# 第 1 講

## 数と式(1)

この講と次の講では，整数問題について学ぶ。入試における整数問題では，整数固有の性質に帰着させて問題を解いていく。ここでは，その整数固有の性質を順に学んでいく。以下での文字は特に断らない限り整数とする。

## 1.1 除法の原理

整数の集合においては，除法（割り算）を行うと，割り切れて整数になる場合と，割り切れず整数にならない場合がある。割り切れない場合は余りが出る。例えば7を3で割るとき，2余り1となる。7の中に3個ずつのものを2セット作って，作りきれなかった部分が余りである。すなわち，

$$\text{余り}=7-2\cdot3=1$$

となり，これを定式化したものが次の除法の原理である。

**除法の原理**

$a$ を整数，$b$ を正の整数とするとき，

$$a=bq+r,\ 0\leqq r<b$$

を満たす整数 $q$，$r$ がただ1組存在する。$q$，$r$ を $a$ を $b$ で割ったときの**商**，**余り**（**剰余**）という。

除法の原理から得られる用語を確認する。

(1) 「$a$ は $b$ の**倍数**」$\Longleftrightarrow$「$a=bq$ なる $q$ がある」
このとき「$b$ は $a$ の**約数**」という。除法の原理により，これは $a$ を $b$ で割った余り $r$ が0であることに他ならない。よって，「$a$ は $b$ で割り切れる」「$b$ は $a$ を割り切る」とも言える。なお $0=0\cdot x$ より，0は任意の整数 $x$ の倍数で，$x=1\cdot x$ より，1は任意の整数の約数である。

(2) 2つ以上の整数 $a$，$b$，$c$，…に共通な倍数をそれらの整数の公倍数という。式で表現するなら，
「$\ell$ が $a$ と $b$ の公倍数」
$\Longleftrightarrow$「$\ell=am$，$\ell=bn$ となる $m$，$n$ がある」
と表せるが，「$\ell$ は $a$ の倍数かつ $b$ の倍数」というだけである。正の公倍数のうち最小のものを**最小公倍数**という。

(3) 2つ以上の整数 $a$，$b$，$c$，…に共通な約数をそれらの整数の公約数という。式で表現するなら，
「$g$ が $a$ と $b$ の公約数」
$\Longleftrightarrow$「$a=gm$，$b=gn$ となる $m$，$n$ がある」
と表せるが，「$g$ は $a$ の約数かつ $b$ の約数」というだけである。公約数のうち最大のものを**最大公約数**という。また，$a$ と $b$ の最大公約数が1であるとき $a$ と $b$ は**互いに素**という。

(4) 「$p$ が**素数**」
$\Longleftrightarrow$「2以上の整数 $p$ の正の約数は1と $p$ のみ」
素数がらみの問題では，
(i) 素数で偶数は2だけ（3以上の素数は奇数）
(ii) 「$mn$ が素数 $p$ で割り切れる」
$\Longrightarrow$「$m$，$n$ の少なくとも一方は $p$ で割り切れる」
特に $a$，$b$ を自然数，$p$ を素数とするとき
「$ab=p\Longrightarrow(a,\ b)=(1,\ p),\ (p,\ 1)$」
(iii) 自然数 $m$，$n$，素数 $p$ に対して，
「$m^n$ が $p$ の倍数 $\Longrightarrow$ $m$ が $p$ の倍数」
を用いる。

実際の問題においては，「商と余りがただ一通り（一意性という）$\Longrightarrow$ 式の両辺で比較できる」と考えることが多い。式の左辺（右辺）で得られた余りが右辺（左辺）の余りと一致するという使い方をする。

## 1.2 素因数分解

約数を考察するのに素因数分解が有用である。ここではそれについて確認する。

**素因数分解の一意性**

2以上の整数は素因数の順序を無視すると，ただ一通りに素因数分解が可能である。

この性質を用いることにより，除法の原理の用語の確認(4)「素数」(ii)の性質も導け，約数を列挙したり，文字の個数よりも少ない数の方程式（不定方程式という）の整数解を考察することなどが可能となる。

例題 1

72 の正の約数の個数とそれらの和を求めよ。

**【解答】**

$72=2^3\cdot3^2$ となり，正の約数は，

$2^a\cdot3^b$ $(0\leqq a\leqq3,\ 0\leqq b\leqq2)$

で表せる。正の約数と整数の組 $(a,\ b)$ は 1 対 1 に対応するから，$a,\ b$ が何通りかと数えて，正の約数の個数は

$4\cdot3=\mathbf{12}$（個）

また正の約数の和は，

$$2^0(3^0+3^1+3^2)+2^1(3^0+3^1+3^2)+2^2(3^0+3^1+3^2)+2^3(3^0+3^1+3^2)$$
$$=(2^0+2^1+2^2+2^3)(3^0+3^1+3^2)$$
$$=\mathbf{195}$$

**【注】**

**1°** $N=p^aq^br^c\cdots\cdots$（素因数分解）

と表されたとき，$N$ の正の約数は

$p^iq^jr^k\cdots\cdots$

$(0\leqq i\leqq a,\ 0\leqq j\leqq b,\ 0\leqq k\leqq c)$

と表せるので，その個数は，

$(a+1)(b+1)(c+1)\cdots\cdots$（個）

である。正の約数の和は解答同様に考えて

$$(p^0+p^1+p^2+\cdots+p^a)\cdot(q^0+q^1+q^2+\cdots+q^b)\cdot(r^0+r^1+r^2+\cdots+r^c)\cdots\cdots$$

と表せる。

例題 2

(1) $x,\ y,\ z,\ a$ を正の整数とするとき，

$175x=1323y=5832z=a^2$

を満たす最小の $a$ の値を求めよ。

(2) $\dfrac{m}{175},\ \dfrac{m^2}{1323},\ \dfrac{m^3}{5832}$ がすべて整数となるような正の整数 $m$ のうち，最小のものを求めよ。

**【解答】**

(1) $175=5^2\cdot7,\ 1323=3^3\cdot7^2,\ 5832=2^3\cdot3^6$

これらの公倍数であり，平方数となるのは，各素因数の指数が偶数となるものである。そのうち指数が最小となるものを考えて，

$2^4\cdot3^6\cdot5^2\cdot7^2=(2^2\cdot3^3\cdot5\cdot7)^2=(3780)^2$

$\therefore\quad a=\mathbf{3780}$

(2) $\dfrac{m}{5^2\cdot7},\ \dfrac{m^2}{3^3\cdot7^2},\ \left(\dfrac{m}{2\cdot3^2}\right)^3$

これらがすべて整数となるので，$m$ は $5^2\cdot7,\ 3^2\cdot7,\ 2\cdot3^2$ のすべてで割り切れる。このような $m$ のうち最小のものは，$5^2\cdot7,\ 3^2\cdot7,\ 2\cdot3^2$ の最小公倍数だから，

$m=2\cdot3^2\cdot5^2\cdot7=\mathbf{3150}$

**【注】**

**1°** 素因数分解して考える。平方数から各素因数の指数が偶数であること，分数が整数から約分できることに注意する。

例題 3

$\dfrac{x^2-3x}{x+1}$ が整数となるような整数 $x$ の値を求めよ。

**【解答】**

$x^2-3x=(x+1)(x-4)+4$

だから，

$$\lceil\frac{x^2-3x}{x+1}\text{ が整数}\rfloor$$
$$\Longleftrightarrow\lceil\frac{(x+1)(x-4)+4}{x+1}\text{ が整数}\rfloor$$
$$\Longleftrightarrow\lceil x-4+\frac{4}{x+1}\text{ が整数}\rfloor$$
$$\Longleftrightarrow\lceil\frac{2^2}{x+1}\text{ が整数}\rfloor$$
$$\Longleftrightarrow\lceil x+1\text{ が }2^2\text{ の約数}\rfloor$$
$$\Longleftrightarrow x+1=\pm1,\ \pm2,\ \pm4$$
$$\Longleftrightarrow x=\mathbf{-5,\ -3,\ -2,\ 0,\ 1,\ 3}$$

**【注】**

**1°** 分数式は帯分数にして扱う。整数問題では，不定方程式をある1つの文字について解いた後に分数が出てくることが多いので，帯分数にして，

(i) $\dfrac{c\text{(整数)}}{f(x)}=\text{整数}\Longrightarrow f(x)$ は $c$ の約数

(ii) $\dfrac{g(x)}{f(x)}$＝整数 $\Longrightarrow g(x)=0$ or $\left|\dfrac{g(x)}{f(x)}\right|\geqq 1$

のいずれかで扱うことになる。

## 1.3 Euclid の互除法

除法の原理により約数，倍数などの用語が定義できたが，その中でも最大公約数に関して，大きな数を素因数分解して考えるのは面倒である。そこで，割り算を繰り返すことで最大公約数を効率よく求める方法があり，**Euclid の互除法**と呼ばれている。

