r_1 で割った商を q_1，余りを r_2 とすると，

$$r_0 = r_1 q_1 + r_2, \quad 0 \le r_2 < r_1 \qquad (m = nq_1 + r_2, \quad 0 \le r_2 < n)$$

が成り立つ.

定理 2.3.1 を使うと

$$\begin{aligned}(a^m - b^m,\, a^n - b^n) &= \left(a^m - b^m - a^{m-n}(a^n - b^n),\, a^n - b^n\right) \\ &= \left(b^n\left(a^{m-n} - b^{m-n}\right),\, a^n - b^n\right)\end{aligned}$$

が成り立つ．a と b は互いに素だから，$(b^n,\, a^{m-n} - b^{m-n}) = 1$ なので

$$\left(b^n\left(a^{m-n} - b^{m-n}\right),\, a^n - b^n\right) = \left(a^{m-n} - b^{m-n},\, a^n - b^n\right).$$

よって，

$$(a^m - b^m,\, a^n - b^n) = \left(a^{m-n} - b^{m-n},\, a^n - b^n\right)$$

が成り立つ.

これを繰り返すと

$$\begin{aligned}(a^{r_0} - b^{r_0},\, a^{r_1} - b^{r_1}) = (a^m - 1,\, a^n - 1) &= \left(a^{m-n} - a^{m-n},\, a^n - b^n\right) \\ &= \left(a^{m-2n} - b^{m-2n},\, a^n - b^n\right) \\ &= \cdots \\ &= \left(a^{m-q_1 n} - b^{m-q_1 n},\, a^n - b^n\right) \\ &= (a^{r_2} - b^{r_2},\, a^{r_1} - b^{r_1}).\end{aligned}$$

よって

$$(a^{r_0} - b^{r_0},\, a^{r_1} - b^{r_1}) = (a^{r_1} - b^{r_1},\, a^{r_2} - b^{r_2})$$

が成り立つ．$r_2 \neq 0$ のとき，r_1 を r_2 で割った商を q_2，余りを r_3 とすると，

$$r_1 = r_2 q_2 + r_3, \quad 0 \le r_3 < r_2$$

で上で示したことから

$$(a^{r_1} - b^{r_1},\, a^{r_2} - b^{r_2}) = (a^{r_2} - a^{r_2},\, a^{r_3} - b^{r_3})$$

が成り立つ.

この操作を続けると余りの列

$$m = r_0 > r_1 > r_2 > \cdots \geq 0$$

は m 個より多くの正整数を含み得ないから，いつかは余りは 0 となる.

すなわち

$$\left.\begin{aligned} r_0 &= r_1 q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots \qquad\qquad \vdots & \\ r_{l-2} &= r_{l-1} q_{l-1} + r_l, & 0 < r_l < r_{l-1} \\ r_{l-1} &= r_l q_l + r_{l+1}, & r_{l+1} = 0 \end{aligned}\right\}$$

となる正の整数 l が存在する.

$r_l = \gcd(m, n)$ で

$$\begin{aligned} (a^m - b^m,\, a^n - b^n) &= (a^{r_0} - b^{r_0},\, a^{r_1} - a^{r_1}) \\ &= (a^{r_1} - b^{r_1},\, a^{r_2} - b^{r_2}) \\ &= \cdots \\ &= (a^{r_{l-1}} - b^{r_{l-1}},\, a^{r_l} - b^{r_l}) \\ &= (a^{r_l} - b^{r_l},\, a^{r_{l+1}} - b^{r_{l+1}}) \\ &= \left(a^{r_l} - b^{r_l},\, a^0 - b^0\right) \\ &= a^{r_l} - b^{r_l} = a^{\gcd(m,\,n)} - b^{\gcd(m,\,n)}. \end{aligned}$$

したがって，(11.1) は成り立つ. □

別解　$m + n$ に関する数学的帰納法で示す.

(I) $m + n = 2$ のとき，$m = n = 1$ で，(11.1) は成り立つ.

(II) $m + n < k$ のとき成り立つと仮定して，$m + n = k$ のとき (11.1) が成り立つことを示す.

$m = n$ のとき (11.1) は成り立つから，$m > n$ と仮定する.

$$\begin{aligned} (a^m - b^m,\, a^n - b^n) &= \left(a^m - b^m - a^{m-n}(a^n - b^n),\, a^n - b^n\right) \\ &= \left(b^n \left(a^{m-n} - b^{m-n}\right),\, a^n - b^n\right) \end{aligned}$$

が成り立つ．a と b は互いに素だから，$(b^n,\, a^{m-n} - b^{m-n}) = 1$ なので

$$\left(b^n \left(a^{m-n} - b^{m-n}\right),\, a^n - b^n\right) = \left(a^{m-n} - b^{m-n},\, a^n - b^n\right).$$

よって，

$$(a^m - b^m,\, a^n - b^n) = \left(a^{m-n} - b^{m-n},\, a^n - b^n\right)$$

が成り立つ.

$(m-n)+n=m<m+n=k$ だから，仮定が使えて，

$$\left(a^{m-n}-b^{m-n},\, a^n-b^n\right)=a^{(m-n,n)}-b^{(m-n,n)}.$$

ところで，$(m-n,n)=((m-n)+n,n)=(m,n)$ だから，

$$(a^m-b^m,\, a^n-b^n)=\left(a^{m-n}-b^{m-n},\, a^n-b^n\right)=a^{(m-n,n)}-b^{(m-n,n)}=a^{(m,n)}-b^{(m,n)}.$$

したがって，$m+n=k$ のときも (11.1) が成り立つ.

(III) (I)，(II) から，(11.1) は成り立つ. □

問題 2.3.9　2 つの奇数 a,b に対して，$m=11a+b$, $n=3a+b$ とおく．次の (1)，(2) を証明せよ.

(1) m,n の最大公約数は，a,b の最大公約数を d として，$2d,4d,8d$ のいずれかである.
(2) m,n がともに平方数であることはない.（整数の 2 乗である数を平方数という.）

(1989 京都大・医・薬・工・農・教・経・後期)

解答

(1)
$$\begin{aligned}\gcd(m,n)=\gcd(11a+b,3a+b)&=\gcd(11a+b-(3a+b),3a+b)\\&=\gcd(8a,3a+b).\end{aligned}$$

a,b は奇数だから，$3a+b$ は偶数である．しかし，$3a+b$ は 2 の何乗で割り切れるかわからないので，

$$3a+b=2^kp\ (k,p\in\mathbb{N},\ p\text{ は奇数})$$

とおく.

(i) $1\le k\le 3$ の場合

$$\begin{aligned}\gcd(8a,3a+b)&=\gcd(8a,2^kp)\\&=2^k\gcd(2^{3-k}a,p)\\&=2^k\gcd(a,p)\qquad p\text{ は奇数}\\&=2^k\gcd(a,2^kp)\qquad a\text{ は奇数}\\&=2^k\gcd(a,3a+b).\end{aligned}$$

ここで，$\gcd(a,3a+b)=\gcd(a,3a+b-3a)=\gcd(a,b)=d$ であるから，$\gcd(m,n)=2^kd$ となり，m,n の最大公約数は $2d,4d,8d$ のいずれかである.

(ii) $k \geq 4$ の場合

$$\begin{aligned}\gcd(8a, 3a+b) &= \gcd(8a, 2^k p)\\ &= 2^3 \gcd(a, 2^{k-3}p)\\ &= 2^3 \gcd(a, p) \qquad a \text{ は奇数}\\ &= 2^k \gcd(a, 2^k p) \qquad a \text{ は奇数}\\ &= 2^3 \gcd(a, 3a+b).\end{aligned}$$

ここで，$\gcd(a, 3a+b) = \gcd(a, 3a+b-3a) = \gcd(a, b) = d$ であるから，$\gcd(m, n) = 2^3 d$ となり，m, n の最大公約数は $8d$ である．

(i)，(ii) より，m, n の最大公約数は $2d, 4d, 8d$ のいずれかである．

(2) m と n は偶数だから，ともに平方数だとすると

$$m = (2M)^2 = 4M^2,\ n = (2N)^2 = 4N^2\ (M, N \in \mathbb{Z})$$

とおける．

$$8a = m - n = 4\left(M^2 - N^2\right) = 4(M+N)(M-N)$$

から

$$(M+N)(M-N) = 2a. \qquad \cdots\cdots ①$$

$(M+N) + (M-N) = 2M$ は偶数だから，$M+N$ と $M-N$ の偶奇は一致するから，①より，$M+N$, $M-N$ はともに偶数である．すると，$(M+N)(M-N)$ は 4 の倍数となり，①から a は偶数となる．これは，a が奇数であることに矛盾する． □

問題 2.3.10　$43x + 782y = 1$ と $2 < |x + 18y| < 12$ を満たす整数 x, y で，$\left|\dfrac{x}{y}\right|$ が最大であるものを求めよ．　(1987 芝浦工大・電気工・建築・工業経営)

解 1　$43x + 782y = 1$　$\cdots\cdots ①$，　$2 < |x + 18y| < 12$　$\cdots\cdots ②$ とおく．

$782 = 43 \times 18 + 8,\ 43 = 8 \times 5 + 3,\ 8 = 3 \times 2 + 2,\ 3 = 2 \times 1 + 1$ だから

$$\begin{aligned}1 &= 3 - 2 \times 1\\ &= 3 - (8 - 3 \times 2) = -8 + 3 \times 3\\ &= -8 + (43 - 8 \times 5) \times 3 = 43 \times 3 - 8 \times 16\\ &= 43 \times 3 - (782 - 43 \times 18) \times 16\\ &= 43 \times 291 + 782 \times (-16).\end{aligned}$$

よって

$$43 \times 291 + 782 \times (-16) = 1 \qquad \cdots\cdots ③$$

が成り立つから，① − ③ から，$43(x-291)=-782(y+16)$.
43 と 782 は互いに素だから，k を整数として $x-291=782k,\ y+16=-43k$ すなわち

$$x=782k+291,\ y=-43k-16$$

と表せる．これらの式を②に代入すると，$2<|8k+3|<12$ となり，$k\in\Big\{-1,\,0,\,1\Big\}$ を得る．

$k=-1$ のとき，$x=-491,\ y=27$ で，$\left|\dfrac{x}{y}\right|=\dfrac{491}{27}=18.185\cdots$,

$k=0$ のとき，$x=291,\ y=-16$ で，$\left|\dfrac{x}{y}\right|=\dfrac{291}{16}=18.187\cdots$,

$k=1$ のとき，$x=1073,\ y=-59$ で，$\left|\dfrac{x}{y}\right|=\dfrac{1073}{59}=18.186\cdots$.

これらの中で，$\left|\dfrac{x}{y}\right|$ が最大となるのは，$x=291, y=-16$ のときである． □

- ①の特殊解は *Blankinship's method* を適用して求めてもよい．

$$A=\begin{pmatrix}43 & 1 & 0\\ 782 & 0 & 1\end{pmatrix}$$
$$\downarrow\quad(\text{第}2\text{行})-(\text{第}1\text{行})\times 18\qquad 782=43\times 18+8$$
$$\begin{pmatrix}43 & 1 & 0\\ 8 & -18 & 1\end{pmatrix}$$
$$\downarrow\quad(\text{第}1\text{行})-(\text{第}2\text{行})\times 5\qquad 43=8\times 5+3$$
$$\begin{pmatrix}3 & 91 & -5\\ 8 & -18 & 1\end{pmatrix}$$
$$\downarrow\quad(\text{第}2\text{行})-(\text{第}1\text{行})\times 3\qquad 8=3\times 3-1(*)$$
$$\begin{pmatrix}3 & 91 & -5\\ -1 & -291 & 16\end{pmatrix}$$
$$\downarrow\quad(\text{第}2\text{行})\times(-1)$$
$$\begin{pmatrix}3 & 91 & -5\\ 1 & 291 & -16\end{pmatrix}$$
$$\downarrow\quad(\text{第}1\text{行})-(\text{第}2\text{行})\times 3\qquad 3=1\times 3$$
$$\begin{pmatrix}0 & -782 & 43\\ 1 & 291 & -16\end{pmatrix}.$$

$\gcd(43,\,782)=1$ で不定方程式 $43x+782y=11$ の特殊解として $x=291,\ y=-16$ が得られる．（以下省略．） □

注　$(*)$ のところは，$8=3\times 2+2$ として考えてもよい．

解 2　$43x+782y=1$　$\cdots\cdots$①，$2<|x+18y|<12$　$\cdots\cdots$② とおく．
①を　mod 43 で考えると，

$$782y\equiv 1 \pmod{43} \qquad (43\cdot 18+8)y\equiv 1 \pmod{43} \qquad 8y\equiv 1 \pmod{43}.$$
$$8y\equiv 1\equiv -42 \pmod{43}.$$

2 と 43 は互いに素だから
$$4y\equiv -21 \pmod{43}$$

この式の両辺に 11 をかけると

$$44y\equiv -231 \pmod{43} \qquad (43+1)y\equiv -(43\cdot 5+16) \pmod{43}.$$
$$y\equiv -16 \pmod{43}.$$

これから，l を整数として，$y=43l-16$ とかける．これを①に代入すると

$$43x+782(43l-16)=1 \qquad 43(x+782l)=782\cdot 16+1=12513=43\cdot 291.$$

よって，$x+782l=291$ となる．（以下省略．）　□

注 筆者が高校生のとき，次のようにして①の特殊解を求める方法を参考書で学んだ．

$$43x+782y=1. \qquad \cdots\cdots ①$$
$$43x+(43\times 18+8)y=1 \qquad 43(x+18y)+8y=1.$$

$X=x+18y$ とおくと，$43X+8y=1$ となり

$$(8\times 5+3)X+8y=1 \qquad 3X+8(5X+y)=1.$$

$Y=5X+y$ とおくと，$3X+8Y=1$ となる．この操作を続けてもよいが，$3X+8Y=1$ の特殊解が $X=3, Y=-1$ と見つかるので，$y=Y-5X=-16,\ x=X-18y=3-18\cdot(-16)=291$ と特殊解が 1 組求まる．

問題 2.3.11(Japan 1996)
m, n がは互いに素な正の整数とする．このとき

$$\gcd\left(5^m+7^m,\, 5^n+7^n\right)$$

を求めよ．

解答　$m=n=1$ のとき，

$$\gcd\left(5^m+7^m,\, 5^n+7^n\right)=\gcd\left(5+7,\, 5+7\right)=\gcd(12,12)=1.$$

$m\neq n$ のときは，対称性から $m>n$ と仮定しても一般性を失わない．

(i) $2n > m > n$ の場合

$$\begin{aligned} 5^m + 7^m &= (5^n + 7^n)\left(5^{m-n} + 7^{m-n}\right) - 5^n 7^{m-n} - 5^{m-n} 7^n \\ &= (5^n + 7^n)\left(5^{m-n} + 7^{m-n}\right) - 5^{m-n} 7^{m-n}\left(5^{2n-m} + 7^{2n-m}\right) \end{aligned}$$

を使うと

$$\begin{aligned} &\gcd\left(5^m + 7^m,\, 5^n + 7^n\right) \\ &= \gcd\left(5^m + 7^m - (5^n + 7^n)\left(5^{m-n} + 7^{m-n}\right),\, 5^n + 7^n\right) \\ &= \gcd\left(-5^{m-n} 7^{m-n}\left(5^{2n-m} + 7^{2n-m}\right),\, 5^n + 7^n\right) \\ &= \gcd\left(5^{m-n} 7^{m-n}\left(5^{2n-m} + 7^{2n-m}\right),\, 5^n + 7^n\right). \end{aligned}$$

$5 \nmid 5^n + 7^n$, $7 \nmid 5^n + 7^n$ より $\gcd\left(5^{m-n} 7^{m-n}, 5^n + 7^n\right) = 1$ だから，

$$\gcd\left(5^{m-n} 7^{m-n}\left(5^{2n-m} + 7^{2n-m}\right),\, 5^n + 7^n\right) = \gcd\left(5^{2n-m} + 7^{2n-m},\, 5^n + 7^n\right)$$

となる．ゆえに

$$\gcd\left(5^m + 7^m,\, 5^n + 7^n\right) = \gcd\left(5^n + 7^n,\, 5^{2n-m} + 7^{2n-m}\right) \qquad \cdots ①$$

を得る．①の右辺の式の指数について，

- $n > 2n - m > 0$
- $\gcd(n, 2n - m) = \gcd(n, 2n - m - 2n) = \gcd(n, -m) = \gcd(n, m) = 1$
- $n + (2n - m) = m + n + 2n - 2m \equiv m + n \pmod 2$

を満たしていることがわかる．

(ii) $m \geq 2n$ の場合

$$\begin{aligned} 5^m + 7^m &= (5^n + 7^n)\left(5^{m-n} + 7^{m-n}\right) - 5^n 7^{m-n} - 5^{m-n} 7^n \\ &= (5^n + 7^n)\left(5^{m-n} + 7^{m-n}\right) - 5^n 7^n\left(5^{m-2n} + 7^{m-2n}\right) \end{aligned}$$

を使うと

$$\begin{aligned} &\gcd\left(5^m + 7^m,\, 5^n + 7^n\right) \\ &= \gcd\left(5^m + 7^m - (5^n + 7^n)\left(5^{m-n} + 7^{m-n}\right),\, 5^n + 7^n\right) \\ &= \gcd\left(-5^n 7^n\left(5^{m-2n} + 7^{m-2n}\right),\, 5^n + 7^n\right) \\ &= \gcd\left(5^n 7^n\left(5^{m-2n} + 7^{m-2n}\right),\, 5^n + 7^n\right). \end{aligned}$$

$5 \nmid 5^n + 7^n$, $7 \nmid 5^n + 7^n$ より $\gcd\left(5^n 7^n, 5^n + 7^n\right) = 1$ だから，

$$\gcd\left(5^n 7^n\left(5^{m-2n} + 7^{m-2n}\right),\, 5^n + 7^n\right) = \gcd\left(5^{m-2n} + 7^{m-2n},\, 5^n + 7^n\right)$$

となる．ゆえに

$$\gcd\left(5^m+7^m,\,5^n+7^n\right)=\gcd\left(5^n+7^n,\,5^{m-2n}+7^{m-2n}\right)\qquad\cdots②$$

を得る．

②の右辺の式の指数 n と $m-2n$ の大小は不明．

m を $2n$ で割った商を $q\,(\geq 1)$ 余りを r とすると，

$$m=2nq+r,\ \ 0\leq r<2n$$

が成り立つ．

②を q 回繰り返し用いると

$$\begin{aligned}\gcd\left(5^m+7^m,\,5^n+7^n\right)&=\gcd\left(5^n+7^n,\,5^{m-2n}+7^{m-2n}\right)\\&=\gcd\left(5^n+7^n,\,5^{m-4n}+7^{m-4n}\right)\\&=\cdots\\&=\gcd\left(5^n+7^n,\,5^{m-2qn}+7^{m-2qn}\right)\\&=\gcd\left(5^n+7^n,\,5^r+7^r\right)\end{aligned}$$

から

$$\gcd\left(5^m+7^m,\,5^n+7^n\right)=\gcd\left(5^n+7^n,\,5^r+7^r\right)\qquad\cdots③$$

を得る．

$0\leq r<2n$ であったから，場合分けをする．

$\star$ $0<r<n$ の場合

③の右辺の式の指数について，

- $n>r>0$
- $\gcd(n,r)=\gcd(n,m-2nq)=\gcd(n,m-2nq+2nq)=\gcd(n,m)=1$
- $n+r=m+m-2nq\equiv m+n\pmod 2$

を満たしていることがわかる．

$\star$ $n>r=0$ の場合

$m=2nq$, $\gcd(m,n)=1$ から $n=1, m=2q\,(q\geq 1)$ となる．

③の右辺の式の指数について，

- $n>r=0$
- $\gcd(n,r)=\gcd(1,0)=1$
- $m+m=2q+1\equiv 1\equiv n+r\pmod 2$

を満たしていることがわかる．

③から

$$\gcd\left(5^m+7^m,\,5^n+7^n\right)=\gcd\left(5^n+7^n,\,5^r+7^r\right)=\gcd\left(5^1+7^1,\,5^0+7^0\right)=2.$$

を得る．

$\star$ $r=n>0$ の場合

$m=(2q+1)n$, $\gcd(m,n)=1$ から $n=1, m=2q+1\,(q\geq 1)$ となる．

③の右辺の式の指数について，

- $n=r>0$
- $\gcd(n,r)=\gcd(n,n)=\gcd(1,1)=1$
- $m+m=(2q+1)+1\equiv 2\equiv n+r \pmod 2$

をみたしていることがわかる．

③から

$$\gcd\left(5^m+7^m,\,5^n+7^n\right)=\gcd\left(5^n+7^n,\,5^r+7^r\right)=\gcd\left(5^1+7^1,\,5^1+7^1\right)=12.$$

を得る．

$\star$ $2n>r>n$ の場合

③の右辺の式に (i) の場合を用いると

$$\gcd\left(5^r+7^r,\,5^n+7^n\right)=\gcd\left(5^n+7^n,\,5^{2n-r}+7^{2n-r}\right)$$

が成り立つから

$$\gcd\left(5^m+7^m,\,5^n+7^n\right)=\gcd\left(5^n+7^n,\,5^{2n-r}+7^{2n-r}\right)\qquad\cdots④$$

を得る．④の右辺の式の指数について，

- $n>2n-r>0$
- $\gcd(n,2n-r)=\gcd(n,2n-m+2nq)=\gcd(n,-m)=\gcd(n,m)=1$
- $n+(2n-r)=3n-m+2nq=m+n+2nq+2n-2m\equiv m+n \pmod 2$

をみたしていることがわかる．

準備ができたので，数列を作る．

$m=n$ のとき，$\gcd(m,n)=1$ から $m=n=1$ となり

$$\gcd\left(5^m+7^m,\,5^n+7^n\right)=\gcd\left(5+7,\,5+7\right)=\gcd(12,12)=1.$$

$m\neq n$ のときは，対称性から $m>n$ と仮定しても一般性を失わない．

$(m_0,n_0)=(m,n),\ m_0>n_0,\ \gcd(m_0,n_0)=1$ として，以下，

$(m_i,n_i),\ m_i>n_i\geq 1,\ \gcd(m_i,n_i)=1$ から $(m_{i+1},n_{i+1}),\ m_{i+1}\geq n_{i+1}\geq 0,\ m_i>m_{i+1}>0,\ n_i\geq n_{i+1}\geq 0,\ \gcd(m_{i+1},n_{i+1})=1$ を次のように帰納的に作る．

(ア) $2n_i > m_i > n_i$ の場合

(i) から

$$\gcd\left(5^{m_i}+7^{m_i},\, 5^{n_i}+7^{n_i}\right) = \gcd\left(5^{n_i}+7^{n_i},\, 5^{2n_i-m_i}+7^{2n_i-m_i}\right)$$

が成り立つから，$m_{i+1} = n_i,\ n_{i+1} = 2n_i - m_i$ とおくと，

$m_{i+1} > n_{i+1} > 0,\ \gcd(m_{i+1}, n_{i+1}) = 1,\ m_{i+1} + n_{i+1} \equiv m_i + n_i \pmod 2$

が成り立つ．また，$m_i > n_i = m_{i+1} > n_{i+1}$ から

$m_i > m_{i+1} > 0,\ n_i > n_{i+1} > 0.$

(イ) $m_i \geq 2n_i$ の場合　(ii) の場合を用いる．

m_i を $2n_i$ で割った商を q_i 余りを r_i とおくと $m_i = 2n_iq_i + r_i,\ \ 0 \leq r_i < 2n_i.$ が成り立つ．

(a) $0 < r_i < n_i$ のとき，③から

$$\gcd\left(5^{m_i}+7^{m_i},\, 5^{n_i}+7^{n_i}\right) = \gcd\left(5^{n_i}+7^{n_i},\, 5^{r_i}+7^{r_i}\right)$$

が成り立つから，$m_{i+1} = n_i,\ n_{i+1} = r_i$ とおくと，

$m_{i+1} > n_{i+1} > 0,\ \gcd(m_{i+1}, n_{i+1}) = 1,\ m_{i+1} + n_{i+1} \equiv m_i + n_i \pmod 2$

が成り立つ．また，$m_i > n_i = m_{i+1} > n_{i+1}$ から

$m_i > m_{i+1} > 0,\ n_i > n_{i+1} > 0.$

(b) $n_i > r_i = 0$ のとき，

$m_i = 2n_iq_i, \gcd(m_i, n_i) = 1$ から $n_i = 1, m_i = 2q_i\ (q_i \geq 1)$

③から

$$\gcd\left(5^{m_i}+7^{m_i},\, 5^{n_i}+7^{n_i}\right) = \gcd\left(5^{n_i}+7^{n_i},\, 5^{r_i}+7^{r_i}\right) = \gcd\left(5^1+7^1,\, 2\right) = 2$$

が成り立つから，$m_{i+1} = n_i,\ n_{i+1} = r_i = 0$ とおくと，

$m_{i+1} > n_{i+1} = 0,\ \gcd(m_{i+1}, n_{i+1}) = 1,\ m_{i+1} + n_{i+1} \equiv m_i + n_i \equiv 1 \pmod 2$

が成り立つ．また，$m_i > n_i = m_{i+1} > n_{i+1} = 0$ から

$m_i > m_{i+1} > 0,\ n_i > n_{i+1} = 0.$　　(ここで終了．)

(c) $n_i = r_i > 0$ のとき，

$m_i = (2q_i + 1)n_i, \gcd(m_i, n_i) = 1$ から $n_i = 1, m_i = 2q_i + 1\ (q_i \geq 1)$

③から

$$\begin{aligned}\gcd\left(5^{m_i}+7^{m_i},\, 5^{n_i}+7^{n_i}\right) &= \gcd\left(5^{n_i}+7^{n_i},\, 5^{r_i}+7^{r_i}\right)\\ &= \gcd\left(5^1+7^1,\, 5^1+7^1\right)\\ &= 12\end{aligned}$$

が成り立つから，$m_{i+1} = n_i,\ n_{i+1} = r_i$ とおくと，

$m_{i+1}=n_{i+1}$, $\gcd(m_{i+1},n_{i+1})=1$, $m_{i+1}+n_{i+1}\equiv m_i+n_i\equiv 0 \pmod 2$
が成り立つ．また，$m_i>n_i=m_{i+1}=n_{i+1}$ から
$m_i>m_{i+1}>0$, $n_i=n_{i+1}>0$.　　（ここで終了．）

(d) $2n_i>r_i>n_i$ のとき，④から

$$\gcd\left(5^{m_i}+7^{m_i},\, 5^{n_i}+7_i^n\right)=\gcd\left(5^{n_i}+7^{n_i},\, 5^{2n_i-r_i}+7^{2n_i-r_i}\right)$$

が成り立つから，$m_{i+1}=n_i$, $n_{i+1}=2n_i-r_i$ とおくと，
$m_{i+1}>n_{i+1}>0$, $\gcd(m_{i+1},n_{i+1})=1$, $m_{i+1}+n_{i+1}\equiv m_i+n_i \pmod 2$
が成り立つ．また，$m_i>n_i=m_{i+1}>n_{i+1}$ から
$m_i>m_{i+1}>0$, $n_i>n_{i+1}>0$.

以上のように，数列 $\{(m_i,n_i)\}$ を作ると，
$(c):m_i=n_i=1$ または $(b):n_i=0$ となったところで終了する．
$m_{i+1}+n_{i+1}\equiv m_i+n_i \pmod 2$ が成り立つので，
(c) の場合，$m+n$ が偶数のとき，

$$\gcd\left(5^m+7^m,\, 5^n+7^n\right)=\gcd\left(5^1+7^1,\, 5^1+7^1\right)=12.$$

(b) の場合，$m+n$ が奇数のとき，

$$\gcd\left(5^m+7^m,\, 5^n+7^n\right)=\gcd\left(5^1+7^1,\, 5^0+7^0\right)=2.$$

したがって，

$$\gcd\left(5^m+7^m,\, 5^n+7^n\right)=\begin{cases}12 & m+n \text{ は偶数}\\ 2 & m+n \text{ は奇数}\end{cases}$$

となる．　□

• 例　$a_{m,n}=\gcd\left(5^m+7^m,\, 5^n+7^n\right)$ とおくと

$$a_{23,5}=a_{13,5}=a_{3,5}=a_{3,1}=a_{1,1},$$

$$a_{24,5}=a_{14,5}=a_{4,5}=a_{4,3}=a_{2,3}=a_{2,1}=a_{0,1}.$$

問題 2.3.12 (IMO 1983)
a,b,c はどの 2 つをとっても互いに素である正の整数とする．
$2abc-ab-bc-ca$ は $xbc+yca+zab$ $(x,y,z\in\mathbb{N}_0)$ と表されない最大の整数であることを示せ．

解答 $2abc-ab-bc-ca=xbc+yca+zab\ (x,y,z\in\mathbb{N}_0)$ と表されたとすると

$$2abc=(x+1)bc+(y+1)ca+(z+1)ab \qquad \cdots\cdots ①$$

と変形できて，$x+1,y+1,z+1\in\mathbb{N}$ となる．

①を　mod a で考えると，$0\equiv(x+1)bc\pmod a$ となる．$\gcd(a,bc)=1$ だから，$x+1\equiv 0\pmod a$ を得る．

同様にして，①を　mod b で考えると，$0\equiv(y+1)ca\pmod b$ となる．$\gcd(b,ca)=1$ だから，$y+1\equiv 0\pmod b$ を得る．

よって，$x+1=ax',y+1=by'\ (x',y'\in\mathbb{N})$ とおき①に代入すると，

$$2abc=x'abc+y'abc+(z+1)ab$$

から

$$z+1=(2-x'-y')c.$$

x',y' は正の整数だから，$2-x'-y'\leq 0$ となり，$z+1=(2-x'-y')c\leq 0$.
これは，$z+1$ が正の整数であることに矛盾する．
したがって，$2abc-ab-bc-ca$ は $xbc+yca+zab\ (x,y,z\in\mathbb{N}_0)$ と表されない．

次に，$2abc-ab-bc-ca$ より大きい正の整数は $xbc+yca+zab\ (x,y,z\in\mathbb{N}_0)$ と表されることを示す．

$k\geq 1$ のとき，$2abc-ab-bc-ca+k=xbc+yca+zab$ を満たす整数 $x,y,z\in\mathbb{N}_0$ が存在することを示せばよい．

$x=a-m,y=b-n$ とおくと，方程式は，

$$2abc-ab-bc-ca+k=(a-m)bc+(b-n)ca+zab$$

から

$$(m-1)bc+(n-1)ca+k=(z+1)ab \qquad \cdots\cdots ②$$

となるから，これを満たす $m\in\left\{1,2,\ldots,a\right\},n\in\left\{1,2,\ldots,b\right\},z\in\mathbb{N}_0$ が存在することを示せばよい．

②を　mod a で考えると，$(m-1)bc+k\equiv 0\pmod a$ となる．

a 個の正の整数 $0\cdot bc+k,1\cdot bc+k,\ldots,(a-1)\cdot bc+k$ を a で割った余りはすべて異なる．
もしも，等しいものがあったとすると，$ibc+k\equiv jbc+k\pmod a\ (0\leq i<j\leq a-1)$ となる整数 i,j が存在する．
合同式から，$(j-i)bc\equiv 0\pmod a$ となり，$\gcd(a,bc)=1$ を使うと，$j-i\equiv 0\pmod a$ を得る．

これから，$j-i$ は a で割り切れるが，$0<j-1\leq a-1$ より不可能である．
したがって，a 個の正の整数 $0\cdot bc+k, 1\cdot bc+k, \ldots, (a-1)\cdot bc+k$ を a で割った余りはすべて異なるから，a 個の正の整数 $0\cdot bc+k, 1\cdot bc+k, \ldots, (a-1)\cdot bc+k$ のなかに a の倍数が一つだけ存在する．
よって，ある $m\in\left\{1,\,2,\,\ldots,\,a\right\}$ が存在して，

$$(m-1)bc+k=ap_1\ (p_1\in\mathbb{N}) \qquad \cdots\cdots③$$

と書ける．

同様にしてで考えると，ある $n\in\left\{1,\,2,\,\ldots,\,b\right\}$ が存在して，

$$(n-1)ca+k=bp_2\ (p_2\in\mathbb{N}) \qquad \cdots\cdots④$$

と書ける．

③から，②の左辺は a で割り切れ，④から，②の左辺は b で割り切れることがわかる．$\gcd(a,b)=1$ なので，結局②の左辺は ab で割り切れるから

$$(m-1)bc+(n-1)ca+k=abq$$

となる正の整数 q が存在する．したがって，$z=q-1\in\mathbb{N}_0$ とおけば，②を満たす $m\in\left\{1,\,2,\,\ldots,\,a\right\}, n\in\left\{1,\,2,\,\ldots,\,b\right\}, z\in\mathbb{N}_0$ が存在することになる． □

IMO の問題を一般化すると次のようになる．

> $a_1, a_2, \ldots, a_n$ はどの 2 つをとっても互いに素である正の整数とする．
> $a_1a_2\cdots a_n\left(n-1-\sum_{k=1}^{n}\frac{1}{a_k}\right)$ は $\sum_{k=1}^{n}x_k\prod_{l\neq k}a_l\quad(x_1,x_2,\ldots,x_n\in\mathbb{N}_0)$ と表されない最大の整数である．

解答 $n=4$ の場合を示す．一般の場合も全く同じである．($n=3$ のときの IMO の問題の解答と本質的におなじである．)

$$\begin{aligned}&3a_1a_2a_3a_4-a_2a_3a_4-a_1a_3a_4-a_1a_2a_4-a_1a_2a_3\\&=x_1a_2a_3a_4+x_2a_1a_3a_4+x_3a_1a_2a_4+x_4a_1a_2a_3\ (x_1,x_2,x_3,x_4\in\mathbb{N}_0)\end{aligned}$$

と表されたとすると

$$\begin{aligned}&3a_1a_2a_3a_4\\&=(x_1+1)a_2a_3a_4+(x_2+1)a_1a_3a_4+(x_3+1)a_1a_2a_4+(x_4+1)a_1a_2a_3 \qquad \cdots\cdots①\end{aligned}$$

と変形できて，$x_1+1, x_2+1, x_3+1, x_4+1\in\mathbb{N}$ となる．

①を　mod a_1 で考えると，$0 \equiv (x_1+1)a_2a_3a_4 \pmod{a_1}$ となる．$\gcd(a_1, a_2a_3a_4) = 1$ だから，$x_1 + 1 \equiv 0 \pmod{a_1}$ を得る．

同様にして，①を　mod a_2，mod a_3 で考えると，$x_2 + 1 \equiv 0 \pmod{a_2}$，$x_3 + 1 \equiv 0 \pmod{a_3}$ を得る．

よって，$x_i + 1 = a_i x_i'$ $(x_i' \in \mathbb{N})$ $(1 \leq i \leq 3)$ とおき①に代入すると，

$$\begin{aligned} &3a_1a_2a_3a_4 \\ &= x_1'a_1a_2a_3a_4 + x_2'a_1a_2a_3a_4 + x_3'a_1a_2a_4a_4 + (x_4+1)a_1a_2a_3 \end{aligned}$$

から

$$x_4 + 1 = (3 - x_1' - x_2' - x_3')a_4.$$

x_1', x_2', x_3' は正の整数だから，$3-x_1'-x_2'-x_3' \leq 0$ となり，$x_4+1 = (3-x_1'-x_2'-x_3')a_4 \leq 0$. これは，$x_4 + 1$ が正の整数であることに矛盾する．

したがって，$3a_1a_2a_3a_4 - a_2a_3a_4 - a_1a_3a_4 - a_1a_2a_4 - a_1a_2a_3$ は $x_1a_2a_3a_4 + x_2a_1a_3a_4 + x_3a_1a_2a_4 + x_4a_1a_2a_3$ $(x_1, x_2, x_3, x_4 \in \mathbb{N}_0)$ と表されない．

次に，$3a_1a_2a_3a_4 - a_2a_3a_4 - a_1a_3a_4 - a_1a_2a_4 - a_1a_2a_3$ より大きい正の整数は

$$x_1a_2a_3a_4 + x_2a_1a_3a_4 + x_3a_1a_2a_4 + x_4a_1a_2a_3 \ (x_1, x_2, x_3, x_4 \in \mathbb{N}_0)$$

と表されることを示す．

このためには，$k \geq 1$ のとき，

$$\begin{aligned} &3a_1a_2a_3a_4 - a_2a_3a_4 - a_1a_3a_4 - a_1a_2a_4 - a_1a_2a_3 + k \\ &= x_1a_2a_3a_4 + x_2a_1a_3a_4 + x_3a_1a_2a_4 + x_4a_1a_2a_3 \end{aligned}$$

を満たす整数 $x_1, x_2, x_3, x_4 \in \mathbb{N}_0$ が存在することを示せばよい．

$x_i = a_i - y_i$ とおくと，方程式は，

$$\begin{aligned} &3a_1a_2a_3a_4 - a_2a_3a_4 - a_1a_3a_4 - a_1a_2a_4 - a_1a_2a_3 + k \\ &= (a_1 - y_1)a_2a_3a_4 + (a_2 - y_2)a_1a_3a_4 + (a_3 - y_3)a_1a_2a_4 + x_4a_1a_2a_3 \end{aligned}$$

から

$$(y_1 - 1)a_2a_3a_4 + (y_2 - 1)a_1a_3a_4 + (y_3 - 1)a_1a_2a_4 + k = (x_4 + 1)a_1a_2a_3 \quad \cdots\cdots ②$$

となるから，これを満たす $y_i \in \left\{1, 2, \ldots, a_i\right\}, x_4 \in \mathbb{N}_0$ $(1 \leq i \leq 3)$ が存在することを示せばよい．

②を　mod a_1 で考えると，$(y_1 - 1)a_2a_3a_4 + k \equiv 0 \pmod{a_1}$ となる．

a_1 個の正の整数

$$0 \cdot a_2a_3a_4 + k, 1 \cdot a_2a_3a_4 + k, \ldots, (a_1 - 1) \cdot a_2a_3a_4 + k$$

を a_1 で割った余りはすべて異なる．
もしも，等しいものがあったとすると，

$$ia_2a_3a_4 + k \equiv ja_2a_3a_4 + k \pmod{a} \ (0 \leq i < j \leq a_1 - 1)$$

となる整数 i, j が存在する．
合同式から，$(j - i))a_2a_3a_4 \equiv 0 \pmod{a_1}$ となり，$\gcd(a_1, a_2a_3a_4) = 1$ を使うと，$j - i \equiv 0 \pmod{a_1}$ を得る．
これから，$j - i$ は a_1 で割り切れるが，$0 < j - 1 \leq a_1 - 1$ より不可能である．
したがって，a_1 個の正の整数

$$0 \cdot a_2a_3a_4 + k, 1 \cdot a_2a_3a_4 + k, \ldots, (a_1 - 1)\cdot)a_2a_3a_4 + k$$

を a_1 で割った余りはすべて異なるから，a_1 個の正の整数

$$0 \cdot a_2a_3a_4 + k, 1 \cdot a_2a_3a_4 + k, \ldots, (a_1 - 1) \cdot a_2a_3a_4 + k$$

のなかに a_1 で割り切れるものが一つだけ存在する．
よって，ある $y_1 \in \left\{1, 2, \ldots, a_1\right\}$ が存在して，

$$(y_1 - 1))a_2a_3a_4 + k = a_1p_1 \ (p_1 \in \mathbb{N}) \qquad \cdots\cdots ③$$

とかける．
同様にしてで考えると，ある $y_2 \in \left\{1, 2, \ldots, a_2\right\}$ が存在して，

$$(y_2 - 1)a_1a_3a_4 + k = a_2p_2 \ (p_2 \in \mathbb{N}) \qquad \cdots\cdots ④$$

とかける．
また，ある $y_3 \in \left\{1, 2, \ldots, a_3\right\}$ が存在して，

$$(y_3 - 1)a_1a_2a_4 + k = a_3p_3 \ (p_3 \in \mathbb{N}) \qquad \cdots\cdots ⑤$$

とかける．③から，②の左辺は a_1 で割り切れ，④から，②の左辺は a_2 で割り切れ，⑤から，②の左辺は a_3 で割り切れることがわかる．a_1, a_2, a_3 からどの 2 つをとっても互いに素なので，結局②の左辺は $a_1a_2a_3$ で割り切れるから

$$(y_1 - 1)a_2a_3a_4 + (y_2 - 1)a_1a_3a_4 + (y_3 - 1)a_1a_2a_4 + k = a_1a_2a_3q$$

となる正の整数 q が存在する．したがって，$x_4 = q - 1 \in \mathbb{N}_0$ とおけば，②を満たす $y_i \in \left\{1, 2, \ldots, a_i\right\}, x_4 \in \mathbb{N}_0 \ (1 \leq i \leq 3)$ が存在することになる． □

問題 3.1.1

(1) p は奇数の素数とする．このとき

$$\sum_{k=1}^{p-1}\left[\frac{k^3}{p}\right]=\frac{(p-2)(p-1)(p+1)}{4}$$

が成り立つことを示せ．(German Mathematical Olympiad 2002)

(2) p は奇数の素数，q は p で割り切れない整数とする．このとき

$$\sum_{k=1}^{p-1}\left[(-1)^k k^2\frac{q}{p}\right]=\frac{(p-1)(q-1)}{2}$$

が成り立つことを示せ．

解答 (1) $f:\mathbb{N}_0\longrightarrow\mathbb{R}$ として $f(x)=x^3$ をとる．

(i) $\dfrac{f(k)}{p}=\dfrac{k^3}{p^2}\notin\mathbb{Z}$ $(k=1,2,\ldots,p-1)$ を満たす．

$$\begin{aligned}f(k)+f(p-k)&=k^3+(p-k)^3\\&=p(p^2-3pk+3k^2)\end{aligned}$$

より，$f(k)+f(p-k)$ は p で割り切れる整数 $(k=1,2,\ldots,p-1)$ となり，(ii) を満たす．

したがって，例題 3.1.3 より，$\displaystyle\sum_{k=1}^{p-1}\left[f(k)\frac{q}{p}\right]=\frac{q}{p}\sum_{k=1}^{p-1}f(k)-\frac{p-1}{2}$ が成り立つから，$f(x)=x^3, q=1$

とおくと

$$\begin{aligned}\sum_{k=1}^{p-1}\left[k^3\frac{1}{p}\right]&=\frac{1}{p}\sum_{k=1}^{p-1}k^3-\frac{p-1}{2}\\&=\frac{1}{p}\left(\frac{(p-1)p}{2}\right)^2-\frac{p-1}{2}=\frac{(p-1)^2p}{4}-\frac{p-1}{2}\\&=\frac{p-1}{4}\big(p(p-1)-2\big)=\frac{(p-1)\left(p^2-p-2\right)}{4}\\&=\frac{(p-1)(p+1)(p-2)}{4}=\frac{(p-2)(p-1)(p+1)}{4}.\end{aligned}$$

(2) $f:\mathbb{N}_0\longrightarrow\mathbb{R}$ として $f(x)=(-1)^x x^2$ をとる．

(i) $\dfrac{f(k)}{p} = \dfrac{(-1)^k k^2}{p^2} \notin \mathbb{Z}$ $(k = 1, 2, \ldots, p-1)$ を満たす.

$$\begin{aligned} f(k) + f(p-k) &= (-1)^2 k^2 + (-1)^{p-k}(p-k)^2 \\ &= (-1)^k \big(k^2 + (-1)^p (p-k)^2\big) \\ &= (-1)^k \big(k^2 - (p-k)^2\big) \\ &= (-1)^k \big(2pk - p^2\big) \\ &= p(-1)^k (2k-p) \end{aligned}$$

より, $f(k) + f(p-k)$ は p で割り切れる整数 $(k = 1, 2, \ldots, p-1)$ となり, (ii) を満たす.

