不定方程式の特殊解の小手技

市立札幌旭丘高校　中村文則

○テクマクマヤコン小さくなーれ

<先　生>　今日は，次の問題に挑戦してみよう。

Ex1) まなぶは，50 円缶と 500 円缶の貯金缶に貯金をしている。
貯金缶は 50 円硬貨と 500 円硬貨専用のもので，空缶の重さは
50 円缶は 50g，500 円缶は 100g である。
かず子はまなぶに頼まれて，貯金後の貯金缶の重さを調べたところ，
どちらも同じ重さになっていて，1 つの缶の重さは 500g 以上あった。
硬貨の重さは右表のように定められている。これを利用して，まなぶ
が貯金した金額の最小値を求めよ。

硬 貨	重 さ	直 径
50 円	4 (g)	21.0(㎜)
500 円	7 (g)	26.5(㎜)

<まなぶ> 先生，いつものあっさりした問題の設定とずいぶん違うよ。だいたいなんで僕が登場するの。それにかず子に僕の大事な財産を預けてしまっている。そんなことあり得ないでしょ。よしおかアリスにしてもらえないだろうか。

<かず子> 私だって，頼まれてもこんな手伝いしたくないわ。まなぶが貯金をするとは思えないし，貯金したとしても空缶の重さとそれほど変わりはないと思うから，調べる必要はないでしょ。

<先　生> そこまで 2 人の抵抗があるとは思わなかった。そうしたら，まなぶを生徒 M に変えようか。

<まなぶ> 先生，わざといってない。いいですよ，そのままで。

<アリス> 先生，硬貨の表の重さは正しい数値なのですか。

<先　生> 法律で定められた数値です。1 円の重さは 1g であることはよく知られているね。ちなみに直径は 20mm だ。

<よしお> 硬貨 1 枚の重さが分かるから，貯金缶を缶切りで開けないで中身の貯金額を調べられるということですね。貯金した 50 円と 500 円硬貨の枚数をそれぞれ x ， y として，2 つの貯金缶の重さの関係から不定方程式を求め，その解を考えればいいと思います。

