数学Ａ　整数の性質

～高校数学のまとめ～

教科書をもとに定義や定理を独自にパネル形式でまとめています．
何度も書き直し，加筆修正を繰り返しており，完成したものではありません．
人によっては不要な部分もあるでしょう．そういうときは読み飛ばしてください．

自然数と整数

$$\cdots, -3, -2, -1, \ 0, \ 1, \ 2, \ 3, \ 4, \ 5, \cdots$$

を **整数**（せいすう） という．

とくに

$$1, \ 2, \ 3, \ 4, \ 5, \cdots$$

を 正の整数 または **自然数**（しぜんすう） という．

整数の四則演算

2 つの整数 a，b に対して

和：$a+b$，　差：$a-b$，　積：ab　はすべて整数になる．

商：$a \div b = \dfrac{a}{b}$ $(b \neq 0)$ は整数にならないことがある．

例 2 つの整数 2，3 について

和：$2+3=5$，差：$2-3=-1$，積：$2\times 3=6$　はすべて整数になる．

商：$2 \div 3 = \dfrac{2}{3}$ は整数にならない

補 商：$\dfrac{a}{b}$ $(b \neq 0)$ は整数になることもある．

整数の除法

a を整数，b を正の整数 とすると

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

となる q，r は 1 通りに定まる．

このとき

q を a を b で割ったときの 商（しょう） という．

r を a を b で割ったときの 余（あま）り という．

とくに

$r = 0$ ならば a は b で 割り切れる という．

$r \neq 0$ ならば a は b で 割り切れない という．

$$\begin{array}{r} q \\ b\overline{)\ a} \\ \vdots \\ \hline r \end{array}$$

例 204，19 について

$204 = 19 \cdot 10 + 14$

204 を 19 で割ったときの商は 10，余りは 14

204 は 19 で割り切れない．

$$\begin{array}{r} 10 \\ 19\overline{)204} \\ \underline{19} \\ 14 \end{array}$$

例 204，12 について

$204 = 12 \cdot 17$

204 を 12 で割ったときの商は 17，余りは 0

204 は 12 で割り切れる．

$$\begin{array}{r} 17 \\ 12\overline{)204} \\ \underline{12} \\ 84 \\ \underline{84} \\ 0 \end{array}$$

分数式の変形

a を整数，b を正の整数とする．

a を b で割ったときの商が q，余りが r ならば

$$\frac{a}{b} = q + \frac{r}{b}$$

考 $\dfrac{a}{b} = \dfrac{bq + r}{b} = \dfrac{bq}{b} + \dfrac{r}{b} = q + \dfrac{r}{b}$

例 $\dfrac{204}{19} = 10 + \dfrac{14}{19}$

$\dfrac{204}{12} = 17$

約数と倍数

2 つの整数 a，b に対して

$$b = ak$$

を満たす整数 k が存在するとき

1 a は b の **約数**（やくすう） という．

2 b は a の **倍数**（ばいすう） という．

3 b は a で **割り切れる** という．ただし，$a > 0$

例 $6 = 2 \cdot 3$

1 2 は 6 の約数

2 6 は 2 の倍数

3 6 は 2 で割り切れる．

注 0 の倍数と約数については次のようになる．

1 $0 = ak$ とすると

任意の整数 a に対して $k = 0$ が存在する．

よって，0 の約数はすべての整数である．

2 $b = 0 \cdot k$ とすると

$b \neq 0$ ならば k は存在しない．

$b = 0$ ならば整数 k は無数に存在する．

よって，0 の倍数は 0 のみである．

3 割る数は 0 以外で考えるので「0 で割り切れる」とは言わない．

倍数の表記

a を 0 以外の整数とする．

a の倍数は

$$0，\ \pm a，\ \pm 2a，\ \pm 3a，\ \cdots$$

と無数にあり

$$ak（k \text{ は整数}）$$

と表せる．

例 3 の倍数は 0, ±3, ±6, ±9, … と無数にあり $3k$（k は整数）と表せる．

倍数の判定法

自然数が倍数になることを判定する方法が次のようにいくつかある.