したがって, 例題 3.1.3 より, $\displaystyle\sum_{k=1}^{p-1} \left[f(k)\frac{q}{p} \right] = \frac{q}{p} \sum_{k=1}^{p-1} f(k) - \frac{p-1}{2}$ が成り立つ. ここで,

$$\begin{aligned} \sum_{p-1}^{k=1} (-1)^k k^2 &= -1^2 + 2^2 - 3^2 + 4^2 \cdots + (-1)^{p-2}(p-2)^2 + (-1)^{p-1}(p-1)^2 \\ &= \big(2^2 - 1^2\big) + \big(4^2 - 3^2\big) + \cdots + \big((p-1)^2 - (p-2)^2\big) \\ &= (2+1) + (4+3) + \cdots + (p-1+p-2) \\ &= (1 + 2 + \cdots + (p-2) + (p-1)) \\ &= \frac{(p-1)p}{2}. \end{aligned}$$

したがって

$$\begin{aligned} \sum_{k=1}^{p-1} \left[(-1)^k k^2 \frac{q}{p} \right] &= \frac{q}{p} \sum_{k=1}^{p-1} (-1)^k k^2 - \frac{p-1}{2} \\ &= \frac{q}{p} \cdot \frac{(p-1)p}{2} - \frac{p-1}{2} \\ &= \frac{(p-1)(q-1)}{2}. \end{aligned}$$

□

問題 3.1.2

(1) 次のことを示せ.

(a) x が整数ならば, $[x] + [-x] = 0$.

(b) x が整数でなければ, $[x] + [-x] = -1$.

(2) p と q が互いに素な整数のとき

$$\left[\frac{p}{q} \right] + \left[\frac{2p}{q} \right] + \cdots + \left[\frac{(q-1)p}{q} \right] = \frac{(p-1)(q-1)}{2}$$

が成り立つことを示せ.

解答

(1) (a) x が整数のとき，$[x]+[-x]=x+(-x)=0$.

(b) x が整数でないときは，$[x]=n$ とおくと，$n<x<n+1$ となるから，$-n-1<-x<-n$.

よって，$[-x]=-n-1$ だから，$[x]+[-x]=n+(-n-1)=-1$.

(2) $\gcd(p,q)=1$ だから，$\dfrac{kp}{q}$ $(k=1,2,\ldots,q-1)$ は整数ではない．$1\leq k\leq q-1$ に対して

$$\begin{aligned}\left[\frac{kp}{q}\right]+\left[\frac{(q-k)p}{q}\right]&=\left[\frac{kp}{q}\right]+\left[p-\frac{kp}{q}\right]\\&=\left[\frac{kp}{q}\right]+p+\left[-\frac{kp}{q}\right]\\&=p-1.\quad\cdots\cdots(*)\end{aligned}$$

ここで，p は整数だから，$[p+\alpha]=p+[\alpha]$ が成り立つことから，

$$\left[p-\frac{kp}{q}\right]=p+\left[-\frac{kp}{q}\right].$$

また，$\dfrac{kp}{q}$ $(k=1,2,\ldots,q-1)$ は整数ではないから，(1) (b) より，

$$\left[\frac{kp}{q}\right]+\left[-\frac{kp}{q}\right]=-1$$

であることを用いている．

$(*)$ で，$k=1,2,\ldots,q-1$ とおいた $q-1$ 個の等式を辺々加えると

$$\sum_{k=1}^{q-1}\left[\frac{pk}{q}\right]+\sum_{k=1}^{q-1}\left[\frac{p(q-k)}{q}\right]=(p-1)(q-1)$$

すなわち

$$2\sum_{k=1}^{q-1}\left[\frac{pk}{q}\right]=(p-1)(q-1)$$

から

$$\sum_{k=1}^{q-1}\left[\frac{pk}{q}\right]=\frac{(p-1)(q-1)}{2}$$

を得る．　□

問題 3.1.3　n が正の整数のとき

$$\sum_{k=0}^{\infty}\left[\frac{n+2^k}{2^{k+1}}\right]=n$$

を示せ.

解答 無限級数ではなく有限級数であることに注意しよう.
エルミートの恒等式 $\left[t+\frac{1}{2}\right]=[2t]-[t]$ を使うと

$$\left[\frac{n+2^k}{2^{k+1}}\right]=\left[\frac{n}{2^{k+1}}+\frac{1}{2}\right]=\left[\frac{n}{2^k}\right]-\left[\frac{n}{2^{k+1}}\right]$$

となるから

$$\begin{aligned}\sum_{k=0}^{\infty}\left[\frac{n+2^k}{2^{k+1}}\right]&=\sum_{k=0}^{\infty}\left(\left[\frac{n}{2^k}\right]-\left[\frac{n}{2^{k+1}}\right]\right)\\&=\left([n]-\left[\frac{n}{2}\right]\right)+\left(\left[\frac{n}{2}\right]-\left[\frac{n}{2^2}\right]\right)+\cdots\cdots\\&=[n]=n.\end{aligned}$$

□

注　x が実数のとき，$\sum\limits_{k=0}^{\infty}\left[\frac{x+2^k}{2^{k+1}}\right]=[x]$ が成り立つ.

問題 3.1.4　n が正の整数，x が実数のとき

$$\sum_{0\le i<j\le n}\left[\frac{x+i}{j}\right]$$

を簡単にせよ.

解答　$S_n=\sum\limits_{0\le i<j\le n}\left[\frac{x+i}{j}\right]$ とおくと

$$S_n-S_{n-1}=\left[\frac{x}{n}\right]+\left[\frac{x}{n}+\frac{1}{n}\right]+\cdots+\left[\frac{x}{n}+\frac{n-1}{n}\right].$$

エルミートの恒等式から

$$\left[\frac{x}{n}\right]+\left[\frac{x}{n}+\frac{1}{n}\right]+\cdots+\left[\frac{x}{n}+\frac{n-1}{n}\right]=\left[n\cdot\frac{x}{n}\right]=[x].$$

よって，$S_n-S_{n-1}=[x]$ となる．また，$S_1=[x]$ だから，$S_n=n[x]$ となり

$$\sum_{0\le i<j\le n}\left[\frac{x+i}{j}\right]=n[x].$$

□

問題 3.1.5　n が正の整数，x が実数のとき

$$\sum_{k=0}^{2000}\left[\frac{3^k+2000}{3^{k+1}}\right]-\sum_{k=0}^{2000}\left[\frac{3^k-2000}{3^{k+1}}\right]$$

を簡単にせよ．

解答 エルミートの恒等式と問題 3.1.2(1)(b) を使う．

$$\sum_{k=0}^{2000}\left[\frac{3^k+2000}{3^{k+1}}\right]-\sum_{k=0}^{2000}\left[\frac{3^k-2000}{3^{k+1}}\right]=\sum_{k=0}^{2000}\left(\left[\frac{1}{3}+\frac{2000}{3^{k+1}}\right]-\left[\frac{1}{3}-\frac{2000}{3^{k+1}}\right]\right)$$

と変形し，$x_k=\dfrac{2000}{3^{k+1}}$ $(k=0,1,\ldots,2000)$ とおき

$$S=\sum_{k=0}^{2000}\left(\left[\frac{1}{3}+x_k\right]-\left[\frac{1}{3}-x_k\right]\right)$$

を求めればよい．

- $0\le k\le 2000$ のとき，$\dfrac{1}{3}-x_k=\dfrac{3^k-2000}{3^{k+1}}$ は整数にならないことを示す．

もしも，$\dfrac{1}{3}-x_k=\dfrac{3^k-2000}{3^{k+1}}$ が整数になることがあったとすると，$\dfrac{3^k-2000}{3^{k+1}}=l$ $(l\in\mathbb{Z})$ とおける．この式を変形すると

$$3^k(1-3l)=2000. \qquad \cdots ①$$

$k=0$ のとき，①を満たす整数 l は存在しない．

$0<k\le 2000$ のとき，2000 は 3 の倍数ではないから①を満たす整数 l は存在しない．

問題 3.1.2(1)(b) より，x が整数でないときは $-[x]=[-x]+1$ が成り立つから，$x=\dfrac{1}{3}-x_k$ とおくと

$$-\left[\frac{1}{3}-x_k\right]=\left[-\frac{1}{3}+x_k\right]+1.$$

よって

$$S=\sum_{k=0}^{2000}\left(\left[\frac{1}{3}+x_k\right]+\left[x_k-\frac{1}{3}\right]+1\right)$$

となる．

エルミートの恒等式

$$[x]+\left[x+\frac{1}{3}\right]+\left[x+\frac{2}{3}\right]=[3x]$$

において $x=x_k-\dfrac{1}{3}$ とおくと

$$\left[x_k-\frac{1}{3}\right]+[x_k]+\left[x_k+\frac{1}{3}\right]=\left[3\left(x_k-\frac{1}{3}\right)\right]=[3x_k-1]=[3x_k]-1.$$

よって

$$\left[x_k-\frac{1}{3}\right]+\left[x_k+\frac{1}{3}\right]+1=[3x_k]-[x_k]$$

から

$$\begin{aligned}
S&=\sum_{k=0}^{2000}\left(\left[\frac{1}{3}+x_k\right]+\left[x_k-\frac{1}{3}\right]+1\right)\\
&=\sum_{k=0}^{2000}\left([3x_k]-[x_k]\right)\\
&=\sum_{k=0}^{2000}\left(\left[\frac{2000}{3^k}\right]-\left[\frac{2000}{3^{k+1}}\right]\right)\\
&=[2000]-\left[\frac{2000}{3}\right]+\left[\frac{2000}{3}\right]-\left[\frac{2000}{3^2}\right]+\cdots+\left[\frac{2000}{3^{2000}}\right]-\left[\frac{2000}{3^{2001}}\right]\\
&=[2000]-\left[\frac{2000}{3^{2001}}\right]\\
&=2000.
\end{aligned}$$

□

問題 3.1.6　n が正の整数のとき

$$\left[\frac{n}{3}\right]+\left[\frac{n+2}{6}\right]+\left[\frac{n+4}{6}\right]=\left[\frac{n}{2}\right]+\left[\frac{n+3}{6}\right]$$

が成り立つことを証明せよ.

解答 エルミートの恒等式

$$[x]+\left[x+\frac{1}{3}\right]+\left[x+\frac{2}{3}\right]=[3x],[x]+\left[x+\frac{1}{2}\right]=[2x]$$

を用いると,

$$\begin{aligned}
\left[\frac{n}{3}\right]+\left[\frac{n+2}{6}\right]+\left[\frac{n+4}{6}\right]+\left[\frac{n}{6}\right]&=\left[\frac{n}{3}\right]+\left[\frac{n}{6}\right]+\left[\frac{n}{6}+\frac{1}{3}\right]+\left[\frac{n}{6}+\frac{2}{3}\right]\\
&=\left[\frac{n}{3}\right]+\left[3\cdot\frac{n}{6}\right]\\
&=\left[\frac{n}{3}\right]+\left[\frac{n}{2}\right],\\
\left[\frac{n}{2}\right]+\left[\frac{n+3}{6}\right]+\left[\frac{n}{6}\right]&=\left[\frac{n}{2}\right]+\left[\frac{n}{6}\right]+\left[\frac{n}{6}+\frac{1}{2}\right]\\
&=\left[\frac{n}{2}\right]+\left[2\cdot\frac{n}{6}\right]\\
&=\left[\frac{n}{3}\right]+\left[\frac{n}{2}\right].
\end{aligned}$$

よって, $\left[\frac{n}{3}\right]+\left[\frac{n+2}{6}\right]+\left[\frac{n+4}{6}\right]=\left[\frac{n}{2}\right]+\left[\frac{n+3}{6}\right]$. □

問題 3.1.7 (Romania MO 2004)

(1) 次の方程式は有理数の解を無数にもつことを示せ.

$$\{x^2\} + \{x\} = 0.99.$$

(2) 次の方程式は正の有理数解をもたないことを示せ.

$$\left\{x^2\right\} + \{x\} = 1.$$

解答 (1) $x = \dfrac{a}{10}$ $(a \in \mathbb{N})$ とおくと

$\{x^2\} + \{x\} = 0.99 \Longleftrightarrow x^2 - \left[x^2\right] + x - [x] = \dfrac{99}{100}$ から

$$\frac{a^2}{100} - \left[\frac{a^2}{100}\right] + \frac{a}{10} - \left[\frac{a}{10}\right] = \frac{99}{100}.$$

よって

$$\frac{a^2 + 10a - 99}{100} = \left[\frac{a^2}{100}\right] + \left[\frac{a}{10}\right] \text{ は整数}$$

$a = 10b + r$ $(0 \leq r < 10)$ とおくと

$$\frac{a^2 + 10a - 99}{100} = b^2 + b + \frac{20br + 10r + r^2 - 99}{100}$$

となるから，$r = 3$ とおくと

$$\frac{20br + 10r + r^2 - 99}{100} = \frac{60b + 30 - 90}{100} = \frac{3(b-1)}{5}.$$

$b - 1 = 5m$ $(m \in \mathbb{N}_0)$ とおくと，$a = 10(5m+1) + 3 = 50m + 13$ より

$x = \dfrac{5m + 13}{10}$ $(m \in \mathbb{N}_0)$ は解になるから，方程式は有理数の解を無数にもつ.

(1) $\left\{x^2\right\} + \{x\} = 1$ から

$$x^2 - \left[x^2\right] + x - [x] = 1 \qquad x^2 + x = \left[x^2\right] + [x] + 1 \in \mathbb{Z}. \qquad \cdots ②$$

$x = \dfrac{p}{q}$ $(p, q \in \mathbb{N}, \gcd(p,q) = 1)$ とおくと，$x^2 + x = \dfrac{p(p+q)}{q^2} \in \mathbb{N}.$

$\dfrac{p(p+q)}{q^2} \in \mathbb{N}$ から $q \cdot \dfrac{p(p+q)}{q^2} = \dfrac{p^2}{q} + p \in \mathbb{N}$ すなわち $\dfrac{p^2}{q} \in \mathbb{Z}.$

p と q は互いに素だから $q = 1$ で，x は整数となり，$\left\{x^2\right\} + \{x\} = 1$ は $0 + 0 = 1$ となり成り立たない. □

問題 4.1.1 $n \in \mathbb{N}_0$ として，N を十進法 (じっしんほう) でかかれた $n+1$ 桁の正の整数

$$\begin{aligned} N &= a_n a_{n-1} \dots a_1 a_{0(10)} = \overline{a_n a_{n-1} \dots a_1 a_0} \\ &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \end{aligned}$$

とすると，次のことが成り立つことを示せ.

(1) N が 2 の倍数 $\iff$ 下 1 桁 (しもひとけた) が 2 の倍数
(2) N が 3 の倍数 $\iff$ $a_0 + a_1 + \cdots + a_n$ が 3 の倍数
(3) N が 4 の倍数 $\iff$ 下 2 桁 (しもふたけた) が 4 の倍数
(4) N が 5 の倍数 $\iff$ 下 1 桁 (しもひとけた) が 0 か 5
(5) N が 8 の倍数 $\iff$ 下 3 桁 (しもみけた) が 8 の倍数
(6) N が 9 の倍数 $\iff$ $a_0 + a_1 + \cdots + a_n$ が 9 の倍数
(7) N が 11 の倍数 $\iff$ $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$ が 11 の倍数

解答

(1) $10 \equiv 0 \pmod 2$ であるから

$$\begin{aligned} N &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot 0^n + a_{n-1} \cdot 0^{n-1} + \cdots + a_1 \cdot 0 + a_0 \\ &\equiv a_0 \pmod 2 \end{aligned}$$

であるから，

N が 2 の倍数 $\iff$ $a_0 \equiv 0 \pmod 2$ $\iff$ 下 1 桁 (しもひとけた) が 2 の倍数

(2) $10 \equiv 1 \pmod 3$ であるから

$$\begin{aligned} N &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot 1^n + a_{n-1} \cdot 1^{n-1} + \cdots + a_1 \cdot 1 + a_0 \\ &\equiv a_0 + a_1 + \cdots + a_n \pmod 3 \end{aligned}$$

であるから，

N が 3 の倍数 $\iff a_0 + a_1 + \cdots + a_n \equiv 0 \pmod 3 \iff a_0 + a_1 + \cdots + a_n$ が 3 の倍数

(3) $10^2 \equiv 0 \pmod 4$ であるから

$$\begin{aligned} N &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot 0^n + \cdots + a_2 \cdot 0 + a_1 \cdot 10 + a_0 \\ &\equiv a_1 \cdot 10 + a_0 \pmod 4 \end{aligned}$$

であるから，

N が 4 の倍数 $\Longleftrightarrow a_1 \cdot 10 + a_0 \equiv 0 \pmod 4 \Longleftrightarrow$ 下 2 桁 $\overline{a_1 a_0}$ が 4 の倍数

(4) $10 \equiv 0 \pmod 5$ であるから

$$\begin{aligned} N &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot 0^n + a_{n-1} \cdot 0^{n-1} + \cdots + a_1 \cdot 0 + a_0 \\ &\equiv a_0 \pmod 5 \end{aligned}$$

であるから，

N が 5 の倍数 $\Longleftrightarrow a_0 \equiv 0 \pmod 5 \Longleftrightarrow$ 下 1 桁が 0 か 5

(5) $10^3 \equiv 0 \pmod 8$ であるから

$$\begin{aligned} N &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot 0^n + \cdots + a_3 \cdot 0^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \pmod 8 \end{aligned}$$

であるから，

N が 8 の倍数 $\Longleftrightarrow a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv 0 \pmod 8 \Longleftrightarrow$ 下 3 桁 $\overline{a_2 a_1 a_0}$ が 8 の倍数

(6) $10 \equiv 1 \pmod 9$ であるから

$$\begin{aligned} N &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot 1^n + a_{n-1} \cdot 1^{n-1} + \cdots + a_1 \cdot 1 + a_0 \\ &\equiv a_0 + a_1 + \cdots + a_n \pmod 9 \end{aligned}$$

であるから，

N が 9 の倍数 $\Longleftrightarrow a_0 + a_1 + \cdots + a_n \equiv 0 \pmod 9 \Longleftrightarrow a_0 + a_1 + \cdots + a_n$ が 9 の倍数

(7) $10 \equiv -1 \pmod{11}$ であるから

$$\begin{aligned} N &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \cdots + a_1 \cdot (-1) + a_0 \\ &\equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \pmod{11} \end{aligned}$$

であるから，

N が 11 の倍数 $\Longleftrightarrow a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \equiv 0 \pmod{11} \Longleftrightarrow a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$ が 11 の倍数　□

問題 4.1.2 どのような負でない 2 つの整数 m と n をもちいても $x = 3m + 5n$ とは表すことができない正の整数 x をすべて求めよ.

(2000 大阪大・理・医・歯・薬・工・基礎工・前期)

● 問題 2.3.2，問題 2.3.3 も参照.

解 1 例題 4.1.1 の表を参考にする.

(i) $x = 3l$ $(l = 1, 2, \dots)$ のとき

$$x = 3l = 3 \cdot l + 5 \cdot 0$$

より，$x = 3m + 5n$ $(m, n \in \mathbb{N}_0)$ と表せる.

(ii) $x = 3l + 1$ $(l = 0, 1, \dots)$ のとき

$$x = 3l + 1 = 3 \cdot (l - 3) + 5 \cdot 2$$

より，$l \geq 3$ のとき，$x = 3m + 5n$ $(m, n \in \mathbb{N}_0)$ と表せる.

$l = 0, 1, 2$ すなわち，$x = 1, 4, 7$ は $x = 3m + 5n$ $(m, n \in \mathbb{N}_0)$ と表せるかどうかは不明.

(iii) $x = 3l + 2$ $(l = 0, 1, \dots)$ のとき

$$x = 3l + 2 = 3 \cdot (l - 1) + 5 \cdot 1$$

より，$l \geq 1$ のとき，$x = 3m + 5n$ $(m, n \in \mathbb{N}_0)$ と表せる.

$l = 0$ すなわち，$x = 2$ は $x = 3m + 5n$ $(m, n \in \mathbb{N}_0)$ と表せるかどうかは不明.

したがって，残るのは $x = 1, 2, 4, 7$ であるが

$3m$ の取り得る値は，$0, 3, 6, 9, \dots$,

$5n$ の取り得る値は，$0, 5, 10, 15, \dots$

であるから，$x = 1, 2, 4, 7$ は $x = 3m + 5n$ $(m, n \in \mathbb{N}_0)$ と表せない.

以上のことから，$x = 3m + 5n$ $(m, n \in \mathbb{N}_0)$ と表すことができない正の整数 x は，$x = 1, 2, 4, 7$. □

解 2　x は正の整数とする.

$$3m + 5n = x \qquad \cdots\cdots ①$$

とおく．$3 \cdot 2 + 5 \cdot (-1) = 1$ から

$$3 \cdot 2x + 5 \cdot (-x) = x. \qquad \cdots\cdots ②$$

① − ② より

$$3(m - 2x) = -5(n + x).$$

3 と 5 は互いに素だから，k を整数として，$m-2x=-5k, n+x=3t$ すなわち

$$m=2x-5k, n=-x+3k$$

と書ける．$m\geq 0, n\geq 0$ だから，

$$\frac{x}{3}\leq k\leq \frac{2x}{5}. \qquad \cdots\cdots ③$$

これを満たす整数 k が存在することが，$x=3m+5n$ $(m,n\in\mathbb{N}_0)$ と表せることと同値である．

(a) $\dfrac{x}{3}$ または $\dfrac{2x}{5}$ が整数のときは，③を満たす整数 k が存在する．

(b) $\dfrac{x}{3}$ も $\dfrac{2x}{5}$ も整数でないときは，③のかわりに

$$\frac{x-1}{3}<k<\frac{2x+1}{5} \qquad \cdots\cdots ④$$

を考えて，

$$\frac{2x+1}{5}-\frac{x-1}{3}=\frac{x+8}{15}>1$$

すなわち，$x>7$ のときは，④を満たす整数 k が存在する．

(a), (b) より，$x=3,5,6$, $x\geq 8$ のときは $x=3m+5n$ $(m,n\in\mathbb{N}_0)$ と表せる．

したがって，残るのは $x=1,2,4,7$ であるが

$3m$ の取り得る値は，$0,3,6,9,\ldots,$

$5n$ の取り得る値は，$0,5,10,15,\ldots$

であるから，$x=1,2,4,7$ は $x=3m+5n$ $(m,n\in\mathbb{N}_0)$ と表せない．

以上のことから，$x=3m+5n$ と表すことができない正の整数 x は，$x=1,2,4,7$. □

注 ④を考えずに，③で，

$$\frac{2x}{5}-\frac{x}{3}=\frac{x}{15}\geq 1$$

すなわち，$x\geq 15$ のときは，③を満たす整数 k が存在することがわかる．したがって，残りの $1\leq x\leq 15$ について，$x=3m+5n$ と表せるかどうか調べてもよい．

解 3　$8=3\cdot 1+5\cdot 1, 9=3\cdot 3+5\cdot 0, 10=3\cdot 0+5\cdot 2$ となり $x=8,9,10$ は $x=3m+5n$ $(m,n\in\mathbb{N}_0)$ と表せる．

x が $x=3m+5n$ $(m,n\in\mathbb{N}_0)$ と表せたとすると，$x+3=3(m+1)+5n$ と表せるから，$x+3$ は $x+3=3m'+5n'$ $(m',n'\in\mathbb{N}_0)$ と表せる．

以上のことから，$x\geq 8$ のとき，x は $x=3m+5n$ $(m,n\in\mathbb{N}_0)$ と表せることがわかった．

残るのは $1\leq x\leq 7$ のときであるが，

$3m$ の取り得る値は，$0, 3, 6, 9, \ldots$，　$5n$ の取り得る値は，$0, 5, 10, 15, \ldots$
であるから，$x = 1, 2, 4, 7$ は $x = 3m + 5n$ $(m, n \in \mathbb{N}_0)$ と表せない．

以上のことから，$x = 3m + 5n$ と表すことができない正の整数 x は，$x = 1, 2, 4, 7$．　□

問題 4.1.3　n を自然数とする．以下の各問いに答えよ．

(1) n を 3 で割った余りが 1 であるならば，すべての自然数 m に対して n^m を 3 で割った余りは 1 であることを示せ．
(2) n を 3 で割った余りが 2 であるならば，すべての奇数 m に対して n^m を 3 で割った余りは 2 であることを示せ．
(3) n^m を 3 で割った余りが 2 となる自然数 m があれば，n を 3 で割った余りも 2 であることを示せ．　(2007 お茶の水女子大・理・前期)

解答

(1) $n \equiv 1 \pmod 3$ のとき，$n^m \equiv 1^m \equiv 1 \pmod 3$.
(2) $n \equiv 2 \equiv -1 \pmod 3$ のとき，m は奇数だから，$n^m \equiv (-1)^m \equiv -1 \equiv 2 \pmod 3$.
(3) (i) $n \equiv 0 \pmod 3$ のとき，$n^m \equiv 0^m \equiv 0 \pmod 3$.
n^m を 3 で割った余りは 0 で 2 とはならない．(ii) $n \equiv 1 \pmod 3$ のとき，$n^m \equiv 1^m \equiv 1 \pmod 3$.
n^m を 3 で割った余りは 1 となり 2 とはならない．(iii) $n \equiv 2 \equiv -1 \pmod 3$ のとき，$n^m \equiv (-1)^m \pmod 3$.
m が奇数ならば，$n^m \equiv (-1)^m \equiv -1 \equiv 2 \pmod 3$.
n^m を 3 で割った余りがは 2 となる．
m が偶数ならば，$n^m \equiv (-1)^m \equiv 1 \pmod 3$.
n^m を 3 で割った余りは 1 となり 2 とはならない．
したがって，n^m を 3 で割った余りが 2 となる自然数 m があれば，n を 3 で割った余りも 2 である．　□

問題 4.3.1 選択肢から最も適切なものを選びその番号を解答欄に記入しなさい．
相異なる自然数 a と b が 1 以外に共通の約数を持たないとき，a と b は互いに素であるという．自然数 n を素数 p で割った余りを $M_p(n)$ で表すことにする．また $p-1$ 以下の自然数 x, y に対して $x \otimes y = M_p(xy)$ と演算 $\otimes$ を定義する．ただし右辺の xy は通常の積である．例えば，$M_{11}\left(6 \times \boxed{\text{ア}}\right) = 2$ である．この演算 $\otimes$ は交換法則 $\boxed{\text{イウ}}$ や結合法則 $\boxed{\text{エオ}}$ を満たす．ここで，x, y, z は $p-1$ 以下の然数である．

次の命題はフェルマーの小定理と呼ばれている．

命題　自然数 a と素数 p が互いに素ならば a^{p-1} を p で割った余りは 1 である．

この命題を証明しよう．上の記号を用いれば $M_p\left(\boxed{\text{カ}}\right) = \boxed{\text{キ}}$ を示せばよい．以下，M_p の添字 p は省略する．x, y は $p-1$ 以下の然数とする．

$M(ax) = M(ay)$ ならば $a(x-y)$ は $\boxed{\text{クケ}}$ の $\boxed{\text{コサ}}$ となる．よって $x = y$ でなければならない．この $\boxed{\text{シス}}$ を考えれば，$\boxed{\text{セソ}}$ ならば $\boxed{\text{タチ}}$ である．このことから

$$M(1a),\ M(2a),\ \ldots\ldots,\ M((p-1)a)$$

は異なった自然数である．よって

$$M(1a) \otimes M(2a) \otimes \cdots\cdots \otimes M((p-1)a) = 1 \otimes 2 \otimes \cdots\cdots \otimes \boxed{\text{ツテ}}$$

となる．

一方，M の性質を使えば

$$M(1a) \otimes M(2a) \otimes \cdots\cdots \otimes M((p-1)a) = M\left(\boxed{\text{ト}}\right) \otimes 1 \otimes 2 \otimes \cdots\cdots \otimes \boxed{\text{ナニ}}$$

となる．$x \otimes y = y$ のとき，$x = \boxed{\text{ヌ}}$ となることに注意すれば，$M\left(\boxed{\text{カ}}\right) = \boxed{\text{キ}}$ を得る．

[選択肢]

(1) 1　(2) 2　(3) 3　(4) 4　(5) 0

(6) a　(7) a^{p-1}　(8) a^p　(9) a^{p+1}　(10) $x-y$

(11) $x \otimes y$　(12) xy　(13) $x+y$

(14) $x \neq y$　(15) $M(ax) = M(ay)$　(16) $x = y$

(17) $p+1$　(18) p　(19) $p-1$

(20) $M(ax) \neq M(ay)$　(21) 逆　(22) 対偶

(23) 裏　(24) 否定　(25) 矛盾

(26) 倍数　(27) 約数　(28) 素数

(29) 互いに素　(30) $p-1$ 以下　(31) $x \otimes y = 0$

(32) $x \otimes y = y \otimes x$　(33) $x \otimes y \otimes z = y \otimes z \otimes x = z \otimes x \otimes y$

(34) $x \otimes (y \otimes z) = (x \otimes y) \otimes z$　(35) $x \otimes (y+z) = x \otimes y + x \otimes z$

(2005 慶応大・総合政策)

解答 (省略)

相異なる自然数 a と b が 1 以外に共通の約数を持たないとき，a と b は互いに素である

という．自然数 n を素数 p で割った余りを $M_p(n)$ で表すことにする．また $p-1$ 以下の自然数 x, y に対して $x \otimes y = M_p(xy)$ と演算 $\otimes$ を定義する．ただし右辺の xy は通常の積である．例えば，$M_{11}\left(6 \times \boxed{4}\right) = 2$ である．この演算 $\otimes$ は交換法則 $\boxed{x \otimes y = y \otimes x}$ や結合法則 $\boxed{x \otimes (y \otimes z) = (x \otimes y) \otimes z}$ を満たす．ここで，x, y, z は $p-1$ 以下の然数である．

次の命題はフェルマーの小定理と呼ばれている．

命題　自然数 a と素数 p が互いに素ならば a^{p-1} を p で割った余りは 1 である．

この命題を証明しよう．上の記号を用いれば $M_p\left(\boxed{a^{p-1}}\right) = \boxed{1}$ を示せばよい．以下，M_p の添字 p は省略する．x, y は $p-1$ 以下の然数とする．

$M(ax) = M(ay)$ ならば $a(x-y)$ は $\boxed{p}$ の $\boxed{\text{倍数}}$ となる．よって $x = y$ でなければならない．この $\boxed{\text{対偶}}$ を考えれば，$\boxed{x \neq y}$ ならば $\boxed{M(ax) \neq M(ay)}$ である．このことから

$$M(1a),\ M(2a),\ \ldots\ldots,\ M((p-1)a)$$

は異なった自然数である．よって

$$M(1a) \otimes M(2a) \otimes \cdots\cdots \otimes M((p-1)a) = 1 \otimes 2 \otimes \cdots\cdots \otimes \boxed{p-1}$$

となる．

一方，M の性質を使えば

$$M(1a) \otimes M(2a) \otimes \cdots\cdots \otimes M((p-1)a) = M\left(\boxed{a^{p-1}}\right) \otimes 1 \otimes 2 \otimes \cdots\cdots \otimes \boxed{p-1}$$

となる．$x \otimes y = y$ のとき，$x = \boxed{1}$ となることに注意すれば，$M\left(\boxed{a^{p-1}}\right) = \boxed{1}$ を得る．

□

問題 4.6.1 正の奇数 p に対して，3 つの自然数の組 (x, y, z) で，$x^2 + 4yz = p$ を満たすものの全体の集合を S とおく．すなわち，

$$S = \left\{(x,\ y,\ z)\,|\,x,\ y,\ z \text{ は自然数},\ x^2 + 4yz = p\right\}$$

次の問いに答えよ．

(1) S が空集合でないための必要十分条件は，$p = 4k + 1$ (k は自然数) と書けることであることを示せ．

(2) S の要素の個数が奇数ならば S の要素 (x, y, z) で $y = z$ となるものが存在することを示せ．　(2012　旭川医大)

解答　$x^2+4yz=p$ ……①

とおく．

(1) S が空集合ではないと仮定すると，①を満たす自然数 x,y,z が存在する．

$x\equiv 0 \pmod 2$ のとき，$4\mid x^2, 4\mid 4yz$ より $4\mid x^2+4yz=p$．これは p が正の奇数であることに矛盾する．

よって，x は奇数であり，$x^2\equiv 1 \pmod 4$ が成り立つ．

このとき，$p=x^2+4yz\equiv 1+0\equiv 1 \pmod 4$.

したがって，$p=4k+1$ (k は自然数) と書ける．

$p=4k+1$ (k は自然数) と書けるとする．

$x^2+4yz=4k+1$ を満たす自然数の組 (x,y,z) の 1 つとして，$(x,y,z)=(1,1,k)$ がとれるので，S は空集合ではない．

(2) S のすべての要素 (x,y,z) に対して，$y\neq z$ であると仮定する．①は y,z に関して対称だから，$(x,y,z)\in S$ のとき，$(x,z,y)\in S$ である．

$$S_1=\left\{(x,\,y,\,z)\,\middle|\,x,\,y,\,z \text{ は自然数},\ x^2+4yz=p,\ y>z\right\},$$
$$S_2=\left\{(x,\,y,\,z)\,\middle|\,x,\,y,\,z \text{ は自然数},\ x^2+4yz=p,\ y<z\right\}$$

とおくと，$|S_1|=|S_2|$ より，S の要素の個数が偶数となり，S の要素の個数が奇数であることに矛盾する．

したがって，S の要素の個数が奇数ならば S の要素 (x,y,z) で $y=z$ となるものが存在する．　□

問題 4.7.1　$a_1 = 7,\ a_n = 7^{a_{n-1}}$ で定義される数列 $\{a_n\}$ において，a_{1001} の下 2 桁を求めよ．

解答　$a_0 = 1$ と定義しておく．$a_n > a_{n-1}$ だから，

$$a_{n+1} - a_n = 7^{a_n} - 7^{a_{n-1}} = 7^{a_{n-1}} \left(7^{a_n - a_{n-1}} - 1\right)$$

と変形できる．a_n, a_{n-1} は奇数だから，$a_n - a_{n-1}$ は偶数となり，$7^2 - 1 \mid 7^{a_n - a_{n-1}} - 1$ が成り立つので，

$$16 \mid 48 = 7^2 - 1 \mid 7^{a_n - a_{n-1}} - 1$$

すなわち

$$a_{n+1} \equiv a_n \pmod{16} \qquad \cdots\cdots (*)$$

を得る．

$n \geq 2$ のとき，

$$a_{n+2} \equiv a_{n+1} \pmod{100} \quad \text{すなわち} \quad 7^{a_{n+1}} \equiv 7^{a_n} \pmod{100} \qquad \cdots\cdots ①$$

が成り立つことを示したい．

$\gcd(7, 100) = 1,\ \varphi(100) = \varphi\left(5^2 \cdot 2^2\right) = \varphi\left(5^2\right)\varphi\left(2^2\right) = \left(5^2 - 5\right)\left(2^2 - 2\right) = 40$ だから，①が成り立つことを示すためには，

$$a_{n+1} \equiv a_n \pmod{40} \quad \text{すなわち} \quad 7^{a_n} \equiv 7^{a_{n-1}} \pmod{40} \qquad \cdots\cdots ②$$

が成り立てばよい．

$\gcd(7, 40) = 1,\ \varphi(40) = \varphi\left(2^3 \cdot 5\right) = \varphi\left(2^3\right)\varphi(5) = \left(2^3 - 2^2\right)(5 - 1) = 16$ だから，②が成り立つことを示すためには，

$$a_n \equiv a_{n-1} \pmod{16} \qquad \cdots\cdots ③$$

が成り立てばよい．$(*)$ より，③は $n \geq 2$ のとき成り立つことがわかる．

①が $n \geq 2$ のとき成り立つから，$a_3 \equiv a_4 \equiv \cdots \pmod{100}$ より，

$$a_{1001} \equiv a_3 \pmod{100}.$$

100 を法として $a_3 = 7^{7^7}$ を考える．$100 = 25 \cdot 4$ だから，a_3 を 25 で割った余りと，4 で割った余りを求める．

$\varphi(25) = 5^2 - 5 = 20$ であるから，7^7 を 20 で割った余りを求める．

$$7^2 \equiv 9, 7^3 \equiv 3, 7^4 \equiv 1, 7^5 \equiv 7, 7^6 \equiv 9, 7^7 \equiv 3 \pmod{20}$$

と，$\gcd(7,25)=1$ より

$$a_3 = 7^{7^7} \equiv 7^3 \pmod{25}.$$

さらに計算すると，$7^3 \equiv 7^2 \cdot 7 \equiv (-1)\cdot 7 \equiv 18 \pmod{25}$ となるから，

$$a_3 \equiv 18 \pmod{25}. \qquad \cdots\cdots ④$$

次に．a_3 を 4 で割った余りを求める．$\varphi(4) = 2^2 - 2 = 2$ であるから，7^7 を 2 で割った余りを求める．

$$7^7 \equiv 1^7 \equiv 1 \pmod{2}$$

と，$\gcd(7,4)=1$ より

$$a_3 = 7^{7^7} \equiv 7^1 \equiv 3 \pmod{4}. \qquad \cdots\cdots ⑤$$

④，⑤より，$a_3 = 25l + 18 = 4m + 3$ $(l, m \in \mathbb{Z})$ とおける．mod 4 で考えると，

$$25l + 18 \equiv l + 2,\ 4m + 3 \equiv 3 \pmod{4}$$

より

$$l + 2 \equiv 3 \pmod{4} \qquad l \equiv 3 - 2 \equiv 1 \pmod{4}.$$

$l = 4l_1 + 1$ $(l_1 \in \mathbb{Z})$ とおくと，

$$a_3 = 25l + 18 = 25(4l_1 + 1) + 18 = 100l_1 + 43 \equiv 43 \pmod{100}.$$

よって，$a_{1001} \equiv a_3 \equiv 43 \pmod{100}$ より，a_{1001} の下 2 桁は 43. □

類題（ Putnam 1985）

$a_1 = 3,\ a_n = 3^{a_{n-1}}$ で定義される数列 $\{a_n\}$ がある．大きな n に対して a_n を 100 で割ったときの余りを求めよ．

解答 まず，すべての $n \in \mathbb{N}$ に対して，$a_n \equiv 3 \pmod{4}$ $\cdots\cdots (*)$

を示しておく．

すべての n に対して，a_n は奇数であるから，$n \geq 2$ のとき，

$$a_n = 3^{a_{n-1}} \equiv (-1)^{a_{n-1}} = -1 \equiv 3 \pmod{4}.$$

また，$a_1 = 3 \equiv 3 \pmod{4}$ であるから，$a_n \equiv 3 \pmod{4}$ が成り立つ．

$n \geq 3$ のとき，

$$a_{n+1} \equiv a_n \pmod{100} \qquad \cdots\cdots ①$$

が成り立つことを示したい．

このためには，

$$a_{n+1} \equiv a_n \pmod{4} \qquad \cdots\cdots ②$$

$$a_{n+1} \equiv a_n \pmod{25} \quad \text{すなわち} \quad 3^{a_n} \equiv 3^{a_{n-1}} \pmod{25} \qquad \cdots\cdots ③$$

を示せばよく，$(*)$ より②は常に成り立つから，③を示せばよい．

$\gcd(3, 25) = 1$, $\varphi(25) = \varphi\left(5^2\right) = 5^2 - 5 = 20$ だから，③が成り立つことを示すためには，

$$a_n \equiv a_{n-1} \pmod{20} \qquad \cdots\cdots ④$$

が成り立てばよい．

このためには，

$$a_n \equiv a_{n-1} \pmod{4} \qquad \cdots\cdots ⑤$$

$$a_n \equiv a_{n-1} \pmod{5} \quad \text{すなわち} \quad 3^{a_{n-1}} \equiv 3^{a_{n-2}} \pmod{5} \qquad \cdots\cdots ⑥$$

を示せばよく，$(*)$ より⑤は常に成り立つから，⑥を示せばよい．

$\gcd(3, 5) = 1$, $\varphi(5) = 5 - 1 = 4$ だから，⑥が成り立つことを示すためには，

$$a_{n-1} \equiv a_{n-2} \pmod{4} \qquad \cdots\cdots ⑦$$

が成り立てばよい．$(*)$ より，⑦は $n \geq 3$ のとき成り立つことがわかる．

①が $n \geq 3$ のとき成り立つから，$a_3 \equiv a_4 \equiv \cdots \pmod{100}$ より，100 を法として $a_3 = 3^{3^3} = 3^{27}$ を考える．$100 = 25 \cdot 4$ だから，a_3 を 25 で割った余りと，4 で割った余りを求める．

$\varphi(25) = 5^2 - 5 = 20$ であるから，$3^3 = 27$ を 20 で割った余りは 7 だから，$3^{27} \equiv 3^7 \pmod{25}$. さらに計算すると，$3^7 \equiv 27^2 \cdot 3 \equiv 2^2 \cdot 3 \equiv 12 \pmod{25}$ となるから，

$$a_3 \equiv 12 \pmod{25}. \qquad \cdots\cdots ⑧$$

次に．a_3 を 4 で割った余りを求める．$\varphi(4) = 2^2 - 2 = 2$ であるから，$3^3 = 27$ を 2 で割った余りは 1 だから，$3^{27} \equiv 3^1 \equiv 3 \pmod{4.}$

$$a_3 \equiv 3 \pmod{4}. \qquad \cdots\cdots ⑨$$

⑧，⑨より，$a_3 = 25l + 12 = 4m + 3$ $(l, m \in \mathbb{Z})$ とおける．mod 4 で考えると，

$$25l + 12 \equiv l,\ 4m + 3 \equiv 3 \pmod{4}$$

より

$$l \equiv 3 \pmod{4}.$$

$l = 4l_1 + 3$ $(l_1 \in \mathbb{Z})$ とおくと，

$$a_3 = 25l + 12 = 25(4l_1 + 3) + 12 = 100l_1 + 87 \equiv 87 \pmod{100}.$$

よって，$n \geq 3$ のとき，$a_n \equiv 87 \pmod{100}$. □

問題 4.7.2 (Senior Hanoi Open MO 2006)
$2005^{11}+2005^{112}+\cdots+2005^{2006}$ の下 3 桁を求めよ．

解答　mod 1000 で計算するわけであるが，mod 125 と mod 8 に分けて考える．
まず，

$$2005^{11}+2005^{112}+\cdots+2005^{2006}\equiv 5^{11}+5^{12}+\cdots+5^{2006} \pmod{1000}.$$

明らかに，$5^{11}+5^{112}+\cdots+5^{2006} \pmod{1000} \equiv 0 \pmod{125}$. 次に，$5^{11}+5^{12}+\cdots+5^{2006} \pmod 8$ を考える．

$5^2 \equiv 1 \pmod 8$ であるから，$k\in\mathbb{N}$ のとき，$5^{2k}\equiv 1 \pmod 8$, $5^{2k+1}\equiv 5 \pmod 8$. よって

$$\begin{aligned}5^{11}+5^{12}+\cdots+5^{2006} &= \left(5^{11}+5^{13}+\cdots+5^{2005}\right)+\left(5^{12}+5^{14}+\cdots+5^{2006}\right)\\ &\equiv \left(\underbrace{5+5+\cdots+5}_{998}\right)+\left(\underbrace{1+1+\cdots+1}_{998}\right)\\ &\equiv 998(1+5)\equiv 5988\equiv 8\cdot 748+4\\ &\equiv 4 \pmod 8.\end{aligned}$$

$x=5^{11}+5^{12}+\cdots+5^{2006}$ とおくと，$x\equiv 0 \pmod{125}$, $x\equiv 4 \pmod 8$ だから，$x=125l=8m+4$ $(l,m\in\mathbb{N})$ とおける．mod 8 で考えると，

$$125l\equiv 5l \pmod 8,\ 8m+4\equiv 4 \pmod 8$$

より，$5l\equiv 4 \pmod 8$. $\gcd(5,8)=1$ だから，8 を法とする 5 の逆数 $5^{-1}\equiv 5 \pmod 8$ が存在するから，$5l\equiv 4 \pmod 8$ の両辺にかけると，$l\equiv 5^{-1}\cdot 4\equiv 20 \pmod 8$.

