全体を見ると美しい（コレクション）

今回のレポートでは、個々のものを注視するのではなく、全体的に捉えると、何かが見えてくるという例を探し集めてみた。

【解と係数の関係】

n は然数、a_i $(i = 0, 1, 2, \ldots, n)$ は $(n+1)$ 個の複素数で、$a_0 \neq 0$ とする。また、n 次方程式

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

の n 個の解を $\alpha_1, \alpha_2, \ldots, \alpha_n$ とすると、次の式が成り立つ。

$$\sum_{i_1 < i_2 < \cdots < i_k} \alpha_1 \alpha_2 \ldots \alpha_k = (-1)^k \frac{a_k}{a_0} \quad (k = 1, 2, \ldots, n) \tag{1}$$

(証明)

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = a_0 (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$$

は恒等式である。この右辺を展開して各校の係数を比較すれば、(1) の成り立つことがわかる。（証明終わり）

＜説明＞

5 次以上の方程式は、根号と四則を有限個用いての解の公式が見つけられない。つまり、普通には一つ一つの解がいくらになるかは不明である。しかし、その解を全てたした値及び全てかけた値がいくらになるかはわかる。また、一般に『n 個の解からとった異なる k 個の解の積の総和の値がいくらになるかはわかる』と (1) は言っている。

【整数の問題】

$a_1, a_2, \ldots, a_n$ は n 個の整数であるとする。このとき、$a_1, a_2, \ldots, a_n$ の中から幾つかの数を選び、加えると n の倍数になるようにすることは常に可能であることを証明せよ。

但し、0 個選ぶというのは認めないものとする。

（証明）

$n+1$ 個の整数 0 , a_1 , $a_1 + a_2, \ldots, a_1 + a_2 + \cdots + a_n$ を考えると、これらの数を n で割ると、余りは $0, 1, 2, \ldots, n-1$ の n 種類しかないので、少なくとも 2 つは余りが同じになる。その同じ余りになった数を $a_1 + a_2 + \cdots + a_i$, $a_1 + a_2 + \ldots, a_j$ $(i < j)$ とすると

$$a_1 + a_2 + \cdots + a_i \equiv a_1 + a_2 + \ldots, a_j \pmod{n}$$

$$a_{i+1} + a_{i+2} + \cdots + a_j \equiv 0 \pmod{n}$$

よって示された。

（注）

この問題は、*Weil* が *Maxwell Rosenlicht* と共同で書いた *Number Theory for Beginners* という本にヒント付の練習問題として出ていたものです。

【フェルマーの小定理】

p が素数で、a が p で割り切れないとき、

$$a^{p-1} \equiv 1 \pmod{p}$$

（証明）

$1 \leqq k \leqq p-1$ とする。a も k も p と互いに素なので、ak も p では割り切れない。また、1 より大きく $p-1$ より小さな二つの自然数 k, k' について、ak , ak' を p で割った余りが等しいとすると、

$$a(k-k') = ak - ak' \equiv 0 \pmod{p}$$

であり、a と p は互いに素なので、$k - k' \equiv \pmod{p}$ つまり、$k = k'$ であることがわかる。よって、

$$\{ak \text{ を } p \text{ で割った余り} \mid 1 \leqq k \leqq p-1\} = \{1, 2, \ldots, p-1\}$$

がわかる。このことから、$a, 2a, \ldots, (p-1)a$ を全てかけ合わせると

$$\begin{aligned} a \cdot 2a \cdots (p-1)a &\equiv 1 \cdot 2 \cdots (p-1) \pmod{p} \\ \{1 \cdot 2 \cdots (p-1)\}a^{p-1} &\equiv \{1 \cdot 2 \cdots (p-1)\} \pmod{p} \\ \therefore \quad a^{p-1} &\equiv 1 \pmod{p} \quad (\because\ 1 \cdot 2 \cdots (p-1) \text{ は } p \text{ と互いに素}) \end{aligned}$$

＜説明＞

この証明を初めて見たとき、実に見事な証明だと感じた。「一つ一つの ak については、p で割った余りはよくわからないが、全体集めると、集まった全部は集合として同じなので、それが利用できてうまく処理された」。自分もいつかこんな綺麗な方法で何かを処理できればなあ、と思った。

【オイラーの関数 $\varphi(n)$ の性質】

自然数 $1, 2, \ldots, n$ の中に、n と互いに素な数がいくつあるか、その数を $\varphi(n)$ と表す（これをオイラーの関数と呼んでいる）。

このオイラーの関数について、次のことが成り立つ。任意の自然数 n について、

$$\sum_{d \mid n} \varphi(d) = n \tag{2}$$

が成り立つ（ここに、$\sum_{d \mid n}$ は、n の全ての約数 d について総和を取ることを意味する）。

（証明）

$r \mid n$ のとき、集合 N_r を次のように決める。

$$N_r = \{i \mid 1 \leqq i \leqq n \text{ , } n \text{ と } i \text{ の最大公約数は } r \text{ である }\}$$