**互除法**

整数 $a$，$b$ の最大公約数を $(a,\ b)$ と書くことにする。$a$ を $b$ で割った余りを $r$ とすると，

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

が成り立つ。一般に整数 $q$ に対して，

$$(a,\ b)=(b,\ a-bq)$$

が成り立つ。

**【証明】**

$g_1=(a,\ b)$，$g_2=(b,\ r)$，$a$ を $b$ で割った商を $p$ として，

$$a=bp+r\quad(0\leqq r<b)\qquad\cdots\cdots①$$

と表せるので

$$r=a-bp\qquad\cdots\cdots②$$

$g_1$ は $a$，$b$ の公約数だから，②より $r$ の約数でもある。したがって，$g_1$ は $b$，$r$ の公約数で，$g_2$ は $b$，$r$ の最大公約数だから

$$g_1\leqq g_2\qquad\cdots\cdots③$$

$g_2$ は $b$，$r$ の公約数だから，①より $a$ の約数でもある。したがって，$g_2$ は $a$，$b$ の公約数で，$g_1$ は $a$，$b$ の最大公約数だから

$$g_2\leqq g_1\qquad\cdots\cdots④$$

③，④より，$g_1=g_2$

$(a,\ b)=(b,\ a-bq)$ については，

$$r_1=a-bq$$

とおけば，上の議論と同様にして示せる。 ■

**【注】**

**1°** 最大公約数を設定しておき，約数であるという条件と除法の原理により得られる式から，どの文字の約数になるかを考えていくだけである。ここでは細かい定式化をしていないが，約数になるところも式で議論すると，

「$g_1=(a,\ b)$ より，整数 $A$，$B$ に対して，

$a=g_1A$，$b=g_1B$，$(A,\ B)=1$

と表せるので，②より，

$r=g_1(A-Bp)$

と書けて，$g_1$ は $r$ の約数である。」

などと議論していけばよい。

**2°** 公約数の集合について

$\{a,\ b$ の公約数$\}=\{b,\ r$ の公約数$\}$

が成り立つことから示してもよい。

$A=\{a,\ b$ の公約数$\}$，$B=\{b,\ r$ の公約数$\}$

と定めて，

$x\in A\Longrightarrow x\in B$，$x\in B\Longrightarrow x\in A$

の両方を示せばよく，議論の要旨は【証明】と変わらない。

例題 4

1085 と 341 の最大公約数を求めよ。

**【解答】**

$a$，$b$ の最大公約数を $(a,\ b)$ と表すと，

$(1085,\ 341)=(341,\ 1085-341\cdot 3)$

$=(341,\ 62)=(62,\ 341-62\cdot 5)$

$=(62,\ 31)=\mathbf{31}$

**【注】**

**1°** 大きい数字の最大公約数では Euclid の互除法を用いればよい。

## 1.4 互いに素

最大公約数に関する大切な内容に「互いに素」がある。除法の原理から得られる用語でも確認したが，

「$x$ が $y$ が**互いに素**」

$\Longleftrightarrow$「$x$ と $y$ の最大公約数は 1」(定義)

である。また，正の整数 $a$，$b$ の最大公約数を $g$，最小公倍数を $\ell$ とすると，互いに素な整数 $A$，$B$ を用いて，

$$a=gA,\ b=gB$$

と表せて，このとき

$$\ell = ABg,\quad ab = g\ell$$

が成り立つ。

実際の問題で互いに素を扱う際は条件内か，結論内によって扱い方が変わる。

**互いに素を扱う**

(i)　条件内の互いに素

$p$，$q$ を互いに素な整数とするとき，

(ア)　$\dfrac{aq}{p}$＝整数 $\Longleftrightarrow$ $\dfrac{a}{p}$＝整数

(イ)　$aq = p\cdot$(整数) $\Longleftrightarrow$ $a = p\cdot$(整数)

(ii)　結論内の互いに素

「$x$ と $y$ が**互いに素**」

$\Longleftrightarrow$「$x$ と $y$ をともに割り切る素数はない」

もしくは Euclid の互除法を用いる。

(i)の(ア)，(イ)はどちらも同じ意味であるが，(ア)の分数形の方が $\Longrightarrow$ を考える際に，「どこで約分するか」のように考えることができて扱いやすい。

互いに素を証明するときには，この言いかえをした上で示す。否定的な命題になるので**背理法**を用いると証明しやすい。その際，公約数を素数でおくのがポイントとなる。ここで，背理法についても確認しておく。

命題 $p \Longrightarrow q$ が真であることを証明するために $p \Longrightarrow q$ と同値な他の命題が真であることを証明する方法を間接証明法といい，よく使われるものに**背理法**がある。その手順は次のようなものであった。

**背理法の流れ**

①　$p$ かつ $\overline{q}$ を仮定する。

②　①のもとで議論すると

(i)　数学的事実

(ii)　$\overline{q}$ と仮定したこと

(iii)　$p$ であること

のいずれかに矛盾する。

③　②により $p \Longrightarrow q$ が真であると示せる。

②(iii)を考えればわかる通り，背理法は対偶法を含んでいる。共通テストの数学では誘導に従い対偶法を用いるが，記述の問題では自分で方針を選べることが多いため，適用範囲の広さから，対偶を使うより背理法を使う方がよい。

また，互いに素が使われるものとして，$a$，$b$ の最大公約数を $(a,\ b)$ と表すと，

・$(n,\ 1)=1$，$(n,\ n+1)=1$

・素数 $p$ が $x$ の約数でないとき，$(x,\ p)=1$

・$(p,\ q)=1 \Longrightarrow (p^a,\ q^b)=1$　($a$，$b$：自然数)

などがある。

例題 5

$p$ を素数とする。${}_pC_k$ ($k=1, 2, \cdots\cdots, p-1$) は，いずれも $p$ で割り切れることを証明せよ。

**【解答】**

$${}_pC_k = \frac{p(p-1)\cdots\cdots(p-k+1)}{k(k-1)\cdots\cdots 2\cdot 1}$$

の左辺は整数であり，右辺で $1 \leqq k \leqq p-1$ ($<p$) より，$p$ と $k!$ は互いに素である。したがって，右辺の分子の $p$ は約分されず，

$${}_pC_k = p\cdot(\text{整数})$$

と表される。　■

**【注】**

**1°**　条件に互いに素がある場合である。既約分数の議論から攻めていくことになる。本質的には同じであるが，2 項係数の性質

$$k\,{}_pC_k = p\,{}_{p-1}C_{k-1}$$

から導いてもよい。

例題 6

正の整数 $n$ に対して，$n$ と $n+1$ は互いに素であることを示せ。

**【解答】**

$n$，$n+1$ をともに割り切る素数$p$が存在すると仮定すると，$a$，$b$ を自然数として，

$$n = pa,\quad n+1 = pb$$

と表せる。$n$ を消去すると，

$p(b-a)=1$

となるが，$p$ は素数より成立せず矛盾。

よって，$n$ と $n+1$ は互いに素である。 ■

**【注】**

**1°** 互いに素を証明するときは「ともに割り切る素数が存在する」と仮定して矛盾を導くとよい。慣れないうちは解答のように丁寧に書いて，慣れてきたら（$n$，$n+1$ の素因数を見る感覚が養われたら）差をとり

$(n+1)-n=1$

から互いに素であると素早く議論すればよい。同様の議論により，$k$を整数として

$kn+1$，$n$ も互いに素

であると分かる。つまり，ある自然数 $N$ を $n$ で割って余りが 1 なら，$N$ と $n$ は互いに素になるわけである。

**2°** Euclid の互除法を用いると

$(n+1,\ n)=(n,\ n+1-n)=(n,\ 1)=1$

となり，素早く議論できる。

例題 7

$x$，$y$，$n$ は自然数とする。

(1) $x+y$，$xy$ が互いに素であるための必要十分条件は $x$，$y$ が互いに素であることを示せ。

(2) $x$，$y$，$n$ は自然数とする。$x$，$y$ が互いに素で $xy=n^2$ を満たすとき，$x$，$y$ はともに平方数となることを示せ。

**【解答】**

(1) $x$，$y$ が互いに素であるとき，$x+y$，$xy$ をともに割り切る素数 $p$ が存在すると仮定して，自然数 $a$，$b$ に対して，

$x+y=pa$ ……①

$xy=pb$ ……②

と表せる。$p$ は素数だから，②より，

$x$ は $p$ の倍数，または，$y$ は $p$ の倍数

(i) $x$ が $p$ の倍数のとき，

$x=pc$ （$c$：自然数）

と表せて，①より，

$y=p(a-c)$

だから，$p$ は $x$，$y$ の公約数になるが，$x$，$y$ は互いに素だから矛盾する。

(ii) $y$ が $p$ の倍数のとき，

$y=pd$ （$d$：自然数）

と表せて，①より，

$x=p(a-d)$

だから，$p$ は $x$，$y$ の公約数になるが，$x$，$y$ は互いに素だから矛盾する。

(i)，(ii)より，$x+y$，$xy$ は互いに素である。

逆に，$x+y$，$xy$ が互いに素であるとき，$x$，$y$ をともに割り切る素数 $q$ が存在すると仮定して，自然数 $c$，$d$ に対して，

$x=qc$，$y=qd$

と表せる。このとき，

$x+y=q(c+d)$，$xy=q^2cd$

となり，$q$ は $x+y$，$xy$ の公約数だから，$x+y$，$xy$ が互いに素であることに矛盾する。よって $x$，$y$ は互いに素である。

以上により題意は成立する。 ■

(2) $n$ の素因数 $p$ に対して，$n^2$ の中に素因数 $p$ は偶数個ある。$xy$ が $p$ の倍数で $x$，$y$ が互いに素だから，偶数個の $p$ はすべて $x$ に含まれるか，すべて $y$ に含まれるかのどちらかである。各素因数すべてでこれが言えて，$x$，$y$ ともに各素因数の個数は偶数個だから，平方数である。 ■