$l=8l_1+20$ $(l_1\in\mathbb{N})$ とおくと，

$$x=125l=125(8l_1+20)=1000l_1+2500\equiv 2500\equiv 500 \pmod{1000}.$$

よって，$2005^{11}+2005^{112}+\cdots+2005^{2006}$ の下 3 桁は 500. □

問題 4.7.3 (PuMAC^a)
$2008^{2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}}$ の下 3 桁を求めよ．
(Princeton University Mathematics Competition)

解答 明らかに，$2008^{2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}}\equiv 0 \pmod 8$, $\gcd(2008,125)=1$ だから

$$2008^{2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}}\equiv 2008^{2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}} \pmod{\varphi(125)}} \pmod{125}. \qquad \cdots\cdots ①$$

$\varphi(125)=\varphi\left(5^3\right)=5^3-5^2=100$ だから，100 を法として，$2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}$ を考える．

$$2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}} \equiv 7^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}} \pmod{100}.$$

$7^4-1\equiv\left(7^2+1\right)\left(7^2-1\right)\equiv 50\cdot 48\equiv 0 \pmod{100}$ から $7^4\equiv 1 \pmod{100}$ が成り立ち，$4 \mid 2006^{\cdot^{\cdot^{\cdot^{2^1}}}}$ だから，$100 \mid 7^4-1 \mid 7^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}$．よって

$$2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}} \equiv 7^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}} \equiv 1 \pmod{100}.$$

①より

$$2008^{2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}} \equiv 2008^1 \equiv 8 \pmod{125}.$$

$x=2008^{2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}}$ とおくと，$x\equiv 0 \pmod 8, x\equiv 8 \pmod{125}$ より，

$$x=8l=125m+8 \ (l,m\in\mathbb{N})$$

とかける．これから，$8(l-1)=125m$．8 と 125 は互いに素だから，$l-1=125k \ (k\in\mathbb{N})$ とおける．よって，$x=8l=8(125k+1)=1000k+8$ となり，$2008^{2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}}$ の下 3 桁は，8. □

問題 4.7.4 (PuMAC2008)
$f(x)=x^{x^{x^x}}$ と定義する．$f(17)+f(18)+f(19)+f(20)$ の下 2 桁を求めよ．

解答
- $f(20)\equiv 0 \pmod{100}$.
- $f(17)\equiv 77 \pmod{100}$.

$f(17)=17^{17^{17^{17}}}\equiv 1^{17^{17^{17}}}\equiv 1 \pmod 4$.
$\gcd(17,25)=1$, $\varphi(25)=5^2-5=20$ だから，

$$f(17)=17^{17^{17^{17}}}\equiv 17^{17^{17^{17}} \pmod{20}} \pmod{25}$$

$\gcd(17,20)=1$, $\varphi(20)=\varphi(4)\varphi(5)=\left(2^2-2\right)(5-1)=8$ だから，

$$17^{17^{17}}\equiv 17^{17^{17} \pmod 8} \pmod{20}$$

$17^{17}\equiv 1^{17}\equiv 1 \pmod 8$ だから，$17^{17^{17}}\equiv 17^1 \pmod{20}$ となり，

$$f(17)=17^{17^{17^{17}}}\equiv 17^{17} \pmod{25}.$$

$17^{16} \equiv \left(17^2\right)^8 \equiv 289^8 \equiv 14^8 \equiv \left(14^2\right)^4 \equiv 196^4 \equiv (-4)^4 \equiv 256 \equiv 6 \pmod{25}$ より，
$17^{17} \equiv 17 \cdot 6 \equiv 102 \equiv 2 \pmod{25}$.

$f(17) = 4l + 1 = 25m + 2$ $(l, m \in \mathbb{N})$ とおける．mod 4 で考えると，

$$4l + 1 \equiv 1 \pmod{4},\ 25m + 2 \equiv m + 2 \pmod{4}$$

より，$1 \equiv m + 2 \pmod{4}$ すなわち $m \equiv -1 \equiv 3 \pmod{4}$.
よって，$m = 4m_1 + 3$ $(m_1 \in \mathbb{N})$ とおくと，

$$f(17) = 25m + 2 = 25(4m_1 + 3) + 2 = 100m_1 + 77 \equiv 77 \pmod{100}.$$

- $f(18) \equiv 76 \pmod{100}$.

$f(18) = 18^{18^{18^{18}}} \equiv 0 \pmod{4}$.

$18^4 - 1 = (18 - 1)(18 + 1)\left(18^2 + 1\right) = 17 \cdot 19 \cdot 325 = 17 \cdot 19 \cdot 13 \cdot 25 \equiv 0 \pmod{25}$ で，$4 \mid 18^{18^{18}}$ より，

$$25 \mid 18^4 - 1 \mid 18^{18^{18^{18}}} - 1$$

すなわち

$$f(18) = 18^{18^{18^{18}}} \equiv 1 \pmod{25}.$$

$f(18) = 4l = 25m + 1$ $(l, m \in \mathbb{N})$ とおける．mod 4 で考えると，

$$4l \equiv 0 \pmod{4},\ 25m + 1 \equiv m + 1 \pmod{4}$$

より，$0 \equiv m + 1 \pmod{4}$ すなわち $m \equiv -1 \equiv 3 \pmod{4}$.
よって，$m = 4m_1 + 3$ $(m_1 \in \mathbb{N})$ とおくと，

$$f(18) = 25m + 1 = 25(4m_1 + 3) + 1 = 100m_1 + 76 \equiv 76 \pmod{100}.$$

- $f(19) \equiv 79 \pmod{100}$.

$f(19) = 19^{19^{19^{19}}} \equiv (-1)^{19^{19^{19}}} \equiv -1 \pmod{4}$.
$\gcd(19, 25) = 1$, $\varphi(25) = 5^2 - 5 = 20$ だから，

$$f(19) = 19^{19^{19^{19}}} \equiv 19^{19^{19^{19}} \pmod{20}} \pmod{25}.$$

$19^{19^{19}} \equiv (-1)^{19^{19}} \equiv -1 \pmod{20}$ だから

$$f(19) \equiv 19^{-1} \equiv 4 \pmod{25}.$$

$f(19) = 4l - 1 = 25m + 4$ $(l, m \in \mathbb{N})$ とおける．mod 4 で考えると，

$$4l - 1 \equiv -1 \pmod{4},\ 25m + 4 \equiv m \pmod{4}$$

より，$-1 \equiv m \pmod 4$ すなわち $m \equiv -1 \equiv 3 \pmod 4$.
よって，$m = 4m_1 + 3$ $(m_1 \in \mathbb{N})$ とおくと，

$$f(19) = 25m + 4 = 25(4m_1 + 3) + 4 = 100m_1 + 79 \equiv 79 \pmod{100}.$$

以上のことから，

$$f(17) + f(18) + f(19) + f(20) \equiv 77 + 76 + 79 + 0 \equiv 232 \equiv 32 \pmod{100}.$$

$f(17) + f(18) + f(19) + f(20)$ の下 2 桁は 32. □

問題 4.7.5 (AoPS)
c は整数，p は素数とする．このとき，合同式 $x^x \equiv c \pmod p$ は解を持つことを示せ．

x が合同式，$x \equiv c \pmod p$ かつ $x \equiv 1 \pmod{\underbrace{p-1}_{\varphi(p)}}$ を満たすならば，$x^x \equiv c \pmod p$ は $x^x \equiv x \pmod p$ となるから，$\gcd(x, p) = 1$ ならば，命題 4.7.1 より，合同式 $x^x \equiv x \pmod p$ は解を持つことがわかる．

解答　$p \mid c$ のとき $p \mid x$ とすれば，合同式 $x^x \equiv c \pmod p$ は解を持つ．
以下，$\gcd(c, p) = 1$ とする．

x が合同式，$x \equiv c \pmod p$ かつ $x \equiv 1 \pmod{\underbrace{p-1}_{\varphi(p)}}$ を満たすものとする．

すると，$\gcd(x, p) = 1$ で，フェルマーの小定理より，$x^{p-1} \equiv 1 \pmod p$ が成り立つ．

$p - 1 \mid x - 1$ より，$x^{p-1} - 1 \mid x^{x-1} - 1$ が成り立つから，$x^{x-1} \equiv 1 \pmod p$.
よって，$x^x \equiv x \equiv c$.

したがって，実際に $x \equiv c \pmod p$ かつ $x \equiv 1 \pmod{p-1}$ を満たす x が存在することを示せばよい．

$$x - c = ps \quad (s \in \mathbb{Z}) \qquad \cdots\cdots ①$$

$$x - 1 = (p-1)t \quad (t \in \mathbb{Z}) \qquad \cdots\cdots ②$$

とおく．① − ② から

$$ps - (p-1)t = 1 - c. \qquad \cdots\cdots ③$$

$p - (p-1) = 1$ の両辺に $1 - c$ をかけると

$$p(1-c) - (p-1)(1-c) = 1 - c. \qquad \cdots\cdots ④$$

③ − ④ から，$p(s - 1 + c) = (p-1)(t - 1 + c)$.

p と $p-1$ は互いに素だから，k を整数として，$s - 1 + c = (p-1)k$, $t - 1 + c = pk$ とおける．この式を①に代入すると，x が存在することがわかる． □

問題 4.7.6 (Putnam 1997)

2 以上の正の整数 n に対して

$$\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n} \equiv \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n-1} \pmod{n}$$

が成り立つことを証明せよ.

数学的帰納法で，$\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n} \equiv \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n-1} \pmod{n}$ を証明しようとしてもうまくいかないので，解答の $(*)$ を示すとよい．これは例題 4.7.1 から予測がつくとおもう.

解答　$a_0 = 1, a_1 = 2, a_n = 2^{a_{n-1}}$ $(n \geq 2)$ とおき，

$n \geq 2$ のとき

$$a_{n-1} \equiv a_n \equiv a_{n+1} \equiv \cdots \pmod{n} \qquad \cdots\cdots(*)$$

が成り立つことを示す.

- 最初に $n = 2^k$ $(k \in \mathbb{N})$ のときに，$(*)$ が成り立つことを示す.

  $m \geq n$ のとき

  $$a_m \equiv a_{m-1} \pmod{2^k} \Longleftrightarrow 2^{a_{m-1}} \equiv 2^{a_{m-2}} \pmod{2^k}.$$

  $a_{n-2} = a_{2^k-2} \geq k$ が成り立てば，$k \leq a_{n-2} \leq a_{m-2}$ より $2^k \mid 2^{a_{m-2}}$ が成り立つので，$2^{a_{m-1}-a_{m-2}} - 1 > 1$ とあわせると

  $$2^k \mid 2^{a^{m-2}} \left(2^{a^{m-1}-a^{m-2}} - 1\right) = 2^{a_{m-1}} - 2^{a_{m-2}}$$

  すなわち $2^{a_{m-1}} \equiv 2^{a_{m-2}} \pmod{2^k}$ が言える.

  したがって，

  $$a_{2^k-2} \geq k \qquad \cdots\cdots(**)$$

  が成り立つことを k に関する数学的帰納法で示す.

  (I) $k = 1$ のとき，$a_{2^1-2} = a_0 = 1$ より $(**)$ は成り立つ.

  (II) $k\,(\geq 1)$ のとき $(**)$ が成り立つと仮定すると

  $$\begin{aligned} a_{2^{k+1}-2} > a_{2^k-1} = 2^{a_{2^k-2}} \geq 2^k = (1+1)^k \\ = 1 + \binom{k}{1} + \cdots + \binom{k}{k} \\ \geq 1 + \binom{k}{1} = 1 + k \end{aligned}$$

  より，$a_{2^{k+1}-2} > k + 1$ が成り立つ.

  ゆえに，$k + 1$ のときも成り立つ.

(III) (I)，(II) から，すべての正の整数 k に対して $(**)$ は成り立つ．

- $n = 2^k b$ $(k \in \mathbb{N}_0, b \in \mathbb{N}, b$ は奇数$)$ のとき，$(*)$ が成り立つことを b に関する帰納法で証明する．(k は任意であることに注意すること．)

(I) $b = 1$ のとき，$n = 2^k$ $(k \in \mathbb{N})$ であるから，$(*)$ が成り立つことはすでに証明してある．

(II) $b' < b$ $(b' \in \mathbb{N}, b'$は奇数$)$ を満たすすべての b' について $(**)$ が成り立つと仮定する．

$m \geq n = 2^k b$ のとき，$a_m \equiv a_{m-1} \pmod{2^k b}$ が成り立つことを示す．このためには，次の①と②を示せばよい．

$$a_m \equiv a_{m-1} \pmod{2^k}. \qquad \cdots\cdots ①$$

$$a_m \equiv a_{m-1} \pmod{b}. \qquad \cdots\cdots ②$$

$$a_{2^k-1} \equiv a_{2^k} \equiv a_{2^k+1} \equiv \cdots \pmod{2^k}$$

だから，$m \geq 2^k$ が言えれば，①は成り立つので，$m \geq 2^k$ を示す．

$$m \geq n = 2^k b \geq 2^k$$

より，$m \geq 2^k$ は成り立つ．

②は $2^{a_{m-1}} \equiv 2^{a_{m-2}} \equiv \pmod{b}$ と変形できる．$\gcd(2, b) = 1$ だから

$$a_{m-1} \equiv a_{m-2} \pmod{\varphi(b)} \qquad \cdots\cdots ③$$

が成り立てばよい．

$$n' = \varphi(b) = 2^{k'} b' \quad (n' \in \mathbb{N}_0, b' \in \mathbb{N}, b'\text{は奇数})$$

とおくと．$n' = \varphi(b) < b$ より，$b' \leq n' < b$ だから，帰納法の仮定より

$$a_{n'-1} \equiv a_{n'} \equiv a_{n'+1} \equiv \cdots \pmod{n'}$$

すなわち

$$a_{n'-1} \equiv a_{n'} \equiv a_{n'+1} \equiv \cdots \pmod{\varphi(b)}$$

が成り立つ．

$n' = \varphi(b) < b \leq 2^k b = n$ より $n' - 1 < n - 1$ だから

$$a_{n-1} \equiv a_n \equiv a_{n+1} \equiv \cdots \pmod{\varphi(b)}$$

となり，③が成り立つ．

(III) (I)，(II) より，$n = 2^k b$ を満たすすべての奇数 b に対して，$(*)$ が成り立つ． □

別解　$a_0=1, a_1=2, a_n=2^{a_{n-1}}$ $(n\geq 2)$ とおく.
最初に $n=2^k$ $(k\in\mathbb{N})$ のときに

$$a_n \equiv a_{n-1} \pmod{n} \qquad \cdots\cdots(*)$$

が成り立つことを示す.

$$a_n \equiv a_{n-1} \pmod{2^k} \Longleftrightarrow 2^{a_{n-1}} \equiv 2^{a_{n-2}} \pmod{2^k}.$$

$a_{n-2}=a_{2^k-2}\geq k$ が成り立てば，$k\leq a_{n-2}$ より $2^k \mid 2^{a^{n-2}}$ が成り立つので，$2^{a^{n-1}-a^{n-2}}-1>1$ とあわせると

$$2^k \mid 2^{a^{n-2}}\left(2^{a^{n-1}-a^{n-2}}-1\right)=2^{a_{n-1}}-2^{a_{n-2}}$$

すなわち $2^{a_{n-1}} \equiv 2^{a_{n-2}} \pmod{2^k}$ が言える.
したがって,

$$a_{2^k-2}\geq k \qquad \cdots\cdots(**)$$

が成り立つことを k に関する数学的帰納法で示す.
(I)　$k=1$ のとき，$a_{2^1-2}=a_0=1$ より $(**)$ は成り立つ.
(II)　$k\,(\geq 1)$ のとき $(**)$ が成り立つと仮定すると

$$\begin{aligned} a_{2^{k+1}-2} > a_{2^k-1} = 2^{a_{2^k-2}} \geq 2^k &= (1+1)^k \\ &= 1+\binom{k}{1}+\cdots+\binom{k}{k} \\ &\geq 1+\binom{k}{1}=1+k \end{aligned}$$

より，$a_{2^{k+1}-2}>k+1$ が成り立つ.
ゆえに，$k+1$ のときも成り立つ.
(III)　(I)，(II) から，すべての正の整数 k に対して $(**)$ は成り立つ.

- $a_n\geq n+1$ が成り立つ.

$n=0,1$ のとき明らかに $a_n\geq n+1$ は成り立つ.
$n\geq 2$ のとき，$2^m\leq n<2^{m+1}$ $(m\in\mathbb{N})$ となる正の整数 m をとると，$a_{2^m-2}\geq m$ が成り立つから,

$$a_n \geq a_{2^m}=2^{a_{2^m-1}}=2^{2^{a_{2^m-2}}}\geq 2^{2^m}\geq 2^{m+1}>n.$$

よって，$a_n\geq n+1$ が成り立つ.
任意の正の整数 n に対して，x が $1\leq x\leq n$ を満たす正の整数ならば

$$a_n \equiv a_{n-1} \pmod{x} \qquad \cdots\cdots(\star)$$

が成り立つことを n に関する数学的帰納法で示す.

(I) $n=1$ のとき，$a_1=2, a_0=1, x=1$ となるから，$(\star)$ は成り立つ．

(II) n のとき成り立つと仮定する．

$$a_{n+1} \equiv a_n \pmod{y} \quad (\forall y \leq n+1)$$

が成り立つことを示す．

- $\gcd(2,y)=1$ のとき

$2^{a_n} \equiv 2^{a_{n-1}} \pmod{y}$ を示すには，$a_n \equiv a_{n-1} \pmod{\varphi(y)}$ を示せばよい．
$x=\varphi(y)$ とおくと，$x=\varphi(y) \leq y-1 \leq n$ だから，帰納法の仮定より，
$a_n \equiv a_{n-1} \pmod{x}$ $(\forall x \leq n)$ は成り立つ．

- $\gcd(2,y)>1$ のとき

$y=2^k b$ $(k \in \mathbb{N}, b$ は奇数$)$ とおけるから，

$$a_{n+1} \equiv a_n \pmod{2^k} \qquad \cdots\cdots ①$$

と

$$a_{n+1} \equiv a_n \pmod{b} \qquad \cdots\cdots ②$$

が成り立つことを示せばよい．

$a_{n-1} \geq (n-1)+1 = n \geq y-1 = 2^k b-1 \geq 2^k-1 \geq (k+1)-1 = k$ より

$$2^k \mid 2^{a_{n-1}} \mid 2^{a_{n-1}}\left(2^{a_n-a_{n-1}}-1\right) = 2^{a_n}-2^{a_{n-1}} = a_{n+1}-a_n.$$

したがって，①は成り立つ．

②は $2^{a_n} \equiv 2^{a_{n-1}} \equiv \pmod{b}$ と変形できる．$\gcd(2,b)=1$ だから

$$a_n \equiv a_{n-1} \pmod{\varphi(b)} \qquad \cdots\cdots ③$$

が成り立てばよい．

$2b \leq 2^k b = y \leq n+1$ から $b \leq \dfrac{n}{2}+\dfrac{1}{2} \leq n$. よって，$\varphi(b) < b \leq n$ だから，
帰納法の仮定より，③は成り立つ．

(III) (I)，(II) より，すべての正の整数 n に対して，$(\star)$ が成り立つ． □

問題 5.6.1

(1) $p \neq 3$ を奇数の素数とすれば,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{12} \\ -1 & p \equiv \pm 5 \pmod{12} \end{cases}$$

が成り立つことを示せ.

(2) $p \neq 3$ を奇数の素数とすれば,

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{6} \\ -1 & p \equiv -1 \pmod{6} \end{cases}$$

が成り立つことを示せ.

(3) p を奇数の素数とすれば,

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{8} \text{ または } p \equiv 3 \pmod{8} \\ -1 & p \equiv 5 \pmod{8} \text{ または } p \equiv 7 \pmod{8} \end{cases}$$

が成り立つことを示せ.

解答 (1)　$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$ から

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & p \equiv 1 \pmod{4} \\ -\left(\frac{p}{3}\right) & p \equiv 3 \pmod{4} \end{cases} \quad \cdots\cdots ①$$

となる.

$p \equiv 1 \pmod 3$ のとき, $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$.

$p \equiv 2 \pmod 3$ のとき, $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$.

すなわち

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv 1 \pmod{3} \\ -1 & p \equiv 2 \pmod{3} \end{cases} \quad \cdots\cdots ②$$

となる.

①と②から, $\left(\frac{p}{3}\right) = 1$ となるための必要十分条件は

(i) $p \equiv 1 \pmod 4$ かつ $p \equiv 1 \pmod 3$

または

(ii) $p \equiv 3 \pmod 4$ かつ $p \equiv 2 \pmod 3$

である.

(i) から $p \equiv 1 \pmod{12}$ がでる.

(ii) のときは，中国の剰余定理より，$3 \cdot (-1) \equiv 1 \pmod 4$, $4 \cdot 1 \equiv 1 \pmod 3$ だから $p \equiv 3 \cdot 3 \cdot (-1) + 2 \cdot 4 \cdot 1 \equiv -1 \pmod{12}$ となる.

$\left(\dfrac{p}{3}\right) = -1$ となるのは，これ以外の場合で，$p \equiv \pm 5 \pmod{12}$ のときである.

よって

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{12} \\ -1 & p \equiv \pm 5 \pmod{12} \end{cases}$$

が成り立つ.

(2) $\left(\dfrac{-3}{p}\right) = \left(\dfrac{-1}{p}\right)\left(\dfrac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\dfrac{3}{p}\right)$.

前問の結果を利用する.

$p \equiv 1 \pmod{12}$ のとき，$\dfrac{p-1}{2}$ は偶数，$\left(\dfrac{3}{p}\right) = 1$ より $\left(\dfrac{-3}{p}\right) = 1$.

$p \equiv -1 \pmod{12}$ のとき，$\dfrac{p-1}{2}$ は奇数，$\left(\dfrac{3}{p}\right) = 1$ より $\left(\dfrac{-3}{p}\right) = -1$.

$p \equiv 5 \pmod{12}$ のとき，$\dfrac{p-1}{2}$ は偶数，$\left(\dfrac{3}{p}\right) = -1$ より $\left(\dfrac{-3}{p}\right) = -1$.

$p \equiv -5 \pmod{12}$ のとき，$\dfrac{p-1}{2}$ は奇数，$\left(\dfrac{3}{p}\right) = -1$ より $\left(\dfrac{-3}{p}\right) = 1$.

以上のことから，

$\left(\dfrac{-3}{p}\right) = 1$ となるのは $p \equiv 1 \pmod{12}$ または $p \equiv -5 \equiv 7 \pmod{12}$ のときであるから，まとめて $p \equiv 1 \pmod 6$ となる.

$\left(\dfrac{-3}{p}\right) = -1$ となるのは $p \equiv -1 \pmod{12}$ または $p \equiv 5 \equiv -7 \pmod{12}$ のときであるから，まとめて $p \equiv -1 \pmod 6$ となる.

よって

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 6 \\ -1 & p \equiv -1 \pmod 6 \end{cases}$$

が成り立つ.

(3) $\left(\dfrac{-2}{p}\right) = \left(\dfrac{-1}{p}\right)\left(\dfrac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}$.

ここで,

$$\frac{p-1}{2} + \frac{p^2-1}{8} = \frac{p-1}{2}\left(1 + \frac{p+1}{4}\right) = \frac{(p-1)(p+5)}{8}$$

となる．$k \in \mathbb{N}_0$ とする.

$p=8k+1$ または $p=8k+3$ のとき，$\dfrac{(p-1)(p+5)}{8}$ は偶数で，$\left(\dfrac{-2}{p}\right)=1.$

$p=8k+5$ のとき，$\dfrac{p-1}{4}$，$\dfrac{p+5}{2}$ は奇数だから，$\dfrac{(p-1)(p+5)}{8}$ は奇数で，$\left(\dfrac{-2}{p}\right)=-1.$

$p=8k+7$ のとき，$\dfrac{p-1}{2}$，$\dfrac{p+5}{4}$ は奇数だから，$\dfrac{(p-1)(p+5)}{8}$ は奇数で，$\left(\dfrac{-2}{p}\right)=-1.$

よって

$$\left(\frac{-2}{p}\right)=\begin{cases}1 & p\equiv 1 \pmod 8 \text{ または } p\equiv 3 \pmod 8\\ -1 & p\equiv 5 \pmod 8 \text{ または } p\equiv 7 \pmod 8\end{cases}$$

が成り立つ．□

問題 5.6.2 (Vietnam TST 2003)

任意の正の整数 n に対して，2^n+1 は $8k-1$ の形をした素数の約数をもたないことを証明せよ．

解答 背理法で示すため，2^n+1 が $8k-1$ の形をした素数の約数をもつと仮定する．すると，$p=8k-1, k\in\mathbb{N}$ で $p\mid 2^n+1$.

(1) n が偶数の場合

$p\mid 2^n+1$ から $2^n+1\equiv 0 \pmod p$.

よって

$$-1\equiv 2^n\equiv \left(2^{\frac{n}{2}}\right)^2 \pmod p$$

となるから，$\left(\dfrac{-1}{p}\right)=1.$

$p=8k-1$ であったから，$\left(\dfrac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ が成り立つことを用いると

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=(-1)^{4k-1}=-1$$

となり，$\left(\dfrac{-1}{p}\right)=1$ に矛盾する．

(2) n が奇数の場合

$2^n\equiv -1 \pmod p$ の両辺に 2 をかけて変形すると

$$\left(2^{\frac{n+1}{2}}\right)^2\equiv -2 \pmod p$$

が成り立つから

$$\left(\frac{-2}{p}\right) = 1.$$

$p = 8k-1$ であったから，

$$\begin{aligned}\left(\frac{-2}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}\\ &= (-1)^{4k-1}(-1)^{2k(4k-1)} = (-1)\cdot 1 = -1\end{aligned}$$

となり，$\left(\frac{-2}{p}\right) = 1$ に矛盾する．

したがって，2^n+1 は $8k-1$ の形をした素数の約数をもたない． □

問題 5.6.3 (Gabriel Dospinescu)
任意の正の整数 n に対して，$2^{3^n}+1$ は $8k+3$ の形をした素数の約数を少なくとも n 個もつことを証明せよ．

解答 前問の結果から，2^m+1 は $8k+7$ の形をした素数の約数をもたない．

• m が奇数ならば，2^m+1 は $8k+5$ の形をした素数の約数をもたない．

p を $p \mid 2^m+1$ を満たす $8k+5$ の形の素数の約数とする．

$2^m \equiv -1 \pmod p$ を $\left(2^{\frac{m+1}{2}}\right)^2 \equiv -2 \pmod p$ と変形できるから，$\left(\frac{-2}{p}\right) = 1$ が成り立つ．

ところが，$p = 8k+5$ であったから，

$$\begin{aligned}\left(\frac{-2}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}\\ &= (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}\\ &= (-1)^{(2k+1)(4k+5)} = -1\end{aligned}$$

となり，$\left(\frac{-2}{p}\right) = 1$ に矛盾する．

$n=1$ のとき，$2^{3^1}+1 = 9 = 3^2$ だから，$8k+3$ の形をした素数の約数は 3 の 1 個である．

$n=2$ のとき，$2^{3^2}+1 = 513 = 3^3\cdot 19$ だから，$8k+3$ の形をした素数の約数は 3 と 19 の 2 個である．

以下 $n \geq 3$ とする．

- 次の等式が成り立つ.

$$2^{3^n}+1=(2+1)\left(2^2-2+1\right)\left(2^{2\cdot 3}-2^3+1\right)\cdots\left(2^{2\cdot 3^{n-1}}-2^{3^{n-1}}+1\right). \quad \cdots\cdots ①$$

これは

$$\begin{aligned}2^{3^n}+1&=\left(2^{3^{n-1}}\right)^3+1=\left(2^{3^{n-1}}+1\right)\left(\left(2^{3^{n-1}}\right)^2-2^{3^{n-1}}+1\right)\\&=\left(2^{3^{n-1}}+1\right)\left(2^{2\cdot 3^{n-1}}-2^{3^{n-1}}+1\right)\\&=\left(2^{3^{n-2}}+1\right)\left(2^{2\cdot 3^{n-2}}-2^{3^{n-2}}+1\right)\left(2^{2\cdot 3^{n-1}}-2^{3^{n-1}}+1\right)\\&=\cdots\cdots\\&=(2+1)\left(2^2-2+1\right)\left(2^{2\cdot 3}-2^3+1\right)\\&\qquad\cdots\cdots\left(2^{2\cdot 3^{n-2}}-2^{3^{n-2}}+1\right)\left(2^{2\cdot 3^{n-1}}-2^{3^{n-1}}+1\right)\end{aligned}$$

から成り立つ.

- すべての $1\leq i<j\leq n-1$ に対して

$$\gcd\left(2^{2\cdot 3^i}-2^{3^i}+1,2^{2\cdot 3^j}-2^{3^j}+1\right)=3$$

が成り立つ.

$$2^{2\cdot 3^i}-2^{3^i}+1\equiv(-1)^{2\cdot 3^i}-(-1)^{3^i}+1\equiv 1-(-1)+1\equiv 3\equiv 0 \pmod 3$$

すなわち，$3\mid 2^{2\cdot 3^i}-2^{3^i}+1, 3\mid 2^{2\cdot 3^j}-2^{3^j}+1$ が成り立つことがわかる.

p を $p\mid\gcd\left(2^{2\cdot 3^i}-2^{3^i}+1,2^{2\cdot 3^j}-2^{3^j}+1\right)$ となる素数とすると，

$2^{3^{i+1}}+1=\left(2^{3^i}\right)^3+1=\left(2^{3^i}+1\right)\left(2^{2\cdot 3^i}-2^{3^i}+1\right)$ は p で割り切れるから，

$$2^{3^{i+1}}\equiv -1 \pmod p.$$

$j>i+1$ のとき，$2^{3^j}\equiv\left(2^{3^{i+1}}\right)^{3^{j-i-1}}\equiv(-1)^{3^{j-i-1}}\equiv -1 \pmod p$.

$j=i+1$ のとき，$2^{3^j}\equiv 2^{3^{i+1}}\equiv -1 \pmod p$ はすでに示してある.

したがって，$2^{3^j}\equiv -1 \pmod p$ が成り立つから

$$2^{2\cdot 3^j}-2^{3^j}+1\equiv(-1)^2-(-1)+1\equiv 3 \pmod p.$$

ところが，$p\mid\gcd\left(2^{2\cdot 3^i}-2^{3^i}+1,2^{2\cdot 3^j}-2^{3^j}+1\right)$ であったから，$2^{2\cdot 3^j}-2^{3^j}+1\equiv 0 \pmod p$ なので，$3\equiv 0 \mod p$ となる．これから，$p=3$ でなければならない.

次に，

$$v_3\left(\gcd\left(2^{2\cdot 3^i}-2^{3^i}+1, 2^{2\cdot 3^j}-2^{3^j}+1\right)\right)=1$$

が成り立つことを示す． mod 9 で考えると

$$2^{3^i}\equiv\left(2^3\right)^{3^{i-1}}\equiv(-1)^{3^{i-1}}\equiv -1 \pmod 9,\ 2^{2\cdot 3^i}\equiv(2^{3^i})^2\equiv(-1)^2\equiv 1 \pmod 9$$

より

$$2^{2\cdot 3^i}-2^{3^i}+1\equiv 1-(-1)+1\equiv 3\not\equiv 0 \pmod 9.$$

同様にして

$$2^{2\cdot 3^j}-2^{3^j}+1\equiv 1-(-1)+1\equiv 3\not\equiv 0 \pmod 9$$

なので，$v_3\left(\gcd\left(2^{2\cdot 3^i}-2^{3^i}+1, 2^{2\cdot 3^j}-2^{3^j}+1\right)\right)=1$ が成り立つ．
よって，すべての $1\leq i<j\leq n-1$ に対して

$$\gcd\left(2^{2\cdot 3^i}-2^{3^i}+1, 2^{2\cdot 3^j}-2^{3^j}+1\right)=3$$

が成り立つ．

各 i $(1\leq i\leq n-1)$ に対して $2^{2\cdot 3^i}-2^{3^i}+1$ は 3 と異なる $8k+3$ の形の素数の約数をもつことを示せばよい．

①より，$2^{2\cdot 3^i}-2^{3^i}+1$ の素数の約数は $2^{3^n}+1$ の素数の約数で，$8k+5, 8k+7$ の形ではないから，$8k+1$ か $8k+3$ の形でなければならない．$2^{2\cdot 3^i}-2^{3^i}+1$ が 3 以外に $8k+3$ の形の素因数をもたないとする．

$$2^{2\cdot 3^i}-2^{3^i}+1=3\cdot p_1^{\alpha_1}\cdots p_r^{\alpha_r},\ 3, p_1, \ldots, p_r\text{は異なる素数},\ \alpha_1, \ldots, \alpha_r\in\mathbb{N}$$

と素因数分解すると，$p_l\equiv 1 \pmod 8$ $(1\leq l\leq r)$ だから

$$2^{2\cdot 3^i}-2^{3^i}+1\equiv 3\cdot p_1^{\alpha_1}\cdots p_r^{\alpha_r}\equiv 3\cdot 1\cdots 1\equiv 3 \pmod 8.$$

ところが，$2^{2\cdot 3^i}-2^{3^i}+1\equiv\left(2^3\right)^{2\cdot 3^{i-1}}-\left(2^3\right)^{3^{i-1}}+1\equiv 8^{2\cdot 3^{i-1}}-8^{3^{i-1}}+1\equiv 0-0+1\equiv 1 \pmod 8$ であるから，$2^{2\cdot 3^i}-2^{3^i}+1\equiv 3 \pmod 8$ に矛盾する．

したがって，すべての i $(1\leq i\leq n-1)$ に対して $2^{2\cdot 3^i}-2^{3^i}+1$ は 3 以外の $8k+3$ の形の素数の約数をもち，$\gcd\left(2^{2\cdot 3^i}-2^{3^i}+1, 2^{2\cdot 3^j}-2^{3^j}+1\right)=3,\ 1\leq i<j\leq n-1$ であったから，これらの $8k+3$ の形の約数は異なるから，3 を含めて，$2^{3^n}+1$ は $8k+3$ の形をした素数の約数を少なくとも n 個もつ． □

問題 5.6.4 (Taiwan Mathematical Olympiad 1997)
ある正の整数 n に対して，$k = 2^{2^n} + 1$ とおく．このとき，k が素数となるための必要十分条件は，k が $3^{\frac{k-1}{2}} + 1$ の因数であることを証明せよ．

解答 （$\Longleftarrow$）十分条件であることの証明.

$k \mid 3^{\frac{k-1}{2}} + 1$ と仮定すると，$3^{\frac{k-1}{2}} \equiv -1 \pmod{k}$.

両辺を平方すると，$3^{k-1} \equiv 1 \pmod{k}$.

$d = \mathrm{ord}_k(3)$ とすると，$3^d \equiv 1 \pmod{k}$ で

$$d \mid k-1 = 2^{2^n},\ d \nmid \frac{k-1}{2} = 2^{2^n-1}.$$

$d \neq 2^{2^n}$ だとすると，$d = 2^{2^n-i}\ (2 \leq i \leq 2^n - 1)$ とかける．

$2^{2^n-i} \mid 2^{2^n-1}$ だから，$k \mid 3^d - 1 = 3^{2^{2^n-i}} - 1 \mid 3^{2^{2^n-1}} - 1 = 3^{\frac{k-1}{2}} - 1$ となり，$3^{\frac{k-1}{2}} \equiv 1 \pmod{k}$．これは，$3^{\frac{k-1}{2}} \equiv -1 \pmod{k}$ に矛盾する．

したがって，$d = 2^{2^n} = k - 1$ である．

k が素数でないとすると，$p \mid k \mid 3^{\frac{k-1}{2}} + 1$ となる素数 p が存在する．$3^{\frac{k-1}{2}} \equiv -1 \pmod{p}$.

両辺を平方すると，$3^{k-1} \equiv 1 \pmod{p}$.