<まなぶ> なるほどね。そうすると，2 つの缶の重さは同じなのだから，空の貯金缶の重さも考慮すると，

$$4x+50=7y+100 \qquad \text{すなわち，} \quad 4x-7y=50 \quad \cdots(*)$$

この不定方程式の一般解を求めればいいのか。

<かず子> まず，特殊解を求めなくては。x, y は硬貨の枚数だから， $x \geqq 0$ ， $y \geqq 0$ で考えればいいわ。

<まなぶ> $x=0$ ， $y=0$ はまったく貯金していないということだろ。$x \geqq 10$ ， $y \geqq 5$ ぐらいにしようよ。

<かず子> なんとまあ小さな目標だこと。あくまで特殊解を求めるための目安でいっているだけよ。

<よしお> ところで，右辺の 50 なんだけど，このような場合は，4 と 7 が互いに素であることより，

$$4x-7y=1$$

この特殊解を求めればいいと思う。

<先　生> そうだね。よしおの言っていることは，ユークリッドの互除法の原理でもある大事な性質だった。

<アリス> うーん，そのことよくわからないけど，右辺が 1 の場合の解の 1 つは，

$$x=2 \text{ ， } y=1$$

すぐ求められるわ。

<先　生> 確認してみよう。

$$4\times 2-7\times 1=1$$

では，これから，右辺が 50 の解を求めるにはどうすればいいだろうか。

<アリス> そうか，分かりました。両辺を 50 倍するのですね。

$$4\times 100-7\times 50=50 \quad \cdots①$$

だから， $x=100$ ， $y=50$ が(*)の特殊解です。

<まなぶ> あとはいつもの方法だ。(*)と①を辺々引く。

$$4(x-100)-7(y-50)=0$$

これから，

$$4(x-100)=7(y-50)$$

ここで，4 と 7 は互いに素であることから，

$$x=7k+100 \text{ ， } y=4k+50 \quad (k \text{ は整数})$$

一般解が求められた。次は，後半の 1 つの貯金缶の重さが 500g 以上ってやつだ。

<かず子> 50 円缶の方で調べてみるわ。1 枚の重さが 4g で x 枚あり，そして空の貯金缶の重さが 50g だから，重さ M は，

$$M=4x+50=4(7k+100)+50=28k+450$$

$M \geqq 500$ より，$28k + 450 \geqq 500$　　$\therefore$　$k \geqq 1\dfrac{11}{14}$

k は整数より，$k \geqq 2$

だから，$k = 2$ のときを求めればいい。

このとき，$x = 114$ ，$y = 58$ だから，貯金額の合計は，

$$114 \times 50 + 58 \times 500 = 34,700 \text{ (円)}$$

ちょっとまなぶには無理そうな金額ね。

<アリス> そうなんですか。ところで，右辺の大きな数を小さな数に変えてから，元の数に戻すって方法，面白いですね。「テクマクマヤコン小さくなーれ」，そんな感じがします。

<まなぶ> なに，その妙な呪文。

<アリス> 知らないんですか。不思議のアッコちゃんが変身するときに唱える呪文。アニメは日本の文化です。

<かず子> 小さい頃よく唱えたわ。この呪文は素敵な女の子に変身する魔法なんだけど，大きさや形を変えるということだから整数を小さくする場合も使えそうだわ。元に戻るときは，ラミパス ラミパス ルルルルル～。

実は私としては他にも小さくしたい人間と，小さくしたい整数があるんだけど。

整数の方をいうと，さきほどの方法で求めた特殊解 $x = 100$ ，$y = 50$ は，ずいぶん大きい整数ですねよ。だから一般解もこの整数で表されてしまう。この問題のように合計金額を求めるときには計算が大変になると思うの。それと，まなぶの貯金額の初期値としては不適切だわ。

<まなぶ> 小さくしたい人間が誰かは知らないけど，僕の貯金の初期値は何が不適切なんだろう。それに，この初期値は下位の桁はゼロになっているから計算はラクでしょ。

<よしお> この場合はまなぶのいうように計算は簡単だけどいつもそういうわけではないよ。だから，特殊解は小さな整数で表せた方がいろいろ便利だと思う。そこで思ったのだけど，(*)の不定方程式は次のように表せる。

$$2(x - 25) = 7y$$

ここで，2 と 7 は互いに素なのだから，y は 2 の倍数になり，特殊解の候補はだいぶ絞られることになる。

<アリス> 具体的に 2 の倍数を入れてみるということですね。$y = 2$ とすると，

$$2(2x - 25) = 7 \times 2 \qquad \therefore \quad 2x - 25 = 7 \text{ より，} x = 16$$

あれ，簡単に見つかっちゃった。

<かず子> $x = 16$ ，$y = 2$ だから，合計金額は 1800 円。うん，妥当な金額だわ。

<まなぶ> 言っている意味分からないよ。 なに，そうすると先ほどの解法は無意味ということ。

<先　生> よしおが考えたように式変形をすることもひとつの方法だけどいつも上手く特殊解を見つけられるわけではない。それに，最初の方法でも特殊解を「テクマクマヤコン小さくなーれ」で小さくできる。

<まなぶ> 先生って，ひょっとしてアニオタ。でも，どうやって小さくするの。

<先　生> 不定方程式の一般解は，特殊解を用いて求めた。ということは，一般解の一つの解が特殊解ということだ。

<かず子> 何か言葉遊びみたい，あっ，でも分かった。一般解から特殊解を求めればいいんだ。一般解は，

$x = 7k + 100$ ，$y = 4k + 50$

だから k に適当な整数を代入すると特殊解になる。

<まなぶ> そういうことか。例えば，$k = -10$ にすると，

$x = 30$ ，$y = 10$

だから，一般解は，

$x = 7k + 30$ ，$y = 4k + 10$

こうしてもいいってことだ。確かにこの一般解の方が合計金額を求めるにしてもずっと簡単だ。

<アリス> よしおが先ほど求めた特殊解は，$k = -12$ の場合ということですね。

<先　生> それでは，「テクマクマヤコン小さくなーれ」の呪文で次は硬貨の直径に関する問題を考えてみよう。

Ex2) よしおとアリスは 50 円玉硬貨と 500 円硬貨を，硬貨の円の中心が図のように一直線上になるように並べるとき，硬貨の左端から右端までの長さが 1m になることがあるか調べることにした。
先ほどの表を用いて調べよ。また，1m になることがある場合は，50 円硬貨，500 円硬貨のそれぞれの枚数を求めよ。