倍数	判定法
2 の倍数	一の位が 0，2，4，6，8
3 の倍数	各位の和が 3 の倍数
4 の倍数	下 2 桁が 4 の倍数 または 00(偶数)
5 の倍数	一の位が 0，5 (5 の倍数)
6 の倍数	2 の倍数 かつ 3 の倍数
8 の倍数	下 3 桁が 8 の倍数 または 000
9 の倍数	各位の和が 9 の倍数
10 の倍数	一の位が 0
11 の倍数	最高位から一の位まで和と差の計算を繰り返した値が 11 の倍数
12 の倍数	3 の倍数 かつ 4 の倍数

㊟ 132 は一の位が 2(偶数) であるから 2 の倍数.
132 は 1＋3＋2＝6 (3 の倍数) であるから 3 の倍数.
312 は下 2 桁 12(4 の倍数) であるから 4 の倍数.
125 は一の位が 5(5 の倍数) であるから 5 の倍数.
132 は 2 の倍数かつ 3 の倍数であるから 6 の倍数.
3120 は下 3 桁 120(8 の倍数) であるから 8 の倍数.
153 は 1＋5＋3＝9(9 の倍数) であるから 9 の倍数.
120 は一の位が 0 であるから 10 の倍数.
91432 は 9－1＋4－3＋2＝11(11 の倍数) であるから 11 の倍数
312 は 3 の倍数かつ 4 の倍数であるから 12 の倍数.

素数と合成数

2 以上の自然数において

1 正の約数が 1 とその数自身のみである数を **素数**（そすう） という.

2 素数ではないものを **合成数**（ごうせいすう） という.

例 1 素数を小さい順に並べると 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, …
2 合成数を小さい順に並べると 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, …

素因数分解

整数がいくつかの積で表されるとき，それぞれの整数をもとの数の **因数**（いんすう） といい

素数である因数を **素因数**（そいんすう） という.

自然数を素数だけの積の形に表すことを **素因数分解**（そいんすうぶんかい） するという.

素因数分解は積の順序を考えなければ 1 通りに定まる.（素因数分解の一意性）

例 60 を素因数分解すると $60 = 2^2 \cdot 3 \cdot 5$
2，3，5 は素数なので素因数という.
注 $60 = 12 \cdot 5$ は 12 が素数ではないので素因数分解とは言わない.

整数の正の約数の個数

正の整数 N を素因数分解し

$$N = p^a q^b r^c \cdots$$（$p, q, r, \cdots$ は異なる素数，$a, b, c, \cdots$ は正の整数）

と表せるとき，正の約数の個数は

$$(a+1)(b+1)(c+1)\cdots$$

（各素数の指数に 1 をたしてかけていく）

例 $504 = 2^3 \cdot 3^2 \cdot 7$
504 の正の約数は $2^x 3^y 7^z$（$x = 0, 1, 2, 3$　$y = 0, 1, 2$　$z = 0, 1$）
504 の正の約数の個数は 組 (x, y, z) の組数で $(3+1)(2+1)(1+1) = 4 \cdot 3 \cdot 2 = 24$（個）

公約数と最大公約数

2 つ以上の整数に共通する約数を，それらの**公約数**（こうやくすう）という．

また，ともに 0 でない 2 つの整数の
公約数のうちで最大のものを **最大公約数**（さいだいこうやくすう）という．

これは G.C.M. または G.C.D とかくことがある．

補 最小公倍数は英語で「Greatest Common Measure」または「Greatest Common Divisor」
例 24 と 36 の公約数は ±1, ± 2, ± 3, ± 4, ± 6, ± 12
　24 と 36 の最大公約数は 12
注 0 と 0 の公約数はすべての整数であり，最大公約数は存在しない．