$d_1 = \mathrm{ord}_p(3)$ とすると，$3^d \equiv 1 \pmod{p}$ で

$$d_1 \mid k-1 = 2^{2^n},\ d_1 \nmid \frac{k-1}{2} = 2^{2^n-1}.$$

上の議論と同様にして，$d_1 = k - 1$ が成り立つ.

$p \mid 3^{\frac{k-1}{2}} + 1$ から $p \nmid 3$ とわかるから，フェルマーの小定理より，$3^{p-1} \equiv 1 \pmod{p}$.

これから，$d_1 \mid p - 1$ が成り立ち，$k - 1 \mid p - 1$．よって $k - 1 \leq p - 1$ から $k \leq p$.

$p \mid k$ より $p \leq k$ であったから $k = p$ となる．これから k が素数となり，k が素数でないことに矛盾する．

したがって，k は素数である.

（$\Longrightarrow$）必要条件であることの証明.

k は素数とする．$k = 2^{2^n} + 1 = 4l + 1\ (l \in \mathbb{N})$ より $\dfrac{k-1}{2} = 2l$.

平方剰余の相互法則より

$$\begin{aligned}\left(\frac{3}{k}\right) &= \left(\frac{k}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{k-1}{2}} = \left(\frac{k}{3}\right) \\ &= \left(\frac{2}{3}\right) \qquad k = 2^{2^n} + 1 = \left(2^2\right)^{2^{n-1}} \equiv 1 + 1 \equiv 2 \pmod{3} \\ &= (-1)^{\frac{3^2-1}{8}} = -1.\end{aligned}$$

また，定理 5.4.1 (2) の Euler's Criterion より，$\left(\dfrac{3}{k}\right) \equiv 3^{\frac{k-1}{2}} \pmod{k}$ が成り立つから，$-1 \equiv 3^{\frac{k-1}{2}} \pmod{k}$ すなわち，$k \mid 3^{\frac{k-1}{2}} + 1$ が成り立つ．□

問題 6.2.1 整数 x, y が $x^2 - 2y^2 = 1$ を満たすとき，次の問いに答えよ．

(1) 整数 a, b, u, v が $\left(a + b\sqrt{2}\right)\left(x + y\sqrt{2}\right) = u + v\sqrt{2}$ を満たすとき，u, v を a, b, x, y で表せ．さらに $a^2 - 2b^2 = 1$ のときの $u^2 - 2v^2$ の値を求めよ．ともに答えのみでよい．

(2) $1 < x + y\sqrt{2} \leqq 3 + 2\sqrt{2}$ のとき，$x = 3, y = 2$ となることを示せ．

(3) 自然数 n に対して，$\left(3 + 2\sqrt{2}\right)^{n-1} < x + y\sqrt{2} \leqq \left(3 + 2\sqrt{2}\right)^{n}$ のとき，$x + y\sqrt{2} = \left(3 + 2\sqrt{2}\right)^{n}$ を示せ．　(2015 早稲田大・理工)

解答　x, y は整数で，

$$x^2 - 2y^2 = 1 \qquad \cdots\cdots ①$$

とおく．

(1) $\left(a + b\sqrt{2}\right)\left(x + y\sqrt{2}\right) = (ax + 2by) + (bx + ay)\sqrt{2} = u + v\sqrt{2}$ が成り立ち，$ax + 2by, bx + ay, u, v$ は有理数で，$\sqrt{2}$ は無理数だから，

$$u = ax + 2by,\ v = bx + ay. \qquad \text{(答)}$$

ゆえに，

$$\begin{aligned} u^2 - 2v^2 &= (ax + 2by)^2 - 2(bx + ay)^2 \\ &= a^2x^2 + 4b^2y^2 - 2b^2x^2 - 2a^2y^2 \\ &= \left(a^2 - 2b^2\right)x^2 - 2\left(a^2 - 2b^2\right)y^2 \\ &= \left(a^2 - 2b^2\right)\left(x^2 - 2y^2\right) = 1 \cdot 1 \\ &= 1. \end{aligned}$$

よって，$u^2 - 2v^2 = 1$.　(答)

(2) $1 < x + y\sqrt{2} \leqq 3 + 2\sqrt{2}$　$\cdots\cdots ②$

とおく．$x^2 - 2y^2 = 1$ より $\left(x + y\sqrt{2}\right)\left(x - y\sqrt{2}\right) = 1$ が成り立つから

$$x - y\sqrt{2} = \frac{1}{x + y\sqrt{2}}.$$

②を使うと，$1 > \dfrac{1}{x + y\sqrt{2}} \geq \dfrac{1}{3 + 2\sqrt{2}} = 3 - 2\sqrt{2}$ だから

$$3 - 2\sqrt{2} \leq x - y\sqrt{2} < 1. \qquad \cdots\cdots ③$$

②，③から，$1+\left(3-2\sqrt{2}\right)<x+y\sqrt{2}+x-y\sqrt{2}<\left(3+2\sqrt{2}\right)+1$ すなわち

$$2-\sqrt{2}<x<2+\sqrt{2}.$$

x は整数だから，$x\in\left\{1,\,2,\,3\right\}$.

$x=1$ のとき，①から，$y=0$ となるが，これは②を満たさない.

$x=2$ のとき，①から，$y^2=\dfrac{3}{2}$ となるが，これは満たす整数 y は存在しない.

$x=3$ のとき，①から，$y=\pm2$ となるが，③を満たすのは，$y=2$ である.

したがって，$1<x+y\sqrt{2}\leqq3+2\sqrt{2}$ を満たすならば，$x=3,y=2$ となる.

(3) x,y は整数で，$x^2-2y^2=1$ を満たしている.

(P) $\left(3+2\sqrt{2}\right)^{n-1}<x+y\sqrt{2}\leqq\left(3+2\sqrt{2}\right)^{n}$ のとき，$x+y\sqrt{2}=\left(3+2\sqrt{2}\right)^{n}$.

とおく．(P) が成り立つことを数学的帰納法で示す.

(I) $n=1$ のとき

$1<x+y\sqrt{2}\leqq3+2\sqrt{2}$ ならば，(2) より，$x=3,y=2$ すなわち，$x+y\sqrt{2}=3+2\sqrt{2}$ となるから，(P) は成り立つ.

(II) $n=k$ のとき，(P) が成り立つと仮定すると，

X,Y は整数で，$X^2-2Y^2=1$ を満たしているとき，

$\left(3+2\sqrt{2}\right)^{k-1}<X+Y\sqrt{2}\leqq\left(3+2\sqrt{2}\right)^{k}$ ならば，$X+Y\sqrt{2}=\left(3+2\sqrt{2}\right)^{k}$.

x,y は整数で，$x^2-2y^2=1$ を満たしているとき，

$\left(3+2\sqrt{2}\right)^{k}<x+y\sqrt{2}\leqq\left(3+2\sqrt{2}\right)^{k+1}$ が成り立つとする.

この不等式の各辺を $3+2\sqrt{2}$ で割ると

$$\left(3+2\sqrt{2}\right)^{k-1}<\frac{x+y\sqrt{2}}{3+2\sqrt{2}}\leqq\left(3+2\sqrt{2}\right)^{k}.\qquad\cdots\cdots④$$

$\dfrac{x+y\sqrt{2}}{3+2\sqrt{2}}=\left(x+y\sqrt{2}\right)\left(3-2\sqrt{2}\right)$ で，$(3,-2)$ は①の整数解だから，(1) より

$$\left(x+y\sqrt{2}\right)\left(3-2\sqrt{2}\right)=u+v\sqrt{2}$$

の形に書けて，$u^2-2v^2=1$ を満たす.

よって，u,v は整数で，$u^2-2v^2=1$ を満たし，④は

$$\left(3+2\sqrt{2}\right)^{k-1}<u+v\sqrt{2}\leqq\left(3+2\sqrt{2}\right)^{k}.\qquad\cdots\cdots⑤$$

と書き直せる．仮定から，$u+v\sqrt{2}=\left(3+2\sqrt{2}\right)^{k}$ が言える.

よって，$\dfrac{x+y\sqrt{2}}{3+2\sqrt{2}}=u+v\sqrt{2}$ から

$$x+y\sqrt{2}=\left(3+2\sqrt{2}\right)\left(u+v\sqrt{2}\right)=\left(3+2\sqrt{2}\right)\left(3+2\sqrt{2}\right)^{k}=\left(3+2\sqrt{2}\right)^{k+1}.$$

ゆえに，$n=k+1$ のときも (P) は成り立つ．

(III) (I)，(II) から，すべての正の整数に対して (P) は成り立つ． □

(3) の別解　x, y は整数で，$x^2-2y^2=1$ を満たしている．

n は正の整数で，$\left(3+2\sqrt{2}\right)^{n-1} < x+y\sqrt{2} \leqq \left(3+2\sqrt{2}\right)^{n}$ が成り立つとする．

この不等式の各辺を $\left(3+2\sqrt{2}\right)^{n-1}$ で割ると，

$$1 < \frac{x+y\sqrt{2}}{\left(3+2\sqrt{2}\right)^{n-1}} \leq 3+2\sqrt{2}. \qquad \cdots\cdots ④$$

$A=\left\{p+q\sqrt{2} : p,\, q\in\mathbb{Z},\ p^2-2q^2=1\right\}$ とおくと，(1) より，$a+b\sqrt{2},\ x+y\sqrt{2}\in A$ ならば，$\left(a+b\sqrt{2}\right)\left(x+y\sqrt{2}\right)\in A$ が成り立つから，帰納的に，m が正の整数のとき，$a_i+b_i\sqrt{2}\in A\ (i=1,\ldots,m)$ ならば $\left(a_1+b_1\sqrt{2}\right)\cdots\left(a_m+b_m\sqrt{2}\right)\in A$ が言える．

$3-2\sqrt{2}\in A$ だから $\left(3-2\sqrt{2}\right)^{n-1}\in A$ となり，

$$\left(3-2\sqrt{2}\right)^{n-1} = u+v\sqrt{2}\ \left(u^2-2v^2=1,\, u,v\in\mathbb{Z}\right)$$

とおける．

$$\frac{x+y\sqrt{2}}{\left(3+2\sqrt{2}\right)^{n-1}} = \left(x+y\sqrt{2}\right)\left(3-2\sqrt{2}\right)^{n-1} = \left(x+y\sqrt{2}\right)\left(u+v\sqrt{2}\right)\in A$$

であるから

$$\left(x+y\sqrt{2}\right)\left(u+v\sqrt{2}\right) = X+Y\sqrt{2}\ \left(X^2-2Y^2=1,\, X,Y\in\mathbb{Z}\right)$$

とおける．④は $1<X+Y\sqrt{2}\leqq 3+2\sqrt{2}$ となり，②より $X=3, Y=2$ である．

よって，$\dfrac{x+y\sqrt{2}}{\left(3+2\sqrt{2}\right)^{n-1}} = X+Y\sqrt{2} = 3+2\sqrt{2}$ から

$$x+y\sqrt{2} = \left(3+2\sqrt{2}\right)^{n}$$

を得る． □

(3) の別解の証明は，定理 6.2.1(2) の証明と同じ方法であるが，次の京都大学の問題の証明方法は，早稲田大学の問題の証明方法とは異なっている．

問題 6.2.2 $A=\begin{pmatrix}2 & -3\\ -1 & 2\end{pmatrix}$ とする.

(1) $\begin{pmatrix}x'\\ y'\end{pmatrix}=A\begin{pmatrix}x\\ y\end{pmatrix}$ で，$x^2-3y^2=1,\ x>0, y\geqq 1$ ならば,

$x'^2-3y'^2=1,\ 0\leqq y'<y$ が成立することを示せ.

(2) x, y が $x^2-3y^2=1$ を満たす自然数ならば，ある自然数 n をとると

$\begin{pmatrix}1\\ 0\end{pmatrix}=A^n\begin{pmatrix}x\\ y\end{pmatrix}$ となることを示せ.　（1988　京都大）

解答

(1) $\begin{pmatrix}x'\\ y'\end{pmatrix}=A\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}2 & -3\\ -1 & 2\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}2x-3y\\ -x+2y\end{pmatrix}$ から $x'=2x-3y, y'=-x+2y$.

このとき，$x'^2-3y'^2=(2x-3y)^2-3(-x+2y)^2=x^2-3y^2=1$.

$x>0, y\geqq 1, x^2=3y^2+1$ であるから

$$y'\geqq 0\Leftrightarrow 2y\geqq x\Leftrightarrow 4y^2\geqq x^2\Leftrightarrow 4y^2\geqq 3y^2+1\Leftrightarrow y^2\geqq 1.$$

$y\geqq 1$ であるから，$y^2\geqq 1$ は成り立つので，$y'\geqq 0$.

同様にして

$$y>y'\Leftrightarrow y>-x+2y\Leftrightarrow x>y\Leftrightarrow x^2>y^2\Leftrightarrow 3y^2+1>y^2\Leftrightarrow 2y^2+1>0.$$

明らかに，$2y^2+1>0$ は成り立つので，$y>y'$.

(2) x, y が $x^2-3y^2=1$ を満たす自然数のとき，$\begin{pmatrix}x_1\\ y_1\end{pmatrix}=A\begin{pmatrix}x\\ y\end{pmatrix}$ とおくと，(1) から

x_1, y_1 は整数で，$x_1^2-2y_1^2=1,\ 0\leqq y_1<y$ を満たす.

x_1 は自然数であることを示す.

$x_1>0\Leftrightarrow 2x>3y\Leftrightarrow 4x^2>9y^2\Leftrightarrow 4\left(3y^2+1\right)>9y^2\Leftrightarrow 3y^2+4>0.$

明らかに，$3y^2+4>0$ は成り立つので，$x>0$.

$y_1\geqq 1$ ならば，$\begin{pmatrix}x_2\\ y_2\end{pmatrix}=A\begin{pmatrix}x_1\\ y_1\end{pmatrix}$ とおくと，x_2, y_2 は整数で,

$$x_2^2-2y_2^2=1,\ 0\leqq y_2<y_1, x_2\geqq 1$$

を満たす.

$y_2 \geqq 1$ ならば，同様な操作を繰り返すと，ある自然数 n が存在して，$y_n = 0$ となる．
x_n は $x_n^2 - 3y_n^2 = 1$ を満たす自然数だから，$x_n = 1$ となる．
したがって，$\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}x_n\\y_n\end{pmatrix} = A^n\begin{pmatrix}x\\y\end{pmatrix}$ となる． □

問題 6.2.3　次の□の中に適当な数または式を入れよ．また (イ)〜(ホ) の「 」で囲まれた文章の理由を，最後の (イ)〜(ホ) の解答のところで述べよ．

方程式　　$x^2 - 3y^2 = 1$　　……①

を満たす整数の組 (x, y) を求めることを考える（以下この方程式の整数解を単に解と略称する）．準備のために次のことを確かめておく．

(イ)　「a, b, c, d が整数であって，$a + b\sqrt{3} = c + d\sqrt{3}$ ならば，$a = c, b = d$ である．」

次に (x, y) が解であれば，$(x, -y), (-x, y), (-x, -y)$ も解であることは，方程式①により明らかであるから，(x, y) がともに負でない解を求めることが基本的である．それで，そのような解を求める手段として

$$(2 + \sqrt{3})^n = x_n + y_n\sqrt{3} \qquad \cdots\cdots\cdots ②$$

$(x_n, y_n$ は負でない整数，$n = 0, 1, 2, \ldots)$ とおく．そうすると (イ) によって

$$x_0 = 1, y_0 = 0, x_1 = 2, y_1 = 1 \qquad \cdots\cdots\cdots ③$$

$x_2 = \square, y_2 = \square, x_3 = \square, y_3 = \square$ である．

一方，$(2 + \sqrt{3})^2$ と $(2 - \sqrt{3})^2, (2 + \sqrt{3})^3$ と $(2 - \sqrt{3})^3$ などを比較することによって，一般に

$$(2 - \sqrt{3})^n = x_n - y_n\sqrt{3},\ n = 0, 1, \cdots \qquad \cdots\cdots\cdots ④$$

であることがわかる．

② と④ と $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$ とを使って

$$1 = (2 + \sqrt{3})^n(2 - \sqrt{3})^n = {x_n}^2 - 3{y_n}^2$$

となるから，② で定まる (x_n, y_n) は方程式 ① の解であることがわかる．とくに，x, y の一方が 0 となるような負でない解は，明らかに $x = 1, y = 0$ で，それは③の (x_0, y_0) に外ならない．

次に (x_{n-1}, y_{n-1}) と (x_n, y_n) との関係を求めてみる $(n \geqq 1)$.

$$x_n + y_n\sqrt{3} = (2 + \sqrt{3})^n = (x_{n-1} + y_{n-1}\sqrt{3})(2 + \sqrt{3}) = \square$$

ゆえに，$x_n = \square, y_n = \square$

したがって，(x_0, y_0) から出発して，負でない解 (x_1, y_1)，(x_2, y_2)，…，$(x_n, y_n), \ldots\ldots$ を順次求めて行くことができる．しかも $y_1 < y_2 < y_3 < \ldots$ である．

以上のことで負でない解を多数みつけたのであるが，これらで負でない解が尽くされているかどうかを次に吟味する．

いま任意の正の解 $(x,y),(x>0,y>0)$ をとると

$$(x+y\sqrt{3})(2-\sqrt{3})=(2x-3y)+(2y-x)\sqrt{3}$$

(ロ)「$x'=2x-3y, y'=2y-x$ とおくとき，(x',y') も解である．」

(ハ)「そして，$x>x'>0, y>y'\geqq 0$ である．」

(ニ)「それで，任意の正の解 (x,y) から出発して，(ロ) における (x',y') を求める操作を順次行うことによって，③に示す負でない解 (x_0,y_0) に達する．」

(ホ)「したがって，任意の負でない解 (x,y) は式②によって定まる (x_n,y_n) $(n=0,1,2,\ldots)$ のどれか 1 つである．」　（1967　京都大）

解答 (イ) の理由　a,b,c,d が整数であって，$a+b\sqrt{3}=c+d\sqrt{3}$ が成り立つとする．$a+b\sqrt{3}=c+d\sqrt{3}$ を変形すると，

$$a-c=(b-d)\sqrt{3}.$$

$b-d\neq 0$ ならば，$\sqrt{3}=\dfrac{a-c}{b-d}$ となり，右辺は有理数だから，$\sqrt{3}$ が有理数となる．これは $\sqrt{3}$ が無理数であることに矛盾する．したがって，$b-d=0$ でなければならない．このとき，$a-c=(b-d)\sqrt{3}$ より $a-c=0$.

ゆえに，$a=c, b=d$.

(ロ) の理由 (x,y) は正の整数解だから，$x'=2x-3y, y'=2y-x$ はともに整数で，

$$(x')^2-2(y')^2=(2x-3y)^2-2(2y-x)^2=x^2-3y^2=1.$$

ゆえに，(x',y') も解である．

(ハ) の理由 (x,y) は正の整数解であるから，$x\geq 1, y\geq 1, x^2=3y^2+1$.

$$x'>0\Leftrightarrow 2x>3y\Leftrightarrow 4x^2>9y^2\Leftrightarrow 4\left(3y^2+1\right)>9y^2\Leftrightarrow 3y^2+4>0.$$

明らかに，$3y^2+4>0$ は成り立つので，$x'>0$.

$$y'\geq 0\Leftrightarrow 2y\geq x\Leftrightarrow 4y^2\geq x^2\Leftrightarrow 4y^2\geq 3y^2+1\Leftrightarrow y^2\geq 1.$$

$y\geq 1$ であるから，$y^2\geq 1$ は成り立つので，$y'\geq 0$.

$$x>x'\Leftrightarrow x>2x-3y\Leftrightarrow 3y>x\Leftrightarrow 9y^2>x^2\Leftrightarrow 9y^2>3y^2+1\Leftrightarrow 6y^2>1.$$

$y\geq 1$ であるから，$6y^2>1$ は成り立つので，$x>x'$.

$$y>y'\Leftrightarrow y>-x+2y\Leftrightarrow x>y\Leftrightarrow x^2>y^2\Leftrightarrow 3y^2+1>y^2\Leftrightarrow 2y^2+1>0.$$

明らかに，$2y^2+1>0$ は成り立つので，$y>y'$.

(ニ) の理由 $y'>0$ ならば，(x,y) から出発して，(ロ) における (x',y') を求める操作を行うことによって，(x'',y'') を求める．
すると，$x'>x''\geq 1, y'>y''\geq 0, (x'')^2-3(y'')^2=1$ が成り立つ．$y''>0$ ならば，この操作を続ける．このようにして，操作を続けると，
y は正の整数だから，m 回（最大で y 回）の操作で，$\left(x^{(m)},y^{(m)}\right)$ $\left(y^{(m)}=0\right)$ に達するような正の整数 m が存在する．
このとき，$\left(x^{(m)}\right)^2-3\left(y^{(m)}\right)^2=1, x^{(m)}\geq 1$ より，$x^{(m)}=1$ となるから，

$$\left(x^{(m)},y^{(m)}\right)=(1,0)=(x_0,y_0).$$

したがって，任意の正の解 (x,y) から出発して，(ロ) における (x',y') を求める操作を順次行うことによって，③に示す負でない解 (x_0,y_0) に達することが言えた．

(ホ) の理由 負でない解 (x,y) は (x_0,y_0) と正の解 (x,y) に分けられる．

(x_0,y_0) のとき，$x_0+y_0\sqrt{3}=1=\left(3+2\sqrt{3}\right)^0$.

任意の正の解 (x,y) は，(x,y) から出発して，(ロ) における (x',y') を求める操作を順次行うことによって，③に示す負でない解 (x_0,y_0) に操作が m 回で達したとすると，$\left(x+y\sqrt{3}\right)\left(3-2\sqrt{3}\right)^m=x_0+y_0\sqrt{3}=1$ が成り立つ．ゆえに，

$$x+y\sqrt{3}=\frac{1}{\left(3-2\sqrt{3}\right)^m}=\left(3+2\sqrt{3}\right)^m.$$

したがって，任意の負でない解 (x,y) は式②によって定まる (x_n,y_n) $(n=0,1,2,\dots)$ のどれか 1 つであることが言えた．

□の中には次の数または式が入る．

7, 4, 26, 15, $(2x_{n-1}+3y_{n-1})+(x_{n-1}+2y_{n-1})\sqrt{3}$, $2x_{n-1}+3y_{n-1}$, $x_{n-1}+2y_{n-1}$. □

問題 6.3.1　$a \mid b^2+1$ かつ $b \mid a^2+1$ を満たすような正の整数 a, b の組 (a, b) をすべて求めよ．

解答　$a \mid b^2+1$ から a と b は互いに素である．

$a \mid b^2+1$ から $a \mid (b^2+1)+a^2$, $b \mid a^2+1$ から $b \mid (a^2+1)+b^2$.

すなわち，$a \mid a^2+b^2+1$ かつ $b \mid a^2+b^2+1$ が成り立つ．

a と b は互いに素であるから，$ab \mid a^2+b^2+1$ が成り立つ．

したがって，例題 6.1.3 より，$\dfrac{a^2+b^2+1}{ab} = 3$ が言える．この式を次のように変形する．

$$a^2-3ab+b^2+1=0 \qquad (2a-3b)^2-5b^2=-4.$$

例題 6.3.1 より，$x^2-5y^2=-4$ のすべての正の整数解 (x_n, y_n) は

$$\frac{x_n+y_n\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2}\right)^n \qquad (n=1,2,\dots)$$

から得られるので，

$$2a-3b=\pm x_n,\ b=y_n$$

すなわち

$$(a,b) = \left(\frac{x_n+3y_n}{2}, y_n\right),\ \left(\frac{-x_n+3y_n}{2}, y_n\right)$$

となる．

例題 6.3.1 の解答の途中で

$$x_{m+1} = \frac{3x_m+5y_m}{2},\ y_{m+1} = \frac{x_m+3y_m}{2} \quad (m \geq 1)$$

を示したのでこれを利用する．

$3y_1-x_1 = 3-1 = 2 > 0$ で

$$3y_{m+1}-x_{m+1} = 3\cdot\frac{x_m+3y_m}{2} - \frac{3x_m+5y_m}{2} = 2y_m > 0$$

が成り立つから，$-x_n+3y_n > 0$ $(n=1,2,\dots)$ が言えた．

したがって，求める (a, b) は

$$(a,b) = \left(\frac{x_n+3y_n}{2}, y_n\right),\ \left(\frac{-x_n+3y_n}{2}, y_n\right) \quad (n=1,2,\dots)$$

となる．　□

問題 6.3.2　D は平方数でない正の整数で，$\gcd(D,2)=1$ とする．
このとき，方程式 $x^2-Dy^2=4$ は正整数解 (x,y) をもつ．このような正整数解のうちで x が最小のものを (x_1,y_1) とすれば，すべての解 (x_n,y_n) は

$$\frac{x_n+y_n\sqrt{D}}{2}=\left(\frac{x_1+y_1\sqrt{D}}{2}\right)^n \quad (n=1,2,\dots)$$

から得られることを示せ．

解答　D は奇数だから，$x^2-Dy^2=4$ を満たす整数解 x,y の偶奇は一致する．

$$\frac{x_n+y_n\sqrt{D}}{2}=\left(\frac{x_1+y_1\sqrt{D}}{2}\right)^n \ (n=1,2,\dots)$$

から得られる数列 $\{x_n\}$，$\{y_n\}$ について調べる．

$$\begin{aligned}\frac{x_{n+1}+y_{n+1}\sqrt{D}}{2}&=\left(\frac{x_1+y_1\sqrt{D}}{2}\right)^{n+1}\\&=\left(\frac{x_1+y_1\sqrt{D}}{2}\right)\left(\frac{x_1+y_1\sqrt{D}}{2}\right)^n\\&=\left(\frac{x_1+y_1\sqrt{D}}{2}\right)\frac{x_n+y_n\sqrt{D}}{2}\\&=\frac{x_1x_n+Dy_1y_n}{4}+\frac{y_1x_n+x_1y_n}{4}\sqrt{D}\end{aligned}$$

から

$$x_{n+1}=\frac{x_1x_n+Dy_1y_n}{2},\ y_{n+1}=\frac{y_1x_n+x_1y_n}{2}.$$

行列を用いると

$$\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}=\frac{1}{2}\begin{pmatrix}x_1&Dy_1\\y_1&x_1\end{pmatrix}\begin{pmatrix}x_n\\y_n\end{pmatrix}$$

と表せる．

このようにして得られた (x_n,y_n) が $x^2-Dy^2=4$ の解であることを数学的帰納法で示す．

(I) $n=1$ のとき，$x^2-Dy^2=4$ の正整数解のうちで x が最小のものを (x_1,y_1) とおいたのだから，$x_1^2-Dy_1^2=4$ は明らかに成り立つ．

(II) n のとき成り立つと仮定すると，$x_n^2-Dy_n^2=4$.

$$\begin{aligned}x_{n+1}^2-Dy_{n+1}^2&=\frac{1}{4}\left((x_1x_n+Dy_1y_n)^2-D(y_1x_n+x_1y_n)^2\right)\\&=\frac{1}{4}\left(x_1^2-Dy_1^2\right)\left(x_n^2-Dy_n^2\right)\end{aligned}$$

$$= \frac{1}{4} \cdot 4 \cdot 4$$
$$= 4$$

となり，$n+1$ のときも成り立つ．

(III) (I)，(II) よりすべての正の整数 n に対して成り立つ．

◎ (u, v) を $x^2 - Dy^2 = 4$ を満たす任意の正の整数解とすると，

$$\frac{u + v\sqrt{D}}{2} = \left(\frac{x_1 + y_1\sqrt{D}}{2} \right)^k$$

となる正の整数 k が存在することを示す．

$z = \dfrac{x_1 + y_1\sqrt{D}}{2}$, $r = \dfrac{u + v\sqrt{D}}{2}$ とおく．

$z > 1$ であるから，$z, z^2, \ldots, z^n, \ldots$ は増加数列で，$\lim\limits_{n\to\infty} z^n = \infty$ を満たしている．

したがって

$$z^k \leq r < z^{k+1}$$

を満たす正の整数 k が存在する．

z^k で割ると $1 \leq \dfrac{r}{z^k} < z$.

$z^k = \dfrac{x_k + y_k\sqrt{D}}{2}$ が成り立つので

$$\frac{1}{z^k} = \frac{2}{x_k + y_k\sqrt{D}} = \frac{2\left(x_k - y_k\sqrt{D}\right)}{x_k^2 - 5y_k^2} = \frac{x_k - y_k\sqrt{D}}{2}.$$

これから，

$$\frac{r}{z^k} = \frac{u + v\sqrt{D}}{2} \frac{x_k - y_k\sqrt{D}}{2}$$
$$= \frac{(ux_k - Dvy_k) + (vx_k - uy_k)\sqrt{D}}{4}$$

となるので，$s = \dfrac{ux_k - Dvy_k}{4}, t = \dfrac{vx_k - uy_k}{4}$ とおくと，

$$1 \leq s + t\sqrt{5} < z \qquad \cdots\cdots ①$$

が成り立つ．

また，

$$s^2 - Dt^2 = \frac{1}{16}\left((-ux_k + Dvy_k)^2 - D(-vx_k + uy_k)^2\right)$$
$$= \frac{1}{16}\left(x_k^2 - Dy_k^2\right)\left(u^2 - Dv^2\right)$$

$$= \frac{1}{16} \cdot 4 \cdot 4 = 1$$

から

$$s^2 - Dt^2 = 1 \qquad \cdots\cdots ②$$

が成り立つ.

- $s = 1$ かつ $t = 0$ を示す.
  ②から $\left(s + t\sqrt{D}\right)\left(s - t\sqrt{D}\right) = 1$.
  ①から $s + t\sqrt{D} > 0$ だから，上の等式より $s - t\sqrt{D} > 0$ が言える.
  よって，$2s = \left(s + t\sqrt{D}\right) + \left(s - t\sqrt{D}\right) > 0$ から，$s > 0$ が成り立つ.
  もしも $t < 0$ だとすると，①から $s + t\sqrt{D} \geq 1$ なので

$$1 = s^2 - Dt^2 = \left(s - t\sqrt{D}\right)\left(s + t\sqrt{D}\right) > \left(s + t\sqrt{D}\right)^2 \geq 1$$

  と矛盾が生じる.
  よって $t \geq 0$ である.
  $t > 0$ だとすると，②から $(2s)^2 - D(2t)^2 = 4$.
  また，$2s = \dfrac{ux_k - Dvy_k}{2}$, $2t = \dfrac{vx_k - uy_k}{2}$ において x_k, y_k の偶奇と u, v の偶奇は一致するから，$2s, 2t$ は整数である．$(2s, 2t)$ は $x^2 - Dy^2 = 4$ の正の整数解となる.
  $x^2 - Dy^2 = 4$ の正の最小整数解は (x_1, y_1) だから，$2s \geq x_1$ でなければならない.
  このとき,

$$(2t)^2 = \frac{(2s)^2 - 4}{D} \geq \frac{x_1^2 - 4}{D} = y_1^2$$

  から $2t \geq y_1$ が成り立つ.
  すると，$2s + 2t\sqrt{D} \geq x_1 + y_1\sqrt{D} = 2z$ となり，①の $s + t\sqrt{5} < z$ に矛盾する.
  よって，$t = 0$ でなければならず，このとき②より $s = 1$ となる.

$s = 1$ かつ $t = 0$ より，$\dfrac{r}{z^k} = s + t\sqrt{D} = 1$ で，$u + v\sqrt{D} = r = z^k$ となる. □

- 問題 6.3.2 において，$\gcd(D, 2) > 1$ のときは次のようになる.
  $4 \mid D$ のとき $D = 4D'$ (D' は平方数ではない正の整数) とおく．$x^2 = Dy^2 + 4$ から整数解 (x, y) は x^2 が 4 の倍数になるから，x は 2 の倍数である．$x = 2X$, $X \in \mathbb{Z}$ とおき，$x^2 - Dy^2 = 4$ に代入すると，$X^2 - D'y^2 = 1$ というペル方程式になる.
  また，$2 \mid D$ かつ $4 \nmid D$ のとき $x^2 = Dy^2 + 4$ から整数解 (x, y) は x^2 が 2 の倍数になるから，x は 2 の倍数である．$x = 2X$, $X \in \mathbb{Z}$ とおき，$x^2 - Dy^2 = 4$ に代入すると，$Dy^2 = 4\left(X^2 - 1\right)$ となり，Dy^2 は 4 の倍数である．仮定から，$2 \mid D$ かつ $4 \nmid D$ なので y^2 は 2 の倍数，すなわち y は 2 の倍数である．$y = 2Y$, $Y \in \mathbb{Z}$ とおき，$4X^2 - Dy^2 = 4$ に代入すると，$X^2 - Dy^2 = 1$ というペル方程式になる.

ペル方程式に関連する数列の問題をまとめてみた.

基本問題 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n = a+b\sqrt{3}$　(a, b は正の整数) と表せることを示せ.

解答　n に関する数学的帰納法で証明する.

(I) $n=1$ のときは，$a_1=2$, $b_1=1$ とおくと，$2+\sqrt{3}=a_1+b_1\sqrt{3}$ と表せる.

(II) $n=k$ のとき成り立つと仮定すると，$\left(2+\sqrt{3}\right)^k = a_k+b_k\sqrt{3}$　(a_k , b_kは正の整数) と表せる.

$$\begin{aligned}\left(2+\sqrt{3}\right)^{k+1} &= \left(2+\sqrt{3}\right)\left(2+\sqrt{3}\right)^k \\ &= \left(2+\sqrt{3}\right)\left(a_k+b_k\sqrt{3}\right) \\ &= 2a_k+3b_k+(a_k+2b_k)\sqrt{3}\end{aligned}$$

となるから，$a_{k+1}=2a_k+3b_k$, $b_{k+1}=a_k+2b_k$ とおくと，a_{k+1}, b_{k+1} は正の整数で

$$\left(2+\sqrt{3}\right)^{k+1} = a_{k+1}+b_{k+1}\sqrt{3}$$

と表せるから，$n=k+1$ のときも成り立つ.

(III) (I), (II) よりすべての正の整数に対して，$\left(2+\sqrt{3}\right)^n = a+b\sqrt{3}$　(a, b は正の整数) と表せる. □

別解 二項定理より

$$\begin{aligned}\left(2+\sqrt{3}\right)^n &= \sum_{k=0}^{n} {}_n\mathrm{C}_k 2^{n-k}\left(\sqrt{3}\right)^k \\ &= \sum_{k:\text{偶数}}^{n} {}_n\mathrm{C}_k 2^{n-k}\left(\sqrt{3}\right)^k + \sum_{k:\text{奇数}}^{n} {}_n\mathrm{C}_k 2^{n-k}\left(\sqrt{3}\right)^k \\ &= \sum_{m=1}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m}\left(\sqrt{3}\right)^{2m} + \sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)}\left(\sqrt{3}\right)^{2m-1} \\ &= \sum_{m=1}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m}3^m + \sqrt{3}\sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)}3^{m-1}\end{aligned}$$

したがって

$$a = \sum_{m=1}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m}3^m,\ b = \sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)}3^{m-1}$$

とおくと，a, b は正の整数で，$\left(2+\sqrt{3}\right)^n = a+b\sqrt{3}$ と表せることがわかった． □

注　解答で数列 $\{a_n\}$ を用いたのは，問題 6.3.3 等を解くために便利だからである．

- $\left(2+\sqrt{3}\right)^n = a+b\sqrt{3}$　(a, b は正の整数) と表すことができ，表し方はただ 1 通りである．

$\left(2+\sqrt{3}\right)^n = a+b\sqrt{3}$　(a, b は正の整数)，$\left(2+\sqrt{3}\right)^n = c+d\sqrt{3}$　(c, d は正の整数) と表せたとすると

$$a+b\sqrt{3} = c+d\sqrt{3}.$$

この式を変形すると

$$(b-d)\sqrt{3} = c-a. \qquad \cdots\cdots ①$$

$b \neq d$ と仮定すると

$$\sqrt{3} = \frac{c-a}{b-d}.$$

左辺は無理数，右辺は有理数であるから矛盾が生じる．

よって，$b=d$ でなければならず，①より $a=c$ となる． □

問題 6.3.3 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n = a_n+b_n\sqrt{3}$　(a_n, b_nは正の整数) と表すとき，a_{n+1}, b_{n+1} をそれぞれ a_n, b_n で表せ．

解答

$$\begin{aligned}\left(2+\sqrt{3}\right)^{n+1} &= \left(2+\sqrt{3}\right)\left(2+\sqrt{3}\right)^n \\ &= \left(2+\sqrt{3}\right)\left(a_n+b_n\sqrt{3}\right) \\ &= 2a_n+3b_n+(a_n+2b_n)\sqrt{3}.\end{aligned}$$

また

$$\left(2+\sqrt{3}\right)^{n+1} = a_{n+1}+b_{n+1}\sqrt{3}$$

と表せるから，

$$a_{n+1}+b_{n+1}\sqrt{3} = 2a_n+3b_n+(a_n+2b_n)\sqrt{3}.$$

$2a_n+3b_n$, a_n+2b_n, a_{n+1}, b_{n+1} は正の整数で，$\sqrt{3}$ は無理数だから，

$$a_{n+1} = 2a_n+3b_n,\ b_{n+1} = a_n+2b_n.$$ □

問題 6.3.4 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n = a_n+b_n\sqrt{3}$　(a_n, b_nは正の整数) と表すとき，$\left(2-\sqrt{3}\right)^n = a_n-b_n\sqrt{3}$ と表されることを示せ．

解 1　n に関する数学的帰納法で証明する．

(I) $n=1$ のとき

$2+\sqrt{3}=a_1+b_1\sqrt{3}$　(a_1, b_1は正の整数) と表せることから，$a_1=2$, $b_1=1$ となるから $2-\sqrt{3}=a_1-b_1\sqrt{3}$ と表せる．

(II) $n=k$ のとき成り立つと仮定すると，$\left(2-\sqrt{3}\right)^k=a_k-b_k\sqrt{3}$ と表せる．

$$\begin{aligned}\left(2-\sqrt{3}\right)^{k+1}&=\left(2-\sqrt{3}\right)\left(2-\sqrt{3}\right)^k\\&=\left(2-\sqrt{3}\right)\left(a_k-b_k\sqrt{3}\right)\\&=2a_k+3b_k-(a_k+2b_k)\sqrt{3}\end{aligned}$$

となる．問題 6.3.3 の結果から，$a_{k+1}=2a_k+3b_k$，$b_{k+1}=a_k+2b_k$ が成り立つから，

$$\left(2-\sqrt{3}\right)^{k+1}=a_{k+1}-b_{k+1}\sqrt{3}$$

と表せるから，$n=k+1$ のときも成り立つ．

(III) (I)，(II) よりすべての正の整数に対して成り立つ．

解 2 問題 6.3.3 の結果より

$$\begin{aligned}a_{n+1}-b_{n+1}\sqrt{3}&=2a_n+3b_n-(a_n+2b_n)\sqrt{3}\\&=\left(2-\sqrt{3}\right)\left(a_n-b_n\sqrt{3}\right)\end{aligned}$$

$\left\{a_n-b_n\sqrt{3}\right\}$ は初項 $a_1-b_1\sqrt{3}$，公比 $2-\sqrt{3}$ の等比数列であるから

$$a_n-b_n\sqrt{3}=\left(a_1-b_1\sqrt{3}\right)\left(2-\sqrt{3}\right)^{n-1}$$

ここで，$a_1+b_1\sqrt{3}=2+\sqrt{3}$ より $a_1=2\,,b_1=1$

よって

$$a_n-b_n\sqrt{3}=\left(a_1-b_1\sqrt{3}\right)\left(2-\sqrt{3}\right)^{n-1}=\left(2-\sqrt{3}\right)^n.\qquad\square$$

解 3 二項定理より

$$\begin{aligned}\left(2+\sqrt{3}\right)^n&=\sum_{k=0}^{n}{}_n\mathrm{C}_k2^{n-k}\left(\sqrt{3}\right)^k\\&=\sum_{k:\text{偶数}}^{n}{}_n\mathrm{C}_k2^{n-k}\left(\sqrt{3}\right)^k+\sum_{k:\text{奇数}}^{n}{}_n\mathrm{C}_k2^{n-k}(\sqrt{3})^k\\&=\sum_{m=1}^{\left[\frac{n}{2}\right]}{}_n\mathrm{C}_{2m}2^{n-2m}\left(\sqrt{3}\right)^{2m}+\sum_{m=1}^{\left[\frac{n+1}{2}\right]}{}_n\mathrm{C}_{2m-1}2^{n-(2m-1)}\left(\sqrt{3}\right)^{2m-1}\end{aligned}$$

$$= \sum_{m=1}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m} 3^m + \sqrt{3} \sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)} 3^{m-1}$$

したがって

$$a_n = \sum_{m=1}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m} 3^m \,,\; b_n = \sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)} 3^{m-1}$$

を得る.