<まなぶ> 意義あり。僕とかず子の問題は貯金額を調べる，言ってみれば現実的というか俗っぽい問題だったのに，よしおとアリスの問題は，数学的な楽しい問題になっている。それはおかしいでしょ。

<かず子> その意見には私も賛成よ。なんで私とまなぶがペアだったんですか。

<まなぶ> かず子，問題の中身よりそこなの。

<アリス> とりあえず，私とよしおが指名されているので，私がまず考えてみます。これも不定方程式の問題ですね。さっきより立式は簡単だわ。

50 円硬貨と 500 円硬貨の枚数をそれぞれ x ， y とすると，

$$21x + 26.5y = 1000$$

この特殊解を求めるのですね。でも y の係数が小数になっている。

<よしお> それは両辺を 2 倍することで解決できる。

$$42x + 53y = 2000$$

これも 42 と 53 は互いに素だから，右辺が 1 の場合の特殊解を求めて 2000 倍して調整すればいいけど，ものすごく大きな数になってしまう。

<先　生> 大きな数でも特殊解を求めてから「テクマクマヤコン小さくなーれ」ができることは前の問題で説明した。でも最初から小さくしておけばその手間が省けることにもなる。それにはどうすればいいだろうか。

<まなぶ> 先生，やっぱりアニオタなんだ。2000 を小さくするということか，どうやればいいのだろう。

<アリス> わたし，分かったと思う。2000 を 42 または 53 で割るとその余りを右辺にできるのではないでしょうか。

<先　生> その通りです。呪文，使いこなしているね。アリス，やってみてごらん。

<アリス>　42 で割ってみます。テクマクマヤコン小さくなーれ。

$$2000 = 42 \times 47 + 26$$

これから，

$$42x + 53y = 42 \times 47 + 26 \quad \therefore \quad 42(x - 47) + 53y = 26$$

ここで， $z = x - 47$ とおくと，

$$42z + 53y = 26 \quad \cdots(**)$$

小さくなりました。

<かず子> ここまできたらあとはできる。

$$42z + 53y = 1$$

この不定方程式の特殊解を求めます。

ただ，前の問題と違い，特殊解はすぐに求められそうにないからユークリッドの互除法の出番ね。

まず互除法の割り算をしてから，高速シミュレートをすると，

特殊解は， $z = 24$ ， $y = -19$ になります。

これを 26 倍すればいいですけど，まだ結構大きい数になるわ。

呪文，失敗かしら。

	42	53	
3	33	42	1
	9	11	
4	8	9	1
	1	2	

⇨

	0	1
1	1	0
3	−1	1
1	4	−3
4	−5	4
	24	−19

<よしお> 互除法を途中で止めればいいよ。

不定方程式の右辺が 1 の場合を求めるのならこれでいいけど，

(**)の右辺は 26 だから， $26 = 2 \times 13$ 。そうみると，

$$42z + 53y = 2$$

これからも求めることができる。その場合の特殊解は，高速シミュレートの結果の 1 行上をみると，

$$z = -5 \text{ ， } y = 4$$

だから，次の等式が成り立つ。

$$42 \times (-5) + 53 \times 4 = 2$$

両辺を 13 倍すると，

$$42 \times (-65) + 53 \times 52 = 26$$

<アリス> 本当だ。特殊解は， $z = -65$ ， $y = 52$ 。だいぶ小さくなりましたね。

あとは，(**)から辺々引くと，

$$42(z + 65) + 53(y - 52) = 0 \qquad 42(z + 65) = -53(y - 52)$$

ここで，42 と 53 は互いに素だから，

$$z + 65 = 53k \text{ ， } y - 52 = -42k$$

すなわち，

$$x = (z + 47) = (53k - 65) + 57 = 53k - 18 \text{ ， } y = -42k + 52 \qquad (k \text{ は整数})$$