**【注】**

**1°** $x+y$，$xy$ をともに割り切る素数 $p$ が存在すると仮定したからこそ，②から $x$，$y$ のいずれかに素因数 $p$ が含まれると考えられるのである。公約数を設定するのでなく，素数を設定する意識をもっておきたい。なお，②から素因数に注目することができなければ，$x$，$y$ のうちの一文字を消去して，次のように考えてもよい。

「①より，$y=pa-x$ だから，②より，

$x(pa-x)=pb$

$\therefore\quad x^2=p(ax-b)$

$p$ は素数だから，$x$ の約数，つまり $x$ が $p$ の倍数である。」

結局得られる結果は同じだから，【解答】のようにできるのが簡明でよい。

**2°** (2)では，$x$，$y$ をともに割り切る素数はないの

で，$n^2$ の各素因数を $x$，$y$ に分配する際，すべて $x$ に入るか，すべて $y$ に入るかしかない（$x$，$y$ の両方に入るとともに $p$ で割れて矛盾する）。加えて平方数になる条件「各素因数の個数が偶数個」も考えればすぐに導ける。当然という感覚が持てるとよい。

例題 8

$a$，$b$ を互いに素な正の整数とするとき，$\dfrac{3a+7b}{2a+5b}$ は既約分数であることを示せ。

**【解答】**

既約分数でないと仮定すると，$3a+7b$，$2a+5b$ をともに割り切る素数$p$が存在する。$A$，$B$ を正の整数として，

$$3a+7b=pA,\quad 2a+5b=pB$$

と表せるから，

$$a=p(5A-7B),\quad b=p(3B-2A)$$

となり，$a$，$b$ がともに $p$ で割り切れ矛盾する。

よって，$\dfrac{3a+7b}{2a+5b}$ は既約分数である。 ■

**【注】**

**1°** 本質的には同じだが，一文字消去の要領で，分母と分子を連立してもよい。

$$-2(3a+7b)+3(2a+5b)=b$$
$$5(3a+7b)-7(2a+5b)=a$$

より，$3a+7b$，$2a+5b$ の公約数は$a$，$b$ の公約数となる。

**2°** Euclid の互除法でもよい。整数 $a$，$b$ の最大公約数を $(a,\ b)$ と表すと，整数 $q$ に対して，

$$(a,\ b)=(a-bq,\ b)=(a,\ b-aq)$$

が成り立つ。

**【解答 2】**

$a$，$b$ の最大公約数を $(a,\ b)$ とすると，

$(a,\ b)=1$ のもとで，$(3a+7b,\ 2a+5b)=1$

を示せばよい。

$$\begin{aligned}&(3a+7b,\ 2a+5b)\\&=(3a+7b-(2a+5b),\ 2a+5b)\\&=(a+2b,\ 2a+5b)\\&=(a+2b,\ 2a+5b-2(a+2b))\\&=(a+2b,\ b)\\&=(a+2b-2b,\ b)\\&=(a,\ b)\\&=1\end{aligned}$$ ■

例題 9

$\dfrac{x^3-3x+2}{2x+1}$ が整数となるような整数 $x$ の値を求めよ。

**【解答】**

$2x+1$ と 8 は互いに素だから，

$$\text{「}\frac{x^3-3x+2}{2x+1}\text{ が整数」}$$
$$\Longleftrightarrow\ \text{「}\frac{8(x^3-3x+2)}{2x+1}\text{ が整数」}\quad(*)$$

ここで，

$$8(x^3-3x+2)=(2x+1)(4x^2-2x-11)+27$$

だから，

$$\frac{8(x^3-3x+2)}{2x+1}=4x^2-2x-11+\frac{27}{2x+1}$$

となり，

$$(*)\Longleftrightarrow\ \text{「}\frac{27}{2x+1}\text{ が整数」}$$
$$\Longleftrightarrow 2x+1=\pm1,\ \pm3,\ \pm9,\ \pm27$$
$$\Longleftrightarrow x=\mathbf{-14,\ -5,\ -2,\ -1,\ 0,\ 1,\ 4,\ 13}$$

**【注】**

**1°** 分数式は帯分数にして扱う。ただ，このまま帯分数にしようとすると

$$\frac{x^3-3x+2}{2x+1}$$
$$=\frac{1}{8}(4x^2-2x-11)+\frac{27}{8(2x+1)}$$

となり第一項が整数とは限らず面倒である。これを 8 倍して考えてもよいのだが，

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

とすれば，そのまま 8 倍すると

$$4x^2-2x-11+\frac{27}{2x+1}=8k$$

となるため，左辺の値が 8 の倍数になっているかを確認する必要が出て面倒である。そこで，

分母が奇数であることに注意して，8 と奇数は互いに素だから，互いに素の扱い方である「$p$，$q$ が互いに素な整数であるとき，整数 $a$ に対して，

$$\frac{aq}{p}=\text{整数} \Longleftrightarrow \frac{a}{p}=\text{整数}」$$

を思い出すことになる。

## 1.5 有理数・無理数

互いに素が絡む用語として有理数がある。ここでは有理数，無理数の扱いを確認する。

**有理数**とは $\frac{q}{p}$（$p$, $q$ は互いに素な整数で，$p>0$）とかける数のことをいう。整数 $N$ が $\frac{N}{1}$ と表されることに注意すると，有理数は整数と分数を含むもので，どんな有理数も既約分数（約分済みの分数）の形で表せる。小数で表すと，有理数は，整数，有限小数，循環（無限）小数のいずれかとなる。有理数でない実数を**無理数**という。特に，無理数を示す際は，「有理数でないこと」を示す（否定命題の証明）から，背理法を用いる。小数で表すと，無理数は循環しない無限小数となる。

例題 10

$\sqrt{2}$ が無理数であることを示せ。

**【解答】**

$\sqrt{2}$ が有理数であると仮定すると，$\sqrt{2}>0$ だから，互いに素な自然数 $p$，$q$ に対して，

$$\sqrt{2}=\frac{q}{p}$$

と表せる。

$$\therefore \quad 2p^2=q^2$$

右辺の $q^2$ の素因数分解の中に素因数2は偶数個ある。左辺の $2p^2$ の素因数分解の中に素因数 2 は奇数個ある。これは素因数分解の一意性と矛盾する。よって，$\sqrt{2}$ は無理数である。 ■

**【注】**

**1°** 素因数分解に注目すると素早く議論できる。このとき，互いに素は用いていないが，とりあえずつけておく癖をつける方がよいので【解答】ではつけたままにしてある。

**2°** 互いに素を用いて議論すると，次の【解答 2】【解答 3】のいずれかとなる。

**【解答 2】**

$\sqrt{2}$ が有理数であると仮定すると，$\sqrt{2}>0$ だから，互いに素な自然数 $p$，$q$ に対して，

$$\sqrt{2}=\frac{q}{p}$$

と表せる。

$$2=\frac{q^2}{p^2}$$

$p$, $q$ が互いに素のとき，$p^2$, $q^2$ も互いに素だから，

$$p^2=1 \qquad \therefore \quad p=1$$

このとき，$q^2=2$ となるが，

$$1=1^2<2<2^2=4$$

より，連続する平方数 1, 4 の間の 2 は平方数でなく矛盾する。よって，$\sqrt{2}$ は無理数となる。 ■

**【解答 3】**

$\sqrt{2}$ が有理数であると仮定すると，$\sqrt{2}>0$ だから，互いに素な自然数 $p$，$q$ に対して，

$$\sqrt{2}=\frac{q}{p}$$

と表せる。

$$\therefore \quad 2p^2=q^2$$

左辺は偶数だから右辺も偶数で，2 は素数だから $q$ が偶数となる。このとき

$$q=2q_1 \quad (q_1\text{：自然数})$$

とおけて，

$$2p^2=(2q_1)^2 \qquad \therefore \quad p^2=2q_1^2$$

右辺は偶数だから左辺も偶数で，2 は素数だから $p$ が偶数となる。このとき $p$，$q$ がともに 2 で割れて，互いに素であることに矛盾する。よって，$\sqrt{2}$ は無理数となる。 ■