このとき,

$$\begin{aligned}
\left(2-\sqrt{3}\right)^n &= \sum_{k=0}^{n} {}_n\mathrm{C}_k 2^{n-k} \left(-\sqrt{3}\right)^k \\
&= \sum_{k:\text{偶数}}^{n} {}_n\mathrm{C}_k 2^{n-k} \left(-\sqrt{3}\right)^k + \sum_{k:\text{奇数}}^{n} {}_n\mathrm{C}_k 2^{n-k} \left(-\sqrt{3}\right)^k \\
&= \sum_{m=1}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m} (-\sqrt{3})^{2m} + \sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)} (-\sqrt{3})^{2m-1} \\
&= \sum_{m=1}^{\left[\frac{n}{2}\right]} {}_n\mathrm{C}_{2m} 2^{n-2m} 3^m - \sqrt{3} \sum_{m=1}^{\left[\frac{n+1}{2}\right]} {}_n\mathrm{C}_{2m-1} 2^{n-(2m-1)} 3^{m-1} \\
&= a_n - b_n\sqrt{3}. \qquad \square
\end{aligned}$$

問題 6.3.5 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n = a_n + b_n\sqrt{3}$ $(a_n\,, b_n$は正の整数$)$ と表すとき，$a_n\,, b_n$ を求めよ.

解答 問題 6.3.4 の結果より

$$a_n + b_n\sqrt{3} = \left(2+\sqrt{3}\right)^n,\; a_n - b_n\sqrt{3} = \left(2-\sqrt{3}\right)^n$$

この連立方程式を解くと

$$a_n = \frac{\left(2+\sqrt{3}\right)^n + \left(2-\sqrt{3}\right)^n}{2},\; b_n = \frac{\left(2+\sqrt{3}\right)^n - \left(2-\sqrt{3}\right)^n}{2\sqrt{3}} \quad . \qquad \square$$

問題 6.3.6 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n = a_n + b_n\sqrt{3}$ $(a_n,\, b_n$は正の整数$)$ と表すとき，${a_n}^2 - 3{b_n}^2$ を求めよ.

解答 問題 6.3.4 の結果より

$$\begin{aligned} {a_n}^2 - 3{b_n}^2 &= \left(a_n + b_n\sqrt{3}\right)\left(a_n - b_n\sqrt{3}\right) \\ &= \left(2+\sqrt{3}\right)^n \left(2-\sqrt{3}\right)^n \\ &= (4-3)^n = 1. \end{aligned}$$

□

別解 問題 6.3.3 の結果より

$$a_{n+1} = 2a_n + 3b_n,\ b_{n+1} = a_n + 2b_n$$

これを使うと

$$\begin{aligned} {a_{n+1}}^2 - 3{b_{n+1}}^2 &= (2a_n + 3b_n)^2 - 3(a_n + 2b_n)^2 \\ &= {a_n}^2 - 3{b_n}^2 \end{aligned}$$

が成り立つから

$${a_n}^2 - 3{b_n}^2 = {a_1}^2 - 3{b_1}^2$$

ところで，$2+\sqrt{3} = a_1 + b_1\sqrt{3}$ より $a_1 = 2\,, b_1 = 1$ となるから ${a_1}^2 - 3{b_1}^2 = 1$
よって，${a_n}^2 - 3{b_n}^2 = 1$ □

注 n に関する数学的帰納法で証明することもできるが，本質的なところは，別解と同じである．

- 問題 6.3.6 の結果から，(a_n, b_n) は双曲線 $x^2 - 3y^2 = 1$ 上にあることがわかる．

双曲線 $x^2 - 3y^2 = 1$ 上の第 1 象限における格子点は，(a_n, b_n) に限るかということが問題になるが，京都大学や早稲田大学の本格的なペル方程式の問題を解いて，答えを見つけてほしい．

問題 6.3.7 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n = \sqrt{M+1} + \sqrt{M}$ となる整数 M が存在することを示せ．

解答 問題 6.3.6 の結果より，${a_n}^2 - 3{b_n}^2 = 1$ だから

$$\begin{aligned} \left(2+\sqrt{3}\right)^n &= a_n + b_n\sqrt{3} \\ &= \sqrt{{a_n}^2} + \sqrt{3{b_n}^2} \\ &= \sqrt{3{b_n}^2 + 1} + \sqrt{3{b_n}^2} \end{aligned}$$

$M = 3{b_n}^2 \geq 3$ とおくと，M は正の整数で

$$\left(2+\sqrt{3}\right)^n = \sqrt{M+1} + \sqrt{M}.$$

□

注　正の整数 n に対して，$\left(2-\sqrt{3}\right)^n=\sqrt{M+1}-\sqrt{M}$ となる正の整数 M が存在する．

問題 6.3.8 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$　(a_n, b_nは正の整数) と表すとき，$\left(2+\sqrt{3}\right)^n$ の整数部分を a_n で表せ．

解答 問題 6.3.5 の結果より

$$2a_n=\left(2+\sqrt{3}\right)^n+\left(2-\sqrt{3}\right)^n$$

ゆえに，

$$\left(2+\sqrt{3}\right)^n=2a_n-\left(2-\sqrt{3}\right)^n=2a_n-1+1-\left(2-\sqrt{3}\right)^n$$

$0<1-\left(2-\sqrt{3}\right)^n<1$ で $2a_n-1$ は整数だから，$\left(2+\sqrt{3}\right)^n$ の整数部分は $2a_n-1$ である．　□

注　$\left(2+\sqrt{3}\right)^n$ の小数部分は $0<1-\left(2-\sqrt{3}\right)^n$ になる．

問題 6.3.9 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$　(a_n, b_nは正の整数) と表すとき，$\lim\limits_{n\to\infty}\dfrac{a_n}{b_n}$ を求めよ．

解答 問題 6.3.5 の結果より

$$a_n=\frac{\left(2+\sqrt{3}\right)^n+\left(2-\sqrt{3}\right)^n}{2},\ b_n=\frac{\left(2+\sqrt{3}\right)^n-\left(2-\sqrt{3}\right)^n}{2\sqrt{3}}\quad .$$

よって

$$\begin{aligned}\lim_{n\to\infty}\frac{a_n}{b_n}&=\lim_{n\to\infty}\sqrt{3}\cdot\frac{\left(2+\sqrt{3}\right)^n+\left(2-\sqrt{3}\right)^n}{\left(2+\sqrt{3}\right)^n-\left(2-\sqrt{3}\cdot\right)^n}\\&=\lim_{n\to\infty}\sqrt{3}\cdot\frac{1+\dfrac{\left(2+\sqrt{3}\right)^n}{\left(2-\sqrt{3}\right)^n}}{1-\dfrac{\left(2+\sqrt{3}\right)^n}{\left(2-\sqrt{3}\right)^n}}=\sqrt{3}\end{aligned}$$

から，$\lim\limits_{n\to\infty}\dfrac{a_n}{b_n}=\sqrt{3}$.　□

問題 6.3.10 正の整数 n に対して，$\left(2+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$　(a_n, b_nは正の整数) と表すとき，不等式 $\left|\sqrt{3}-\dfrac{a_n}{b_n}\right|>\left|\sqrt{3}-\dfrac{a_{n+1}}{b_{n+1}}\right|$ が成り立つことを証明せよ．

解答 問題 6.3.6 の結果より，${a_n}^2 - 3{b_n}^2 = 1$ が成り立つから

$$\left(a_n - \sqrt{3}\, b_n\right)\left(a_n + \sqrt{3}\, b_n\right) = 1.$$

この式を変形すると

$$a_n - \sqrt{3} b_n = \frac{1}{a_n + \sqrt{3}\, b_n}.$$

両辺を $b_n\,(b_n > 0)$ で割ると

$$\frac{a_n}{b_n} - \sqrt{3} = \frac{1}{b_n\left(a_n + \sqrt{3}\, b_n\right)}. \qquad \cdots\cdots ①$$

問題 6.3.3 の結果より，

$$a_{n+1} = 2a_n + 3b_n,\ b_{n+1} = a_n + 2b_n$$

が成り立ち，$a_n > 0, b_n > 0$ だから

$$a_{n+1} = 2a_n + 3b_n > a_n,\ b_{n+1} = a_n + 2b_n > b_n.$$

よって，$a_{n+1} > a_n$, $b_{n+1} > b_n$ を使うと

$$\frac{a_n}{b_n} - \sqrt{3} = \frac{1}{b_n\left(a_n + \sqrt{3}\, b_n\right)} > \frac{1}{b_{n+1}\left(a_{n+1} + \sqrt{3}\, b_{n+1}\right)} = \frac{a_{n+1}}{b_{n+1}} - \sqrt{3}$$

すなわち

$$\frac{a_n}{b_n} - \sqrt{3} > \frac{a_{n+1}}{b_{n+1}} - \sqrt{3}.$$

①から $\dfrac{a_n}{b_n} - \sqrt{3} > 0\ (n = 1, 2, \dots)$ だから $\left|\sqrt{3} - \dfrac{a_n}{b_n}\right| > \left|\sqrt{3} - \dfrac{a_{n+1}}{b_{n+1}}\right|$ が成り立つ．□

- $\dfrac{a_{n+1}}{b_{n+1}}$ は $\dfrac{a_n}{b_n}$ よりもよい近似値であることがわかった．
- 4 世紀に，インドの数学者 Baudhayana は $\sqrt{2}$ の近似値として $\dfrac{577}{408}$ を使い，ペル方程式 $x^2 - 2y^2 = 1$ の 1 つの解 $x = 577, y = 408$ を見つけている．

問題 6.3.11 正の整数 n に対して，$\left(2 + \sqrt{3}\right)^n = a_n + b_n\sqrt{2}$　$(a_n, b_n$は正の整数$)$ と表すとき，すべての正の整数 n に対して a_n と b_n は互いに素であることを証明せよ．

解答　n に関する数学的帰納法で示す．

(I) $n = 1$ のとき

$2 + \sqrt{3} = a_1 + b_1\sqrt{3}$　$(a_1, b_1$は正の整数$)$ と表せることから，$a_1 = 2, b_1 = 1$ となるから，a_1 と b_1 は互いに素である．

(II) $n = k$ のとき成り立つと仮定する．a_{k+1} と b_{k+1} の最大公約数を g とすると，$a_{k+1} = ga'$, $b_{k+1} = gb'$ (a'は b'は互いに素) とおける．
問題 6.3.3 の結果より

$$a_{k+1} = 2a_k + 3b_k,\ b_{k+1} = a_k + 2b_k$$

が成り立つから，これを a_k, b_k について解くと

$$a_k = 2a_{k+1} - 3b_{k+1},\ b_k = -a_{k+1} + 2b_{k+1}.$$

これを用いると

$$a_k = 2a_{k+1} - 3b_{k+1} = g(2a' - 3b'),\ b_k = -a_{k+1} + 2b_{k+1} = g(-a' + 2b')$$

すなわち

$$a_k = g(2a' - 3b'),\ b_k = g(-a' + 2b')$$

を得る．a_k と b_k は互いに素であるから，$g = 1$ でなければならない．よって，a_{k+1} と b_{k+1} は互いに素となり，$n = k + 1$ のときも成り立つ．

(III) (I)，(II) より，すべての正の整数 n に対して a_n と b_n は互いに素である． □

別解 問題 6.3.6 の結果より，${a_n}^2 - 3{b_n}^2 = 1$ が成り立つ．
a_n と b_n の最大公約数を g とすると，$a_n = ga'$, $b_n = gb'$ (a'は b'は互いに素) とおける．
これらを ${a_n}^2 - 3{b_n}^2 = 1$ に代入すると

$$g^2\left((a')^2 - 3(b')^2\right) = 1.$$

よって，$g = 1$ でなければならないから a_n と b_n は互いに素である． □

問題 6.3.12
正の整数 n に対して，$\left(3 + 2\sqrt{2}\right)^n = a_n + b_n\sqrt{2}$ (a_n, b_nは正の整数) と表すとき，すべての正の整数 n に対して

$$\frac{\left(17 + 12\sqrt{2}\right)^n - \left(17 - 12\sqrt{2}\right)^n}{4\sqrt{2}}$$

は整数であるが平方数にならないことを証明せよ．

解答 $17 + 12\sqrt{2} = \left(3 + 2\sqrt{2}\right)^2$ であるから

$$\frac{\left(17 + 12\sqrt{2}\right)^n - \left(17 - 12\sqrt{2}\right)^n}{4\sqrt{2}} = \frac{\left(3 + 2\sqrt{2}\right)^{2n} - \left(3 - 2\sqrt{2}\right)^{2n}}{4\sqrt{2}}$$
$$= \frac{\left(3 + 2\sqrt{2}\right)^n + \left(3 - 2\sqrt{2}\right)^n}{2} \cdot \frac{\left(3 + 2\sqrt{2}\right)^n - \left(3 - 2\sqrt{2}\right)^n}{2\sqrt{2}}.$$

$A_n = \dfrac{\left(3+2\sqrt{2}\right)^n + \left(3-2\sqrt{2}\right)^n}{2}$, $B_n = \dfrac{\left(3+2\sqrt{2}\right)^n - \left(3-2\sqrt{2}\right)^n}{2\sqrt{2}}$ とおく.

$\left(3+2\sqrt{2}\right)^n = a_n + b_n\sqrt{2}$ のとき $\left(3-2\sqrt{2}\right)^n = a_n - b_n\sqrt{2}$ となるから,
$A_n = a_n, B_n = b_n$ が成り立つことがわかる.
すると

$$\frac{\left(17+12\sqrt{2}\right)^n - \left(17-12\sqrt{2}\right)^n}{4\sqrt{2}} = a_n b_n$$

は整数であることがわかる.

$$\begin{aligned} a_n^2 - 2b_n^2 &= \left(a_n + b_n\sqrt{2}\right)\left(a_n - b_n\sqrt{2}\right) = \left(3+2\sqrt{2}\right)^n \left(3-2\sqrt{2}\right)^n \\ &= \left(\left(3+2\sqrt{2}\right)\left(3-2\sqrt{2}\right)\right)^n \\ &= 1 \end{aligned}$$

であるから，a_n と b_n は互いに素である.

したがって，a_n と b_n のうち少なくとも 1 つが平方数でないことを示せばよい.

$3+2\sqrt{2} = \left(1+\sqrt{2}\right)^2$, $3-2\sqrt{2} = \left(1-\sqrt{2}\right)^2$ であることに注意する.

$\left(1+\sqrt{2}\right)^n = x_n + y_n\sqrt{2}$, $\left(1-\sqrt{2}\right)^n = x_n - y_n\sqrt{2}$ となる正の整数 x_n, y_n が存在するから

$$x_n = \frac{\left(1+\sqrt{2}\right)^n + \left(1-\sqrt{2}\right)^n}{2},\ y_n = \frac{\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n}{2\sqrt{2}}.$$

この等式を使うと

$$\begin{aligned} a_n = A_n &= \frac{\left(1+\sqrt{2}\right)^{2n} + \left(1-\sqrt{2}\right)^{2n}}{2} \\ &= \frac{\left(\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n\right)^2 + 2\left(1+\sqrt{2}\right)^n\left(1-\sqrt{2}\right)^n}{2} \\ &= \left(\frac{\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n}{\sqrt{2}}\right)^2 + (-1)^n \\ &= (2y_n)^2 + (-1)^n. \end{aligned}$$

n が偶数のとき，$a_n = (2y_n)^2 + 1$ で $(2y_n)^2 < (2y_n)^2 + 1 < (2y_n+1)^2$ だから，a_n は平方数にならない.

n が奇数のとき，$a_n = (2y_n)^2 - 1$ で $2y_n \geqq 2$ なので，$(2y_n-1)^2 < (2y_n)^2 - 1 < (2y_n)^2$ だから，a_n は平方数にならない. □

問題 7.4.1 Let k be a positive integer. Find all positive integers n such that $3^k \mid 2^n - 1$.

解答 明らかに $n \geq 2$ である．

n が奇数のとき，$2^n - 1 \equiv (-1)^n - 1 \equiv -2 \equiv 1 \not\equiv 0 \pmod 3$ となり $3 \mid 3^k \mid 2^n - 1$ に矛盾する．

したがって，n は偶数で，$3^k \mid 2^n - 1$ より $v_3(2^n - 1) \geq k$.

$3 \mid 4 - 1, 3 \nmid 4, 3 \nmid 1$ だから，定理 7.2.1 より

$$v_3\left(2^n - 1\right) = v_3\left(4^{\frac{n}{2}} - 1^{\frac{n}{2}}\right) = v_3(4-1) + v_3\left(\frac{n}{2}\right) = 1 + v_3\left(\frac{n}{2}\right).$$

よって，$1 + v_3\left(\dfrac{n}{2}\right) \geq k$ から $v_3\left(\dfrac{n}{2}\right) \geq k - 1$.

これから，$\dfrac{n}{2} = 3^{k-1}s,\ s \in \mathbb{N}$ すなわち

$$n = 2 \cdot 3^{k-1} \cdot s,\ s \in \mathbb{N}$$

となる．このとき，n は偶数で，

$$v_3\left(2^n - 1\right) = v_3\left(4^{\frac{n}{2}} - 1^{\frac{n}{2}}\right) = v_3(4-1) + v_3\left(\frac{n}{2}\right) \geq 1 + k - 1 = k$$

となり，$3^k \mid 2^n - 1$ は成り立つ．

したがって，求める n は，$n = 2 \cdot 3^{k-1} \cdot s,\ s \in \mathbb{N}$ □

問題 7.4.2(UNESCO Competition 1995)

Let a, n be two positive integers and let p be an odd prime number such that

$$a^p \equiv 1 \pmod{p^n}.$$

Prove that

$$a \equiv 1 \pmod{p^{n-1}}.$$

解答 $a^p \equiv 1 \pmod{p^n}$. ……①

とおく．フェルマーの小定理より

$$a^p \equiv a \pmod{p}.$$ ……②

①から $a^p \equiv 1 \pmod p$ が成り立つから，②を用いると，$a \equiv 1 \pmod p$.

$p \mid a - 1, p \nmid a, p \nmid 1$ だから，定理 7.2.1 より

$$v_p\left(a^p - 1\right) = v_p\left(a - 1\right) + v_p\left(p\right) = v_p\left(a - 1\right) + 1.$$

$v_p\left(a^p-1\right)\geq n$ を用いると，$v_p\left(a-1\right)=v_p\left(a^p-1\right)-1\geq n-1$ から $p^{n-1}\mid a-1$ すなわち $a\equiv 1\pmod{p^{n-1}}$. □

問題 7.4.3 (Iran Second Round 2008)

Show that the only positive integer value of a for which $4\left(a^n+1\right)$ is a perfect cube for all positive integers n, is 1.

解答 すべての正整数 n について

$$4\left(a^n+1\right)=\left(f(n)\right)^3, f(n)\in\mathbb{N} \qquad \cdots\cdots ①$$

が成り立つ.

$a=1$ のとき，$4\left(a^n+1\right)=8=2^3$ で成り立つ.

$a\geq 2$ のとき

a^2+1 について考えると，

a が偶数のとき，$a^2+1\equiv 1\pmod 4$, a が奇数のとき，$a^2+1\equiv 2\pmod 4$ だから，$a^2+1=2^k$ $(k\in\mathbb{N})$ の形にならない．よって，$p\mid a^2+1$ となる奇素数 p が存在する.

$n=2m$ (m は奇数) とおくと

$$\begin{aligned} v_p\left(4\left(a^n+1\right)\right)&=v_p(4)+v_p\left(a^n+1\right)=v_p\left(a^n+1\right)=v_p\left(a^{2m}+1\right)\\ &=v_p\left(\left(a^2\right)^m+1\right). \end{aligned}$$

$p\mid a^2+1, p\nmid a^2, p\nmid 1$ だから，LTE より

$$v_p\left(\left(a^2\right)^m+1\right)=v_p\left(a^2+1\right)+v_p\left(m\right). \qquad \cdots\cdots ②$$

m は奇数だから

$$p\mid a^2+1\mid a^{2m}+1=a^n+1\mid 4\left(a^n+1\right)=\left(f(n)\right)^3.$$

p は素数だから，$p\mid f(n)$ となる．$p^\alpha\parallel f(n)$ とおくと，$p^{3\alpha}\parallel\left(f(n)\right)^3=4\left(a^n+1\right)$.

p は奇素数だから，$p^{3\alpha}\parallel a^n+1$ を得るから，$v_p\left(a^n+1\right)=3\alpha\equiv 0\pmod 3$. ②を 3 を法として考えると

$$v_p\left(a^2+1\right)+v_p\left(m\right)=v_p\left(a^n+1\right)\equiv 0\pmod 3.$$

これが，任意の奇数 m に対して成り立つことになり，矛盾が生じる.

以上のことから，$a=1$ である. □

Zsigmondy の定理を使うと次のように解ける.

別解 すべての正整数 n について

$$4\left(a^n+1\right)=\left(f(n)\right)^3, f(n)\in\mathbb{N} \qquad \cdots\cdots①$$

が成り立つ.

$4 \mid \left(f(n)\right)^3$ より $2 \mid f(n)$ となるので，$2^3 \mid \left(f(n)\right)^3$.

よって $2 \mid a^n+1$ となるから，a は奇数である．このことから，$2 \mid a+1$.

$a \neq 1$ と仮定する.

Zsigmondy の定理より，$p \mid a^3+1, p \nmid a+1$ を満たす素数 p が存在する.

$p \nmid a+1, 2 \mid a+1$ だから，$p \neq 2$ である.

$p \mid a^3+1, p \nmid a^3, p \nmid 1$ だから，任意の奇数 k に対して，LTE より

$$v_p\left(4\left(a^{3k}+1\right)\right)=v_p\left(a^{3k}+1\right)=v_p\left(\left(a^3\right)^k+1\right)=v_p\left(a^3+1\right)+v_p(k)$$

すなわち

$$v_p\left(4\left(a^{3k}+1\right)\right)=v_p\left(a^3+1\right)+v_p(k). \qquad \cdots\cdots②$$

$p \mid a^3+1 \mid a^{3k}+1 \mid 4\left(a^{3k}+1\right)=\left(f(3k)\right)^3$ が成り立ち，p が素数なので，$p \mid f(3k)$.

$p^\alpha \,||\, f(3k)$ とおくと，$p^{3\alpha} \,||\, \left(f(3k)\right)^3=4\left(a^{3k}+1\right)$ だから

$$v_p\left(4\left(a^{3k}+1\right)\right)=3\alpha \quad \equiv 0 \pmod 3.$$

②より

$$v_p\left(a^3+1\right)+v_p(k)\equiv 0 \pmod 3$$

が任意の奇数 k に対して成り立つことになり，矛盾が生じる.

以上のことから，$a=1$ である. □

問題 7.4.4 (Ireland 1996)

Let p be a prime number, and a and n positive integers. Prove that if

$$2^p+3^p=a^n$$

then $n=1$.

解答 $2^p+3^p=a^n$ $\cdots\cdots①$

(1) $p \geq 3$ の場合

p は奇素数で，$5 \mid 3-(-2), 5 \nmid 3, 5 \nmid -2$ だから，LTE より

$$v_5\left(a^n\right)=v_5\left(3^p+2^p\right)=v_5\left(3^p-(-2)^p\right)=v_5(3+2)+v_5(p)=1+v_5(p)\leq 2.$$

(等号が成り立つのは，$p=5$ のときに限る．)

$1 \leq v_5(a^n) \leq 2$ より $v_5(a^n) \in \{1, 2\}$.

$v_5(a^n) = 2$ のとき，$p = 5$ で，①より

$$a^n = 2^5 + 3^5 = 275.$$

よって，$n = 1, a = 275$ となる．

$v_5(a^n) = nv_5(a) = 1$ のとき，$n = 1, v_5(a) = 1$.

(2) $p = 2$ の場合

①より

$$a^2 = 2^2 + 3^2 = 13.$$

よって，$n = 1, a = 13$ となる．

以上のことから，$n = 1$ となる． □

別解　$2^p + 3^p = a^n$ ……①

$n \geq 2$ と仮定して，①に整数解 n, p がないことを示す．

• $p \neq 2$ すなわち $p \geq 3$ は奇素数の場合

$$2^p + 3^p = (2+3)\left(2^{p-1} - 2^{p-2}3 + \cdots - 2 \cdot 3^{p-2} + 3^{p-1}\right)$$

より，$5 \mid 2^p + 3^p$ がわかるから，$5 \mid 2^p + 3^p = a^n$.

$5 \mid a^n$ から $5 \mid a$ が言えるから，$5^2 \mid a^2$.

$n \geq 2$ だから，$25 \mid a^n$ なので，$25 \mid 2^p + 3^p$.

ところで

$$\begin{aligned}
&2^p + 3^p = 2^p + (5-2)^p \\
&= 2^p + 5^p + \binom{p}{1}5^{p-1}(-2) + \cdots + \binom{p}{p-2}5^2(-2)^{p-2} + \binom{p}{p-1}5(-2)^{p-1} + (-2)^p \\
&= 5^p - \binom{p}{1}5^{p-1}2 + \binom{p}{2}5^{p-2}2^2 - \cdots + \binom{p}{p-2}5^2(-2)^{p-2} + \binom{p}{p-1}5 \cdot 2^{p-1} \\
&= 5p \cdot 2^{p-1} + 25\left(5^{p-2} - \binom{p}{1}5^{p-3}2 + \cdots - \binom{p}{p-2} \cdot 2^{p-2}\right) \\
&\equiv 5p \cdot 2^{p-1} \pmod{25}
\end{aligned}$$

であるから，

$$5p2^{p-1} \equiv 0 \pmod{25}$$

を得る．これから，$5 \mid p$ で p は素数だから，$p = 5$ となる．①より

$$a^n = 2^5 + 3^5 = 275.$$

よって，$n = 1, a = 275$ となる．これは $n \geq 2$ に矛盾する．

$p=2$ の場合は，①より

$$a^2=2^2+3^2=13.$$

よって，$n=1, a=13$ となり $n\geq 2$ に矛盾する．

以上のことから $n=1$. □

問題 7.4.5 (Russia 1996)

Let x, y, p, n, k be positive integers such that n is odd and p is an odd prime. Prove that if $x^n+y^n=p^k$ then n is a power of p.

$n>1$ として解くことにする．

解 1　$x=y$ のとき，$x^n+y^n=p^n$ は $2x^n=p^n$ から $p=2$ となり，p が奇素数であることに矛盾する．したがって，$x\neq y$ であるから，$x>y$ と仮定しても一般性を失わない．

$g=\gcd(x,y)$ とおくと，$x=gx_1, y=gy_1, \gcd(x_1,y_1)=1, x_1>y_1, x_1, y_1\in\mathbb{N}$ とおける．この式を $x^n+y^n=p^k$ に代入すると，

$$g^n\left(x_1^n+y_1^n\right)=p^k.$$

よって，$g=p^\alpha, \alpha\in\mathbb{N}_0$ とおけるから

$$x_1^n+y_1^n=p^{k-n\alpha} \qquad \cdots\cdots ①$$

が成り立つ．

$n>1$ は奇数だから

$$x_1^n+y_1^n=(x_1+y_1)\left(x_1^{n-1}-x_1^{n-2}y_1+x_1^{n-3}y_1^2-\cdots-x_1y_1^{n-2}+y_1^{n-1}\right) \qquad \cdots\cdots ①$$

が成り立つから，

$$A=x_1^{n-1}-x_1^{n-2}y_1+x_1^{n-3}y_1^2-\cdots-x_1y_1^{n-2}+y_1^{n-1}$$

とおく．$n\geq 3$ より

$$\begin{aligned}A&=x_1^{n-1}-x_1^{n-2}y_1+x_1^{n-3}y_1^2-\cdots-x_1y_1^{n-2}+y_1^{n-1}\\&=x_1^{n-2}(x_1-y_1)+x_1^{n-4}y_1^2(x_1-y_1)+\cdots+x_1y_1^{n-3}(x_1-y_1)+y_1^{n-1}\\&\geq x_1^{n-2}+x_1^{n-4}y_1^2+\cdots+x_1y_1^{n-3}+y_1^{n-1}\\&>1\end{aligned}$$

から，$A>1$ がわかる．また，$x_1+y_1\geq 3$ で $p^{k-n\alpha}=(x_1+y_1)A$ より $p\mid x_1+y_1, p\mid A$ が成り立つ．

$p\mid x_1+y_1, \gcd(x_1,y_1)=1$ より $p\nmid x_1, p\nmid y_1$ だから，LTE より

$$v_p\left(x_1^n+y_1^n\right)=v_p\left(x_1+y_1\right)+v_p(n).$$

$x_1^n + y_1^n = (x_1 + y_1)A$ より

$$v_p\left(x_1^n + y_1^n\right) = v_p\left(x_1 + y_1\right) + v_p(A).$$

したがって

$$v_p(n) = v_p\left(x_1^n + y_1^n\right) - v_p\left(x_1 + y_1\right) = v_p(A) \geq 1$$

となり，$p \mid n$ が言える．

$n = pq$ $(q \in \mathbb{N})$ とおくと，$p^k = x^n + y^n = x^{pq} + y^{pq} = (x^p)^q + (y^p)^q$ より

$$(x^p)^q + (y^p)^q = p^k.$$

$q = 1$ のときは，$n = p = p^1$.

$q > 1$ のときは，上と同じ議論で，$p \mid q$．これを繰り返すと，ある正の整数 l が存在して，$n = p^l$ となる．　□

LTE を使わないとすると次のような解答になる．

解 2　$x = y$ のとき，$x^n + y^n = p^k$ は $2x^n = p^k$ から $2 \mid p$ となり，p が奇素数であることに矛盾する．したがって，$x \neq y$ であるから，$x > y$ と仮定しても一般性を失わない．

$g = \gcd(x, y)$ とおくと，$x = gx_1, y = gy_1, \gcd(x_1, y_1) = 1, x_1 > y_1, x_1, y_1 \in \mathbb{N}$ とおける．この式を $x^n + y^n = p^k$ に代入すると，

$$g^n\left(x_1^n + y_1^n\right) = p^k.$$

よって，$g = p^\alpha, \alpha \in \mathbb{N}_0$ とおけるから

$$x_1^n + y_1^n = p^{k - n\alpha} \qquad \cdots\cdots ①$$

が成り立つ．

$n > 1$ は奇数だから

$$x_1^n + y_1^n = \left(x_1 + y_1\right)\left(x_1^{n-1} - x_1^{n-2}y_1 + x_1^{n-3}y_1^2 - \cdots - x_1y_1^{n-2} + y_1^{n-1}\right) \qquad \cdots\cdots ②$$

が成り立つから，

$$A = x_1^{n-1} - x_1^{n-2}y_1 + x_1^{n-3}y_1^2 - \cdots - x_1y_1^{n-2} + y_1^{n-1}$$

とおく．$n \geq 3$ より

$$\begin{aligned} A &= x_1^{n-1} - x_1^{n-2}y_1 + x_1^{n-3}y_1^2 - \cdots - x_1y_1^{n-2} + y_1^{n-1} \\ &= x_1^{n-2}(x_1 - y_1) + x_1^{n-4}y_1^2(x_1 - y_1) + \cdots + x_1y_1^{n-3}(x_1 - y_1) + y_1^{n-1} \\ &\geq x_1^{n-2} + x_1^{n-4}y_1^2 + \cdots + x_1y_1^{n-3} + y_1^{n-1} \\ &> 1 \end{aligned}$$

から，$A>1$ がわかる．また，$x_1+y_1\geq 3$ で $p^{k-n\alpha}=(x_1+y_1)A$ より

$$x_1+y_1=p^{\beta}\ (\beta\in\mathbb{N}),\ A=p^{k-n\alpha-\beta}$$

とおける．

$y_1\equiv -x_1 \pmod p$ を使うと

$$\begin{aligned}A&=x_1^{n-1}-x_1^{n-2}y_1+x_1^{n-3}y_1^2-\cdots-x_1y_1^{n-2}+y_1^{n-1}\\&\equiv x_1^{n-1}+x_1^{n-2}x_1+x_1^{n-3}x_1^2+\cdots+x_1\cdot x_1^{n-2}+x_1^{n-1}\\&\equiv nx_1^{n-1}\pmod p.\end{aligned}$$

$A\equiv 0 \pmod p$ だから，$nx_1^{n-1}\equiv \pmod p$.

$p\mid x_1+y_1, \gcd(x_1,y_1)=1$ より $p\nmid x_1, p\nmid y_1$ だから，$p\mid n$ が言える．

$n=pq\ (q\in\mathbb{N})$ とおくと，$p^k=x^n+y^n=x^{pq}+y^{pq}=(x^p)^q+(y^p)^q$ より

$$(x^p)^q+(y^p)^q=p^k.$$

$q=1$ のときは，$n=p=p^1$.

$q>1$ のときは，上と同じ議論で，$p\mid q$．これを繰り返すと，ある正の整数 l が存在して，$n=p^l$ となる． □

解 3　• $v_p(x)=v_p(y)$ が成り立つ．

$p^e\parallel x, e\in\mathbb{N}_0$ のとき，$x=p^ea, a\in\mathbb{N}, \gcd(p,a)=1$ とおけるから，$x^n+y^n=p^k$ に代入すると，$p^{en}a^n+y^n=p^k$.

$p^{en}\leq p^{en}a^n=x^n<x^n+y^n=p^k$ だから，$en<k$.

したがって

$$y^n=p^{en}\left(p^{k-en}-a^n\right)$$

が成り立つ．

$p^f\parallel y, f\in\mathbb{N}_0$ とおくと，$p^{fn}\parallel y^n=p^{en}\left(p^{k-en}-a^n\right)$ から，$fn=en$ すなわち，$f=e$ である．

$x=p^ea, y=p^eb,\ e\in\mathbb{N}_0,\ a,b\in\mathbb{N}, \gcd(p,a)=1, \gcd(p,b)=1$ とおけるから，これらの式を $x^n+y^n=p^k$ に代入すると，$p^{en}a^n+p^{en}b^n=p^k$ から

$$a^n+b^n=p^{k-en}\qquad\cdots\cdots①$$

となる．

すべての正整数 α に対して，$n\neq p^{\alpha}$ だと仮定すると，$q\mid n, q\neq p$ となる奇素数 q が存在する．

$a^{\frac{n}{q}}+b^{\frac{n}{q}}\mid a^n+b^n=p^{k-en}$ より，$a^{\frac{n}{q}}+b^{\frac{n}{q}}=p^{\alpha_1}, \alpha_1\in\mathbb{N}$ となる α_1 が存在する．

$p \mid a^{\frac{n}{q}} + b^{\frac{n}{q}}$, $p \nmid a^{\frac{n}{q}}, p \nmid b^{\frac{n}{q}}$ だから，LTE より

$$\begin{aligned} v_p\left(a^n + b^n\right) &= v_p\left(\left(a^{\frac{n}{q}}\right)^q + \left(b^{\frac{n}{q}}\right)^q\right) \\ &= v_p\left(a^{\frac{n}{q}} + b^{\frac{n}{q}}\right) + v_p(q) \\ &= v_p\left(a^{\frac{n}{q}} + b^{\frac{n}{q}}\right). \end{aligned}$$

よって

$$a^n + b^n = a^{\frac{n}{q}} + b^{\frac{n}{q}}. \qquad \cdots\cdots ②$$

$a^n \geq a^{\frac{n}{q}}, b^n \geq b^{\frac{n}{q}}$ だから，②が成り立つのは，$a^n = a^{\frac{n}{q}}, b^n = b^{\frac{n}{q}}$ が成り立つときである．ゆえに，$a = b = 1$ を得る．このとき，①は $2 = p^{k-ef}$ となるから，$p = 2, k - ef = 1$ となる．これは p が奇素数であることに矛盾する．

したがって，$n = p^\alpha, \alpha \in \mathbb{N}$ の形でなければならない． □

Zsigmondy の定理を使うと次のような解答になる．

解 4　• $v_p(x) = v_p(y)$ が成り立つ．

$p^e \parallel x, e \in \mathbb{N}_0$ のとき，$x = p^e a, a \in \mathbb{N}, \gcd(p, a) = 1$ とおけるから，$x^n + y^n = p^k$ に代入すると，$p^{en}a^n + y^n = p^k$.

$p^{en} \leq p^{en}a^n = x^n < x^n + y^n = p^k$ だから，$en < k$.

したがって

$$y^n = p^{en}\left(p^{k-en} - a^n\right)$$

が成り立つ．

$p^f \parallel y, f \in \mathbb{N}_0$ とおくと，$p^{fn} \parallel y^n = p^{en}\left(p^{k-en} - a^n\right)$ から，$fn = en$ すなわち，$f = e$ である．

$x = p^e a, y = p^e b$, $e \in \mathbb{N}_0$, $a, b \in \mathbb{N}, \gcd(p, a) = 1, \gcd(p, b) = 1$ とおけるから，これらの式を $x^n + y^n = p^k$ に代入すると，$p^{en}a^n + p^{en}b^n = p^k$ から

$$a^n + b^n = p^{k-en} \qquad \cdots\cdots ①$$

となる．

すべての正整数 α に対して，$n \neq p^\alpha$ だと仮定すると，$q \mid n, q \neq p$ となる奇素数 q が存在する．

$a^{\frac{n}{q}} + b^{\frac{n}{q}} \mid a^n + b^n = p^{k-en}$ より，$a^{\frac{n}{q}} + b^{\frac{n}{q}} = p^{\alpha_1}, \alpha_1 \in \mathbb{N}$ となる α_1 が存在する．

$a = 2, b = 1, n = 3$ のとき，$2^3 + 1^3 = 9 = p^{k-3e}$ から $p = 3$ で，$n = p^1$ となり仮定に矛盾する．

したがって，Zsigmondy の定理より，$r \mid a^n + b^n$, $r \nmid a^l + b^l$ $(l = 1, 2, \ldots, n-1)$ を満たす素数 p が存在する．$r \mid a^n + b^n = p^{k-en}$ より $r = p$ となるが，$p = r \nmid a^{\frac{n}{q}} + b^{\frac{n}{q}}$ は，$a^{\frac{n}{q}} + b^{\frac{n}{q}} = p^{\alpha_1}$ に矛盾する．

したがって，$n = p^{\alpha}, \alpha \in \mathbb{N}$ の形でなければならない． □

類題 (Hungary-Israel Binational 2006)

If natuaral numbers x, y, p, n, k with $n > 1$ odd and p an odd prime satisfy $x^n + y^n = p^k$, prove that n is a power of p.

問題 7.4.6 Find the sum of all the divisors d of $N = 19^{88} - 1$ which of the form $d = 2^a 3^b$ with $a, b \in \mathbb{N}_0$.

解答　19,1 は奇数，88 は正の偶数だから，定理 7.3.2 より

$$v_2(N) = v_2\left(19^{88} - 1^{88}\right) = v_2(19-1) + v_2(19+1) + v_2(88) - 1 = 1 + 2 + 3 - 1 = 5.$$

$3 \mid 19 - 1, 3 \nmid 19, 3 \nmid 1$ だから，定理 7.2.1 より

$$v_3(N) = v_3\left(19^{88} - 1^{88}\right) = v_3(19-1) + v_3(88) = 2.$$

N の $2^a 3^b$ の形の約数は $2^a 3^b$ $(0 \leq a \leq 5, 0 \leq b \leq 2)$ となるから，求める和は

$$\left(1 + 2 + 2^2 + 2^3 + 2^4 + 2^5\right)\left(1 + 3 + 3^2\right) = \frac{2^6 - 1}{2 - 1} \cdot 13 = 63 \cdot 13 = 819. \qquad \square$$

問題 7.4.7 Let p be a prime number. Solve the equation $a^p - 1 = p^k$ in the set of positive integers.

解答 明らかに $a \geq 2$ である．

(1) $p \neq 2$ すなわち p (≥ 3) が奇素数の場合

$a \equiv 0 \pmod{p}$ だとすると，$p^k = a^k - 1 \equiv -1 \pmod{p}$ となり矛盾が生じる．

したがって，$a \not\equiv 0 \pmod{p}$ だから，フェルマーの小定理より

$$a^p \equiv a \pmod{p}.$$

これを使うと

$$a - 1 \equiv a^p - 1 \equiv p^k \equiv 0 \pmod{p}.$$

となり．$p \mid a - 1$ が言える．$p \nmid a, p \nmid 1$ も成り立つから，LTE より

$$k = v_p\left(p^k\right) = v_p\left(a^p - 1\right) = v_p\left(a - 1\right) + v_p\left(p\right) = v_p\left(a - 1\right) + 1$$

すなわち，$v_p\left(a - 1\right) = k - 1$ を得る．$p^{k-1} \mid a - 1$ から $p^{k-1} \leq a - 1$.