かならずしも最小の 1 にする必要はなく最適な大きさになるように，「テクマクマヤコン小さくなーれ」なんですね。

<先　生> これで一般解は求められたけど，もう少し上手に 2000 を 42 と 53 に振り分けることもできる。

$$2000 = 42 \times 11 + 53 \times 29 + 1$$

こうすると，

$$42(x - 11) + 53(y - 29) = 1$$

$u = x - 11$ ， $v = y - 29$ とおくと，

$$42u + 53v = 1$$

これから，先ほどのかず子が求めた高速シミュレートの結果から，

$$u = -53k + 24 \text{ ， } v = 42k - 19$$

となる。これを x, y に戻すと，

$$x = u + 11 = -53k + 35$$

$$y = v + 29 = 42k + 10$$

<まなぶ> その変形，マニアックすぎる。ふつう，考えつかないでしょ。
<先　生> そうだね。だから，よしおが考えたように互除法を柔軟に捉える方がいい解き方ということになる。
ところで，いまは右辺の定数を小さくしたけれど，もっと別なものを小さくすることもできる。何か分かるかな。
<かず子> 大きな整数を小さな整数に変えるということですよね。
<アリス> あっ，分かった。左辺の x ， y の係数のことですか。
<先　生> アリス，絶好調だね。やってごらん。
<アリス> x と y の係数は，それぞれ，42 と 53 だから，大きい方の 53 を 42 で割ると，

$$53 = 42 \times 1 + 11$$

これから，「テクマクマヤコン小さくなーれ」で，

$$42x + (42 \times 1 + 11)y = 2000$$

$$42(x + y) + 11y = 2000$$

y の係数が小さくなりました。さらに先ほどのように 2000 を 42 で割っても小さくします。
<かず子> ちょっとまって。この場合は 2000 を 11 で割った方が小さくできるよ。

$$2000 = 11 \times 181 + 9$$

<よしお> これ，次のようにするとさらに小さくできるよ。

$$2000 = 11 \times 182 - 2$$

<かず子> そうか，何も正の整数でなくてもいいんだ。絶対値が小さいものとみるのね。
そうすると，

$$42(x + y) + 11(y - 182) = -2$$

ここで，　$w = x + y$ ， $z = y - 182$　とすると，

$$42w + 11z = -2$$

これを解けばいいのね。
<まなぶ> あれ？，その特殊解は，

$$w = 1 \qquad z = -4$$

だよね。
<アリス> 本当だ。互除法が必要なくなった。これから不定方程式は次のように変形できる。

$$42(w - 1) = -11(z + 4)$$

42 と 11 は互いに素だから，

$$w = 11k + 1 , \quad z = -42k - 4$$

以上より，

$$y = z + 182 = (-42k - 4) + 182 = -42k + 178$$

$$x = w - y = (11k + 1) - (-42k + 178) = 53k - 177$$

特殊解はちょっと大きいけど無事，求められました。
<まなぶ> 特殊解は $k = 4$ を代入して求めると，新たに一般解は，

$$x = 53k + 35 \quad , \quad y = -42k + 10$$

このようにできるから問題なし。この方法いいね。互除法は 42 と 13 で考えればいいから簡単になるし特殊解も小さくできる。問題なのはなぜこの方法を小出しにしないで早く教えてくれなかったんだろう。そうしたら無用なバディと無駄な苦労をすることがなかった。
<かず子> なにいってんのよ。まなぶがいま特殊解を小さくした方法だって最初の問題のときに習ったものでしょ。
<先　生> 「テクマクマヤコン小さくなーれ」は，いろんな方法があることを理解して欲しい。不定方程式の中のどの整数を小さくするのがいいか，最適な方法を考えるようにしよう。それでは最後に 1m を測ることできるか調べてごらん。
<アリス> 私が求めます。まなぶの求めた一般解を用います。
$x \geqq 0$ ， $y \geqq 0$ だから，

$x = 53k + 35 \geqq 0$ より， $k \geqq -\dfrac{35}{53}$,

$y = -42k + 10 \geqq 0$ より， $k \leqq \dfrac{5}{21}$

$$\therefore \quad -\frac{35}{53} \leqq k \leqq \frac{5}{21}$$

k は整数だから， $k = 0$ 。以上より，

$$x = 35 , \quad y = 10$$

まなぶの求めた特殊解が 1m を測ることのできるただ 1 組の硬貨の組合せだったんですね。
<まなぶ> 最後にやっと僕とアリスのバディが実を結んだということだよ。
<かず子> 最後の呪文よ。テクマクマヤコン小さくなって，消えてしまえ。