例題 11

$\log_3 2$ が無理数であることを示せ。

**【解答】**

$\log_3 2$ が有理数であると仮定すると，$\log_3 2>0$

だから，互いに素な自然数 $p$，$q$ に対して，

$$\log_3 2=\frac{q}{p}$$

と表せる。

$\therefore\quad 2=3^{\frac{q}{p}}\qquad \therefore\quad 2^p=3^q$

左辺は偶数，右辺は奇数で矛盾する。

よって，$\log_3 2$ は無理数である。 ■

**【注】**

**1°** 無理数のような否定命題の証明は背理法の利用が有効である。

有理数，無理数に関して次の性質が成り立つ。

**係数比較**

$p$，$q$，$r$，$s$ を有理数，$\alpha$ を無理数とするとき，次が成り立つ。

(1) $p+q\alpha=0 \Longrightarrow \begin{cases} p=0 \\ q=0 \end{cases}$

(2) $p+q\alpha=r+s\alpha \Longrightarrow \begin{cases} p=r \\ q=s \end{cases}$

**【証明】**

(1) $q\neq 0$ と仮定すると，

$$\alpha=-\frac{p}{q}$$

左辺は無理数，右辺は有理数となり矛盾する。

よって，$q=0$ だから，$p=0$ ■

(2) $p-r+(q-s)\alpha=0$

に(1)を用いて，

$p-r=0$ かつ $q-s=0$

$\therefore\quad p=r$ かつ $q=s$ ■

**【注】**

**1°** 自明な命題は背理法が有効である。そう思えなかったとしても，問題文に書いてある場合以外を考察することはとても大切で，$q=0$ になるかわからないのだから $q\neq 0$ も考えてみなくてはならない。

**2°** この事実から分かる通り，係数比較ができる。問題で出題されるときには $\alpha$ が $\sqrt{2}$，$\sqrt{3}$ などの場合が多い。

**3°** 係数比較がらみの内容として，次もある。

$p$，$q$，$r$，$s$ を実数，$\alpha$ を虚数とするとき，次が成り立つ。

(1) $p+q\alpha=0 \Longrightarrow \begin{cases} p=0 \\ q=0 \end{cases}$

(2) $p+q\alpha=r+s\alpha \Longrightarrow \begin{cases} p=r \\ q=s \end{cases}$

証明も全く同じである。ベクトルにおける係数比較も同じ内容である。

3次方程式 $4x^3+6x^2-1=0$ の解を求めるときに，

$$(2x+1)(2x^2+2x-1)=0$$

と因数分解して解を求めるが，適当な値を代入して因数分解をやみくもに行おうとしても整数でない有理数を解に持つ場合はうまくいかないこともある。そこで次の事実に従って因数分解を行う。

**有理数解の性質**

整数係数の $n$（$\geqq 1$）次方程式

$a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_1x+a_0=0$

の有理数解は（あるとすれば），

$$\frac{a_0\text{ の約数}}{a_n\text{ の約数}}$$

の形のものに限る。

**【証明】**

有理数解は互いに素な整数 $p$（$>0$），$q$ を用いて，$\frac{q}{p}$ と表せるから，

$$a_n\left(\frac{q}{p}\right)^n+a_{n-1}\left(\frac{q}{p}\right)^{n-1}+\cdots\cdots+a_1\left(\frac{q}{p}\right)+a_0=0 \qquad \cdots\cdots①$$

$$\frac{a_nq^n}{p}=-(a_{n-1}q^{n-1}+\cdots\cdots+a_1qp^{n-2}+a_0p^{n-1})$$

$p$，$q$ は互いに素だから，$p$，$q^n$ も互いに素で，

$\frac{a_n}{p}=$整数 $\qquad\therefore\quad p$ は $a_n$ の約数。

また，①より，

$$q(a_nq^{n-1}+a_{n-1}q^{n-2}p+\cdots+a_1p^{n-1})=-a_0p^n$$

$p$，$q$ は互いに素だから，$p^n$，$q$ は互いに素で

$q$ は $a_0$ の約数

したがって，

$$\frac{q}{p}=\frac{a_0\text{ の約数}}{a_n\text{ の約数}}$$ ■

**【注】**

**1°** 有理数解に関する問題で，この証明と同様の流れを要求されるので，事実だけでなく証明も含めて頭に入れておく必要がある。

**2°** 互いに素が条件内にあるとき，

(ア) $\dfrac{aq}{p}=$整数 $\Longleftrightarrow \dfrac{a}{p}=$整数

(イ) $aq=p\cdot$(整数) $\Longleftrightarrow a=p\cdot$(整数)

を用いる。

**3°** $a_n=1$ のときは，$a_n$ の約数 $=\pm1$ なので，有理数解は整数解に限られる。

## 1.6 整数の分類

2 以上の整数 $m$ に対して，整数全体を $m$ で割った余りにより分類することができる。例えば $m=3$ なら，整数を 3 で割った余りは 0，1，2 のいずれかであるから，整数全体は

$3k$，$3k+1$，$3k+2$ （$k$：整数）

と 3 つの種類に分類することができる。なお，計算する上では余りの絶対値が最小になるように，

$3k$，$3k+1$，$3k-1$

の 3 つの種類に分類する方がよい場合も多い。余りによる分類は倍数証明によく用いられる。

例題 12

$n$を整数とするとき，次を示せ。

(1) $n^2$ を 3 で割った余りは 0 か 1 である。

(2) $n^2$ を 4 で割った余りは 0 か 1 である。

**【解答】**

(1) 任意の整数 $n$ は $m$ を整数として，

$3m$，$3m\pm1$

のいずれかの形で表せるから，

$n=3m$：$n^2=3\cdot3m^2$

$n=3m\pm1$：$n^2=3(3m^2\pm2m)+1$

（複号同順）

のいずれかとなり，$n^2$ を 3 で割った余りは 0 か 1 である。 ■

(2) 任意の整数 $n$ は $m$ を整数として，

$2m$，$2m+1$

のいずれかの形で表せるから，

$n=2m$：$n^2=4\cdot m^2$

$n=2m+1$：$n^2=4(m^2+m)+1$

のいずれかとなり，$n^2$ を 4 で割った余りは 0 か 1 である。 ■

**【注】**

**1°** 入試では常識なので記憶しておくのがよい。

(1)は

「平方数を 3 で割ると 2 余ることはない」

と言い換えられ，これを問題にすると

> $x^2=3y+2$ を満たす整数 $x$，$y$ は存在しないことを示せ。

となる。このような問題になると，両辺の余りが比較できるという意識が大切になる。(2)についても同様である。

**2°** (2)は 4 で割った余りで分類して

$4m$，$4m\pm1$，$4m+2$

としてもよいが，合成数（この問題なら 4）の場合は 2 乗してその数（この問題なら 4）が出てくる最小数で考えると分類が少なくなり議論がしやすくなる。逆に，小さい数での分類で上手くいかないときに，より大きな数での分類にして考えることもある。

**3°** この例題と同様にして，

「$n^2$ を 5 で割った余りは 0 か 1 か 4 である」，

「$n^2$ を 7 で割った余りは 0 か 1 か 2 か 4 である」

ことも示せる。

## 1.7 連続する $k$ 個の整数

倍数を証明する際に整数の分類を行うが，$n$ の整式が連続整数の形をしているときは，場合分けをせず素早く示すことが可能となる。

連続する $k$ 個の整数

$n$，$n+1$，$n+2$，……，$n+k-1$

を $k$ で割った余りを順に $r_1$，$r_2$，……，$r_k$ とすると，

$\{r_1,\ r_2,\ \cdots\cdots,\ r_k\}=\{0,\ 1,\ 2,\ \cdots\cdots,\ k-1\}$

が成り立つ。特に，$n$，$n+1$，……，$n+k-1$ の中に $k$ の倍数がただ一つ存在する。

この事実に関連する内容として次の事実がある。

**連続 $k$ 整数の積**

連続する $k$ 個の整数

$n$，$n+1$，$n+2$，……，$n+k-1$

の積 $n(n+1)(n+2)\cdots\cdots(n+k-1)$ は $k!$ の倍数である。

**【証明】**

$n(n+1)(n+2)\cdots\cdots(n+k-1)$

$=k!\cdot{}_{n+k-1}\mathrm{C}_k$

$=k!\cdot$(整数)