この式を $1 + p^{k-1} \leq a$ を変形して，両辺を p 乗すると，

$$\left(1 + p^{k-1}\right)^p \leq a^p \qquad \left(1 + p^{k-1}\right)^p - 1 \leq a^p - 1 = p^k$$

から

$$\left(1+p^{k-1}\right)^p \leq p^k+1. \qquad \cdots\cdots ①$$

$m \geq 2$ が正の整数で，$x>0, x \in \mathbb{R}$ のとき，$(1+x)^m > 1+mx$ が成り立つから，$x=p^{k-1}, m=p$ で使うと

$$\left(1+p^{k-1}\right)^p > 1+p\cdot p^{k-1} = 1+p^k.$$

これは，①に矛盾する．

(2) $p=2$ の場合　　$a^2-1=2^k$.

a は奇数となるから，この式を

$$\frac{a+1}{2}\cdot\frac{a-1}{2}=2^{k-2}$$

と変形する．$\dfrac{a+1}{2}-\dfrac{a-1}{2}=1$ より，$\dfrac{a+1}{2}$ と $\dfrac{a-1}{2}$ は互いに素であるから，$k-2>0$ で

$$\frac{a+1}{2}=2^{k-2},\ \frac{a-1}{2}=1$$

ゆえに，$a=3, k=3$ となる．

(1)，(2) から，解は $a=3, k=3$ □

Zsigmondy の定理を使うと次のように解ける．

別解 明らかに $a \geq 2$ である．

(1) $p \neq 2$ すなわち p (≥ 3) が奇素数の場合

$a^p=1+p^k$ は偶数だから，a は偶数となり，$a+1$ は 2^l $(l \in \mathbb{N})$ の形にならない．

Zsigmondy の定理より，$q \mid a^p-1, q \nmid a-1$ となる素数 q が存在する．

$q \mid a^p-1=p^k$ より $q=p$ である．

$a \equiv 0 \pmod{p}$ だとすると，$p^k=a^k-1 \equiv -1 \pmod{p}$ となり矛盾が生じる．

したがって，$a \not\equiv 0 \pmod{p}$ だから，フェルマーの小定理より

$$a^p \equiv a \pmod{p}.$$

これを使うと

$$a-1 \equiv a^p-1 \equiv p^k \equiv 0 \pmod{p}.$$

となり．$p \mid a-1$ が言える．

しかし，$p=q \nmid a-1$ に矛盾する．

(2) $p=2$ の場合　　$a^2-1=2^k$.

a は奇数となるから，この式を

$$\frac{a+1}{2}\cdot\frac{a-1}{2}=2^{k-2}$$

と変形する．$\dfrac{a+1}{2}-\dfrac{a-1}{2}=1$ より，$\dfrac{a+1}{2}$ と $\dfrac{a-1}{2}$ は互いに素であるから，$k-2>0$ で

$$\frac{a+1}{2}=2^{k-2},\ \frac{a-1}{2}=1$$

ゆえに，$a=3,k=3$ となる．

(1)，(2) から，解は $a=3,k=3$ □

問題 7.4.8 For some positive integer n , the number 3^n-2^n is a perfect power of a prime. Prove that n is aprime.

解 1　$3^n-2^n=p^\alpha$, p は素数, $\alpha\in\mathbb{N}$ とおく．

$n=1$ のとき，$3^1-2^1=1$ はある素数 p を用いて $1=p^\alpha,\alpha\in\mathbb{N}$ と表せないから，$n\geq 2$ である．

• n は異なる 2 つの素数の因数をもたない．

$q_1\neq q_2$, $q_1\mid n$, $q_2\mid n$ を満たす素数 q_1,q_2 が存在したとする．

$q_i\mid n$ から $3^{q_i}-2^{q_i}\mid 3^n-2^n=p^\alpha$ なので，

$$3^{q_i}-2^{q_i}=p^{\alpha_i},\ \alpha_i\in\mathbb{N}$$

とおける．ところで

$$(3^{q_1}-2^{q_1},3^{q_2}-2^{q_2})=3^{(q_1,q_2)}-2^{(q_1,q_2)}=3-2=1$$

なので，$\alpha_1=0$ または $\alpha_2=0$ となる．これは $\alpha_1,\alpha_2\in\mathbb{N}$ に矛盾する．

したがって，$n=q^l$, q は素数, $l\in\mathbb{N}$ とおける．

$l\geq 2$ だとする．

$$3^q-2^q\mid 3^{q^2}-2^{q^2}\mid 3^n-2^n=p^\alpha$$

より

$$3^q-2^q=p^{\alpha_1},\ 3^{q^2}-2^{q^2}=p^{\alpha_2},\alpha_1,\alpha_2\in\mathbb{N}$$

とおける．$3^n-2^n=p^\alpha$ から明らかに $p\neq 2$ で，$p\mid 3^q-2^q$, $p\nmid 3^q$, $p\nmid 2^q$ だから，LTE より

$$v_p\left(3^{q^2}-2^{q^2}\right)=v_p\left((3^q)^q-(2^q)^q\right)=v_p\left(3^q-2^q\right)+v_p(q).$$

p,q は素数だから，$v_p(q)\in\Big\{0,\,1\Big\}$.

$v_p\left(3^{q^2}-2^{q^2}\right)=v_p\left(3^q-2^q\right)$ だとすると，$\alpha_1=\alpha_2$ で

$$3^{q^2}-2^{q^2}=3^q-2^q$$

となる．しかし，$a > b, a, b \in \mathbb{N}$ のとき

$$\begin{aligned} 3^a - 2 - 2^a &= (2+1)^a - 2^a \\ &= \binom{a}{1}2^{a-1} + \binom{a}{2}2^{a-2} + \cdots + \binom{a}{a-1}2^1 + 1 \\ &> \binom{b}{1}2^{b-1} + \binom{b}{2}2^{b-2} + \cdots + \binom{b}{b-1}2^1 + 1 \\ &= 3^b - 2^b \end{aligned}$$

より，$\{3^n - 2^n\}$ は増加数列となる．$q^2 > q$ なので $3^{q^2} - 2^{q^2} > 3^q - 2^q$ となり，$3^{q^2} - 2^{q^2} = 3^q - 2^q$ に矛盾する．
したがって，$v_p\left(3^{q^2} - 2^{q^2}\right) \neq v_p\left(3^q - 2^q\right)$ となるから，$v_p(q) = 1$.
ゆえに，$p = q$ となり

$$3^{q^2} - 2^{q^2} = q\left(3^q - 2^q\right).$$

$s = 3^q, t = 2^q$ $(s > t)$ とおくと，上の等式は

$$s^q - t^q = q(s - t)$$

となる．

$$s^q - t^q = (s-t)\left(s^{q-1} + s^{q-2}t + \cdots + st^{q-1} + t^{q-1}\right)$$

で，$s^{q-1} > 1, s^{q-2}t > 1, \cdots, st^{q-1} > 1, t^{q-1} > 1$ だから

$$s^{q-1} + s^{q-2}t + \cdots + st^{q-1} + t^{q-1} > 1 + 1 + \cdots + 1 + 1 = q.$$

これから $s^q - t^q > q(s-t)$ が成り立ち，$s^q - t^q = q(s-t)$ に矛盾する．

したがって，$l = 1$ でなければならない．よって $n = q$ (n は素数) となり，n は素数である．　□

解 2　$3^n - 2^n = p^\alpha$, p は素数, $\alpha \in \mathbb{N}$ とおくと，$p \neq 2, 3$..

明らかに $n \geq 2$ だから，$q \mid n$ となる素数 q をとる．

$q = n$ ならば証明は終わるから，$q \neq n$ とする．

すると，$n = kq$ $(k > 1, k \in \mathbb{N})$ とおける．

$$\begin{aligned} p^\alpha = 3^n - 2^n &= \left(3^k\right)^q - \left(2^k\right)^q \\ &= \left(3^k - 2^k\right)\left(\left(3^k\right)^{q-1} + \left(3^k\right)^{q-2} \cdot 2^k + \cdots + 3^k \cdot \left(2^k\right)^{q-2} + \left(2^k\right)^{q-1}\right) \end{aligned}$$

より

$$3^k - 2^k = p^\beta,\ \beta \leq \alpha, \beta \in \mathbb{N}$$

とおける．さて

$$p^\alpha = 3^n - 2^n = \left(3^k\right)^q - 2^{kq} = \left(2^k + p^\beta\right)^q - 2^{kq}$$

$$= \binom{q}{1}\left(2^k\right)^{q-1}\cdot p^\beta + \underline{\binom{q}{2}\left(2^k\right)^{q-2}\cdot\left(p^\beta\right)^2 + \cdots + \binom{q}{q}\left(p^\beta\right)^q}. \qquad \cdots\cdots ①$$

$f(x) = 3^x - 2^x\ (x \geq 1)$ とおくと，

$$f'(x) = 3^x \log 3 - 2^x \log 2 > 3^x \log 2 - 2^x \log 2 > 0$$

より，$x \geq 1$ で $f(x)$ は増加関数となる．$n > k$ なので $p^\alpha = 3^n - 2^n > 3^k - 2^k = p^\beta$ から $\alpha > \beta$ となる．よって，$\alpha \geq \beta + 1$ で p^α は少なくとも $p^{\beta+1}$ で割り切れる．

①において，$p^{\beta+1} \mid p^\alpha$ で，下線部 $\binom{q}{2}\left(2^k\right)^{q-2}\cdot\left(p^\beta\right)^2 + \cdots + \binom{q}{q}\left(p^\beta\right)^q$ は $\left(p^\beta\right)^2$ で割り切れるから，$\binom{q}{1}\left(2^k\right)^{q-1}\cdot p^\beta$ は $p^{\beta+1}$ で割り切れる．よって

$$p \mid q\left(2^k\right)^{q-1}$$

が言える．

$p \neq 2$ で p, q は素数だから，$p \mid q$ となり $p = q$ を得る．

$n = kq = kp$ で，$p^\alpha = \left(3^p\right)^k - \left(2^p\right)^k$ は $3^p - 2^p$ で割り切れるから

$$3^p - 2^p = p^\gamma, \gamma \in \mathbb{N}$$

とおける．これから

$$3^p - 2^p \equiv 0 \pmod{p}.$$

フェルマーの小定理より，$3^p \equiv 3 \mod p, 2^p \equiv 2 \mod p$ が成り立つから，$3^p - 2^p \equiv 3 - 2 \equiv 1 \pmod{p}$．これは，$3^p - 2^p \equiv 0 \pmod{p}$ に矛盾する． □

Zsigmondy の定理を使うと次のように解ける．

解 3　$3^n - 2^n = p^k,\ p$ は素数, $k \in \mathbb{N}$ とおく．

n は素数ではないと仮定すると，$n = ab\ (a, b \in \mathbb{N},\ a, b \geq 2)$ とおける．

$$\begin{aligned} 3^n - 2^n &= 3^{ab} - 2^{ab} = \left(3^a\right)^b - \left(2^a\right)^b \\ &= \left(3^a - 2^a\right)\left(\left(3^a\right)^{b-1} + \left(3^a\right)^{b-2}\cdot 2^a + \cdots + 3^a\cdot\left(2^a\right)^{b-2} + \left(2^a\right)^{b-1}\right) \\ &= p^k \end{aligned}$$

が成り立ち，$3^a - 2^a > 1$ だから，$3^a - 2^b = p^l,\ l \in \mathbb{N}, l \leq k$ とおける．

Zsigmondy の定理より，

$$q \mid 3^n - 2^n,\ q \nmid 3^k - 2^k\ (k = 1, 2, \ldots, n-1)$$

を満たす素数 q が存在する．

$q \mid 3^n - 2^n = p^k$ で p, q は素数だから，$p = q$ となる．
ゆえに，$p = q \nmid 3^a - 2^a$ となるが，これは $p \mid p^l = 3^a - 2^b$ に矛盾する．
したがって，n は素数である．　□

問題 7.4.9 (IMO Shortlist 1991)
Find the higest degree k of 1991 for which 1991^k devides the number

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

解答　$N = 1990^{1991^{1992}} + 1992^{1991^{1990}}$ とおくと，$1991 = 181 \times 11$ であるので，$v_{11}(N)$ と $v_{181}(N)$ を求める．
$n = 1991^{1990}$ とおくと，n は奇数であり．

$$N = 1990^{1991^2 \cdot n} + 1992^n = \left(1990^{1991^2}\right)^n + 1992^n.$$

よって，$x = 1990^{1991^2}, y = 1992$ とおくと，

$$x + y = 1990^{1991^2} + 1992 \equiv (-1)^{1991^2} + 1 \equiv (-1) + 1 \equiv 0 \pmod{1991}$$

であるから，$11 \mid x + y, 181 \mid x + y$.
また，$x = 1990^{1991^2} \equiv (-1)^{1991^2} \equiv -1 \pmod{1991}$, $y = 1992 \equiv 1 \pmod{1991}$ であるから，$x \equiv -1 \pmod{11}, x \equiv -1 \pmod{181}, y \equiv 1 \pmod{11}, y \equiv 1 \pmod{181}$ すなわち $11 \nmid x, 11 \nmid y$, $181 \nmid x, 181 \nmid y$.
LTE より

$$v_{11}(N) = v_{11}\left(x^n + y^n\right) = v_{11}(x + y) + v_{11}(n).$$

$m = 1991^2$ とおくと

$$\begin{aligned}
&x + y \\
&= 1990^{1991^2} + 1992 \\
&= (1991 - 1)^m + 1992 \\
&= 1991^m + \binom{m}{1} 1991^{m-1} \cdot (-1) + \cdots + \binom{m}{m-1} 1991 \cdot (-1)^{m-1} + (-1)^m + 1992 \\
&= \underbrace{1991^m + \binom{m}{1} 1991^{m-1} \cdot (-1) + \cdots + 1991^2 \cdot 1991 \cdot (-1)^{m-1}}_{1991^2\text{で割り切れる}} + (-1)^m + 1992 \\
&\equiv (-1)^m + 1992 \\
&\equiv (-1) + 1992 \qquad (m \text{ は奇数}) \\
&\equiv 1991 \pmod{1991^2}
\end{aligned}$$

より

$$x+y \equiv 1991 \equiv 55 \not\equiv 0 \pmod{11^2},\ x+y \equiv 1991 \not\equiv 0 \pmod{181^2}$$

が成り立つから，

$$v_{11}(x+y)=1,\ v_{181}(x+y)=1.$$

$v_{11}(n)=v_{11}\left(11^{1990}\cdot 181^{1990}\right)=1990$ であるから，

$$v_{11}(N)=v_{11}(x+y)+v_{11}(n)=1+1990=1991$$

となる．全く同様にして，

$$v_{181}(N)=v_{181}(x+y)+v_{181}(n)=1+1990=1991$$

となるから，求める答えは 1991. □

問題 7.4.10 (China Western Mathematical Olympiad 2010)

Suppose that m and k are non-negative integers, and $p=2^{2^m}+1$ is a prime number. Prove that

(1) $2^{2^{m+1}p^k} \equiv 1 \pmod{p^{k+1}}$;

(2) $2^{m+1}p^k$ is the smallest positive integer n satisfying the congruence equation $2^n \equiv 1 \pmod{p^{k+1}}$.

解答 (1) $2^{2^m}=p-1\equiv -1 \pmod{p}$ の両辺を平方すると，$\left(2^{2^m}\right)^2 \equiv 1 \pmod{p}$.

よって，$2^{2^{m+1}} \equiv 1 \pmod{p}$ より，$p \mid 2^{2^{m+1}}-1$ で，明らかに $p \nmid 2^{2^{m+1}}, p \nmid 1$ である．LTE より

$$\begin{aligned} v_p\left(2^{2^{m+1}p^k}-1\right) &= v_p\left(\left(2^{2^{m+1}}\right)^{p^k}-1^{p^k}\right) \\ &= v_p\left(2^{2^{m+1}}-1\right)+v_p\left(p^k\right) \\ &= v_p\left(2^{2^{m+1}}-1\right)+k \\ &\geq 1+k. \end{aligned}$$

よって，$2^{2^{m+1}p^k} \equiv 1 \pmod{p^{k+1}}$.

(2) $d=\mathrm{ord}_{p^{k+1}}(2)$ とおくと，$2^{2^{m+1}p^k} \equiv 1 \pmod{p^{k+1}}$ であるから，

$$d \mid 2^{m+1}p^k$$

が成り立つ．

$p = 2^{2^m} + 1$ は素数だから，$1, 2, \ldots, p-1 = 2^{2^m}$ は p で割り切れないので，2^m 以下の正整数は p で割り切れない．したがって，d は $2^s p^t$ $(m \leq s \leq m+1, 0 \leq t \leq k)$ の形である．

$2^{2^m p^t} - 1 \equiv 0 \pmod{p^{k+1}}$ が成り立つと仮定する．

$2^{2^m} \equiv -1 \pmod{p}$ より

$$1 \equiv \left(2^{2^m}\right)^{p^t} \equiv (-1)^{p^t}$$

より，p^t は偶数となるが，p^t は奇数だから矛盾が生じる．

$2^{2^{m+1} p^t} - 1 \equiv 0 \pmod{p^{k+1}}$ が成り立つと仮定する．

$p \mid 2^{2^{m+1}} - 1$, $p \nmid 2^{2^{m+1}}, p \nmid 1$ である．LTE より

$$\begin{aligned} v_p\left(2^{2^{m+1} p^t} - 1\right) &= v_p\left(\left(2^{2^{m+1}}\right)^{p^t} - 1^{p^t}\right) \\ &= v_p\left(2^{2^{m+1}} - 1\right) + v_p\left(p^t\right) \\ &= v_p\left(2^{2^{m+1}} - 1\right) + t. \end{aligned}$$

ここで, $2^{2^{m+1}} - 1 = \left(2^{2^m}\right)^2 - 1 = (p-1)^2 - 1 = p^2 - 2p$ だから, $v_p\left(2^{2^{m+1}} - 1\right) = 1$.

よって,

$$k + 1 \leq v_p\left(2^{2^{m+1} p^t} - 1\right) = 1 + t$$

から，$k \leq t$. $t \leq k$ であったから，$t = k$ を得る．

$d = 2^{m+1} p^k$ となり，題意は証明された． □

(2) **の別解**　$d = \mathrm{ord}_{p^{k+1}}(2)$ とおくと，$2^{2^{m+1} p^k} \equiv 1 \pmod{p^{k+1}}$ であるから，

$$d \mid 2^{m+1} p^k$$

が成り立つ．

$d \nmid 2^m p^k$ かつ $d \nmid 2^{m+1} p^{k-1}$ を示せばよい．

• $d \nmid 2^m p^k$ である．

$d \mid 2^m p^k$ とすると，$2^{2^m p^k} \equiv 1 \pmod{p^{k+1}}$.

$2^{2^m} \equiv -1 \pmod{p}$ より，$2^{2^m} - 1 \equiv -2 \not\equiv 0 \pmod{p}$.

$$\begin{aligned} 2^{2^m p^k} - 1 &= \left(2^{2^m}\right)^{p^k} - 1 \\ &= \left(2^{2^m} - 1\right)\left(\left(2^{2^m}\right)^{p^k - 1} + \left(2^{2^m}\right)^{p^k - 2} + \cdots + 2^{2^m} + 1\right) \end{aligned}$$

が成り立ち，$p \nmid 2^{2^m} - 1$ で,

$$\left(2^{2^m}\right)^{p^k - 1} + \left(2^{2^m}\right)^{p^k - 2} + \cdots + 2^{2^m} + 1$$

$$\equiv \underbrace{(-1)^{p^k-1}+(-1)^{p^k-2}+\cdots+(-1)}_{p^k-1}+1$$
$$\equiv 1 \not\equiv 0 \pmod{p}.$$

したがって，$p \nmid 2^{2^m p^k}-1$ となり，$2^{2^m p^k} \equiv 1 \pmod{p^{k+1}}$ は成り立たない．

• $d \nmid 2^{m+1}p^{k-1}$ である．

$d \mid 2^{m+1}p^{k-1}$ とすると，$2^{2^{m+1}p^{k-1}} \equiv 1 \pmod{p^{k+1}}$.

$p \mid 2^{2^{m+1}}-1$, $p \nmid 2^{2^{m+1}}, p \nmid 1$ だから，LTE より

$$\begin{aligned} v_p\left(2^{2^{m+1}p^{k-1}}-1\right) &= v_p\left(\left(2^{2^{m+1}}\right)^{p^{k-1}}-1^{p^{k-1}}\right) \\ &= v_p\left(2^{2^{m+1}}-1\right)+v_p\left(p^{k-1}\right) \\ &= v_p\left(2^{2^{m+1}}-1\right)+k-1 \geq k+1 \end{aligned}$$

より

$$v_p\left(2^{2^{m+1}}-1\right) \geq 2.$$

これから，$p^2 \mid 2^{2^{m+1}}-1=\left(2^{2^m}+1\right)\left(2^{2^m}-1\right)$ が成り立たねばならない．

$p \nmid 2^{2^m}-1$ であったから，$p^2 \mid 2^{2^m}+1=p$ でなければならない．これは明らかに矛盾する． □

問題 7.4.11 Let $p \geq 5$ be a prime. Find the maximum value of positive integer k such that

$$p^k \mid (p-2)^{2(p-1)}-(p-4)^{p-1}.$$

解答　$p \geq 5$ は奇素数である．

$$\begin{aligned} (p-2)^4 &= p^4-8p^3+24p^2-32p+16 \equiv 16 \not\equiv 0 \pmod{p} \\ (p-4)^2 &= p^2-8p+16 \equiv 16 \not\equiv 0 \pmod{p} \\ (p-2)^4-(p-4)^2 &= p^4-8p^3+23p^2-24p \equiv 0 \pmod{p} \end{aligned}$$

だから，$x=(p-2)^4, y=(p-4)^2$ とおくと，$p \mid x-y, p \nmid x, p \nmid y$.

$p \geq 5$ は奇素数だから，$\gcd\left(p, \dfrac{p-1}{2}\right)=1$. また，$x-y=(p-2)^4-(p-4)^2=p^4-8p^3+23p^2-24p \equiv -24p \equiv -3 \cdot 2^3 p \not\equiv 0 \pmod{p^2}$ LTE より

$$\begin{aligned} v_p\left((p-2)^{2(p-1)}-(p-4)^{p-1}\right) &= v_p\left(x^{\frac{p-1}{2}}-y^{\frac{p-1}{2}}\right) \\ &= v_p(x-y)+v_p\left(\frac{p-1}{2}\right) \\ &= 1+0=1. \end{aligned}$$

したがって，求める k の値は $k=1$. □

問題 7.4.12 (China TST 2009)

Let $a>b>1$ be positive integers and b be an odd number, let n be a positive integer. If $b^n \mid a^n-1$, then show that $a^b > \dfrac{3^n}{n}$.

解答　● この問題は b が素数であるときに成り立つことを示せばよい.

b が合成数とし，$p \mid b$ となる素数とする．すると，$p^n \mid b^n \mid a^n-1$ でしかも，$p^n \mid a^n-1$ から $a^p > \dfrac{3^n}{n}$ が言えれば，$a^b > a^p > \dfrac{3^n}{n}$ が言えるから，b が素数であるときに成り立つことを示せばよい.

$b=p$ は奇素数とする．$p \mid p^n \mid a^n-1$ から $a^n-1 \equiv 0 \pmod p$ となるから，$d=\mathrm{ord}_p(a)$ とおくと，$d \mid n$.

$p \mid a^d-1$ から，$p \nmid a^d, p \nmid 1$ となるから，LTE より

$$n \le v_p\left(a^n-1\right)=v_p\left(\left(a^d\right)^{\frac{n}{d}}-1\right)=v_p\left(a^d-1\right)+v_p\left(\frac{n}{d}\right).$$

よって

$$v_p\left(a^d-1\right)+v_p\left(\frac{n}{d}\right) \ge n. \qquad \cdots ①$$

$p \nmid a$ なので，フェルマーの小定理より，$a^{p-1} \equiv 1 \pmod p$ が成り立つから，$d \mid p-1$ すなわち $d \le p-1$.

これから，$p \nmid d$ が成り立つから，$v_p(d)=0$.

よって，$v_p(d)=0$ と①を使うと

$$v_p\left(n\left(a^d-1\right)\right)=v_p\left(a^d-1\right)+v_p(n)-v_p(d)=v_p\left(a^d-1\right)+v_p\left(\frac{n}{d}\right) \ge n.$$

これから，$p^n \mid n\left(a^d-1\right)$ が成り立つから，$p^n \le n\left(a^d-1\right)$.

この不等式から

$$a^d-1 \ge \frac{p^n}{n} \ge \frac{3^n}{n}.$$

ところで，$d \le p-1$ であったから

$$a^p \ge a^{d+1} > a^d > a^d-1 \ge \frac{3^n}{n}.$$

これで，$a^p > \dfrac{3^n}{n}$ が成り立つことがわかったことになる. □

問題 7.4.13 (Romanian Junior Balkan TST 2008)

Let p be a prime number, $p \neq 3$, and integers a, b such that $p \mid a+b$ and $p^2 \mid a^3+b^3$. Prove that $p^2 \mid a+b$ or $p^3 \mid a^3+b^3$.

解 1　$p \nmid a$ かつ $p \nmid b$ の場合

$p \mid a+b$ だから，LTE より

$$v_p\left(a^3+b^3\right) = v_p\left(a+b\right) + v_p(3) = v_p(a+b).$$

$p^2 \mid a^3+b^3$ より $v_p\left(a^3+b^3\right) \geq 2$ だから $v_p(a+b) \geq 2$.

よって，$p^2 \mid a+b$.

(2) $p \mid a$ または $p \mid b$ の場合

$p \mid a$ のとき，$p \mid a+b$ だから，$p \mid (a+b)-a = b$.

このとき，$p^3 \mid a^3, p^3 \mid b^3$ だから，$p^3 \mid a^3+b^3$.

$p \mid b$ のときも同様にして，$p^3 \mid a^3+b^3$ が言える． □

LTE を使わないと次のような解になる．

解 2　$p^2 \mid a^3+b^3 = (a+b)\left(a^2-ab+b^2\right)$ より，$p^2 \mid a+b$ ならば，ここで証明は終了する．

$p^2 \nmid a+b$ ならば，$p \mid a^2-ab+b^2$ が成り立つ．$p \mid a+b$ より，$p \mid a+b \mid (a+b)^2$ だから，

$$p \mid (a+b)^2 - \left(a^2-ab+b^2\right) = 3ab.$$

$p \neq 3$ だから，$p \mid ab$.

p は素数だから，$p \mid a$ または $p \mid b$ が成り立つ．

$p \mid a$ のとき，$p \mid a+b$ だから，$p \mid (a+b)-a = b$.

このとき，$p^3 \mid a^3, p^3 \mid b^3$ だから，$p^3 \mid a^3+b^3$.

$p \mid b$ のときも同様にして，$p^3 \mid a^3+b^3$ が言える． □

問題 7.4.14 (IMO 1990)

Determine all integers $n > 1$ such that

$$\frac{2^n+1}{n^2}$$

is an integer.

解答　2^n+1 は奇数で，$\dfrac{2^n+1}{n^2}$ が整数だから，n は奇数であることがわかる．

（n が偶数だと，$2^n+1 = n^2 l$ $(l \in \mathbb{N})$ は偶数になってしまう．）

• $n = 3^k$ $(k \in \mathbb{N})$ とかけることを示す．

$n \geq 3$ より n の素因数のうち最小のものを p とする．n は奇数なので，p も奇数である．

$\dfrac{2^n+1}{n^2}$ が整数より，$p \mid 2^n+1$ となるから，$p \mid 2^n+1 \mid (2^n+1)(2^n-1) = 2^{2n}-1$.

よって

$$p \mid 2^{2n} - 1. \qquad \cdots\cdots ①$$

p は奇素数だから，フェルマー の小定理より

$$p \mid 2^{p-1} - 1. \qquad \cdots\cdots ②$$

①，②から

$$p \mid \gcd\left(2^{2n} - 1, 2^{p-1} - 1\right) = 2^{\gcd(2n,p-1)} - 1. \qquad \cdots\cdots ③$$

$$\gcd(2n, p-1) = 2\gcd\left(n, \frac{p-1}{2}\right).$$

$2n, p-1$ は偶数で，もしも，$\gcd(2n, p-1) = 2r$ $(r > 1, r \in \mathbb{N})$ となったとすると，n は奇数だから r は奇数である．$r \mid n, r \mid p-1, r \geq 3$ より r の素因数をとると，p より小さい n の素因数が存在することになり，p の最小性に矛盾する．
したがって，$\gcd(2n, p-1) = 2$ となる．③から $p \mid 2^2 - 1 = 3$ なので，$p = 3$ である．
よって，$n = 3^k\alpha$ $(k, \alpha \in \mathbb{N}, \gcd(3, \alpha) = 1)$ とかける．

ここで，$\alpha \geq 2$ だとすると，n が奇数であることから，$\alpha \geq 3$ は奇数となる．α の最小素因数 q がとれて，上と同じ議論から，$q = 3$ となり，$\gcd(3, \alpha) = 1$ に矛盾する．
したがって，$\alpha = 1$ で，$n = 3^k (k \geq 1)$ とかける．

$3 \mid 2 - (-1), 3 \nmid 2, 3 \nmid -1$ だから，LTE より

$$v_3\left(2^n + 1\right) = v_3\left(2^n - (-1)^n\right) = v_3(2 - (-1)) + v_3(n) = 1 + v_3(n).$$

$\dfrac{2^n + 1}{n^2}$ が整数だから，

$$v_3\left(2^n + 1\right) \geq v_3(n^2) = 2v_3(n)$$

が成り立つことを用いると

$$1 + v_3(n) \geq 2v_3(n) \qquad v_3(n) \leq 1.$$

$v_3(n) \geq 1$ だから，$v_3(n) = 1$ となり，$n = 3$.

このとき，$\dfrac{2^n + 1}{n^2} = \dfrac{2^3 + 1}{3^2} = 1$ となり整数である．
求める n の値は，$n = 3$. □

問題 7.4.15

Find all pairs of prime p, q such that $pq \mid \left(5^p - 2^p\right)\left(5^q - 2^q\right)$.

解答　$pq \mid \left(5^p - 2^p\right)\left(5^q - 2^q\right)$ $\cdots\cdots ①$

$p \mid 5^p - 2^p$ または $p \mid 5^q - 2^q$ が成り立つ．同様に，$q \mid 5^p - 2^p$ または $q \mid 5^q - 2^q$ が成り立つ．

(1) $p \mid 5^p - 2^p$ または $q \mid 5^q - 2^q$ の場合

$p \mid 5^p - 2^p$ と仮定する．フェルマーの小定理より，$5^p \equiv 5, 2^p \equiv 2 \pmod{p}$ が成り立つから，$5^p - 2^p \equiv 5 - 2 \equiv 3 \equiv 0 \pmod{p}$．よって，$p = 3$ となる．

①から，$3q \mid \left(5^3 - 2^3\right)\left(5^q - 2^q\right) = 3^2 \cdot 13\left(5^q - 2^q\right)$.

よって，$q \mid 3 \cdot 13$ または $q \mid 5^q - 2^q$.

$q \mid 3 \cdot 13$ からは $q \in \left\{3,\, 13\right\}$.

$q \mid 5^q - 2^q$ からは，$q = 3$.

$q \mid 5^q - 2^q$ の場合も考慮して，

$(p, q) = (3, 3), (3, 13), (13, 3)$.

(2) $p \nmid 5^p - 2^p$ かつ $q \nmid 5^q - 2^q$ の場合

$p \neq 3, q \neq 3$ で，$p \mid 5^q - 2^q,\ q \mid 5^p - 2^p$ となる．

$p \mid 5^q - 2^q,\ q \mid 5^p - 2^p$ より $\gcd(2, p) = 1,\ \gcd(2, q) = 1$ だから，$\gcd(2, pq) = 1$.

したがって，$2 \cdot 2^{-1} \equiv 1 \pmod{pq}$ を満たす 2 の逆数 2^{-1} が存在する．すると，$p \mid pq \mid 2 \cdot 2^{-1} - 1$ より，$2 \cdot 2^{-1} \equiv 1 \pmod{p}$ が成り立つ．同様にして，$2 \cdot 2^{-1} \equiv 1 \pmod{q}$ が成り立つ．

$5^q - 2^q \equiv 0 \pmod{p}$ の両辺に $\left(2^{-1}\right)^q$ をかけると，$\left(5 \cdot 2^{-1}\right)^q - 1 \equiv 0 \pmod{p}$.

同様にして，$\left(5 \cdot 2^{-1}\right)^p - 1 \equiv 0 \pmod{q}$.

$a \equiv 5 \cdot 2^{-1} \pmod{pq}$ とおくと，$\mathrm{ord}_p(a) \mid q$ かつ $\mathrm{ord}_q(a) \mid p$ が成り立つ．

p, q は素数だから，

$$\mathrm{ord}_p(a) \in \left\{1,\, q\right\}, \mathrm{ord}_p(a) \mid \phi(p) = p-1,\ \ \mathrm{ord}_q(a) \in \left\{1,\, p\right\}, \mathrm{ord}_q(a) \mid \phi(q) = q-1.$$

$\mathrm{ord}_p(a) = q$ かつ $\mathrm{ord}_q(a) = p$ が成り立つとすると，$q \mid p - 1$ かつ $p \mid q - 1$ から $q \leq p - 1$ かつ $p \leq q - 1$.

よって，$q + 1 \leq p \leq q - 1$ となり矛盾が生じる．

したがって，$\mathrm{ord}_p(a) = 1$ または $\mathrm{ord}_q(a) = 1$ が成り立つ．

$\mathrm{ord}_p(a) = 1$ とすると，$a - 1 \equiv 0 \pmod{p}$.

$a \equiv 5 \cdot 2^{-1} \pmod{pq}$ より，$a \equiv 5 \cdot 2^{-1} \pmod{p}$ だから，$a \equiv 1 \pmod{p}$ を使うと

$$5 \cdot 2^{-1} \equiv 1 \pmod{p} \qquad 5 \equiv 2 \pmod{p} \qquad 3 \equiv 0 \pmod{p}.$$

これから，$p = 3$ となり，$p \neq 3$ に矛盾する．

$\mathrm{ord}_q(a) = 1$ のときも同様に，矛盾が生じる．

したがって，求める解は

$$(p, q) = (3, 3), (3, 13), (13, 3). \qquad \square$$

問題 7.4.16 For some natural number n let a be the greatest natural number for which $5^n - 3^n$ is divisible by 2^a. Also let b be the greatest natural number such that $2^b \leq n$. Prove that $a \leq b + 3$.

解答　$a = v_2\left(5^n - 3^n\right)$ である.

(1) n が偶数の場合

$2 \mid 5-3, 2 \nmid 5, 2 \nmid 3$ だから，LTE より

$$a = v_2\left(5^n - 3^n\right) = v_2(5-3) + v_2(5+3) + v_2(n) - 1 = v_2(n) + 3.$$

$2^m \leq n < 2^{m+1}$ のとき，$b = m$.

n は偶数だから，n のとる値は $2^m, 2^m + 2, 2^m + 2^2, \ldots, 2^m + 2^m - 2$ なので，

$v_2(n) \leq m = b$.

したがって，

$$a = v_2(n) + 3 \leq b + 3.$$

(2) n が奇数の場合

$$5^n - 3^n = (5-3)\left(5^{n-1} + 5^{n-2} \cdot 3 + 5^{n-3} \cdot 3^2 + \cdots + 5 \cdot 3^{n-2} + 3^{n-1}\right)$$

が成り立ち，　mod 2 で考えると

$$\begin{aligned} & 5^{n-1} + 5^{n-2} \cdot 3 + 5^{n-3} \cdot 3^2 + \cdots + 5 \cdot 3^{n-2} + 3^{n-1} \\ \equiv & \underbrace{1 + 1 + \cdots + 1}_{n} \pmod 2 \\ \equiv & n \equiv 1 \not\equiv 0 \pmod 2 \end{aligned}$$

であるから

$$v_2\left(5^n - 3^n\right) = v_2(5-3) + v_2\left(5^{n-1} + 5^{n-2} \cdot 3 + 5^{n-3} \cdot 3^2 + \cdots + 5 \cdot 3^{n-2} + 3^{n-1}\right) = 1.$$

よって，$a = 1$ で，$b \geq 0$ であることから，$a \leq b + 3$ は明らかに成り立つ.　□

問題 7.4.17 (Romania TST 1994)

Let n be an odd positive integer. Prove that $\left((n-1)^n + 1\right)^2$ divides $n(n-1)^{(n-1)^n+1} + n$.

解答　$N = (n-1)^n + 1 > 1$ とおき，$N^2 \mid n(n-1)^N + n$ が成り立つことを示す.

$N \equiv (-1)^n + 1 \equiv 0 \pmod n$ であることがわかる.

$N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ ($p_1, \ldots, p_r$は異なる素数, $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$) と素因数分解する.

各 $i\,(1 \leq r \leq r)$ に対して，$p_i \mid N$ だから，$N \equiv 0 \pmod{p_i}$.

$p_i \mid (n-1)^n - (-1) = N, p_i \nmid (n-1)^n, p_i \nmid -1$ だから，LTE より

$$\begin{aligned} v_{p_i}\left((n-1)^N + 1\right) &= v_{p_i}\left(((n-1)^n)^{\frac{N}{n}} - ((-1)^n)^{\frac{N}{n}}\right) \\ &= v_{p_i}\left((n-1)^n - (-1)^n\right) + v_{p_i}\left(\frac{N}{n}\right) \\ &= v_{p_i}(N) + v_{p_i}\left(\frac{N}{n}\right) \\ &= v_{p_i}(N) + v_{p_i}(N) - v_{p_i}(n) \\ &= \alpha_i + \alpha_i - v_{p_i}(n) = 2\alpha_i - v_{p_i}(n). \end{aligned}$$

よって，$v_{p_i}\left((n-1)^N + 1\right) = 2\alpha - v_{p_i}(n)$ より

$$v_{p_i}\left(n\left((n-1)^N + 1\right)\right) = v_{p_i}(n) + v_{p_i}\left((n-1)^N + 1\right) = 2\alpha_i.$$

したがって，$N^2 \mid n(n-1)^N + n$ が成り立つ． □

問題 7.4.18 Find all positive integers n such that $3^n - 1$ is divisible by 2^n.

解答 (i)　n が偶数の場合

$3, 1$ は奇数で，n は偶数だから，LTE より

$$\begin{aligned} v_2\left(3^n - 1\right) &= v_2(3-1) + v_2(3+1) + v_2(n) - 1 = 1 + 2 + v_(n) - 1 \\ &= v_2(n) + 2. \end{aligned}$$

$2^n \mid 3^n - 1$ より，$v_2\left(3^n - 1\right) \geq n$ だから，$v_2(n) + 2 \geq n$ すなわち $v_2(n) \geq n - 2$.
これから，$2^{n-2} \mid n$ が言えて，

$$2^{n-2} \leq n. \qquad \cdots\cdots ①$$

$n \geq 5$ のとき，数学的帰納法で $2^{n-2} > n$ が成り立つことが示せるから，①は成り立たない．
$n \leq 4$ のときは，$n = 2$ または $n = 4$ である．
$n = 2$ のとき，$3^2 - 1 = 8 = 2^3$ は 2^2 で割り切れる．
$n = 4$ のとき，$3^4 - 1 = 80 = 2^4 \cdot 5$ は 2^4 で割り切れる．

(ii) n が奇数の場合
$\gcd(n, 2) = 1, 2 \mid 3 - 1, 2 \nmid 3, 2 \nmid 1$ で n が奇数だから，LTE の補助定理より

$$v_2\left(3^n - 1\right) = v_2(3-1) = 1.$$

また，$v_2\left(2^n\right) = n$ が成り立つ．
$2^n \mid 3^n - 1$ より，$v_2\left(3^n - 1\right) \geq n$ だから，$1 \geq n$ すなわち $n = 1$.
このとき，$3^1 - 1 = 2$ は 2^1 で割り切れる．

したがって，求める解は，$n = 1, 2, 4$. □

問題 7.4.19 (Romania TST 2009)
Let $a, n \geq 2$ be two integers, which have the following property:
there exists an integer $k \geq 2$, such that n divides $(a-1)^k$.
Prove that n also divides $a^{n-1} + a^{n-2} + \cdots + a + 1$.

解答　$n \mid (a-1)^k$ のとき $n \mid a^{n-1} + a^{n-2} + \cdots + a + 1 = \dfrac{a^n - 1}{a - 1}$ を示せばよい．
$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ $(p_1, \ldots, p_r$は異なる素数$, \alpha_1, \ldots, \alpha_r \in \mathbb{N})$ と素因数分解する．

(i) p_i が奇素数の場合
$p_i \mid n \mid (a-1)^k$ より，$p_i \mid a - 1$ が言える．これから，明らかに $p_i \nmid a, p_i \nmid 1$ だから，LTE より

$$v_{p_i}\left(a^n - 1\right) = v_{p_i}(a-1) + v_{p_i}(n).$$

したがって，

$$v_{p_i}\left(\frac{a^n-1}{a-1}\right)=v_{p_i}\left(a^n-1\right)-v_{p_i}(a-1)=v_{p_i}(n)=\alpha_i$$

から，$p_i^{\alpha_i}\left|\dfrac{a^n-1}{a-1}\right.$.

(ii) $p_i=2$ の場合

n は偶数で，$n\mid(a-1)^k$ より a は奇数である．$a,1$ は奇数，n は偶数だから，LTE より

$$v_2\left(a^n-1\right)=v_2(a-1)+v_2(a+1)+v_2(n)-1$$

したがって，

$$\begin{aligned}v_2\left(\frac{a^n-1}{a-1}\right)&=v_2\left(a^n-1\right)-v_2(a-1)\\&=v_2(n)+v_2(a+1)-1\\&\geq v_2(n)+1-1\qquad\left(v_2(a+1)\geq 1\right)\\&=v_2(n)=\alpha_i\end{aligned}$$

から，$p_i^{\alpha_i}=2^{\alpha_i}\left|\dfrac{a^n-1}{a-1}\right.$.

(i)，(ii) から，$n\left|\dfrac{a^n-1}{a-1}\right.$ が成り立つ． □

問題 7.4.20 Find all the positive integers a sucn that $\dfrac{5^a+1}{3^a}$ is a positive integer.