このとき、n 以下の任意の自然数 i について、i と n の最大公約数は必ず存在し、1 以上 n 以下の自然数であり、

$$\{1, 2, \ldots, n\} = \bigcup_{r \mid n} N_r$$

が成り立つ。しかも、$r \neq r'$ なら $N_r \cap N_{r'} = \phi$ であることは明らか。よって、集合 A の要素の個数を $\sharp(A)$ で表すことにすると、

$$n = \sum_{r|n} \sharp(N_r)$$

が成り立つ。

N_r について考える。n と i の最大公約数が r であるということは、互いに素な自然数 n_1, i_1 を用いて

$$n = n_1 r\ ,\ i = i_1 r$$

と表せることと同じ。

$$\therefore \quad N_r = \{ i_1 \mid 1 \leqq i_1 \leqq n_1 \quad , \quad n_1 \text{と } i_1 \text{は互いに素} \}$$

$$\therefore \quad \sharp(N_r) = \varphi(\frac{n}{r}) \quad (\because\ n_1 = \frac{n}{r})$$

$$\therefore \quad n = \sum_{r|n} \varphi(\frac{n}{r})$$

ここで、r が n の全ての約数を動くとき、$\frac{n}{r}$ も n の全ての約数を動くので、

$$\sum_{d|n} \varphi(d)$$

よって証明された。

＜説明＞

n という数そのものに注視するのではなく、1 から n までの自然数全体を考えて処理されている。

（注１）　このオイラーの関数を用いれば、先ほどのフェルマーの小定理を含むより一般の定理：互いに素な 2 つの自然数 a, n について、

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

が成り立つ。

（注２）

(2) は初等整数論で必ずと言って良いほど紹介される定理で、これにまつわる話題をレポートの最後に付録としてつけておいた。

【漸化式と母関数】

数列 $\{a_n\}$ があるとき、この数列を元にして考えた多項式

$$a_1 + a_2 x + a_3 x^2 + \cdots + a_n x^{n-1} + \cdots$$

を数列 $\{a_n\}$ の母関数と言う（このベキ級数が収束するかどうかは気にしない）。

この母関数を用いて漸化式から一般項を求める方法がある。有名なフィボナッチ数列を例に紹介する。

（フィボナッチ数列）

次の漸化式で与えられる数列 $\{a_n\}$ の一般項を求めよ。$\begin{cases} a_1 = a_2 = 1 \\ a_{n+2} = a_{n+1} + a_n \end{cases}$

（母関数の方法）

数列 $\{a_n\}$ の母関数を $f(x)$ とおく。

$$xf(x) = a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} + \cdots \tag{3}$$
$$f(x) = a_1 + a_2 x + a_3 x^2 + \cdots + a_n x^{n-1} + \cdots \tag{4}$$

であるが、この辺々を相加えると

$$\begin{aligned} (x+1)f(x) &= a_1 + (a_2 + a_1)x + (a_3 + a_2)x^2 + \cdots + (a_n + a_{n-1})x^{n-1} + \cdots \\ &= a_2 + a_3 x + a_4 x^2 + \cdots + a_{n+1}x^{n-1} + \cdots \quad (\because \text{ 元の漸化式 }) \\ &= \frac{1}{x}\{f(x) - 1\} \\ \therefore \quad f(x) &= \frac{1}{1 - x - x^2} \end{aligned}$$

ここで、2 次方程式 $t^2 - t - 1 = 0$ の二つの解を α, β とすると、

$$t^2 - t - 1 = (t - \alpha)(t - \beta)$$

$t = \frac{1}{x}$ とおき、上の式に代入し両辺に x^2 をかけると

$$1 - x - x^2 = (1 - \alpha x)(1 - \beta x)$$

が得られる。

$$\begin{aligned} \therefore \quad f(x) &= \frac{1}{(1 - \alpha x)(1 - \beta x)} \\ &= \frac{1}{\alpha - \beta}\left(\frac{1}{1 - \alpha x} - \frac{1}{1 - \beta x}\right)\frac{1}{x} \\ &= \frac{1}{\alpha - \beta}\left(\sum_{n=1}^{\infty} \alpha^n x^{n-1} - \sum_{n=1}^{\infty} \beta^n x^{n-1}\right) \\ &= \frac{1}{\alpha - \beta}\sum_{n=1}^{\infty}(\alpha^n - \beta^n)x^{n-1} \end{aligned}$$

ここで、$f(x)$ の x^{n-1} の係数を比較して

$$\begin{aligned} a_n &= \frac{1}{\alpha - \beta}(\alpha^n - \beta^n) \\ &= \frac{1}{\sqrt{5}}\left\{\left(\frac{1 + \sqrt{5}}{2}\right)^n - \left(\frac{1 - \sqrt{5}}{2}\right)^n\right\} \end{aligned}$$

＜説明＞

数列の一つ一つの項を係数にし、全体で一つのべき級数を考えたところが面白い。

【チェビシェフの不等式】

数列 $\{a_n\}, \{b_n\}$ が共に単調増加数列（or 共に単調減少数列）ならば

$$\left(\frac{a_1 + a_2 + \cdots + a_n}{n}\right)\left(\frac{b_1 + b_2 + \cdots + b_n}{n}\right) \leqq \frac{a_1b_1 + a_2b_2 + \cdots + a_nb_n}{n}$$