あとがき

今回はn元1次不定方程式(ディオフォントス方程式)の代表的なものである2元1次不定方程式 $ax+by=c$ (ベズー方程式)に関する小手技を取り上げました。

なお，本文の問題は，本校の定期試験問題をアレンジしたものです。大学入学共通テストでは，太郎と花子がナビゲーターになり，思考，判断，表現を引き出す道案内をすることが予想されます(これをタロハナ問題と勝手に命名)。本校の大学入試演習系の講座では，タロハナの会話調問題を多く取り上げ，定期試験ではいくつかの分野でオリジナル問題を作成しました。小手技は，4 名の生徒と先生の乱打戦で，各自が言いたい放題ですが，それに比べればタロハナ問題はかわいいものです。

さて，本問では，不定方程式の中にある整数を複数の方法で小さくすることを説明しています。
本文で示した具体的な方法は次のようになります。

不定方程式 $ax+by=c$ の係数(特殊解)のミニマム化
① $(a,b)=1$ のときc を1に小さくする
② 大きな整数の特殊解を小さくする
③ c をa またはb で割り小さくする
④ 互除法の途中の値から特殊解を小さくする
⑤ $a>b$ のとき，$a=bq+r$ として係数a を小さくする

⑤のミニマム化は，一番有効な方法といえます。次の不定方程式でもう一度考えてみましょう。

Ex) $42x+53y=1$ の整数解を求めよ。

解) $53=42\times1+11$ より $42(x+y)+11y=1$

$42=11\times4-2$ より $-2(x+y)+11(4x+5y)=1$

この等式を満たす$x+y$，$4x+5y$ の値の1組は，

$$x+y=5,\quad 4x+5y=1$$

よって，

$$-2(x+y-5)+11(4x+5y-1)=0$$

2と11は互いに素であることより，

$$x+y-5=11k$$
$$4x+5y-1=2k \qquad (k\in Z)$$

x，y の連立方程式を解いて，

$$x=53k+24,\quad y=-42k-19 \qquad (k\in Z)$$

計算のプロセスをみると，この方法はユークリッドの互除法をトレースしていることが分かります。

ユークリッドの互除法で機械的に計算するか，不定方程式の解が見つかるまでx とy の係数で交互に割り算を繰り返すか，その選択の違いということになります。そのユークリッドの互除法を途中で切り上げる方法が④になります。

また，⑤と③のミニマム化は合同式がその背景にあります。。

合同式では，次の計算法則を用いることで方程式の一般解を求めることができます。

計算法則Ⅰ
$a\equiv b\pmod n$ $c\equiv d\pmod n$ のとき，
(1) $a+c\equiv b+d\pmod n$
(2) $a-c\equiv b-d\pmod n$
(3) $ac\equiv bd\pmod n$
(4) $a^m\equiv b^m\pmod n, m\in N$

計算法則Ⅱ
(1) $(k,n)=1$ のとき，
$ak\equiv bk \Leftrightarrow a\equiv b\pmod n$
(2) $ac\equiv bc\pmod{nc} \Leftrightarrow a\equiv b\pmod n$

計算法則Ⅰは，四則演算で除法以外は成立していることを示しています。

これから，

$$ka\equiv kb\pmod n,\quad k\in Z$$

さらに，通常の数の計算とは異なる次の式も成立します。

$$a+kn\equiv b+ln\pmod n,\quad k,l\in Z$$

計算法則Ⅱはとても有用性の高い法則であり，条件付きで除法が成立することを示しています。

合同式を用いて，本文の不定方程式の解を求めてみましょう。

Ex) $42x+53y=2000$ の一般解を求めよ。

解) $42x+53y\equiv 2000 \pmod{42}$

$53=42+11$，$2000=42\times 47+26$ より，　$11y\equiv 26 \pmod{42}$

$26+42\times 2=110$ より，　$11y\equiv 110 \pmod{42}$

$(11,42)=1$ より，　$y\equiv 10 \pmod{42}$

∴　$y=10$ は特殊解より，与式に代入すると，$x=35$

以上より，$x=53k+35$，$y=42k+10$　$(k\in Z)$

なお, 法は x,y の係数の絶対値が小さい方にして計算するのが一般的ですが, 52 を法とする場合は次のようになります。

$42x+53y\equiv 2000 \pmod{53}$

$42x\equiv -14 \pmod{53}$　　$(14,53)=1$ より，$3x\equiv -1\equiv -54 \pmod{53}$

$(3,53)=1$ より，$x\equiv -18\equiv 35 \pmod{53}$

合同式は，これ以外にも計算法則のいろいろな組み合わせにより，解を得ることができます。

①のミニマム化はユークリッドの互除法の原理により保証される性質ですが，完全剰余系の性質から導いてみましょう。

n を法とする n 個の剰余類からそれぞれ 1 つずつ代表元をとって作られる n 個の整数の組を，n を法とする完全剰余系といい，次の性質が成立します。

> 正の整数 n を法として，
> $$x_1,x_2,x_3,\cdots\cdots,x_{n-1},x_n$$
> が完全剰余系であるとき，n と互いに素である整数 a に対して，
> $$ax_1,ax_2,ax_3,\cdots\cdots,ax_{n-1},ax_n$$
> もまた，n を法とする完全剰余系である。