よりただちに従う。 ■

例題 13

整数 $n$ に対して，$P(n)=n^3-n$ とする。

(1) $P(n)$ は 6 の倍数であることを示せ。

(2) $n$ が奇数ならば，$P(n)$ は 24 の倍数であることを示せ。

(3) $P(n)$ が 48 の倍数となる偶数 $n$ をすべて求めよ。

**【解答】**

(1) $P(n)=(n-1)n(n+1)$

であり，これは連続する 3 個の整数の積だから，$3!=6$ の倍数である。 ■

(2) $n=2m+1$ （$m$：整数）

として，

$P(n)=P(2m+1)$

$=2m(2m+1)(2m+2)$

$=4m(m+1)(2m+1)$

$=4m(m+1)\{(m-1)+(m+2)\}$

$=4\{(m-1)m(m+1)+m(m+1)(m+2)\}$

$(m-1)m(m+1)$，$m(m+1)(m+2)$ はともに連続する 3 個の整数の積だから $3!=6$ の倍数である。したがって，$P(n)$ は $4\cdot6=24$ の倍数である。 ■

(3) $n=2m$ （$m$：整数）

とすると，

$P(n)=P(2m)=2m(2m-1)(2m+1)$

連続する 3 個の整数の積だから 3 の倍数なので，48 の倍数になる条件は，

「$2m(2m-1)(2m+1)$ が 16 の倍数」

$\Longleftrightarrow$「$m(2m-1)(2m+1)$ が 8 の倍数」

$2m\pm1$ は奇数だから，求める条件は

「$m$ が 8 の倍数」

となる。したがって，

$n$ は $2\cdot8=16$ の倍数

となり，

$\boldsymbol{n=16k}$ （$\boldsymbol{k}$：整数）

**【注】**

**1°** 連続整数に注意して積を考えると速い。(2)では無理やり作りだす意識をもつ。気がつかなければ，3 で割った余りと 2 で割った余りで分類することになる。

例題 14

3 より大きい整数 $p$ に対して，$p$ と $p+2$ がともに素数のとき，$p+1$ が 6 の倍数であることを示せ。

**【解答】**

$p(p+1)(p+2)$ は連続する 3 個の整数の積だから，$3!=6$ の倍数である。$p$，$p+2$ はともに 3 より大きい素数だから，3 の倍数でも 2 の倍数でもない。したがって，$p+1$ が 6 の倍数である。 ■

**【注】**

**1°** 連続整数に注意して積を考えると速い。気がつかなければ，3 で割った余りと 2 で割った余りで分類することになる。

## 1.8 合同式

整数の分類において余りに注意して場合分けをした。そのとき商よりも余りに注目していたので，余りだけで議論できると楽である。そこで，余りだけ取りだして考えられる合同式というもの

がある。

**合同式**

整数 $a$ と $b$ の差が $m$ の倍数であるとき,「$a$ と $b$ は $m$ を法として合同である」といい,

$a \equiv b \pmod{m}$

と表す。

合同式と余りの間に次の関係が成り立つ。

「$a$ と $b$ が $m$ を法として合同である」

$\Longleftrightarrow$「$a$, $b$ を $m$ で割った余りが等しい」

**【証明】**

$a$ と $b$ が $m$ を法として合同であるとき，$q$ を整数として，

$$a-b=mq \quad \cdots\cdots①$$

とおける。$a$, $b$ を $m$ で割った商と余りをそれぞれ $q_1$, $q_2$, $r_1$, $r_2$ とすると，

$$a=mq_1+r_1,\ b=mq_2+r_2$$

差をとり，①より，

$$mq=(q_1-q_2)m+r_1-r_2$$

$$m(q-q_1+q_2)=r_1-r_2$$

$$\therefore\ |m||q-q_1+q_2|=|r_1-r_2|$$

$q-q_1+q_2 \neq 0$ とすると，

$$|r_1-r_2|<m \leqq |m||q-q_1+q_2|$$

より矛盾するので，

$$q-q_1+q_2=0$$

$$\therefore\ r_1=r_2$$

逆に $a$, $b$ を $m$ で割った余りが等しいとすると，

$$a=mq_1+r,\ b=mq_2+r$$

と表せて，

$$a-b=m(q_1-q_2)$$

となり，$a$ と $b$ は $m$ を法として合同である。 ■

合同式は次の性質を使うことで簡単な計算に帰着できる。

**合同式の性質**

(1) $m$ を法として，$a \equiv b$, $c \equiv d$ のとき

(i) $a+c \equiv b+d$

(ii) $a-c \equiv b-d$

(iii) $ac \equiv bd$

(iv) $a^k \equiv b^k$ （$k$：2 以上の自然数）

が成り立つ。

(2) $a$ と $p$ が互いに素のとき $p$ を法として，

(i) $ax \equiv 0 \Longrightarrow x \equiv 0$

(ii) $ax \equiv ab \Longrightarrow x \equiv b$

(3) $a$ と $p$ の最大公約数が $d$（$>1$）のとき

(i) $ax \equiv 0 \pmod{p}$

$$\Longrightarrow x \equiv 0 \left(\bmod \frac{p}{d}\right)$$

(ii) $ax \equiv ab \pmod{p}$

$$\Longrightarrow x \equiv b \left(\bmod \frac{p}{d}\right)$$

(1)は合同式が普通の等式のように辺々足したり，引いたり，掛けたりすることができることを意味している。合同式の両辺で余りが等しいと読めば，(i), (ii), (iii)が成り立つのも頷ける。(iv)は(iii)の特別な場合である。また,(iii)は非常によく用い,「積の余りは余りの積（の余り）」ということを意味している。整数の分類とも対応するが，平方数 $x^2$ や指数を含む形 $2^n$ などで，先に $x$ や 2 を割った余りを求めて考えることが大切なのである。

(2)は式で書かれている意識があるとよい。

$ax \equiv 0 \pmod{m}$ は，

$$ax=pm \quad (m：整数) \quad \cdots\cdots①$$

であることを意味しており，例で考えると，

$2x=3y$ という形から，2，3 が互いに素だから，$y$ が 2 の倍数，$x$ が 3 の倍数と導いているだけである。これと同様に $a$ と $p$ が互いに素だから，①から $x$ は $p$ の倍数となり，合同式で書けば $x \equiv 0$ となる。(ii)の $ax \equiv ab$ のときは，$a(x-b) \equiv 0$ と直して(i)を用いるだけである。ちなみに，この事実は「互いに素を扱う」の(i)条件内の互いに素の(ア), (イ)の事実そのものでもある。(3)(i)も式を具体例で考えると $12x=18y$ という形から，12，18 の最大公約数 6 で割り，$2x=3y$ となるので，さらに(2)の議論を用いて，$y$ は $2\left(=\dfrac{12}{6}\right)$ の倍数，$x$ は $3\left(=\dfrac{18}{6}\right)$ の倍数と導いているだけである。これを文字で同様に行えばよい。(ii)も(2)と同じ流れになる。

合同式で記載してはいるが，略記しただけなの

で，気になるところがあれば式で丁寧に議論すればよい。そうすると意味がよく分かり，意味がよく分かった後はそれを素早く導けるように形を頭に入れておくだけである。

これらを用いると先の有理数解の性質の【証明】，例題 12 の【解答】を略記することができる。

**有理数解の性質**〔再掲〕

整数係数の $n$（≧1）次方程式

$$a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_1x+a_0=0$$

の有理数解は（あるとすれば），

$$\frac{a_0\text{ の約数}}{a_n\text{ の約数}}$$

の形のものに限る。

**【証明 2】**

有理数解は互いに素な整数 $p$（$>0$），$q$ を用いて，$\dfrac{q}{p}$ と表せるから，

$$a_n\left(\frac{q}{p}\right)^n+a_{n-1}\left(\frac{q}{p}\right)^{n-1}+\cdots\cdots+a_1\left(\frac{q}{p}\right)+a_0=0 \quad \cdots\cdots①$$

$$a_nq^n+a_{n-1}pq^{n-1}+\cdots\cdots+a_1p^{n-1}q+a_0p^n=0$$

$$\therefore \begin{cases} a_nq^n\equiv 0 \pmod p \\ a_0p^n\equiv 0 \pmod q \end{cases}$$