解答 (i) a が偶数の場合

mod 3 で考えると

$$5^a+1\equiv(-1)^a+1\equiv 2\not\equiv 0\pmod 3$$

だから，$\dfrac{5^a+1}{3^a}$ は整数にならない．

(ii) a が奇数の場合

$3\mid 5-(-1),3\nmid 5,3\nmid -1$ だから，LTE より

$$v_3\left(5^a+1\right)=v_3\left(5^a-(-1)^a\right)=v_3\left(5-(-1)\right)+v_3(a)=1+v_3(a).$$

$3^a\mid 5^a+1$ より，$v_3\left(5^a+1\right)\geq a$ が成り立つことを用いると，$1+v_3(a)\geq a$ すなわち

$$v_3(a)\geq a-1$$

を得る．$3^{a-1}\mid a$ から

$$3^{a-1}\leq a. \qquad \cdots\cdots ①$$

$a \geq 3$ のとき，数学的帰納法を用いると，不等式 $3^{a-1} > a$ が成り立つことがわかるので，①を満たす a は存在しない．

$a < 3$ を満たす奇数は $a = 1$ で①を満たす．

$a = 1$ のとき $\dfrac{5^1+1}{3^1} = 2$ は整数である．

(i)，(ii) から，求める解は，$a = 1$. □

問題 7.4.21　Let $k > 1$ be an integer. Show that there exists infinitely many positive integers n such that

$$n \mid 1^n + 2^n + 3^n + \cdots + k^n.$$

解答 (i) k が偶数の場合

$k = 2l\,(l \in \mathbb{N})$ とおき，$p \mid 2l+1$ を満たす奇素数 p をとり，$n = p^m\,(m \in \mathbb{N})$ とおく．

$$\begin{aligned} &1^n + 2^n + 3^n + \cdots + k^n \\ &= 1^n + 2^n + 3^n + \cdots + l^n + (l+1)^n + \cdots + (2l-1)^n + (2l)^n \\ &= (1^n + (2l)^n) + (2^n + (2l-1)^n) + \cdots + (l^n + (l+1)^n) \end{aligned}$$

と変形して，$a_i = i,\ b_i = 2l+1-i\ (1 \leq i \leq l)$ とおくと，$a_i + b_i = 2l+1$ だから，$p \mid a_i + b_i$ が成り立ち，

$$1^n + 2^n + 3^n + \cdots + k^n = \sum_{i=1}^{l} (a_i^n + b_i^n)\,. \qquad \cdots\cdots ①$$

各 $i\,(1 \leq i \leq l)$ に対して，$n \mid a_i^n + b_i^n$ を示す．

(a) $p \nmid a_i$ かつ $p \nmid b_i$ の場合

LTE より，

$$v_p\,(a_i^n + b_i^n) = v_p(a_i + b_i) + v_p(n) \geq 1 + m > m.$$

よって，$n = p^m \mid a_i^n + b_i^n$.

(ii) $p \mid a_i$ または $p \mid b_i$ の場合

$p \mid a_i$ とすると，$p \mid a_i + b_i$ だから，$p \mid (a_i + b_i) - a_i = b_i$．よって，$p^n \mid a_i^n, p^n \mid b_i^n$ から $p^n \mid a_i^n + b_i^n$.

$p \geq 3$，m は正の整数だから，$p^m > m$ が成り立つので，$n = p^m > m$．よって

$$n = p^m \mid p^n \mid a_i^n + b_i^n.$$

$p \mid b_i$ のときも，$p \mid a_i$ が言えて，$n \mid a_i^n + b_i^n$ が成り立つ．

(a)，(b) より，各 $i\,(1 \leq i \leq l)$ に対して，$n \mid a_i^n + b_i^n$ が成り立つことがわかった．
①を使うと，

$$n \left| \sum_{i=1}^{l} (a_i^n + b_i^n) = 1^n + 2^n + 3^n + \cdots + k^n. \right.$$

m は任意の正整数でよかったから，無限に多くの $n = p^m$ で，

$$n \mid 1^n + 2^n + 3^n + \cdots + k^n$$

が成り立つことが示せた．

(i) k が奇数の場合

$k = 2l + 1\,(l \in \mathbb{N})$ とおき，$p \mid 2l + 1$ を満たす奇素数 p をとり，$n = p^m\,(m \in \mathbb{N})$ とおくと，(i) の結果から

$$n \mid 1^n + 2^n + \cdots + (2l)^n = 1^n + 2^n + 3^n + \cdots + (k-1)^n \qquad \cdots\cdots ②$$

が成り立つ．

$p \geq 3$，m は正の整数だから，$p^m > m$ が成り立つので，$n = p^m > m$．よって

$$n = p^m \mid p^n \mid (2l+1)^n = k^n. \qquad \cdots\cdots ③$$

②，③より

$$n \mid 1^n + 2^n + 3^n + \cdots + k^n.$$

m は任意の正整数でよかったから，無限に多くの $n = p^m$ で，

$$n \mid 1^n + 2^n + 3^n + \cdots + k^n$$

が成り立つことが示せた． □

問題 7.4.22 (IMO shortlist 2010)

Find all pairs (m, n) of nonnegative integers for which

$$m^2 + 2 \cdot 3^n = m\left(2^{n+1} - 1\right).$$

解答　$m^2 + 2 \cdot 3^n = m\left(2^{n+1} - 1\right)$ $\cdots\cdots ①$

とおく．①を変形すると

$$2 \cdot 3^n = m\left(2^{n+1} - 1 - m\right).$$

$m \mid 2 \cdot 3^n$ から $m = 3^p\ (0 \leq p \leq n)$ または $m = 2 \cdot 3^q\ (0 \leq q \leq n)$ と表せる．

$m = 3^p$ $(0 \leq p \leq n)$ のとき，$q = n - p$ とおくと

$$2^{n+1} - 1 = m + \frac{2 \cdot 3^n}{m} = 3^p + 2 \cdot 3^{n-p} = 3^p + 2 \cdot 3^q.$$

$m = 2 \cdot 3^q$ $(0 \leq q \leq n)$ のとき，$p = n - q$ とおくと

$$2^{n+1} - 1 = m + \frac{2 \cdot 3^n}{m} = 2 \cdot 3^q + \cdot 3^{n-q} = 2 \cdot 3^q + 3^p.$$

いずれの場合も

$$3^p + 2 \cdot 3^q = 2^{n+1} - 1,\ p + q = n, p \geq 0, q \geq 0 \qquad \cdots\cdots ②$$

となるので，(2) の非負の整数解を求める．

$n = 0$ のとき (2) は整数解をもたないので，$n \geq 1$ とする．

まず，p, q の値の取り得る範囲を調べる．

$3^p < 2^{n+1} = 8^{\frac{n+1}{3}} < 9^{\frac{n+1}{3}} = 3^{\frac{2(n+1)}{3}}$ から $p < \frac{2(n+1)}{3}$.

$2 \cdot 3^q < 2^{n+1} = 2 \cdot 8^{\frac{n}{3}} < 2 \cdot 9^{\frac{n}{3}} = 2 \cdot 3^{\frac{2n}{3}}$ から $q < \frac{2n}{3}$.

$p + q = n$ を使うと

$$\frac{n}{3} < p < \frac{2(n+1)}{3},\ \frac{n-2}{3} < q < \frac{2n}{3}. \qquad \cdots\cdots ③$$

$h = \min(p, q)$ とおくと，(3) から　$h > \dfrac{n-2}{3}$.

(1) $n \geq 5$ の場合

$h > \dfrac{n-2}{3} \geq 1$ から $h \geq 2$ で，$3^h \mid 3^p + 2 \cdot 3^q = 2^{n+1} - 1$ より $3^h \mid 2^{n+1} - 1$.

$h \geq 2$ だから，

$$9 \mid 2^{n+1} - 1.$$

• $9 \mid 2^{n+1} - 1 \Longleftrightarrow 6 \mid n + 1$ が成り立つことを示す．

$9 \mid 2^{n+1} - 1$ と仮定すると，$3 \mid 2^{n+1} - 1$ だから，$n+1$ は偶数で，$3 \mid 4 - 1, 3 \nmid 3, 3 \nmid 1$ を満たすので，LTE より

$$2 \leq v_3\left(2^{n+1} - 1\right) = v_3\left(4^{\frac{n+1}{2}} - 1\right) = v_3(4-1) + v_3\left(\frac{n+1}{2}\right) = 1 + v_3\left(\frac{n+1}{2}\right)$$

が成り立つから，$v_3\left(\dfrac{n+1}{2}\right) \geq 1$.

よって，$3 \left| \dfrac{n+1}{2} \right.$ より $6 \mid n + 1$.

$6 \mid n + 1$ と仮定すると，$3 \left| \dfrac{n+1}{2} \right.$ で LTE より

$$v_3\left(2^{n+1} - 1\right) = v_3\left(4^{\frac{n+1}{2}} - 1\right) = v_3(4-1) + v_3\left(\frac{n+1}{2}\right) = 1 + v_3\left(\frac{n+1}{2}\right) \geq 2.$$

よって， $9 \mid 2^{n+1}-1$.

$n+1=6r$ $(r \in \mathbb{N})$ とおくと

$$\begin{aligned} 2^{n+1}-1 &= 2^{6r}-1 = 4^{3r}-1 = \left(4^r-1\right)\left(4^{2r}+4^r+1\right) \\ &= \left(2^r-1\right)\left(2^r+1\right)\left(4^{2r}+4^r+1\right). \end{aligned}$$

$4^{2r}+4^r+1=\left(4^r-1\right)^2+3\cdot 4^r$ と変形でき，$4^r-1 \equiv 1-1 \equiv 0 \pmod 3$ より $\left(4^r-1\right)^2 \equiv 0 \pmod 9$ であるから，$4^{2r}+4^r+1$ は 3 で割り切れるが，9 では割り切れない．

また，$\gcd\left(2^r+1, 2^r-1\right)=\gcd\left(2^r+1-\left(2^r-1\right), 2^r-1\right)=\gcd\left(2, 2^r-1\right)=1$ より 2^r+1 と 2^r-1 は互いに素である．

$3^h \mid 2^{n+1}-1=\left(2^r-1\right)\left(2^r+1\right)\left(4^{2r}+4^r+1\right)$ から

$$3^{h-1} \mid \left(2^r-1\right)\left(2^r+1\right)$$

で，2^r+1 と 2^r-1 は互いに素だから，$3^{h-1} \mid \left(2^r-1\right)$ または $3^{h-1} \mid \left(2^r+1\right)$ となる．これから，$3^{h-1} \leq 2^r-1 < 2^r+1$ または $3^{h-1} \leq 2^r+1$ となり，いずれの場合でも $3^{h-1} \leq 2^r+1$ が成り立つ．この不等式から

$$3^{h-1} \leq 2^r+1 \leq 3^r = 3^{\frac{n+1}{6}}$$

すなわち

$$h-1 \leq \frac{n+1}{6}.$$

$h > \dfrac{n-2}{3}$ でもあったから，

$$\frac{n-2}{3}-1 < h-1 \leq \frac{n+1}{6}.$$

この不等式から，$\dfrac{n-2}{3}-1 < \dfrac{n+1}{6}$ を解いて，$n<11$.

$n+1$ (≥ 6) で $n+1=6h$ だから，$n=5$ $(h=1)$.

①は

$$m^2+2\cdot 3^5 = m\left(2^6-1\right) \qquad m^2-63m+486=0 \qquad (m-54)(m-9)=0$$

となるので，$m=9, 54$.

よって，$(m, n)=(9, 5), (54, 5)$.

(2) $1 \leq n \leq 4$ の場合

①は $m^2-\left(2^{n+1}-1\right)m+2\cdot 3^n=0$ と変形できる．

$n=1$ のとき，$m^2-3m+6=0$ $\quad D=-15<0$ より整数解はない．

$n=2$ のとき，$m^2-7m+18=0$　　$D=-23<0$ より整数解はない．

$n=3$ のとき，$m^2-15m+54=0$　　$(m-6)(m-9)=0$　　$m=6,9$ 解は $(m,n)=(6,3),(9,3)$.

$n=4$ のとき，$m^2-31m+162=0$　　$m=\dfrac{31\pm\sqrt{313}}{2}$ より整数解はない．

以上より求める解は，

$(m,n)=(6,3),(9,3),(9,5),(54,5)$. □

注 上記の問題で，①を $m^2-\left(2^{n+1}-1\right)m+2\cdot 3^n=0$ と変形して解くと

$$m=\frac{2^{n+1}-1\pm\sqrt{\left(2^{n+1}-1\right)^2-8\cdot 3^n}}{2}=\frac{2^{n+1}-1\pm\sqrt{2^{n+2}\left(2^n-1\right)-8\cdot 3^n+1}}{2}$$

となるから，$2^{n+2}\left(2^n-1\right)-8\cdot 3^n+1$ が平方数とならなければならない．これが，次の類題になっている．

類題　(Vietmam Team Selection Test 2011)

Find all positive integers n such that $A=2^{n+2}\left(2^n-1\right)-8\cdot 3^n+1$ is a perfect square.

答えは $n=3,5$.

問題 7.4.23 (Gabriel Dospinescu, Mathlinks Contest)

Let a, b two different positive rational numbers such that for infinitely many numbers n, $a^n - b^n$ is integer. Then prove that a, b are also integers.

解答　$a = \dfrac{x}{z}$, $b = \dfrac{y}{z}$, $x, y, z \in \mathbb{N}, g = \gcd(x, y)$ とおき，$a^n - b^n = l_n$, $l_n \in \mathbb{Z}$ とすると，

$$x^n - y^n = z^n l_n$$

が成り立つ．

$g > 1$ だとして，$x = gx_1, y = gy_1, x_1, y_1 \in \mathbb{N}, \gcd(x_1, y_1) = 1$ とおくと

$$x_1^n - y_1^n = \frac{z^n l_n}{g^n}.$$

$\gcd(g, z) = 1$ と考えてよいから，l_n は g^n で割り切れる．$l_n = g^n {l_n}', {l_n}' \in \mathbb{Z}$ とおくと，$x^n - y^n = z^n l_n$ は

$$x_1^n - y_1^n = z^n {l_n}'$$

となるから，最初から $\gcd(x, y) = 1$ としてよいことがわかる．

したがって，$z^n \mid x^n - y^n$, $x, y, z \in \mathbb{N}, \gcd(x, y) = 1$ を満たす n が無限個存在するから

$$S = \left\{ n : z^n \mid x^n - y^n,\ x, y, z \in \mathbb{N},\ \gcd(x, y) = 1,\ n \in \mathbb{N} \right\}$$

とおく．

$z > 1$ として矛盾が生じることを示す．

$p \mid z$ となる素数 p が存在する．

• $p \nmid x, p \nmid y$ である．

$p \mid x$ とすると，$p^n \mid z^n \mid x^n - y^n$, $p^n \mid x^n$ から $p^n \mid x^n - (x^n - y^n) = y^n$．$p$ は素数だから，$p \mid y$ となり，$\gcd(x, y) = 1$ に矛盾する．したがって，$p \nmid x$ でなければならない．

$p \nmid x$ のとき，$p \nmid y$ である．なぜならば，$p \mid y$ とすると，上と同様にして，$p \mid x$ となり，$p \nmid x$ に矛盾する．

(1) $p = 2$ の場合　　$2^n \mid x^n - y^n$

$n = 2^{u_n} v_n, u_n \in \mathbb{N}_0, v_n \in \mathbb{N}, v_n$は奇数, $X = x^{v_n}, Y = y^{v_n}$ とおくと

$$\begin{aligned} x^n - y^n &= x^{2^{u_n} v_n} - y^{2^{u_n} v_n} = \left(x^{v_n}\right)^{2^{u_n}} - \left(y^{v_n}\right)^{2^{u_n}} = X^{2^{u_n}} - Y^{2^{u_n}} \\ &= \left(X^{2^{u_n - 1}} - Y^{2^{u_n - 1}}\right)\left(X^{2^{u_n - 1}} + Y^{2^{u_n - 1}}\right) \\ &= \left(X^{2^{u_n - 2}} - Y^{2^{u_n - 2}}\right)\left(X^{2^{u_n - 2}} + Y^{2^{u_n - 2}}\right)\left(X^{2^{u_n - 1}} + Y^{2^{u_n - 1}}\right) \end{aligned}$$

$$
\begin{aligned}
&= \cdots\cdots \\
&= (X-Y)(X+Y)\left(X^2+Y^2\right)\cdots \\
&\qquad \left(X^{2^{u_n-2}}+Y^{2^{u_n-2}}\right)\left(X^{2^{u_n-1}}+Y^{2^{u_n-1}}\right) \\
&= \left(x^{v_n}-y^{v_n}\right)\left(x^{v_n}+y^{v_n}\right)\left(x^{2v_n}+y^{2v_n}\right)\cdots \\
&\qquad \left(x^{2^{u_n-2}v_n}+y^{2^{u_n-2}v_n}\right)\left(x^{2^{u_n-1}v_n}+y^{2^{u_n-1}v_n}\right)
\end{aligned}
$$

から

$$
v_2\left(x^n-y^n\right) = v_2\left(x^{v_n}-y^{v_n}\right)+v_2\left(x^{v_n}+y^{v_n}\right)+\sum_{k=1}^{u_n-1} v_2\left(x^{2^k v_n}+y^{2^k v_n}\right) \qquad \cdots\cdots ①
$$

が成り立つ.

$2 \nmid x, 2 \nmid y$ で v_n は奇数だから，$2 \mid x-y, \gcd(2, v_n)=1$ となるので，LTE の補助定理より

$$
v_2\left(x^{v_n}-y^{v_n}\right) = v_2(x-y). \qquad \cdots\cdots ②
$$

同様にして

$$
v_2\left(x^{v_n}+y^{v_n}\right) = v_2(x+y). \qquad \cdots\cdots ③
$$

x, y が奇数だから，$k \in \mathbb{N}$ のとき，$x^{2^k v_n} \equiv 1 \pmod 4$, $y^{2^k v_n} \equiv 1 \pmod 4$ となるので,

$$
x^{2^k v_n}+y^{2^k v_n} \equiv 2 \pmod 4.
$$

よって,

$$
v_2\left(x^{2^k v_n}+y^{2^k v_n}\right) = 1. \qquad \cdots\cdots ④
$$

②, ③, ④ を使うと①は

$$
\begin{aligned}
v_2\left(x^n-y^n\right) &= v_2\left(x^{v_n}-y^{v_n}\right)+v_2\left(x^{v_n}+y^{v_n}\right)+\sum_{k=1}^{u_n-1} v_2\left(x^{2^k v_n}+y^{2^k v_n}\right) \\
&= v_2(x-y)+v_2(x+y)+(u_n-1)\cdot 1
\end{aligned}
$$

となるから

$$
v_2\left(x^n-y^n\right) = v_2(x-y)+v_2(x+y)+(u_n-1). \qquad \cdots\cdots ⑤
$$

また，$2^n \mid x^n-y^n$ より，$n \le v_2\left(x^n-y^n\right)$ が成り立つから

$$
2^{u_n} v_n \le v_2(x-y)+v_2(x+y)+(u_n-1). \qquad \cdots\cdots ⑥
$$

⑥から

$$2^{u_n} \leq 2^{u_n} v_n \leq v_2(x-y) + v_2(x+y) + (u_n - 1)$$

が成り立ち，

$$2^{u_n} - u_n \leq v_2(x-y) + v_2(x+y) - 1. \qquad \cdots\cdots ⑦$$

• $\{u_n\}$ は有界である．

$\{u_n\}$ が有界でないとすると，$\{u_n\}$ の部分列 $\{u_{n_i}\}$ で $\lim_{i\to\infty} u_{n_i} = \infty$ となるものがあるから，

$$\lim_{i\to\infty} (2^{u_{n_i}} - u_{n_i}) = \infty$$

となり，⑦に矛盾する．よって，$\{u_n\}$ は有界であるから，$n \in S$ のとき，$|u_n| \leq M$ となる定数 M が存在する．

⑥より

$$2^{u_n} v_n \leq v_2(x-y) + v_2(x+y) + (u_n - 1) \leq v_2(x-y) + v_2(x+y) + M - 1.$$

この不等式から，$\{2^{u_n} v_n\}$ は有界となり，S は有限集合となり，S が無限集合であることに矛盾する．

したがって，$z = 1$ すなわち a, b は整数となる．

(2) p (≥ 3) が奇素数の場合

$p \mid x^k - y^k$ を満たす k の最小値を d とする．$p \mid z \mid z^n \mid x^n - y^n$ であったから，$d \leq n$ である．

• $d \mid n$ である．

n を d で割った商を q，余りを r とおくと

$$n = dq + r,\ 0 \leq r < d$$

が成り立つ．

$p \mid x^d - y^d \mid x^{dq} - y^{dq}$, $p \mid x^n - y^n = x^{dq+r} - y^{dq+r} = \left(x^d\right)^q x^r - \left(y^d\right)^q y^r$ であるから

$$p \left| \left(x^d\right)^q x^r - \left(y^d\right)^q y^r - x^r \left(\left(x^d\right)^q - \left(y^d\right)^q\right) = \left(y^d\right)^q \left(x^r - y^r\right). \right.$$

$p \nmid y$ だから，$p \mid x^r - y^r$ を得る．$r \neq 0$ だと，$0 < r < d$ で $p \mid x^r - y^r$ となり，d の最小性に矛盾する．よって，$r = 0$ で $d \mid n$ である．

$d \mid n$ より $n = md, m \in \mathbb{N}, A = x^d, B = y^d$ とおくと，$p \mid A - B$.

また $p \nmid x, p \nmid y$ から $p \nmid x^d = A, p \nmid y^d = B$.

$T = \left\{m : n = md,\ n \in S\right\}$ とおく．

$p^m \mid p^n \mid x^n - y^n = x^{md} - y^{md} = A^m - B^m$ より

$$m \leq v_p\left(A^m - B^m\right).$$

$p \mid A - B, p \nmid A, p \nmid B$ であるから LTE より

$$v_p\left(A^m - B^m\right) = v_p(A - B) + v_p(m).$$

$m = p^{u_m} v_m, \gcd(p, v_m) = 1, u_m \in \mathbb{N}_0, v_m \in \mathbb{N}$ とおくと，

$$m \leq v_p\left(A^m - B^m\right) = v_p(A - B) + v_p(m) = v_p(A - B) + u_m$$

から

$$p^{u_m} v_m = m \leq v_p(A - B) + u_m. \qquad \cdots\cdots ⑧$$

⑧から $p^{u_m} \leq v_p(A - B) + u_m$ が成り立ち，

$$p^{u_m} - u_m \leq v_p(A - B). \qquad \cdots\cdots ⑨$$

• $\{u_m\}$ は有界である．

$\{u_m\}$ が有界でないとすると，$\{u_m\}$ の部分列 $\{u_{m_i}\}$ で $\lim_{i\to\infty} u_{m_i} = \infty$ となるものがあるから，

$$\lim_{i\to\infty} \left(p^{u_{m_i}} - u_{m_i}\right) = \infty$$

となり，⑨に矛盾する．よって，$\{u_m\}$ は有界であるから，$m \in T$ のとき，$|u_m| \leq M'$ となる定数 M' が存在する．

⑧より

$$p^{u_m} v_m \leq v_p(A - B) + u_m \leq v_p(A - B) + M'.$$

この不等式から，$\{p^{u_m} v_m\}$ は有界となり，T は有限集合となり，T が無限集合であることに矛盾する．

したがって，$z = 1$ すなわち a, b は整数となる．　□

問題 8.3.1　n が相異なる素数 p, q の積，$n = pq$，であるとき，$n-1$ 個の数 ${}_n\mathrm{C}_k$ $(1 \leqq k \leqq n-1)$ の最大公約数は 1 であることを示せ．

(1997 京都大・理系・前期)

例題 8.3.1 の (4) から次のことがわかっている．

> p を素数とし，n を 2 以上の正整数とする．$n-1$ 個の二項係数 $\binom{n}{i}$ $(1 \leq i \leq n-1)$ がすべて p の倍数であるための必要十分条件は，整数 n が適当な正整数 k を用いて $n = p^k$ と表せることである．

このことを使うと，問題 8.3.1 は次のように簡単に解くことができる．

$\binom{n}{1} = pq$ であるから，$n-1$ 個の数 $\binom{n}{k}$ $(1 \leq k \leq n-1)$ の最大公約数 g は pq の公約数であるから，$g \in \Big\{1,\, p,\, q,\, pq\Big\}$.

$n = pq \neq p^k$ $(k \in \mathbb{N})$ であるから，$g \notin \Big\{p,\, pq\Big\}$.

$n = pq \neq q^l$ $(l \in \mathbb{N})$ であるから，$g \notin \Big\{q,\, pq\Big\}$.

したがって，$g = 1$ となる．

解 1 では $v_p()$ を使って解いている．

解 1　$\binom{n}{1} = pq$ であるから，$n-1$ 個の数 $\binom{n}{k}$ $(1 \leq k \leq n-1)$ の最大公約数は pq の公約数である．

$$\begin{aligned}
v_p\left(\binom{n}{p}\right) &= v_p\left(\frac{(pq)!}{p!(pq-p)!}\right) \\
&= v_p\left((pq)!\right) - v_p\left(p!\right) - v_p\left((pq-p)!\right) \\
&= \left[\frac{pq}{p}\right] + \left[\frac{pq}{p^2}\right] + \left[\frac{pq}{p^3}\right] + \cdots \\
&\quad - \left[\frac{p}{p}\right] - \left(\left[\frac{p(q-1)}{p}\right] + \left[\frac{p(q-1)}{p^2}\right] + \left[\frac{p(q-1)}{p^3}\right] + \cdots\right) \\
&= q + \left[\frac{q}{p}\right] + \left[\frac{q}{p^2}\right] + \cdots \\
&\quad - 1 - \left(q - 1 + \left[\frac{q-1}{p}\right] + \left[\frac{q-1}{p^2}\right] + \cdots\right) \\
&= \left[\frac{q}{p}\right] + \left[\frac{q}{p^2}\right] + \cdots - \left(\left[\frac{q-1}{p}\right] + \left[\frac{q-1}{p^2}\right] + \cdots\right) \\
&= v_p\left(q!\right) - v_p\left((q-1)!\right)
\end{aligned}$$

$$
\begin{aligned}
&= v_p\left(\frac{q!}{(q-1)!}\right)\\
&= v_p(q)\\
&= 0
\end{aligned}
$$

から，$p \nmid \binom{n}{p}$.

同様にして，$q \nmid \binom{n}{q}$.

したがって，$n-1$ 個の数 $\binom{n}{k}$ $(1 \leq k \leq n-1)$ の最大公約数は 1 である．　□

解 2　$\binom{n}{1} = pq$ であるから，$n-1$ 個の数 $\binom{n}{k}$ $(1 \leq k \leq n-1)$ の最大公約数は pq の公約数である．

$$
\begin{aligned}
\binom{n}{p} &= \frac{pq(pq-1)(pq-2)\cdots(pq-p+1)}{p\cdot(p-1)\cdot(p-2)\cdots 2\cdot 1}\\
&= \frac{q(pq-1)(pq-2)\cdots(pq-(p-1))}{(p-1)\cdot(p-2)\cdots 2\cdot 1}.
\end{aligned}
$$

分子の因数 $q, pq-1, pq-2, \ldots, pq-(p-1)$ の中には p の倍数は存在しないから，$\binom{n}{p}$ は p を素因数にもたない．

同様に $\binom{n}{q}$ は q を素因数にもたない．

したがって，$n-1$ 個の数 $\binom{n}{k}$ $(1 \leq k \leq n-1)$ の最大公約数は 1 である．　□

問題 10.4.1 (例題 7.4.4 と同じ問題)
Find all solutions of the equation $x^{2009}+y^{2009}=7^z$ for x,y,z positive integers.

解 1　　$2009=7^2\cdot 41$.

$x=y$ のとき，$x^{2009}+y^{2009}=7^z$ は $2x^{2009}=7^z$ となり，これを満たす正整数 x,z は存在しない．よって $x\neq y$ である．

$d=\gcd(x,y), x=da, y=db, \gcd(a,b)=1, a,b\in\mathbb{N}$ とおき，$x^{2009}+y^{2009}=7^z$ に代入すると

$$d^{2009}\left(a^{2009}+b^{2009}\right)=7^z.$$

$d=7^k, k\in\mathbb{N}_0$ とおけるから，上の式に代入して

$$a^{2009}+b^{2009}=7^{z-2009k}$$

と変形できる．$a^{2009}+b^{2009}\geq 2$ だから，$z-2009k\geq 1$ で，$m=z-2009k\in\mathbb{N}$ とおくと

$$a^{2009}+b^{2009}=7^m \qquad \cdots\cdots ①$$

となる．①の左辺を因数分解した式

$$(a+b)\left(a^{2008}-a^{2007}b+a^{2006}b^2-\cdots-ab^{2007}+b^{2008}\right)=7^m$$

と，$a+b\geq 2$ より

$$7\mid a+b$$

がわかる．

$a\neq b$, $\gcd(a,b)=1$ であるから，Zsigmondy の定理より，$p\mid a^{2009}+b^{2009}$ かつ $p\nmid a+b$ となる素数 p が存在する．
$p\mid a^{2009}+b^{2009}=7^m$ で p は素数だから，$p=7$ となる．このとき，$7=p\nmid a+b$ であるが，これは $7\mid a+b$ に矛盾する．
したがって，①に正整数解は存在しない．　□

解 2　　$2009=7^2\cdot 41$.

$d=\gcd(x,y), x=da, y=db, \gcd(a,b)=1, a,b\in\mathbb{N}$ とおき，$x^{2009}+y^{2009}=7^z$ に代入すると

$$d^{2009}\left(a^{2009}+b^{2009}\right)=7^z.$$

$d=7^k, k\in\mathbb{N}_0$ とおけるから，上の式に代入して

$$a^{2009}+b^{2009}=7^{z-2009k}$$

と変形できる．$a^{2009}+b^{2009}\geq 2$ だから，$z-2009k\geq 1$ で，$m=z-2009k\in\mathbb{N}$ とおくと

$$a^{2009}+b^{2009}=7^m \qquad \cdots\cdots ①$$

となる．$a=b$ のとき，$a^{2009}+b^{2009}=7^m$ は $2a^{2009}=7^m$ となり，これを満たす正整数 x,m は存在しない．よって $a\neq b$ である．

①の左辺を因数分解した式

$$(a+b)\left(a^{2008}-a^{2007}b+a^{2006}b^2-\cdots-ab^{2007}+b^{2008}\right)=7^m$$

と，$a+b\geq 2$ より

$$7\mid a+b$$

がわかる．$7\mid a+b$ と $\gcd(a,b)=1$ より，$7\nmid a, 7\nmid b$ なので，LTE より

$$v_7\left(a^{2009}+b^{2009}\right)=v_7(a+b)+v_7(2009)=v_7(a+b)+v_7\left(7^2\cdot 41\right)=v_7(a+b)+2$$

が成り立つ．$v_7\left(a^{2009}+b^{2009}\right)=v_7\left(7^m\right)=m$ だから，$v_7(a+b)=m-2$

$7\mid a+b$ であったから，$m\geq 3$.

また，

$$A=a^{2008}-a^{2007}b+a^{2006}b^2-\cdots-ab^{2007}+b^{2008}$$

とおくと

$$A(a+b)=7^m \qquad \cdots\cdots ②$$

となる．

ところで，$m=v_7\left(a^{2009}+b^{2009}\right)=v_7((a+b)A)=v_7(a+b)+v_7(A)=m-2+v_7(A)$ であるから，$v_7(A)=2$ となる．

$v_7(a+b)=m-2, v_7(A)=2$ と②から

$$a+b=7^{m-2},\ A=7^2 \quad (m\geq 3)$$

である．$a\neq b$ であったから，$a>b$ と仮定する．

$a>b$ だとすると，

$$\begin{aligned}7^2=A&=a^{2007}(a-b)+a^{2005}b^2(a-b)+\cdots+ab^{2006}(a-b)+b^{2007}\\&\geq a^{2007}+a^{2005}b^2+\cdots+ab^{2006}+b^{2007}\\&>a^{2007}+b^{2007}\\&\geq a+b=7^{m-2}\end{aligned}$$

から $7^2>7^{m-2}$ すなわち $m<4$ となる．$m\geq 3$ であったから，$m=3$.

$a+b=7, a^{2009}+b^{2009}=7^3=7^2(a+b)$ となるから

$$a\left(a^{2008}-49\right)+b\left(b^{2008}-49\right)=0. \qquad \cdots\cdots ③$$

$a\geq 2, b\geq 2$ のとき，$a^{2008}-49\geq 2^{2008}-49>0, b^{2008}-49\geq 2^{2008}-49>0$ だから，③は成り立たない．

よって，$a\leq 1$ または $b\leq 1$ となる．

$a=1$ のとき，③は

$$b\left(b^{2008}-49\right)=48 \qquad \cdots\cdots ④$$

となる．

$b\geq 2$ のとき，$b\left(b^{2008}-49\right)\geq 2\left(2^{2008}-49\right)>48$ だから，④は成り立たない．

$b=1$ のとき，④は成り立たない．

$b=1$ のときも同様である．

したがって，①を満たす正整数 a, b, m は存在しない． □

問題 10.4.2 (IMO Shortlist 1997)

Let $b, m, n \in \mathbb{N}$ with $b>1$ and $m\neq n$.
Suppose that b^m-1 and b^n-1 have the same set of prime divisors. Show that $b+1$ must be a power of 2.

解 1　$m>n\geq 1$ と仮定しても一般性を失わない．

- (a) $b=2$ かつ $m=6$
- (b) $m=2$ かつ $b+1$ は 2 のベキ乗

以外について考えると，Zsigmondy の定理より，b^m-1 は b^n-1 を割り切らない素数の因数をもつから，b^m-1 の素因数の集合と b^n-1 の素因数の集合は等しくならない．

したがって，(a) と (b) の場合を考える．

(a) の場合 $b=2, m=6$

$b^m-1=2^6-1=63=3^2\cdot 4$ の素因数の集合は $\left\{3,\, 7\right\}$.

$1\leq n<6$ のとき，$\left\{p : p \mid 2^n-1,\, p \text{ は素数}\right\}=\left\{3,\, 7\right\}$ をみたさない．

(b) の場合

$m=2, n=1,\ b+1=2^s, (s\in\mathbb{N}, s\geq 2)$ である．

$b^m-1=b^2-1=(b+1)(b-1)=2^{s+1}\left(2^{s-1}-1\right)$,

$b^n-1=b-1=2\left(2^{s-1}-1\right)$.

となり，b^m-1 の素因数の集合と b^n-1 の素因数の集合は等しくなる．

したがって，$b+1$ は 2 のベキ乗である． □

解 2　$m > m \geq 1$ と仮定しても一般性を失わない.

次のことが成り立つことを示す.

$$\begin{aligned} & b^m - 1 \text{ の素因数の集合と } b^n - 1 \text{ の素因数の集合は等しくなる} \\ \iff\ & b^m - 1 \text{ の素因数の集合と } b^n - 1 \text{ の素因数の集合と} \\ & \gcd(b^m - 1, b^n - 1) \text{ の素因数の集合はすべて等しくなる} \end{aligned}$$

($\Longrightarrow$) $b^m - 1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r},\ b^n - 1 = p_1^{\beta_1} \cdots p_r^{\beta_r}$, $p_1, \ldots, p_r$は異なる素数, $\alpha_i, \beta_i \in \mathbb{N}\ (i = 1, \ldots, r)$ とおくと

$$\gcd(b^m - 1, b^n - 1) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_r^{\min(\alpha_r, \beta_r)}.$$

$\min(\alpha_i, \beta_i) \geq 1\ (i = 1, \ldots, r)$ だから，$b^m - 1$ の素因数の集合と $b^n - 1$ の素因数の集合と $\gcd(b^m - 1, b^n - 1)$ の素因数の集合はすべて等しくなる.

($\Longleftarrow$) 明らかに成り立つ.

$$\gcd(b^m - 1, b^n - 1) = b^{\gcd(m,n)} - 1$$

が成り立つから,

$b^m - 1$ の素因数の集合と $b^{\gcd(m,n)} - 1$ の素因数の集合は等しくなる.

$d = \gcd(m, n), b^d = a, m = kd, n = ld,\ k, l \in \mathbb{N}, \gcd(l, k) = 1$ とおくと，$b^m - 1$ の素因数の集合と $b^{\gcd(m,n)} - 1$ の素因数の集合は等しくなることから,

$a^k - 1$ の素因数の集合と $a - 1$ の素因数の集合は等しくなる．$b > 1$ より $a = b^d > 1$ で，$m > n$ より $k > l \geq 1$.

- $a > 1, k > 1$ のとき，$a^k - 1$ の素因数の集合と $a - 1$ の素因数の集合が等しければ，$a + 1 = 2^{s_1},\ s_1 \in \mathbb{N}, s_1 \geq 2$ とかけることを示す.

$k \geq 3$ として，p を $p \mid k$ を満たす奇素数とする.

$p^\beta \parallel k$ として，$X = a^{p^\beta - 1} + \cdots + a + 1$ とおくと，$(a - 1)X = a^{p^\beta} - 1 \mid a^k - 1$ だから，$(a - 1)X$ の素因数の集合と $a - 1$ の素因数の集合は等しくなる.

ゆえに，$q \mid X$ を満たす素数 q は，$q \mid a - 1$ を満たす．これから，$a \equiv 1 \pmod{q}$ なので，すべての $i \in \mathbb{N}_0$ に対して，$a^i \equiv 1 \pmod{q}$ が成り立つから

$$\begin{aligned} X &= a^{p^\beta - 1} + \cdots + a + 1 \\ &\equiv 1 + \cdots + 1 + 1 \\ &\equiv p^\beta \pmod{q}. \end{aligned}$$

ゆえに，$q \mid X - p^\beta$ で，$q \mid X$ を使うと，$q \mid p^\beta$ が言える.

p, q は素数だから，$q = p$ となる．したがって，X は p 以外の素因数をもたない.

$q \mid a-1$ であったから，$p=q \mid a-1$ から $p \mid a-1$ なので (もちろん，$p \nmid a, p \nmid 1$)，LTE より

$$v_p\left(a^{p^\beta}-1\right)=v_p(a-1)+v_p\left(p^\beta\right)=v_p(a-1)+\beta.$$

また，

$$v_p\left(a^{p^\beta}-1\right)=v_p((a-1)X)=v_p(a-1)+v_p(X)$$

であるから，$v_p(X)=\beta$ すなわち

$$p^\beta \mid X$$

を得る．X は p 以外の素因数をもたないから

$$X=p^\beta$$

となる．

$h>0, r \geq 2$ が正整数のとき，$(1+h)^r>1+rh$ が成り立つから，$h=a-1, r=p^\beta$ とおくと，$a^{p^\beta}>1+p^\beta(a-1)$ から

$$\frac{a^{p^\beta}-1}{a-1}>p^\beta \quad \text{すなわち} \quad X>p^\beta.$$

これは，$X=p^\beta$ に矛盾する．したがって，$k\ (\geq 3)$ は奇素数を因数に持たないことになり，k は 2 のベキ乗である（$k=2$ のときは，$k=2^1$ となっている)．

$k=2^{k_1}\ (k_1 \in \mathbb{N})$ とおくと，$a^2-1 \mid a^{2^{k_1}}-1=a^k-1,\ a-1 \mid a^2-1$ で，a^k-1 の素因数の集合と $a-1$ の素因数の集合が等しいから，$a^2-1=(a+1)(a-1)$ の素因数の集合と $a-1$ の素因数の集合が等しくなる．

よって，$a+1$ の任意の素因数 q は $a-1$ を割り切らなければならない．

$q \mid a+1, q \mid a-1$ から $q \mid (a+1)-(a-1)=2$ すなわち $q=2$ となる．

$a+1$ は 2 以外の素因数をもたないから，

$$a+1=2^{s_1},\ s_1 \in \mathbb{N}, s_1 \geq 1 \qquad \cdots\cdots ①$$

とかける．

①から $a+1=2^{s_1}$ で $a=b^d$ を満たす d は奇数である．

なぜならば，d が偶数だとして，$a+1=b^d+1$ を考える．

b が偶数のとき，$b^2 \equiv 0 \pmod 4$ より，$b^d+1 \equiv 1 \pmod 4$.

b が奇数のとき，$b^2 \equiv 1 \pmod 4$ より，$b^d+1 \equiv 2 \pmod 4$.

$b^d+1=a+1$ が 4 で割り切れないことになり，$2^2 \mid 2^{s_1}=a+1$ に矛盾する．

したがって，d は奇数となり，

$$b+1 \mid b^d+1=a+1=2^{s_1}.$$

これから

$$b+1=2^s,\ s\in\mathbb{N}, s\geq 1$$

とかける．　□

問題 10.4.3 Determine all positive integer m,n,l,k with $l>1$ such that :

$$(1+m^n)^l=1+m^k.$$

解答　$(1+m^n)^l=1+m^k.$　……①

$m=1$ のとき，①は $2^l=2$ となり $l=1$．これは $l>1$ に矛盾する．

よって，$m\geq 2$ である．

このとき，$1+m^k=(1+m^n)^l>1+m^m$ から，$k>n$.

• $m=2,k=3$

以外のときは，Zsigmondy の定理より，$1+m^k$ は $1+m^n$ を割り切らない素数の因数 p が存在する．これは，①に矛盾する．

したがって，$m=2,k=3$ でなければならない．このとき，①は

$$(1+2^n)^l=1+2^3=9=3^2$$

となる．$l\geq 2, 2^n+1\geq 3$ だから，$l=2, 2^n+1=3$ となり，$l=2,n=1$ を得る．

よって，求める解は，$(m,n,l,k)=(2,1,2,3)$.　□

問題 10.4.4 (Romania TST 1994)

Prove that the sequence $a_n=3^n-2^n$ contains no three terms in geometric progression.