例えば，7 を法とする完全剰余系の 1 つは，

$$1,2,3,4,5,6,7$$

ですが，7 と互いに素である 11 を，その代表元にかけて作られる数の組は，右表のように 7 を法とする完全剰余系になります。

面白い性質ですがその証明は簡単です。

x_i	1	2	3	4	5	6	7
$11x_i$	11	22	33	44	55	66	77
$\bmod 7$	4	1	5	2	6	3	0

証明）$ax_i\equiv ax_j \pmod{n}$　$i\neq j$　$(1\leqq i,j\leqq n)$ とする。

$(a,n)=1$ より，$x_i\equiv x_j \pmod{n}$ 。

これは，x_k $(k=1,2,\cdots,n)$ が n を法とする完全剰余系であることに矛盾する。　(終)

このことを用いて次の整数の重要定理を証明しましょう。

> a と b は互いに素である整数　⇔　$ax+by=1$　は整数解をもつ

証明）

（←）$(a,b)\neq 1$ とすると，$(a,b)=d$ $(d\geqq 2)$ と表すことができる。

このとき，$ax+by$ は d の倍数となり矛盾する。

（→）$1,2,3,\cdots\cdots,b$ は，b を法とする完全剰余系である。

$(a,b)=1$ より，

$$1,2a,3a,\cdots\cdots,ba$$

は b を法とする完全剰余系になる。したがって，

$$ka\equiv 1 \pmod{b}$$

となる k $(1\leqq k\leqq b)$ が存在する。これから，

$ka=\ell b+1$ ($\ell\in Z$) より，$ka+(-\ell)b=1$

以上より，$(x,y)=(k,-\ell)$ は不定方程式の解である。　(終)

完全剰余系の性質を用いると，次の定理の証明することができます。

フェルマーの小定理
p が素数で，a が p と互いに素な整数であるとき，
$$a^{p-1} \equiv 1 \pmod{p}$$

証明）　$1, 2, 3, \cdots\cdots, p-1, p$　　…①
は p を法とする完全剰余系である。
また，$(a, p) = 1$ より，
$a, 2a, 3a, \cdots\cdots, (p-1)a, pa$　…②
も p を法とする完全剰余系である。
ここで，$p \equiv pa \equiv 0 \pmod{p}$ であるから，①の a と②の pa を除いたそれぞれの $(p-1)$ 個の積は，p を法として合同である。これから，
$$(p-1)! \equiv (p-1)!\, a^{p-1} \pmod{p}$$
$(p-1)!$ と p は互いに素であるから，
$$a^{p-1} \equiv 1 \pmod{p}$$　　（終）

13^{100} を 34 で割った余りを求めてみましょう。
$(13, 34) = 1$ であることから，$13^{33} \equiv 1 \pmod{34}$
これから，$13^{100} = \left(13^{33}\right)^3 \cdot 13 \equiv 13 \pmod{34}$
以上より，余りは 13 になります。

フェルマーの小定理を拡張したものにオイラーの定理があります。

オイラーの定理
n が整数$(n \geqq 2)$ で，a が n と互いに素な整数であるとき，
$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

ここで，$\varphi(n)$ は n と互いに素である n を超えない正整数の個数を表す関数で，オイラーの(トーシェント)関数といい，次のように与えられます。

オイラー関数の公式
正整数 n の異なる素因数を p_i $(i = 1, 2, \cdots, k)$ とするとき，
$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

証明は厳密には中国剰余定理等を用いますが，直感的は容易に理解できるものです(大学の入試問題や数研出版のチャートにも掲載されています)。
$n = 30$ のときを考えてみましょう。
1,2,…,30 から 30 と互いに素である整数を抜き出していくと，
1, 7, 11, 13, 17, 19, 23, 29
$\therefore \quad \varphi(30) = 8$