$p$，$q$ は互いに素なので，$p$，$q^n$ や $p^n$，$q$ はともに互いに素であり，

$$\begin{cases} a_n\equiv 0 \pmod p \\ a_0\equiv 0 \pmod q \end{cases}$$

したがって，

$$\frac{q}{p}=\frac{a_0\text{ の約数}}{a_n\text{ の約数}}$$ ■

例題 12〔再掲〕

$n$ を整数とするとき，次を示せ。

(1) $n^2$ を 3 で割った余りは 0 か 1 である。

(2) $n^2$ を 4 で割った余りは 0 か 1 である。

**【解答 2】**

(1) 3 を法として，

$n\equiv 0 \Longrightarrow n^2\equiv 0^2=0$

$n\equiv 1 \Longrightarrow n^2\equiv 1^2=1$

$n\equiv 2\equiv -1 \Longrightarrow n^2\equiv(-1)^2=1$

よって，$n^2$ を 3 で割った余りは 0 か 1 である。 ■

(2) 4 を法として，

$n\equiv 0 \Longrightarrow n^2\equiv 0^2=0$

$n\equiv 1 \Longrightarrow n^2\equiv 1^2=1$

$n\equiv 2 \Longrightarrow n^2\equiv 2^2\equiv 0$

$n\equiv 3\equiv -1 \Longrightarrow n^2\equiv(-1)^2=1$

よって，$n^2$ を 4 で割った余りは 0 か 1 である。 ■

**【注】**〔続き〕

**4°** 合同式を用いると(2)を 4 で割った余りで分類しても大変さはない。このように合同式は「余り」だけを議論する際には大変役に立つ。一方で，合同式を使わない【解答】で 2 で割った余りで分類したときのように，「商」を議論したいときには役に立ちにくい。余りだけで議論してみてうまくいかないときは，あらためて整数を分類して商を見ながら考えていくことになる。

例題 15

正の整数 $n$ に対して，$8^n$ を 3 で割った余りを求めよ。

**【解答】**

3 を法として，$8\equiv -1$ だから，

$$8^n\equiv(-1)^n\equiv\begin{cases}\boldsymbol{1} & \boldsymbol{(n:\text{偶数})} \\ \boldsymbol{2} & \boldsymbol{(n:\text{奇数})}\end{cases}$$

**【注】**

**1°** 「積の余りは余りの積（の余り）」である。まず 8 を 3 で割り，その余りをかけると考える。余りだけなら合同式が便利である。問題で「余り」と明言される場合もあれば，「一の位（10 で割った余り）」のように本質的には余りだが，明言されない場合もある。

**2°** 合同式を用いないなら，2 項定理

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

を用いることになる。

**【解答 2】**

$$8^n=(9-1)^n=\sum_{k=0}^{n}{}_nC_k9^{n-k}(-1)^k$$

となり，$k=0$，1，2，……，$n-1$ のとき $9^{n-k}$ が 3 で割り切れるので，$8^n$ を 3 で割った余りは，9 を因数に持たない項である $k=n$ のときの $(-1)^n$ を 3 で割った余りと一致する。したがって，求める余りは，

$$\begin{cases}\mathbf{1}\quad(\boldsymbol{n}\text{：偶数})\\ \mathbf{2}\quad(\boldsymbol{n}\text{：奇数})\end{cases}$$

例題 16

$a$，$b$，$c$，$d$ を整数とする。整式

$f(x)=ax^3+bx^2+cx+d$

において，$f(-1)$，$f(0)$，$f(1)$ がいずれも 3 で割り切れないならば，方程式 $f(x)=0$ は整数の解をもたないことを証明せよ。

**【解答】**

$f(x)=0$

が整数の解 $\alpha$ をもつと仮定する。以下，3 を法として考える。

(i)　$\alpha\equiv0$ のとき

$f(\alpha)=a\alpha^3+b\alpha^2+c\alpha+d$

$\equiv a\cdot0^3+b\cdot0^2+c\cdot0+d$

$=d=f(0)$

$f(\alpha)=0$ より，$f(0)$ が 3 で割り切れ矛盾。

(ii)　$\alpha\equiv\pm1$ のとき

$f(\alpha)=a\alpha^3+b\alpha^2+c\alpha+d$

$\equiv a\cdot(\pm1)^3+b\cdot(\pm1)^2+c\cdot(\pm1)+d$

$=\pm a+b\pm c+d=f(\pm1)$　（複号同順）

$f(\alpha)=0$ より，$f(\pm1)$ が 3 で割り切れ矛盾。

以上(i)，(ii)より，$f(x)=0$ は整数の解をもたないことが示せた。 ■

**【注】**

**1°**　$f(-1)$，$f(0)$，$f(1)$ を使いたい意識のもと $f(\alpha)$ と見比べつつ，3 で割り切れないという条件を見れば，3 で割った余りで分類すればよいと気がつける。

**2°**　一般に，整数係数の整式 $f(x)$ に対して，

$\alpha\equiv r\pmod p$

ならば，

$f(\alpha)\equiv f(r)\pmod p$

が成り立つ。

例題 5 と合同式を組み合わせることにより，次の事実が成り立つ。

**フェルマーの小定理**

$p$ を素数，$n$ と $p$ が互いに素とするとき，

$n^{p-1}\equiv1\pmod p$

が成り立つ。

**【証明】**

$n^p=\{(n-1)+1\}^p$

だから，2 項定理で展開して，例題 5 の結果を用いると，$p$ を法として，

$n^p\equiv(n-1)^p+1^p$

この操作を繰り返し行うと，

$n^p\equiv(n-2)^p+1^p+1^p$

$\equiv(n-3)^p+1^p+1^p+1^p$

$\equiv\cdots\cdots$

$\equiv\underbrace{1^p+1^p+\cdots+1^p}_{n\text{個}}=n$

$p$，$n$ は互いに素だから，

$n^{p-1}\equiv1$ ■

**【注】**

**1°**　例題 5 を用いると，素数 $p$，自然数 $a$，$b$ に対して，

$(a+b)^p\equiv a^p+b^p\pmod p$

が成り立つ。

**2°**　「$n^p-n$ が $p$ で割り切れることを示せ」と出題されることもある。このときは帰納法で示してもよい。

例題 17

$5x-3y=1$ の整数解を求めよ。

**【解答】**

$5x=3y+1$　……①

3 を法として，

$2x\equiv1$

$x$ に 0，1，2 を代入して成り立つものを探すと，2 でのみ成り立つから，

$$2x \equiv 1 \equiv 2 \cdot 2$$

2，3 は互いに素だから，

$$x \equiv 2$$

このとき

$$x = 3k + 2 \quad (k：整数)$$

と表せて，①より，

$$3y = 5(3k+2) - 1$$

$$\therefore \quad y = 5k + 3$$

$$\therefore \quad \boldsymbol{(x,\ y) = (3k+2,\ 5k+3)}$$

**【注】**

**1°** $ax + by = c$ の形の不定方程式である。一次式で表されたこの式は，「余り」に関する式である。「$5x$ を 3 で割って余り 1 となる $x$ とそのときの商 $y$ を求める」問題だから，$x$ は合同式が用いられ，商 $y$ は整数の分類から考える。余りのうち成り立つものを一つ見つけることで議論が進行する。

**2°** 合同式を用いずに解答するなら次のように，一つの解を見つけて因数分解する【解答 2】，係数の絶対値が小さい文字について解く【解答 3】がある。

**【解答 2】**

$$5x - 3y = 1 \qquad \cdots\cdots①$$

①を満たす整数解として，$(x,\ y) = (2,\ 3)$ があるから，

$$5 \cdot 2 - 3 \cdot 3 = 1 \qquad \cdots\cdots②$$

①−②より，

$$5(x-2) - 3(y-3) = 0$$

$$5(x-2) = 3(y-3)$$

3，5 は互いに素だから，

$$5(x-2) = 3(y-3) = 15k \quad (k：整数)$$

$$\therefore \quad \boldsymbol{(x,\ y) = (3k+2,\ 5k+3)}$$

**【解答 3】**

$$y = \frac{5x-1}{3} = \frac{6x-x-1}{3}$$

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

$y$ は整数だから，整数 $m$ を用いて

$$m = \frac{x+1}{3}$$

と表せて，このとき，

$$\begin{cases} y = 2x - m \\ x = 3m - 1 \end{cases}$$

$$\therefore \quad \boldsymbol{(x,\ y) = (3m-1,\ 5m-2)}$$

**【注】**

**3°** 直線上の格子点（$x$, $y$ 座標がともに整数の点）を求める問題でもある。一つの解 $(-1,\ -2)$ や $(2,\ 3)$ が見つかれば，直線の傾き $\frac{5}{3}$ ごとに格子点が現れるとすぐにわかる。センター試験などでは傾きから解答するのが簡明でよい。