公倍数と最小公倍数

2 つ以上の整数に共通する倍数を，それらの**公倍数**（こうばいすう）という．

また，ともに 0 でない 2 つの整数の
正の公倍数のうちで最小のものを **最小公倍数**（さいしょうこうばいすう）という．

これは L.C.M. とかくことがある．

補 最小公倍数は英語で「Least Common Multiple」
例 24 と 36 の公倍数は 0, ± 72, ± 144, ± 216, …
　24 と 36 の最小公倍数は，正の公倍数のうちで最小のものより 72
注 0 と 0 の公倍数は 0 のみであり，最小公倍数は定義しない．

max の記号

実数 a，b のうち小さくない方を

$$\max\{a, b\}$$

と表す．すなわち

$$\max\{a, b\} = \begin{cases} a & (a \geqq b) \\ b & (a < b) \end{cases}$$

㊟ a，b のうちの「最大の値」と定義してもよいが，$a = b$ のとき，最大の値が決まらないので，「小さくない方」と定義している．

㊐ $\max\{3, 5\} = 5$，　$\max\{3, 3\} = 3$

min の記号

実数 a，b のうち大きくない方を

$$\min\{a, b\}$$

と表す．すなわち

$$\min\{a, b\} = \begin{cases} a & (a \leqq b) \\ b & (a > b) \end{cases}$$

㊟ a，b のうちの「最小の値」と定義してもよいが，$a = b$ のとき，最小の値が決まらないので，「大きくない方」と定義している．

㊐ $\min\{3, 5\} = 3$，　$\min\{3, 3\} = 3$

素因数分解された 2 つの整数の最小公倍数と最大公約数

2 つの正の整数 M，N をそれぞれ素因数分解し

$M = p^x q^y r^z \cdots$（p, q, r, … は異なる素数，x, y, z, … は 0 以上の整数）

$N = p^s q^t r^u \cdots$（p, q, r, … は異なる素数，s, t, u, … は 0 以上の整数）

と表せるとき，次が成り立つ．

1 M と N の最小公倍数 は

$$p^{\max\{x,s\}} q^{\max\{y,t\}} r^{\max\{z,u\}} \cdots$$

ただし $\max\{a, b\}$ は a，b のうち小さくない方を表す．
（各素数の指数で最大のものをかけていく）

2 M と N の最大公約数 は

$$p^{\min\{x,s\}} q^{\min\{y,t\}} r^{\min\{z,u\}} \cdots$$

ただし $\min\{a, b\}$ は a，b のうち大きくない方を表す．
（各素数の指数で最小のものをかけていく）

3 M と N の公倍数 は 最小公倍数の倍数である．

4 M と N の公約数 は 最大公約数の約数である．

例 $72 = 2^3 \cdot 3^2$

$240 = 2^4 \cdot 3 \cdot 5$

1 72 と 240 の最小公倍数は $2^4 \cdot 3^2 \cdot 5 = 720$

2 72 と 240 の最大公約数は $2^3 \cdot 3 = 24$

3 72 と 240 の公倍数は 720 の倍数である

4 72 と 240 の公約数は 24 の約数である

互いに素

2 つの整数 a，b の最大公約数が 1 であることを

a と b は 互(たが)いに素(そ) であるという．

このとき a と b は共通の素因数をもたない．

例 5 と 6 の最大公約数は 1 であるから 5 と 6 は互いに素である．

注 素数ではない

互いに素な整数の性質

a，b，c は整数で，a，b が互いに素であるとすると，次が成り立つ．

1 ac が b の倍数であるならば c は b の倍数である．

2 a の倍数 かつ b の倍数である整数は ab の倍数である．

例 1 c を整数とする．$3c$ が 4 の倍数であるならば c は 4 の倍数である．

2 2 の倍数かつ 3 の倍数である整数は 6 の倍数である．

最大公約数と最小公倍数の性質

2 つの整数 a，b の最大公約数を G，最小公倍数を L とすると

$$\begin{cases} a = Ga' \\ b = Gb' \end{cases} \quad (a',\ b' \text{ は互いに素})$$

と表せて

1 $L = Ga'b'$

2 $ab = GL$

例 $a = 24$ と $b = 36$ の最大公約数は $G = 12$

$$\begin{cases} a = 12 \cdot 2 \\ b = 12 \cdot 3 \end{cases} \quad (2,\ 3 \text{ は互いに素})$$