解答 等比数列をなす 3 項，a_l,a_m,a_n $(l<m<n)$ が存在したとする．$a_m^2=a_la_n$ から

$$(3^m-2^m)^2=\left(3^l-2^l\right)\left(3^n-2^n\right)\qquad\cdots\cdots①$$

Zsigmondy の定理より，3^n-2^n は 3^m-2^m を割り切らない素数の因数 p をもつので，①に矛盾する．

したがって，$\{a_n\}$ は等比数列をなす 3 数を含まない．　□

問題 10.4.5 (Italy TST 2003)

Find all triples of positive integers (a,b,p) with a,b positive integers and p a prime number such that $2^a+p^b=19^a$.

解 1　$19^a-2^a=p^b$ と変形する．$17=19-2\mid 19^a-2^a=p^b$ から，$17\mid p^b$.

p は素数だから，$p = 17$ となる．

$$19^a - 2^a = 17^b \qquad \cdots\cdots ①$$

とおく．

$a \geq 3$ のときは，Zsigmondy の定理より，$19^a - 2^a$ は $19^1 - 2^1$ を割り切らない素数の因数 q をもつ．

$q \mid 19^a - 2^a = 17^b$ より，$q = 17$ となるが，$q \nmid 19^1 - 2^1 = 17$ に矛盾する．

したがって，$a < 3$ でなければならない．

$a = 1$ のとき，①は $17 = 17^b$ となり，$b = 1$.

$a = 2$ のとき，①は $17 \cdot 21 = 17^b$ すなわち $21 = 17^{b-1}$ となり，これを満たす正整数 b は存在しない．

以上のことから，求める解は，$(a, b, p) = (1, 1, 17)$. □

解 2　$2^a + p^b = 19^a \qquad \cdots\cdots ①$

とおく．①より

$$\begin{aligned} p^b = 19^a - 2^a &= (19 - 2)\left(19^{a-1} + 19^{a-2} + \cdots + a + 1\right) \\ &= 17\left(19^{a-1} + 19^{a-2} + \cdots + a + 1\right). \end{aligned}$$

ゆえに，$17 \mid p^b$．p は素数だから，$p = 17$.

$a \geq 2$ だとすると，

$$2^a + 17^b = 19^a = (2 + 17)^a > 2^a + 17^a$$

から，$17^b > 17^a$ が成り立つ．

よって，$b > a$ から

$$b \geq a + 1 \qquad \cdots\cdots ②$$

を得る．

$17 \mid 19 - 2$, $17 \nmid 19$, $17 \nmid 2$ だから，LTE より

$$v_{17}\left(19^a - 2^a\right) = v_{17}(19 - 12) + v_{17}(a) = 1 + v_{17}(a).$$

ところで，$v_{17}\left(19^a - 2^a\right) = v_{17}\left(17^b\right) = b$ だから，

$$b = 1 + v_{17}(a)$$

が成り立つ．ここで，②を使うと

$$v_{17}(a) = b - 1 \geq a \ (\geq 2).$$

よって，$17^a \mid a$ から

$$17^a \leq a. \qquad \cdots\cdots ③$$

$a \geq 2$ のとき，$17^a > a$ が成り立つから，③に矛盾する．

したがって，$a = 1$ でなければならない．このとき，①は $2^1 + 17^b = 19^1$ となるから，$17^b = 1$.

ゆえに，$b = 1$.

以上のことから，求める解は，$(a, b, p) = (1, 1, 17)$. □

問題 10.4.6 Find all nonnegative integers m, n such that $3^m - 5^n$ is perfect square.

解答　$3^m - 5^n = a^2$ ……①

とおく．①を　mod 4 で考えると，$3^m - 5^n \equiv (-1)^m - 1 \pmod 4$.

一方，$a^2 \equiv 0 \pmod 4$ または $a^2 \equiv 1 \pmod 4$ だから，①が成り立つためには，m と a は偶数でなければならない．$m = 2k$ $(k \in \mathbb{N}_0)$ とおくと，①は $3^{2k} - a^2 = 5^n$ となり

$$\left(3^k + a\right)\left(3^k - a\right) = 5^n \quad \cdots\cdots ②$$

と変形できる．これから，

$$3^k + a = 5^x, 3^k - a = 5^y,\ x, y \in \mathbb{N}_0, x \geq y, x + y = n$$

とおける．$\left(3^k + a\right) + \left(3^k - a\right) = 5^x + 5^y$ から

$$2 \cdot 3^k = 5^x + 5^y.$$

これを

$$2 \cdot 3^k = 5^y\left(5^{x-y} + 1\right) \quad \cdots\cdots ③$$

と変形する．

$y \geq 1$ のときは，③の右辺は 5 の倍数となり，$2 \cdot 3^k$ が 5 の倍数となり，矛盾が生じる．

したがって，$y = 0$ で，③は

$$2 \cdot 3^k = 5^x + 1 \quad \cdots\cdots ④$$

となる．

$x \geq 2$ のとき，Zsigmondy の定理より，$p \mid 5^x + 1, p \nmid 5 + 1 = 2 \cdot 3$ を満たす素数 p が存在する．$p \mid 5^x + 1 = 2 \cdot 3^k$ より $p \in \left\{2, 3\right\}$ となるが，これは，$p \nmid 5 + 1 = 2 \cdot 3$ に矛盾する．

したがって，$x \leq 1$ である．

$x = 0$ のとき，④より，$k = 0$．よって，$m = 0, n = 0, a = 0$.

$x = 1$ のとき，④より，$k = 1$．よって，$m = 2, n = 1, a = 2$.

以上のことから，求める解は，$(m, n) = (0, 0), (2, 1)$. □

問題 10.4.7 Find all positive integers $a, n > 1$ and k for which $3^k - 1 = a^n$.

解答　$3^k - 1 = a^n$ ……①

とおく．①を　mod 3 で考えると

$$a^n = 3^k - 1 \equiv -1 \pmod 3.$$

n が偶数だと仮定すると，$a^2 \equiv 0 \pmod 3$ または $a^2 \equiv 1 \pmod 3$ であるから，

$a^n \equiv 0 \pmod 3$ または $a^n \equiv 1 \pmod 3$ となり，$a^n \equiv -1 \pmod 3$ に矛盾する．

したがって，n は奇数，かつ，$a \equiv -1 \pmod 3$ となる．

①より

$$3^k = a^n + 1 = (a+1)\left(a^{n-1} - a^{n-2} + \cdots - a + 1\right)$$

すなわち

$$3^k = (a+1)\left(a^{n-1} - a^{n-2} + \cdots - a + 1\right). \quad \cdots\cdots ②$$

$a + 1 > 2$ だから，$3 \mid a + 1$ となる．

$a^n + 1$ において，$(a, n) = (2, 3)$ 以外だとすると，Zsigmondy の定理より，

$p \mid a^n + 1, p \nmid a + 1$ を満たす素数 p が存在する．

$3 \mid a + 1$ であったから，$p \neq 3$．ところで，$p \mid a^n + 1 = 3^n$ から $p = 3$ となり，これは $p \neq 3$ に矛盾する．

したがって，$(a, n) = (2, 3)$ でなければならない．①に代入して，$3^k = 2^3 + 1 = 3^2$ から $k = 2$.

よって，$(a, n, k) = (2, 3, 2)$. □

問題 10.4.8　Find all positive integers a, b and $c \geq 2$ such that : $a^b + 1 = (a+1)^c$.

解答　$a^b + 1 = (a+1)^c$ ……①

とおく．

$a = 1$ のとき，①は $2 = 2^c$ となり，$c = 1$ であるが，これは $c \geq 2$ に矛盾する．よって，$a \neq 1$ である．

$b \geq 3$ のとき，$a^b + 1$ は $2^3 + 1$ 以外のときは，Zsigmondy の定理より，$p \mid a^b + 1, p \nmid a + 1$ を満たす素数 p が存在するから，①に矛盾する．

したがって，$a = 2, b = 3$ または $b < 3$ となる．

$a = 2, b = 3$ のとき，①は，$2^3 + 1 = (2+1)^c$ となるから，$c = 2$ である．

$b = 1$ のとき，①は，$a + 1 = (a+1)^c$ となるから，$c = 1$ である．これは，$c \geq 2$ に矛盾する．

$b = 2$ のとき，①は，$a^2 + 1 = (a+1)^c$ となる．$(a+1)^2 > a^2 + 1 = (a+1)^c$ から $c < 2$ すなわち $c = 1$ となる．これは，$c \geq 2$ に矛盾する．

以上のことから，求める解は，$(a,b,c)=(2,3,2)$. □

問題 10.4.9 (British Math Olympiad 1996)

Determine all sets of non-negative integers x, y and z which satisfy the equation $2^x+3^y=z^2$.

解 1　$2^x+3^y=z^2$ ……①

とおく．

$y=0$ のとき，①は $2^x=z^2-1=(z+1)(z-1)$ となる．

$z(\geq 3)$ は奇数で，$2^{x-2}=\dfrac{z+1}{2}\cdot\dfrac{z-1}{2}$.

$$\gcd\left(\frac{z+1}{2},\frac{z-1}{2}\right)=\gcd\left(\frac{z+1}{2}-\frac{z-1}{2},\frac{z-1}{2}\right)=\gcd\left(1,\frac{z-1}{2}\right)=1$$

で，$\dfrac{z+1}{2}>\dfrac{z-1}{2}$ だから

$$\frac{z+1}{2}=2^{x-2},\ \frac{z-1}{2}=1.$$

よって，$z=3, x=3$ から，$(x,y,z)=(3,0,3)$.

$y\geq 1$ のとき，①を　mod 3 で考えると

$$z^2=2^x+3^y\equiv(-1)^x+0\equiv(-1)^x \pmod 3.$$

一方，$z^2\equiv 0 \pmod 3$ または $z^2\equiv 1 \pmod 3$ であるから，x は偶数で，$3\nmid z$ となる．

$x=2w$ $(w\in\mathbb{N}_0)$ とおくと，①から

$$3^y=z^2-2^{2w}.$$

$w=0$ のとき，$3^y=z^2-1=(z+1)(z-1),\ z\geq 2.$

$$\gcd(z+1,z-1)=\gcd(z+1-(z-1),z-1)=\gcd(2,z-1)\in\left\{1,2\right\}$$

で，$z+1=3^a, z-1=3^b$ $(a\in\mathbb{N}, b\in\mathbb{N}_0)$ の形だから，$\gcd(z+1,z-1)\neq 2$ なので，$\gcd(z+1,z-1)=1$ となる．

よって，$z+1=3^y, z-1=1$ から，$z=2, y=1$ すなわち，$(x,y,z)=(0,1,2)$.

$w\geq 1$ のとき，$3^y=z^2-2^{2w}$ から，z は奇数であることがわかり，

$$3^y=(z+2^w)(z-2^w).\quad\text{……②}$$

$\gcd(z+2^w,z-2^w)=\gcd(z+2^w-(z-2^w),z-2^w)=\gcd\left(2^{w+1},z-2^w\right)$ で，

z は奇数なので，$2\nmid z-2^w$ だから，$\gcd\left(2^{w+1},z-2^w\right)=1$.

すなわち，$\gcd(z+2^w,z-2^w)=1$ である．

$z+2^w > z-2^w$ だから

$$z+2^w = 3^y,\ z-2^w = 1 \qquad \cdots\cdots ③$$

となる．z を消去すると

$$2^{w+1} = 3^y - 1. \qquad \cdots\cdots ④$$

$y \geq 3$ のとき，Zsigmondy の定理より，$p \mid 3^y - 1, p \nmid 3-1=2$ を満たす素数 p が存在する．

$p \mid 3^y - 1 = 2^{w+1}$ から $p=2$ で，これは $2=p \nmid 2$ に矛盾する．

したがって，$y<3$ である．

$y=1$ のとき，④から，$w=0$ で，これは $w \geq 1$ に矛盾する．

$y=2$ のとき，④から，$w=2$ で，$x=2w=4$．③から，$z=5$ となるから，$(x,y,z)=(4,2,5)$.

したがって，求める解は，$(x,y,z)=(0,1,2),(3,0,3),(4,2,5)$. □

x の値で場合分けをすると，次のような解になる．（ついでに，Zsigmondy の定理を使わないようにしてある．）

解 2　$2^x+3^y=z^2$ $\cdots\cdots ①$

とおく．

$x=0$ のとき，①は $3^y = z^2-1 = (z+1)(z-1)$.

z は偶数で $z \geq 2$ だから，

$$\gcd(z+1, z-1) = \gcd(z+1-(z-1), z-1)\ \gcd(2, z-1) = 1.$$

$\gcd(z+1,z-1)=1, z+1>z-1\geq 1$ で $3^y=(z+1)(z-1)$ だから，$z+1=3^y, z-1=1$.
よって，$z=2, y=1$ から $(x,y,z)=(0,1,2)$.

$x=1$ のとき，①は $3^y=z^2-2$.

mod 3 で考えると，$z^2 \equiv 0 \pmod 3$ または $z^2 \equiv 1 \pmod 3$ だから，

$z^2-2 \equiv -2 \equiv 1 \pmod 3$ または $z^2-2 \equiv 1-2 \equiv -1 \equiv 2 \pmod 3$.

$3^y \equiv 0 \pmod 3$ だから，$3^y = z^2-2$ は解をもたない．

$x \geq 2$ のとき，　mod 4 で考えると，$2^x+3^y \equiv 0+(-1)^y \equiv (-1)^y \pmod 4$.

$z^2 \equiv 0 \pmod 4$ または $z^2 \equiv 1 \pmod 4$ だから，$2^x+3^y=z^2$ より，$(-1)^y \equiv 1 \pmod 4$ とならなければならない．

よって，y は偶数で，z は奇数となる．$y=2y_1$ $(y_1 \in \mathbb{N}_0)$ とおくと，①より

$$2^x = z^2-3^y = z^2-3^{2y_1} = (z+3^{y_1})(z-3^{y_1})$$

すなわち

$$2^x = (z+3^{y_1})(z-3^{y_1}). \qquad \cdots\cdots ②$$

z は奇数だから，$z+3^{y_1}, z-3^{y_1}$ は正の偶数となるので，

$$z+3^{y_1}=2^c,\ z-3^{y_1}=2^d\ c,d\in\mathbb{N}, c+d=x, c>d$$

とおける．z を消去すると，$2\cdot 3^{y_1}=2^c-2^d$ から

$$3^{y_1}=2^{c-1}-2^{d-1}. \qquad \cdots\cdots ③$$

$d-1>0$ だと，③から，$3^{y_1}=2^{d-1}\left(2^{c-d}-1\right)$ で，3^{y_1} が 2 の倍数となり矛盾が生じる．したがって，$d=1$ で，このとき，③は

$$3^{y_1}+1=2^{c-1}. \qquad \cdots\cdots ④$$

y_1 が偶数のとき，$3^{y_1}+1=9^{\frac{y_1}{2}}+1\equiv 1+1\equiv 2 \pmod 4$ より，$2\parallel 3^{y_1}+1=2^{c-1}$ となるから，$c-1=1$.
よって，$c=2$ で，$y_1=0, y=2y_1=0, x=c+d=3, z=2^c-3^{y_1}=3$ から，$(x,y,z)=(3,0,3)$.

y_1 が奇数のとき，　mod 3 で考えると，$0\equiv 3^{y_1}\equiv 2^{c-1}-1\equiv(-1)^{c-1}-1 \pmod 3$ より，$c-1$ は偶数である．

$c-1=2r\ (r\in\mathbb{N}_0)$ とおくと，④は，$3^{y_1}=2^{c-1}-1=2^{2r}-1=\left(2^r+1\right)\left(2^r-1\right)$ となり

$$3^{y_1}=\left(2^r+1\right)\left(2^r-1\right). \qquad \cdots\cdots ⑤$$

明らかに $r\geq 1$ で，

$$\gcd\left(2^r+1, 2^r-1\right)=\gcd\left(2^r+1-\left(2^r-1\right), 2^r-1\right)=\gcd\left(2, 2^r-1\right)=1,$$

$2^r+1>2^r-1$ だから，$2^r+1=3^{y_1}, 2^r-1=1$ となる．
よって，$r=1, y_1=1$ で $y=2y_1=2, c=3, x=c+d=4, z=2^c-3^{y_1}=5$ から，$(x,y,z)=(4,2,5)$.

したがって，求める解は，$(x,y,z)=(0,1,2),(3,0,3),(4,2,5)$. □

問題 10.4.10 Fermat's last theorem asserts that for a positive integer $n\geq 3$, the equation $x^n+y^n=z^n$ has no integral solution with $xyz\neq 0$. Prove this statement when z is a prime.

解答　$x^n+y^n=z^n$ が $xyz\neq 0$ となる整数解を持つとする．一般性を失うことなく，$x,y,z>0$ と仮定してよい．

$d=\gcd(x,y)>1$ のとき，$x=dx_1, y=dy_1, x_1, y_1\in\mathbb{N}, \gcd(x_1,y_1)=1$ とおき，$x^n+y^n=z^n$ に代入すると，$d^n\left(x_1^n+y_1^n\right)=z^n$ となる．

$d^n \mid z^n$ で，d, z を素因数分解して，

$$d = p_1^{\alpha_1} \cdots p_r^{\alpha_r},\ z = p_1^{\beta_1} \cdots p_r^{\beta_r},\ p_1, \ldots, p_r \text{は異なる素数}, \alpha_i, \beta_i \in \mathbb{N}_0\ (1 \leq i \leq r)$$

とおくと

$$d^n = p_1^{n\alpha_1} \cdots p_r^{n\alpha_r} \mid z^n = p_1^{n\beta_1} \cdots p_r^{n\beta_r}$$

から，$n\alpha_i \leq n\beta\ (1 \leq i \leq r)$ すなわち，$\alpha_i \leq \beta\ (1 \leq i \leq r)$ となり，$d \mid z$ が言える．

$z = dz_1\ (z_1 \in \mathbb{N})$ とおき，$d^n\,(x_1^n + y_1^n) = z^n$ に代入すると，

$$x_1^n + y_1^n = z_1^n,\ \gcd(x_1, y_1) = 1$$

となるので，最初から，

$$x^n + y^n = z^n,\ \gcd(x, y) = 1 \qquad \cdots\cdots ①$$

と考えてよい．

$x = y$ だとすると，①は $2x^n = z^n$ となり，$\sqrt[n]{2} = \dfrac{z}{x}$．これから，$\sqrt[n]{2}$ は有理数となり，無理数であることに矛盾する．したがって，$x \neq y$ である．

(1) $n(\geq 3)$ が奇数の場合

Zsigmondy の定理より，$p_1 \mid x^n + y^n, p_1 \nmid x + y$ となる素数 p_1 が存在する．

また，$x + y \geq 2$ であるから，$p_2 \mid x + y$ となる素数 p_2 が存在する．$p_1 \nmid x + y$ だから，$p_1 \neq p_2$ である．

n は奇数だから，$p_2 \mid x + y \mid x^n + y^n$ より $x^n + y^n$ は異なる素因数 p_1, p_2 をもつことになる．

①から，$p_1 \mid x^n + y^n = z^n, p_2 \mid x^n + y^n = z^n$ すなわち，$p_1 \mid z^n, p_2 \mid z^n$ で，p_1, p_2, z は素数だから，$p_1 = z, p_2 = z.$

よって，$p_1 = p_2$ となり，$p_1 \neq p_2$ に矛盾する．

(2) $n\ (\geq 4)$ が偶数の場合

$n = 2^m n_1$，$m, n_1 \in \mathbb{N}$ (n_1は奇数) とおく．

$n_1 > 1$ だと $x^n + y^n = z^n$ は

$$\left(x^{2^m}\right)^{n_1} + \left(y^{2^m}\right)^{n_1} = \left(z^{2^m}\right)^{n_1}$$

となる．$X = x^{2^m}, Y = y^{2^m}, Z = z^{2^m}$ とおくと

$$X^{n_1} + Y^{n_1} = Z^{n_1},\ n_1(\geq 3) \text{ は奇数},\ \gcd(X, Y) = 1 \qquad \cdots\cdots ②$$

となり，(1) と同じく矛盾が生じる．

したがって，$n_1 = 1$ で $n = 2^m, m \in \mathbb{N}$ である．$n \geq 4$ より $m \geq 2$ となる．

$x^{2^m}+y^{2^m}=z^{2^m}$ は

$$\left(x^{2^{m-2}}\right)^4+\left(y^{2^{m-2}}\right)^4=\left(z^{2^{m-2}}\right)^4$$

となり，$X=x^{2^{m-2}}, Y=y^{2^{m-2}}$ とおくと，$X^4+Y^4=Z^4$ が正整数解をもつことになり矛盾が生じる．　□

「不定方程式 $X^4+Y^4=Z^4$ が正整数解をもたない.」ことは定理 11.0.3 で示す．

定理 11.0.1　不定方程式 $x^2+y^2=z^2,\ x,y,z\in\mathbb{N},\ \gcd(x,y)=1$ の解は

$$(x,y,z)=(2pq,p^2-q^2,p^2+q^2) \text{ または } (x,y,z)=(p^2-q^2,2pq,p^2+q^2)$$

である．ここで，$p,q\in\mathbb{N},\ p>q>0,\ \gcd(p,q)=1,\ pq$ は偶数 とする．

証明　● x,y のどちらか一方が偶数で，他方が奇数である．

x,y がともに奇数だとすると，$x^2\equiv 1\pmod 4, y^2\equiv 1\pmod 4$ より $x^2+y^2\equiv 2\pmod 4$ である．

ところで，$z^2\equiv 0\pmod 4$ または $z^2\equiv 1\pmod 4$ であるから，$x^2+y^2=z^2$ は成り立たない．x,y がともに偶数だとすると，$\gcd(x,y)=1$ に矛盾する．

x が偶数で，y が奇数と仮定しても一般性を失わない．すると，$x^2+y^2=z^2$ から z は奇数であることがわかる．

$x^2+y^2=z^2$ を

$$\left(\frac{x}{2}\right)^2=\frac{z+y}{2}\cdot\frac{z-y}{2}$$

と変形する．

$$\gcd\left(\frac{z+y}{2},\frac{z-y}{2}\right)=\gcd\left(\frac{z+y}{2},\frac{z-y}{2}+\frac{z+y}{2}\right)=\gcd\left(\frac{z+y}{2},z\right).$$

z は奇数だから

$$\gcd\left(\frac{z+y}{2},z\right)=\gcd\left(2\cdot\frac{z+y}{2},z\right)=\gcd(z+y,z)=\gcd(z+y-z,z)=\gcd(y,z)=1.$$

よって，$\gcd\left(\frac{z+y}{2},\frac{z-y}{2}\right)=1$ となり，$\frac{z+y}{2}$ と $\frac{z-y}{2}$ は互いに素である．

したがって

$$\frac{x}{2}=pq,\ \frac{z+y}{2}=p^2,\ \frac{z-y}{2}=q^2,\ p>q>0,\ \gcd(p,q)=1$$

を満たす整数 p,q が存在する．これから

$$x=2pq, y=p^2-q^2, z=p^2+q^2$$

となる．y, z は奇数であったから，p, q のどちらか一方が偶数で，他方が奇数であることもわかる．

x が奇数，y が偶数の場合も考えて，不定方程式の解は

$$(x, y, z) = (2pq, p^2 - q^2, p^2 + q^2) \text{ または } (x, y, z) = (p^2 - q^2, 2pq, p^2 + q^2)$$

である．ここで，$p, q \in \mathbb{N},\ p > q > 0,\ \gcd(p, q) = 1,\ pq$ は偶数 とする． □

定理 11.0.2　不定方程式 $x^4 + y^4 = z^2$ は $xyz \neq 0$ なる整数解をもたない．

証明　$x, y, z > 0$ と仮定してよい．

$$x^4 + y^4 = z^2 \qquad \cdots\cdots ①$$

とおく．①に正の整数解 (x, y, z) があったと仮定して，無限降下法を用いて矛盾が生じることを示す．

• $\gcd(x, y) = 1$ と仮定できる．

$d = \gcd(x, y) > 1$ とすると，$x = dx_1, y = dy_1, x_1, y_1 \in \mathbb{N}, \gcd(x_1, y_1) = 1$ とおける．これらの式を①に代入すると

$$d^4 \left(x_1^4 + y_1^4\right) = z^2 \qquad \cdots\cdots ②$$

となる．$\left(d^2\right)^2 = d^4 \mid z^2$ から $d^2 \mid z$ となる[*1]ので，$z = d^2 z_1\ (z_1 \in \mathbb{N})$ とおき，② に代入すると

$$x_1^4 + y_1^4 = z_1^2,\ \gcd(x_1, y_1) = 1$$

となる正の整数解 (x_1, y_1, z_1) が得られるので，最初から，$\gcd(x, y) = 1$ を満たす正の整数解 (x, y, z) としてもよい．

①は $\left(x^2\right)^2 + \left(y^2\right)^2 = z^2$ と変形できるので，x^2 は偶数（y^2, z は奇数）とすると

$$x^2 = 2pq, y^2 = p^2 - q^2, z = p^2 + q^2$$

とおける．ただし，$p, q \in \mathbb{N},\ p > q > 0,\ \gcd(p, q) = 1,\ pq$ は偶数 とする．

• q は偶数，p は奇数である．

p が偶数，q が奇数だとすると，$p^2 \equiv 0 \pmod 4, q^2 \equiv 1 \pmod 4$.

$p^2 - q^2 \equiv 0 - 1 \equiv 3 \pmod 4$ から $y^2 \equiv p^2 - q^2 \equiv 3$ となるが，y は奇数だから，$y^2 \equiv 1 \pmod 4$ に矛盾する．したがって，q は偶数，p は奇数である．

$x^2 = 2pq$ から

$$\left(\frac{x}{2}\right)^2 = p \cdot \frac{q}{2}.$$

[*1] 問題 10.4.10 の解答の中で $d^n \mid z^n \iff d \mid z$ を示してある．

これから，$p = z_1^2, \dfrac{q}{2} = w^2,\ z_1, w \in \mathbb{N}, \gcd(z_1, w) = 1$ を満たす整数 z_1, w が存在する．

$p = z_1^2, q = 2w^2$ を $q^2 + y^2 = p^2$ に代入すると

$$\left(2w^2\right)^2 + y^2 = \left(z_1^2\right)^2.$$

再び，定理 11.0.1 より，

$$2w^2 = 2u_1v_1, y = u_1^2 - v_1^2, z_1^2 = u_1^2 + v_1^2$$

とおける．ただし，$u_1, v_1 \in \mathbb{N},\ u_1 > v_1 > 0,\ \gcd(u_1, v_1) = 1,\ u_1v_1$は偶数 とする．

$w^2 = u_1v_1, \gcd(u_1, v_1) = 1$ から，$u_1 = x_1^2, v_1 = y_1^2,\ x_1, y_1 \in \mathbb{N}, \gcd(x_1, y_1) = 1$ を満たす整数 x_1, y_1 が存在する．これらを，$u_1^2 + v_1^2 = z_1^2$ に代入すると

$$x_1^4 + y_1^4 = z_1^2,\ \gcd(x_1, y_1) = 1.$$

ここで，

$$z = p^2 + q^2 = \left(z_1^2\right)^2 + \left(2w^2\right)^2 = z_1^4 + 4w^4 > z_1^4 \geq z_1$$

より

$$1 \leq z_1 < z.$$

①の正整数解 $(x, y, z), \gcd(x, y) = 1$ から，①の正整数解 $(x_1, y_1, z_1), \gcd(x_1, y_1) = 1,$ $z_1 < z$ が得られた．この操作を繰り返すと，無限列

$$(x, y, z), (x_1, y_1, z_1), (x_2, y_2, z_2), \ldots, (x_n, y_n, z_n), \ldots \qquad z > z_1 > z_2 > \cdots > z_n > \ldots$$

が得られるが，z は正の整数なので無限に続くことは不可能である．

したがって，①は $xyz \neq 0$ なる整数解をもたない． □

定理 11.0.3　不定方程式 $x^4 + y^4 = z^4$ は $xyz \neq 0$ なる整数解をもたない．

証明 もしも $x^4 + y^4 = z^4$ が $xyz \neq 0$ なる整数解 (a, b, c) をもったとすると，

$$a^4 + b^4 = c^4,\ a, b, c \in \mathbb{Z}, a \neq 0, b \neq 0, c \neq 0.$$

より

$$a^4 + b^4 = \left(c^2\right)^2,\ a, b, c \in \mathbb{Z}, a \neq 0, b \neq 0, c^2 \neq 0.$$

$x^4 + y^4 = z^2$ は $xyz \neq 0$ なる整数解 (a, b, c^2) をもつことになり，定理 11.0.2 に矛盾する．

したがって，不定方程式 $x^4 + y^4 = z^4$ は $xyz \neq 0$ なる整数解をもたない． □

問題 10.4.11 (Russia 1996) (例題 7.4.1 と同じ問題)

Find all positive integers n for which there exist positive integers x, y and k such that $\gcd(x, y) = 1$, $k > 1$ and $3^n = x^k + y^k$.

解 1　k は奇数である．k が偶数だとすると，$3 \mid 3^n = x^k + y^k$ と $\gcd(x, y) = 1$ より，$3 \nmid x, 3 \nmid y$ である．

k は偶数だから，$x^k \equiv 1 \pmod 3$, $y^k \equiv 1 \pmod 3$ より $x^k + y^k \equiv 2 \pmod 3$ となり，$x^k + y^k \equiv 0 \pmod 3$ に矛盾する．

したがって，k は奇数でなければならない．

$x = y$ だとすると，$3^n = x^k + y^k$ は $3^n = 2x^k$ となりこれを満たす正整数 n, x, k は存在しないから，$x \neq y$ である．

Zsigmondy の定理より，$x^k + y^k$ は $2^3 + 1^3$ の場合を除くと，$p \mid x^k + y^k$, $p \nmid x + y$ となる素数 p が存在する．

$p \mid x^k + y^k = 3^n$ で p は素数だから，$p = 3$ となるので，$3 = p \nmid x + y$.

ところで，k は奇数だから，

$$3^n = x^k + y^k = (x + y)\left(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}\right).$$

$x + y \geq 2$ より $3 \mid x + y$ となり，$3 = p \nmid x + y$ に矛盾する．

したがって，$x^k + y^k$ は $2^3 + 1^3$ の形でなければならないから，$k = 3$ で，$3^n = 2^3 + 1^3$ から $n = 2$ である．

以上のことから，求める n の値は $n = 2$. □

解 2　k は奇数である．k が偶数だとすると，$3 \mid 3^n = x^k + y^k$ と $\gcd(x, y) = 1$ より，$3 \nmid x, 3 \nmid y$ である．

k は偶数だから，$x^k \equiv 1 \pmod 3$, $y^k \equiv 1 \pmod 3$ より $x^k + y^k \equiv 2 \pmod 3$ となり，$x^k + y^k \equiv 0 \pmod 3$ に矛盾する．

したがって，k は奇数でなければならない．

$$3^n = x^k + y^k = (x + y)\left(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}\right). \quad \cdots\cdots ①$$

$x + y \geq 2$ より $3 \mid x + y$ となり，①より，

$$x + y = 3^m \quad (m \in \mathbb{N}) \quad \cdots\cdots ②$$

とおける．

$A = x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}$ とおくと，

$$A = 3^{n-m} \quad \cdots\cdots ③$$

$x=y$ だとすると，$3^n=x^k+y^k$ は $3^n=2x^k$ となりこれを満たす正整数 n,x,k は存在しないから，$x\neq y$ である．対称性から $x>y$ と仮定しても一般性を失わない．

$$A=x^{k-2}(x-y)+x^{k-3}y^2(x-y)+\cdots+xy^{k-3}(x-y)+y^{k-1}>1$$

だから，③より $3\mid A$ すなわち，$v_3(A)\geq 1$.

$n=v_3\left(3^n\right)=v_3(x+y)+v_3(A)$ で $v_3(A)\geq 1$ だから，$m=v_3(x+y)\leq n-1$.

$3\mid x+y$ と $\gcd(x,y)=1$ から $3\nmid x, 3\nmid y$ となるので，LTE より

$$n=v_3\left(3^n\right)=v_3\left(x^k+y^k\right)=v_3(x+y)+v_3(k)=m+v_3(k).$$

よって

$$n=m+v_3(k). \qquad \cdots\cdots ④$$

$m=v_3(x+y)\leq n-1$ だから，$v_3(k)=n-m\geq 1$ すなわち

$$v_3(k)\geq 1.$$

(1) $m\geq 2$ の場合

すべての正整数 a に対して，$3^a\geq a+2$ が成り立つ． $\cdots\cdots(*)$

$3^{v_3(k)}\mid k$ より $3^{v_3(k)}\leq k$.

$v_3(k)\geq 1$ だから，$(*)$ を使うと，$v_3(k)+2\leq 3^{v_3(k)}$ が成り立つから，

$$v_3(k)+2\leq 3^{v_3(k)}\leq k \text{ すなわち } v_3(k)+2\leq k$$

が言える．よって

$$v_3(k)\leq k-2.$$

$M=\max(x,y)$ とすると $x+y=3^m\geq 9$ より $M\geq 5$.

すると

$$\begin{aligned} x^k+y^k&>M^k=M\cdot M^{k-1}\\ &\geq \frac{x+y}{2}\cdot 5^{k-1}=3^m\cdot\frac{5^{k-1}}{2}\\ &>3^m\cdot 5^{k-2}\\ &>3^{m+k-2}\\ &\geq 3^{m+v_3(k)}=3^n \end{aligned}$$

から，$x^k+y^k>3^n$ となり，$x^k+y^k=3^n$ に矛盾する．

(2) $m=1$ の場合

$x+y=3$ から $(x,y)=(1,2),(2,1)$.

$n = m + v_3(k) = 1 + v_3(k)$ で $3^n = x^k + y^k = 1^k + 2^k$ から

$$3^{v_3(k)} = 1 + 2^k.$$

$3^{v_3(k)} \mid k$ より $3^{v_3(k)} \leq k$.

ゆえに

$$1 + 2^k = 3^{1+v_3(k)} = 3 \cdot 3^{v_3(k)} \leq 3k.$$

から

$$1 + 2^k \leq 3k$$

が成り立つ.

すべての正整数 $a \geq 4$ に対して，$2^a > 3a - 1$ が成り立つ. $\cdots\cdots (**)$

$k \geq 5$ のときは，$(**)$ から $1 + 2^k > 3k$ となり $1 + 2^k \leq 3k$ に矛盾するから，$k = 3$ となる．このとき，$3^n = 1^3 + 2^3 = 9$ から $n = 2$ となる.

よって，$(x, y, n, k) = (1, 2, 2, 3), (2, 1, 2, 3)$.

以上のことから，求める n の値は $n = 2$. □

問題 10.4.12 Find all quadruples of positive integers (x, y, z, m) such that m is a odd number , $m \geq 3$ and $3^x 7^y + 1 = z^m$.

解答 $3^x 7^y + 1 = z^m$ $\cdots\cdots ①$

とおく．明らかに，$z\ (\geq 2)$ は偶数である.

Zsigmondy の定理より，$p \mid z^m - 1, p \nmid z - 1, p \nmid z^2 - 1 = (z+1)(z-1)$ を満たす素数 p が存在する.

$p \mid z^m - 1 = 3^x 7^y$ より，$p \in \{3, 7\}$.

(i) $p = 3$ の場合

$p \nmid z-1, p \nmid z^2-1 = (z+1)(z-1)$ より $3 \nmid z-1, 3 \nmid z+1$ だから，$3 \mid z$ となる.

$3^x 7^y + 1 \equiv 1 \pmod 3$, $z^m \equiv 0 \pmod 3$ となり，①に矛盾する.

(ii) $p = 7$ の場合

$m \geq 5$ とすると，Zsigmondy の定理より，$p \nmid z - 1, p \nmid z^2 - 1 = (z+1)(z-1)$, $p \nmid z^3 - 1 = (z-1)\left(z^2 + z + 1\right)$ すなわち $7 \nmid z - 1, 7 \nmid z + 1, 7 \nmid z^2 + z + 1$.

よって，$z \not\equiv 1, 2, 4, 6 \pmod 7$. また，$7 \mid z^m - 1$ より $z \not\equiv 0 \pmod 7$ が成り立つから，$z \equiv 3 \pmod 7$ または $z \equiv 5 \pmod 7$ である.

mod 7 で考えると

$$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6 \equiv -1, 3^4 \equiv 4, 3^5 \equiv 5.3^6 \equiv 1 \pmod 7,$$
$$5^1 \equiv 5, 5^2 \equiv 4, 5^3 \equiv 6 \equiv -1, 5^4 \equiv 2, 5^5 \equiv 3, 5^6 \equiv 1 \pmod 7$$

より，$\mathrm{ord}_7(3)=6, \mathrm{ord}_7(5)=6$ となる．$z^m-1\equiv 0 \pmod 7$ であったから，$6 \mid m$.
これは m が奇数であることに矛盾する．
したがって，$m<5$ すなわち $m=3$ でなければならない．このとき，①は

$$3^x 7^y = z^3-1 = (z-1)\left(z^2+z+1\right) \qquad \cdots\cdots ②$$

となる．
$z=2$ のとき，②は $3^x7^y=7$ となり，これを満たす正整数 x,y は存在しない．
よって，$z\geq 4$ とする．
$7 \nmid z-1$ だから，②より，$3 \mid z-1$ となるから，$z-1=3^{x_1}$ $(x_1\in\mathbb{N})$ とおくと，$z^2+z+1=3^{x-x_1}7^y$ となる．
$x_1=1$ のとき，$z=4$ で，$21=3^{x-1}7^y$ から，$x=2, y=1$ すなわち，$(x,y,z,m)=(2,1,4,3)$.
$x_1\geq 2$ のとき，$z\equiv 1 \pmod 9$ で，$z^2+z+1\equiv 3 \pmod 9$ すなわち $3 \parallel z^2+z+1$.
よって，$x-x_1=1$ となるから

$$z-1=3^{x-1},\ z^2+z+1=3\cdot 7^y \ (x\geq 3, z\geq 4, z \text{ は偶数})$$

とかけることになる．
z を消去すると，$3^{2x-3}+3^{x-1}+1=7^y$ から

$$3^{x-1}\left(3^{x-2}+1\right)=7^y-1. \qquad \cdots\cdots ③$$

$3 \mid 7-1, 3 \nmid 7, 3 \nmid 1$ だから，LTE より

$$v_3\left(7^y-1\right)=v_3(7-1)+v_3(y)=1+v_3(y).$$

また，$v_3\left(7^y-1\right)=v_3\left(3^{x-1}\left(3^{x-2}+1\right)\right)=x-1$ であるから，$v_3(y)=x-2$ すなわち

$$3^{x-2} \parallel y.$$

$x\geq 3$ より $3 \mid 3^{x-2} \mid y$ だから，$7^3-1 \mid 7^y-1=3^{x-1}\left(3^{x-2}+1\right).7^3-1=2\cdot 3^2\cdot 19$ だから

$$19 \mid 3^{x-2}+1.$$

mod 19 で考えると

$3^1\equiv 3, 3^2\equiv 9, 3^3\equiv 8, 3^4\equiv 5, 3^5\equiv 15, 3^6\equiv 7, 3^7\equiv 2, 3^8\equiv 6, 3^9\equiv 18\equiv -1 \pmod{19}$,
$3^{10}\equiv 16, 3^{11}\equiv 10, 3^{12}\equiv 11, 3^{13}\equiv 14, 3^{14}\equiv 4, 3^{15}\equiv 12, 3^{16}\equiv 17, 3^{17}\equiv 13,$
$3^{18}\equiv 1 \pmod{19}$

より，$x-2=9l$ (l は正の奇数) の形になる．

$$3^3+1 \mid 3^9+1 \mid 3^{x-2}+1,\ 3^3+1=2^2\cdot 7$$

から，$7 \mid 3^{x-2}+1$ となるが，$7 \nmid 7^y-1$ なので，③に矛盾する．

(i)，(ii) より求める解は，$(x,y,z,m)=(2,1,4,3)$. □

参考文献

[1] Amir Hossein Parvardi, Lifting The Exponent Lemma (LTE)
[2] Yimin Ge, Elementary Properties of Cyclotomic Polynomials
[3] Bart Michels, Zsigmondy's Theorem, 2014
[4] PISOLVE, The Zsigmondy Theorem, 7/31/11
[5] Math 780 : Elementary Number Theory (Instructor's Notes)
[6] Justin Stevens ,Olympiad Number Theory Through Challenging Problems
[7] Titu Andreescu , Dorin Andrica, Number Theory Structures , Examples , and Problems
[8] Titu Andreescu , Gabriel Dospinescu , Problems from the book
[9] Yimin Ge, The Method of Vieta-Jumping
[10] David A.SANTOS , Number Theory for Mathematical Contests

[101] C.L. リウ著　伊理正夫・伊理由美　共訳，組合せ数学入門 I，共立全書
[102] 柳田五夫，教材研究　二項係数を含む等式について（数学のいずみ）
[103] 柳田五夫，二項係数を含む等式について（ 2 ）（数学のいずみ）
[104] 柳田五夫，二項係数を含む等式の証明方法について（数学のいずみ）
[105] 柳田五夫，数学の問題（数学のいずみ）

2017 年 8 月 22 日 Ver 1.1