**4°** 【解答 2】【解答 3】で答えの表記が異なるが，（$k$，$m$ に代入すればわかる通り）もちろん同じ解（集合）となる。実際，$k = m - 1$ とおけばよい。全体としては一致する場合はどう答えても問題はない。

**5°** 【解答 3】で帯分数にする際は，分子の係数の絶対値が小さくなるように割り算する。

$$(5x-1=)3x + 2x - 1 = 6x - x - 1$$

のうち係数の絶対値が小さくなる後者で考えた方が一つの文字について解く回数が少なくなるため考えやすい。

**6°** 係数が大きいときには一つの解を求めるのが容易ではないため，Euclid の互除法を用いるか，上のように係数の絶対値の小さい文字で解くと考えるとよい。

例題 18

$157x + 68y = 3$ の整数解を求めよ。

**【解答】**

$$157 = 68 \cdot 2 + 21 \qquad \cdots\cdots①$$

$$68 = 21 \cdot 3 + 5 \qquad \cdots\cdots②$$

$$21 = 5 \cdot 4 + 1 \qquad \cdots\cdots③$$

これを逆に辿り，5，21 を消去すると，

$$1 = 21 - (68 - 21 \cdot 3) \cdot 4$$

$$= 21 \cdot 13 - 68 \cdot 4$$

$$= (157 - 68 \cdot 2) \cdot 13 - 68 \cdot 4$$

$=157\cdot13+68\cdot(-30)$

$\therefore\quad 157\cdot39+68\cdot(-90)=3$

これと与式で差をとり

$157(x-39)+68(y+90)=0$

$157(x-39)=-68(y+90)$

①，②，③より，Euclid の互除法から 157，68 は互いに素だから，$k$ を整数として，

$157(x-39)=-68(y+90)=157\cdot68k$

$\therefore\quad (\boldsymbol{x},\ \boldsymbol{y})=(\boldsymbol{68k+39},\ \boldsymbol{-157k-90})$

**【注】**

**1°**　Euclid の互除法を用いて一つの解を見つけることになる。途中で出てきた余り 21，5 を一文字消去の要領で式どうしを連立すると一つの解が見つけられる。今回のように，

$157x+68y=1$

の解が見つかれば

$157x+68y=3$

の右辺と対応させて 3 倍することで，一つの解を見つけられる。一連の流れが頭に入っているのが望ましいが，忘れてしまったら本質的に同じ操作である係数を割り算で小さくする方法をとればよい。

$(68\cdot2+21)x+68y=3$

$68(2x+y)+21x=3$

$(21\cdot3+5)(2x+y)+21x=3$

$21(7x+3y)+5(2x+y)=3$

$(5\cdot4+1)(7x+3y)+5(2x+y)=3$

$5(30x+13y)+(7x+3y)=3$

この方程式を満たす解として，

$$\begin{cases}30x+13y=0\\7x+3y=3\end{cases}\quad\therefore\quad\begin{cases}x=39\\y=-90\end{cases}$$

**2°**　係数の絶対値の小さい文字について解くと考えると，次のようになる。

**【解答 2】**

$$y=\frac{-157x+3}{68}=\frac{-(68\cdot2+21)x+3}{68}$$

$$=-2x-\frac{3(7x-1)}{68}$$

3，68 は互いに素で，$y$ は整数だから，$m$ を整数として，

$$m=\frac{7x-1}{68}\qquad\cdots\cdots④$$

とおけて，

$$y=-2x-3m\qquad\cdots\cdots⑤$$

④より，

$$x=\frac{68m+1}{7}=\frac{70m-2m+1}{7}$$

$$=10m-\frac{2m-1}{7}$$

$x$ は整数だから，$\ell$ を整数として，

$$\ell=\frac{2m-1}{7}\qquad\cdots\cdots⑥$$

とおけて，

$$x=10m-\ell\qquad\cdots\cdots⑦$$

⑥より，

$$m=\frac{7\ell+1}{2}=3\ell+\frac{\ell+1}{2}$$

$m$ は整数だから，$n$ を整数として，

$$n=\frac{\ell+1}{2}\qquad\cdots\cdots⑧$$

とおけて，

$$m=3\ell+n\qquad\cdots\cdots⑨$$

このとき，⑧より，

$\ell=2n-1$

だから，⑨より，

$m=3(2n-1)+n=7n-3$

⑦より，

$x=10(7n-3)-(2n-1)=68n-29$

⑤より，

$y=-2(68n-29)-3(7n-3)=-157n+67$

$\therefore\quad (\boldsymbol{x},\ \boldsymbol{y})=(\boldsymbol{68n-29},\ \boldsymbol{-157n+67})$

## 1.9　$ax+by$ がらみ

例題 17，例題18 で見たように，係数によって一つの解の求めやすさが異なることがわかった。さらに言えば，一つの解が求まるかどうかも分からない。そこで $ax+by=1$ の解の存在を証明する。

例題 19

$a$，$b$ はともに 2 以上の整数であり，互いに素であるとする。このとき，次を示せ。

(1)　$a$，$2a$，……，$(b-1)a$，$ba$ を $b$ で割ったと

きの余りはすべて異なる。

(2) $ax+by=1$ を満たす整数 $x$, $y$ の組 $(x, y)$ が存在する。

**【解答】**

(1) $i$, $j$ を $1 \leqq i < j \leqq b$ なる整数として，$ia$, $ja$ を $b$ で割ったときの余りが等しいと仮定する。差をとった

$$ja-ia=(j-i)a$$

は $b$ の倍数となる。$a$, $b$ は互いに素だから，$j-i$ が $b$ の倍数となる。$1 \leqq i < j \leqq b$ より，

$$0<j-i \leqq b-1$$

この範囲に $b$ の倍数は存在せず矛盾する。

したがって，$ia$, $ja$ を $b$ で割った余りはすべて異なる。 ■

(2) 整数を $b$ で割ったときの余りは 0, 1, 2, ……, $b-1$ の $b$ 種類であり，$a$, $2a$, ……, $(b-1)a$, $ba$ を $b$ で割ったときの余り $r_1$, $r_2$, ……, $r_b$ も互いに異なる $b$ 種類のものだから，

$$\{0,\ 1,\ 2,\ \cdots\cdots,\ b-1\}$$
$$=\{r_1,\ r_2,\ \cdots\cdots,\ r_b\}$$

が成り立つ。したがって，$r_1$, $r_2$, ……, $r_b$ の中に 1 であるものが 1 個存在する。それを $ka$ とすると，$k$ は $1 \leqq k \leqq b$ を満たす整数で，$b$ で割ったときの商を $\ell$（整数）と定めて，

$$ka=\ell b+1 \quad \therefore \quad ak+b(-\ell)=1$$

したがって，$ax+by=1$ を満たす整数 $x$, $y$ の組 $(x, y)$ が存在した。 ■

**【注】**

**1°** 「異なる」という否定命題だから背理法で示す。一般に集合の要素数の問題では，背理法ですべて異なることを示して議論していくことが基本となる。

**2°** (1)がポイントになっているのがよく分かる証明である。ここでは次の事実に従っている。

**部屋割り論法**

$m$, $n$, $q$ を自然数とする。

(i) $m$ 人を $n$ 部屋に割り当てるとき，$m \geqq nq+1$ なら $q+1$ 人以上入る部屋が存在する。

(ii) $n$ 人を $n$ 部屋に重複なく割り当てると，すべての部屋には必ず 1 人の人が割り当てられる。

(i)は $q=1$ で等号になった場合の「$n+1$ 人を $n$ 部屋に分けていれると 2 人以上入る部屋が存在する」という形で出題されることが多い。ここでは，(ii)の形が現れている。

$$\{0,\ 1,\ 2,\ \cdots\cdots,\ b-1\}$$
$$=\{r_1,\ r_2,\ \cdots\cdots,\ r_b\}$$

が言えることによって，部屋割り論法が使えている。存在証明では「具体的に見つける」のが基本方針となるが，見つけられないときに定理などを利用して，具体的に求められはしないが存在だけは分かるという形で証明する。この問題は部屋割り論法が使われる有名な例なのでしっかり理解しておくように。

**3°** この例題 19 の結果を用いて，p. 16 のフェルマー（Fermat）の小定理を示してもよい。

**フェルマーの小定理**〔再掲〕

$p$ を素数，$n$ と $p$ が互いに素とするとき，

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

が成り立つ。

**【証明 2】**

例題 19(1)の結果から，$kn$（$k=0,\ 1,\ 2,\ \cdots\cdots,\ p-1$）を $p$ で割った余りはすべて異なる $p$ 種類だから，$kn$ を $p$ で割った余りの集合は

$$\{0,\ 1,\ 2,\ \cdots\cdots,\ p-1\}$$

と一致する。したがって，$p$ を法として，

$$1\cdot 2\cdot\cdots\cdots\cdot(p-1) \equiv n\cdot 2n\cdot\cdots\cdots\cdot(p-1)n$$
$$(p-1)! \equiv (p-1)!\cdot n^{p-1}$$