と表せて

1 $L = 12 \cdot 2 \cdot 3 = 72$

2 $ab = 12 \cdot 12 \cdot 2 \cdot 3 = 12 \cdot 72 = GL$

最大公約数の性質

$(a, b) \neq (0, 0)$ とする．

2 つの整数 a，b の最大公約数 を $g(a, b)$ とすると

1 $g(a, b) = g(b, a)$

2 $g(a, b) = g(|a|, |b|)$

3 $g(a, 0) = |a|$

例 1 $g(24, 36) = g(36, 24) = 12$

2 $g(-24, 36) = g(|-24|, |36|) = g(24, 36)$

3 $g(5, 0) = |5| = 5$

ユークリッドの互除法

2 つの整数 x，y の最大公約数を $g(x, y)$ と表すとする．

$(a, b) \neq (0, 0)$ とし，整数 a，b に対して，整数 q，r が存在し

$$a = bq + r$$

と表されるとき

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

考　$a = bq + r$ ……㊟

とおき，$g(a, b) = m$，$g(b, r) = n$ とする．

m は a と b の公約数であるから，㊟ により m は r の約数である．

これより m は b と r の公約数である．

b と r の最大公約数は n であるから　$m \leqq n$ ……①

また，n は b と r の公約数であるから，㊟ により n は a の約数である．

これより n は a と b の公約数である，

a と b の最大公約数は m であるから　$n \leqq m$ ……②

よって，①，② により $m = n$　すなわち　$g(a, b) = g(b, r)$

例 $204 = 36 \cdot 5 + 24$

$36 = 24 \cdot 1 + 12$

$24 = 12 \cdot 2 + 0$

	2	1	5
12	24	36	204
	24	24	180
	0	12	24

$g(204, 36) = g(36, 24) = g(24, 12) = g(12, 0) = 12$

つまり，204 と 36 の最大公約数は 12

ユークリッドの互除法 2

2 つの整数 x，y の最大公約数を $g(x, y)$ と表すとする．
$(a, b) \neq (0, 0)$ とし，整数 a，b に対して，整数 k があり

$$g(a, b) = g(a - bk, b)$$

㊟ 一方の数字から他方の数字を整数倍してひく値は一方の数字と最大公約数が同じ．

㊟ 整数 a，b に対して，整数 k，r が存在し

$$a = bk + r$$

と表されるならば，ユークリッドの互除法から

$$\begin{aligned} g(a, b) &= g(b, r) \\ &= g(r, b) \end{aligned}$$

$r = a - bk$ であることから

$$g(a, b) = g(a - bk, b)$$

㊟ $g(204, 36) = g(204 - 36 \cdot 5, 36) = g(24, 36) = 12$

㊟ $g(204, 36) = g(204 - 36 \cdot 6, 36) = g(-12, 36) = g(12, 36) = 12$

余りによる整数の分類

整数を 2 以上の整数 m で割ったときの余りは

$$0,\ 1,\ 2,\ \cdots,\ m-1$$

のいずれかになる.

これより，整数は **余りの数** で分類できる.

例 整数を 2 で割ったときの余りは $0, 1$ のいずれかである.
つまり，整数は偶数と奇数に分類できる.

例 整数を 3 で割ったときの余りは $0, 1, 2$ のいずれかである.
つまり，整数は 3 で割った余りが 0，1，2 となる数に分類できる.