これを次のように考えます。
30 を素因数分解すると，$30 = 2 \cdot 3 \cdot 5$
これから，30 個の整数のうち，公約数が 2,3,5 である整数の割合は，それぞれ $\frac{1}{2}, \frac{1}{3}, \frac{1}{5}$ であることより，
30 と互いに素である整数の割合は，$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$ になります。したがって，
$$\varphi(30) = 30 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8$$

なお，オイラーがこの性質を発表したのは1767年ですが，それ以前に日本の和算学者で棋士でもあった久留島義太(1758年没)は，既にこの公式を得ており，彼の遺稿集に記されています。

オイラー関数と完全剰余系の性質を用いると，オイラーの定理を証明することができます。

証明) $\varphi(n)=k$ とする。正整数 n と互いに素である n を超えない整数の組

$$b_1,\ b_2,\ b_3,\cdots\cdots,b_k$$

は，n を法とする(既約)剰余系であり，その集合を A とする。このとき，

$$ab_1,\ ab_2,ab_3\cdots\cdots,ab_k$$

を考えると，n と a ，n と b_i $(1\leqq i\leqq k)$ は互いに素であることより，n と ab_i も互いに素である。

また，$1\leqq j,\ j\leqq k$ のとき，$ab_i\equiv ab_j \pmod n$ とすると，$(a,n)=1$ より，$b_i\equiv b_j \pmod n$ となり矛盾する。

$\therefore$ ab_i はすべて異なる数である。ここで，$ab_i=nq_i+r_i$ $(0\leqq i<n)$ とすると，ユークリッドの互除法の性質より，

$(n,r_i)=(ab_i,n)=1$ 。よって，同様の議論により，r_i はすべて異なる数である。

これらのことから，ab_i の n を法とする剰余 r_i の集合 B は，集合 A と一致する。

以上より，集合 A と集合 B の要素の積は n を法として合同である。

$$\prod_{i=1}^{k}b_i\equiv\prod_{i=1}^{k}ab_i \pmod n$$

ここで，n と $\prod_{i=1}^{k}b_i$ は互いに素であるから，

$$a^k\equiv 1 \pmod n$$

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

オイラーの定理で n が素数 p であるとき，$\varphi(p)=p-1$ となりフェルマーの定理に一致します。

このオイラーの定理を用いることで，不定方程式の解は次のように得られます。

> $(a,b)=1$ のとき，不定方程式 $ax+by=1$ の解 x は，
>
> $x\equiv a^{\varphi(b)-1} \pmod b$

$ax\equiv 1 \pmod b$ および $a^{\varphi(b)}\equiv 1 \pmod b$ より，$ax\equiv a^{\varphi(b)} \pmod b$

$(a,b)\equiv 1$ より，$x\equiv a^{\varphi(b)-1} \pmod b$

同様に考えると，$y\equiv b^{\varphi(a)-1} \pmod a$ となります。

最後に本文の不定方程式をオイラーの定理を用いて解いてみましょう。

Ex) 不定方程式 $42x+53y=1$ の解を求めよ。

解) $53y\equiv 1 \pmod{42}$ ここで，$53=42+11$ より，

$$11y\equiv 1 \pmod{42}$$

$42=2\cdot 3\cdot 7$ より，$\varphi(42)=42\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)=12$

$\therefore$ $y\equiv 11^{\varphi(42)-1}=11^{11} \pmod{42}$

このように，あまり実用的でない特殊解 $y=11^{11}$ が得られます。これを小さくしてみましょう。

$11^2=42\times 3-5$ より，$11^2\equiv -5 \pmod{42}$

$11^8\equiv 625\equiv -5 \pmod{42}$ $\therefore$ $11^{10}\equiv 25 \pmod{42}$

$11^{11}\equiv 275\equiv 23 \pmod{42}$

非常に効率は悪いことが分かります。例えれば，1 本の小枝は手折るだけで済むのにチェーンソーを使って伐採するようなものでベズー方程式程度の解法には不必要といえます。しかし，合同式のような整数の性質はとても面白く，思考，判断，表現の場面が多い内容でありこれからの数学教育には必要な分野なのです。しかし，学習指導要領では合同式は発展的な扱いであり，新学習指導要領では整数の性質そのものがさらに隅っこに追いやられてしまいました。