（証明）

$1 \leqq i < j \leqq n$ のとき、$(a_i - a_j)(b_i - b_j) \geqq 0$ であるから、

$$\begin{aligned}
0 &\leqq \sum_{1 \leqq i < j \leqq n} (a_i - a_j)(b_i - b_j) \\
&= (n-1)\sum_{k=1}^{n} a_k b_k - \sum_{i \neq j} a_i b_j \\
&= (n-1)\sum_{k=1}^{n} a_k b_k - \sum_{k=1}^{n} a_k \sum_{i \neq k} b_i \qquad (5) \\
&= (n-1)\sum_{k=1}^{n} a_k b_k - \sum_{k=1}^{n} \{a_k(b_1 + b_2 + \cdots + b_k + \cdots + b_n) - a_k b_k\} \qquad (6) \\
&= n\sum_{k=1}^{n} a_k b_k - \sum_{k=1}^{n} a_k \sum_{k=1}^{n} b_k
\end{aligned}$$

となる。

$$\therefore \quad \left(\frac{a_1 + a_2 + \cdots + a_n}{n}\right)\left(\frac{b_1 + b_2 + \cdots + b_n}{n}\right) \leqq \frac{a_1b_1 + a_2b_2 + \cdots + a_nb_n}{n}$$

＜説明＞

全部をたし集めることで、非常に綺麗な不等式ができあがっている。また、この証明中の (5) から (6) に変形するところで、$\{b_n\}$ の項一つが抜けた和を、全てが揃った和にしているところでも、私は“ 全体にすると美しくなる ”ような感じがした。

【等差数列の和】

初項が a、公差が d の等差数列を初項から n 項まで加えると、その和 S は

$$S = \frac{n\{2a + (n-1)d\}}{2}$$

（証明）

この等差数列を逆に並べ、末項（第 n 項）の $a + (n-1)d$ を初項、公差を $-d$ とする等差数列を作り、元の数列と各項を加え合わせて数列を作ると、どの項も $2a + (n-1)d$ となる。

$$\therefore \quad 2S = n\{2a + (n-1)d\}$$

これから、求める式が得られる。

＜説明＞

これも、一つ一つの項を加えていくのではなく、全体に着目した処理で美しいと思う。

【最大値・最小値】

$x^2+y^2=1$ のとき、$4x-3y$ の最大値を求めよ。

（解答）

$$(x^2+y^2)\{4^2+(-3)^2\} \geqq (4x-3y)^2 \quad (\because \text{コーシー・シュワルツの不等式})$$
$$25 \geqq (4x-3y)^2$$
$$\therefore \quad -5 \leqq 4x-3y \leqq 5 \tag{7}$$

ここで、$x=\frac{4}{5}, y=-\frac{3}{5}$ ととると、x,y は、$x^2+y^2=1$ を満たし、かつ (7) の等号を成り立たせている。よって、求める最大値は 5 である。

＜説明＞

最大値を求めるだけなら、最大値の定義に沿った求め方が有効なときがある。それが上に示した不等式を用いる方法である。

最大値の定義

実数から成る集合 A において、a が最大値であるとは

1. A の任意の数 x に対して、$x \leqq a$ が成り立つ。
2. $a \in A$

が成り立つことである。

不等式を利用すると、上の定義の 1 のところを集合全体として捉える感じがあり、一つ一つの値にこだわっていないのがスッキリしている気がする。

先ほどの問題の解答はこの定義を意識したものになっていることを確認しておく。

$4x-3y$ のとり得る値の範囲（値域）を A とする。このとき、A の任意の $4x-3y$ について、$4x-3y \leqq 5$ が成り立っている（(7)）。また、$x^2+y^2=1$ を満たす $x=\frac{4}{5}, y=-\frac{3}{5}$ について $4x-3y=5$ なので、$5 \in A$ である。

【付録（オイラーの関数にまつわる話題）】

メービウスの関数と呼ばれる

$$\mu(n)=\begin{cases} 1 & (n=1 \text{ のとき}) \\ 0 & (n \text{ が素数の平方で割り切れるとき}) \\ (-1)^k & (n \text{ が } k \text{ 個の異なる素数の積に等しいとき}) \end{cases}$$

を用いると、証明はしないが、反転公式と呼ばれる次のことが成り立つ。

（反転公式）

$$\sum_{d|n} f(d)=g(n)$$

が全ての自然数 n について成り立つとき

$$f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right) g(d)=\sum_{d|n}\mu(d)\, g\left(\frac{n}{d}\right)$$

が全ての自然数 n について成り立つ。

この反転公式から、オイラーの関数 $\varphi(n)$ は

$$\varphi(n) = \sum_{d|n} \mu(d)\, \frac{n}{d}$$

と表されることがわかる。また今得た $\varphi(n)$ の式を用いると、$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ と素因数分解されていれば、

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$

となることがわかる。