余りがわかる整数の表記

整数 a を 2 以上の整数 m で割ったときの余りが r $(r = 0, 1, 2, \cdots, m-1)$

のとき

$$a = (m \text{ の倍数}) + r$$

であるから 整数 k を用いて $a = mk + r$ と表せる.

また $r = m - s$ ならば

$$a = (m \text{ の倍数}) - s$$

であるから 整数 k を用いて $a = mk - s$ と表すこともできる.

例 整数 a が 3 で割ったときの余りが 2 であるとき

$a = (3 \text{ の倍数}) + 2$

であるから 整数 k を用いて $a = 3k + 2$ と表せる.

また $2 = 3 - 1$ なので

$a = (3 \text{ の倍数}) - 1$

であるから 整数 k を用いて $a = 3k - 1$ と表せる.

連続する整数の性質

連続する n 個の整数について

1 それぞれを n で割ったときの余りはすべて異なる

2 n の倍数が 1 つだけある

例 連続する 3 個の整数 4，5，6 について

1 それぞれ 3 で割ると，余りは 1，2，0 とすべて異なる．

2 6 だけが 3 の倍数である．

連続する 2 つの整数の積

n を整数とする．

連続する 2 個の整数の積 $n(n+1)$ は 2 の倍数である．

考 n，$n+1$ は一方が偶数，他方が奇数であるから $n(n+1)$ は 2 の倍数である．

連続する整数の積

n を正の整数とする．

0 を含まない連続する n 個の整数の積は $n!$ の倍数である．

すなわち

1 連続する 2 個の整数の積は $2! = 2$ の倍数である．

2 連続する 3 個の整数の積は $3! = 6$ の倍数である．

⋮

例 1 m を整数として積 $m(m+1)$ は 2 の倍数である．

2 m を整数として積 $m(m+1)(m+2)$ は 6 の倍数である．

考 正の整数で連続する n 個の整数の積は，N を n 以上の整数として

$$\underbrace{N(N-1)(N-2)\cdots(N-n+1)}_{n\text{ 個}} = n!{}_N\mathrm{C}_n \text{ で } n! \text{ の倍数.}$$

負の整数で連続する n 個の整数の積は N を n 以上の整数として

$$\underbrace{(-N)\{-(N-1)\}\{-(N-2)\}\cdots\{-(N-n+1)\}}_{n\text{ 個}} = n!(-1)^n{}_N\mathrm{C}_n \text{ で } n! \text{ の倍数.}$$

倍数の個数

n を自然数，p を 2 以上の整数とする．

実数 x をこえない最大の整数を $[x]$ として

1 以上 n 以下の整数のうち p の倍数の個数は $\left[\dfrac{n}{p}\right]$

例 1 以上 100 以下の整数のうち 4 の倍数の個数は 4, 8, 12, …, 100 の $\left[\dfrac{100}{4}\right]=25$（個）

1 以上 100 以下の整数のうち 3 の倍数の個数は 3, 6, 9, …, 99 の $\left[\dfrac{100}{3}\right]=33$（個）

階乗を割り切る整数の最大個数

n を 2 以上の整数，p を素数とする．

1 $n!$ を割り切る p の最大個数

2 $n!$ を素因数分解したときの素因数 p の個数

3 $n!=p^m k$（k は整数）を満たす最大の整数 m の値

1, 2, 3 の個数はすべて同じであり $[x]$ が x を超えない最大の整数を表すとして

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots$$

例 $10!=10\cdot9\cdot8\cdot7\cdot6\cdot5\cdot4\cdot3\cdot2\cdot1$

$10!$ を素因数分解したときの素因数 2 の個数は，次のような表を考えると求まる．

素因数 2 を ○ で表し，○ の個数を数える．

1	2	3	4	5	6	7	8	9	10
	○		○		○		○		○
			○				○		
							○		

行（横の並び）ごとに考えると○が周期的に出てくることがわかる．

つまり，○ の数は

（2 の倍数）＋（2^2 の倍数）＋（2^3 の倍数）

であるから

$$\left[\frac{10}{2}\right]+\left[\frac{10}{2^2}\right]+\left[\frac{10}{2^3}\right]=5+2+1=8$$