$p$ は素数より，$(p-1)!$ と $p$ は互いに素だから，

$$n^{p-1} \equiv 1$$ ■

これに関連して，発展事項ではあるが，一般に次の事実が成り立つ。

**一次結合の整数全体の集合**

同時に 0 にならない整数 $a$, $b$ の最大公約

数を $g$ とするとき

(1) $ax+by=g$

を満たす整数 $x$，$y$ が存在する。

(2) $x$，$y$ が任意の整数のとき，$ax+by$ は $g$ の倍数全体を取りうる。つまり

$$\{ax+by \mid x,\ y \text{ は整数}\}$$
$$=\{gn \mid n \text{ は整数}\}$$

(3) $g=1$，$a>0$，$b>0$ のとき，$ab+1$ 以上のすべての自然数は，$x$，$y$ を正の整数として $ax+by$ の形で表される。

## 1.10 $p$ 進法

10 進法で 324.5 は，

$$324.5=3\cdot10^2+2\cdot10+4\cdot1+5\cdot10^{-1}$$

を意味している。これと同様に $p$ 進法を考えることができる。$p$ を 2 以上の自然数，$k$，$\ell$ を非負整数とするとき，任意の自然数 $N$ は，0 以上 $p-1$ 以下の整数 $a_i$（$-\ell\leqq i\leqq k$）を用いて，

$$N=a_kp^k+a_{k-1}p^{k-1}+\cdots+a_1p+a_0$$
$$+a_{-1}p^{-1}+\cdots+a_{-\ell}p^{-\ell}$$

とただ一通りに表すことができ，

$$a_ka_{k-1}\cdots a_1a_0\cdot a_{-1}\cdots a_{-\ell_{(p)}}$$

と表す。ただし，$a_k\neq0$ である。この方法を**$p$ 進法**といい，$N$ の $p$ 進法による表現を整数 $N$ の $p$ 進法表示とよぶ。10 進法で表すときは，$324_{(10)}$ の (10) を省略して単に 324 と書くことが多い。$p$ 進法で表されたとき，$a_i$ を $p^i$ ($i=k,\ k-1,\ \cdots,\ -\ell$) の位の数という。また，$p$ 進法を総称して，位取り記数法という。

$p$ 進法で表された数 を10 進法で表すといつも通りの計算に帰着できるので，$p$ 進法で数が与えられたときは上の定義により，10 進法に直すことを考える。例えば，

$$324_{(7)}=3\cdot7^2+2\cdot7+4\cdot1=165$$

となる。

例題 20

$n$ が 8 以上の偶数のとき，$n$ 進法で表された 2 つの数 1221，12432 の最大公約数 $g$ と最小公倍数 $\ell$ を，ともに $n$ 進法で表せ。

**【解答】**

$p$ 進法で $a$ と表される数を $a_{(p)}$ と表し，$p=10$ のときは $p$ を省略して $a$ と書くことにする。

$$1221_{(n)}=n^3+2n^2+2n+1$$
$$=(n+1)(n^2+n+1)$$
$$12432_{(n)}=n^4+2n^3+4n^2+3n+2$$
$$=(n^2+n+2)(n^2+n+1)$$

ここで，$n+1$，$n^2+n+2$ の最大公約数を $G$ とすると，互いに素な自然数 $a$，$b$ に対して，

$$\begin{cases} n+1=aG \\ n^2+n+2=bG \end{cases}$$

と表せるから，第 2 式から得られる

$$n(n+1)+2=bG$$

に第 1 式を用いて，

$$2=G(b-an)$$

$G>0$ より，$G=1$，2 となるが，$n$ が偶数より $n+1$ は奇数だから $G$ は奇数で，$G=1$。よって，$n+1$，$n^2+n+2$ は互いに素である。したがって，

$$g=n^2+n+1=111_{(n)}$$
$$\ell=(n+1)(n^2+n+2)(n^2+n+1)$$
$$=n^5+3n^4+6n^3+7n^2+5n+2$$
$$=136752_{(n)}$$

$n$ が 8 以上の偶数だから，これらはともに題意を満たす。よって，

$$g=\mathbf{111}_{(n)},\quad \ell=\mathbf{136752}_{(n)}$$

**【注】**

**1°** $n$ 進法の定義に注意する。

**2°** $n^3+2n^2+2n+1$ は，有理数解の性質に注意し，$n=-1$ を代入して 0 であることを見つけて因数分解する。$n^4+2n^3+4n^2+3n+2$ は代入して 0 になる一解が見つからないので，$n^3+2n^2+2n+1$ との最大公約数という問題文から，$n^2+n+1$ で割り切れないか考えることになる。

**3°** 最大公約数 $G$ の議論は互いに素でないと仮定して矛盾を導いても同じである。

**4°** $a=gA$，$b=gB$，$(A,\ B)=1$ のとき，最小公倍数 $\ell$ は，$\ell=ABg$

以上では $p$ 進法で表されたものを 10 進法に直したが，逆に 10 進法のものを $p$ 進法に直すこともある。例えば，10 進法で 294 と表された数を 5 進法で表すとき，5 の累乗 1，5，$5^2$，$5^3$ で表すので，

$$\begin{aligned}294&=250+25+15+4\\&=2\cdot5^3+1\cdot5^2+3\cdot5+4\cdot1\\&=2134_{(5)}\end{aligned}$$

と表せる。一般に $p$ 進法で表すときは，$p$ の累乗で表現することを考えればよい。ただし，累乗で表すのが面倒な場合は，先の式が

$$\begin{aligned}294&=5(2\cdot5^2+1\cdot5+3)+4\\&=5\{5(\underline{\underline{2}}\cdot5+\underline{\underline{1}})+\underline{\underline{3}}\}+\underline{\underline{4}}\end{aligned}$$

と変形できることに注意して，294 を 5 で割った余りと，そのときの商を 5 で割った余りについて考えればよいとわかる。したがって，

$$\begin{aligned}294&=5\cdot58+\underline{\underline{4}}\\58&=5\cdot11+\underline{\underline{3}}\\11&=5\cdot\underline{\underline{2}}+\underline{\underline{1}}\end{aligned}$$

と順次割り算し，最後の商から余りを逆に辿れば $2134_{(5)}$ と楽に表せる。

| | | | |
|---|---|---|---|
| 5 ) | 294 | | （余り） |
| 5 ) | 58 | … | $\underline{\underline{4}}$ |
| 5 ) | 11 | … | $\underline{\underline{3}}$ |
| | $\underline{\underline{2}}$ | … | $\underline{\underline{1}}$ |

次に 10 進法から $p$ 進法へ小数の形で表すことを考える。$N=0.376$ を 5 進法で表すと，

$$N=a_1\cdot5^{-1}+a_2\cdot5^{-2}+a_3\cdot5^{-3}$$

と表せたとして，

$$\begin{aligned}5N&=a_1+a_2\cdot5^{-1}+a_3\cdot5^{-2}\\(5N-a_1)\cdot5&=a_2+a_3\cdot5^{-1}\\\{(5N-a_1)\cdot5-a_2\}\cdot5&=a_3\end{aligned}$$

が成り立つから，$a_1$，$a_2$，$a_3$ はそれぞれ，$5N$，$(5N-a_1)\cdot5$，$\{(5N-a_1)\cdot5-a_2\}\cdot5$ の整数部分として求められる。

$$\begin{aligned}0.376\cdot5&=\underline{\underline{1}}.88\\0.88\cdot5&=\underline{\underline{4}}.4\\0.4\cdot5&=\underline{\underline{2}}\end{aligned}$$

したがって，$N=0.142_{(5)}$ と表せる。小数部分に 5 をかける様子を筆算で書くと次のようになる。

| | | |
|---|---|---|
| 5× ) | 0.376 | |
| 5× ) | $\underline{\underline{1}}$.880 | |
| 5× ) | $\underline{\underline{4}}$.40 | |
| | $\underline{\underline{2}}$.0 | |

$p$ 進法どうしの演算（加減乗除）はすぐにできそうな場合を除けば，10 進法に直して計算し，必要に応じて $p$ 進法に書き直せばよい。

## 1.11　講義用問題

**問題 1**

3 以上 9999 以下の奇数 $a$ で，$a^2-a$ が 10000 で割り切れるものをすべて求めよ。

**問題 2**

正の整数 $a$，$b$，$c$ が $a^2+b^2=c^2$ を満たすとき，次を示せ。

(1)　$a$，$b$ のいずれかは 3 の倍数である。

(2)　$a$，$b$ のいずれかは 4 の倍数である。

**問題 3**

$p$，$q$ を素数とし，2 次関数

$$f(x)=x^2+px+q$$

が次の 2 つの条件

(i)　ある実数 $a$ に対して，$f(a)<0$

(ii)　任意の整数 $n$ に対して，$f(n)\geqq 0$

をみたすとする。$f(x)$ を求めよ。