合同式

a，b は整数，p は 2 以上の整数とする．

$a-b$ が p の倍数である

つまり

$\left(\ a\ \text{を}\ p\ \text{で割ったときの余り}\ \right)=\left(b\ \text{を}\ p\ \text{で割ったときの余り}\ \right)$

であるとき a と b は p を法(ほう)として 合同(ごうどう) といい $a\equiv b\pmod{p}$ と表す．

このような式を 合同式(ごうどうしき) という．

例 $11-5=6$ は 3 の倍数である．
つまり 11 と 5 は 3 で割ったときの余りが等しい．
11 と 5 は 3 を法として合同といい $11\equiv 5\pmod{3}$ と表す．

合同式の性質

a，b，c は整数，p は 2 以上の整数とする．

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

2 $a\equiv b\pmod{p}$ ならば $b\equiv a\pmod{p}$

3 $\begin{cases} a\equiv b\pmod{p} \\ b\equiv c\pmod{p} \end{cases}$ ならば $a\equiv c\pmod{p}$

考 1 $a-a=0$ は p の倍数であるから $a\equiv a\pmod{p}$
2 $a\equiv b\pmod{p}$ ならば $a-b$ は p の倍数である．
このとき $b-a=-(a-b)$ より $b-a$ は p の倍数である．
よって $b\equiv a\pmod{p}$
3 $\begin{cases} a\equiv b\pmod{p} \\ b\equiv c\pmod{p} \end{cases}$ ならば $a-b$，$b-c$ はともに p の倍数であるから
整数 k，l を用いて $\begin{cases} a-b=pk \\ b-c=pl \end{cases}$ 表せて，辺々たして $a-c=p(k+l)$
$a-c$ は p の倍数であるから $a\equiv c\pmod{p}$ である．

合同式の和・差・積・累乗

a，b は整数，p は 2 以上の整数とする．

$$\begin{cases} a \equiv b \pmod{p} \\ c \equiv d \pmod{p} \end{cases}$$

のとき

1 $a+c \equiv b+d \pmod{p}$

2 $a-c \equiv b-d \pmod{p}$

3 $ac \equiv bd \pmod{p}$

4 $a^n \equiv b^n \pmod{p}$（$n = 1, 2, 3, \cdots$）

考 $\begin{cases} a \equiv b \pmod{p} \\ c \equiv d \pmod{p} \end{cases}$ のとき，整数 k，l を用いて

$\begin{cases} a-b = kp \\ c-d = lp \end{cases}$ すなわち $\begin{cases} a = kp+b \\ c = lp+d \end{cases}$

と表せる．

1 $(a+c)-(b+d) = (a-b)+(c-d) = kp+lp = (k+l)p$

よって $(a+c)-(b+d)$ は p の倍数であるから $a+c \equiv b+d \pmod{p}$ である．

2 $(a-c)-(b-d) = (a-b)-(c-d) = kp-lp = (k-l)p$

よって $(a-c)-(b-d)$ は p の倍数であるから $a-c \equiv b-d \pmod{p}$ である．

3 $ac-bd = (b+kp)(d+lp)-bd = (kd+lb+klp)p$

よって $ac-bd$ は p の倍数であるから $ac \equiv bd \pmod{p}$ である．

4 $a^n-b^n = (a-b)(a^{n-1}+a^{n-2}b+\cdots+b^{n-1}) = kp(a^{n-1}+a^{n-2}b+\cdots+b^{n-1})$

ここで $(a^{n-1}+a^{n-2}b+\cdots+b^{n-1})$ は整数である．

よって a^n-b^n は p の倍数であるから $a^n \equiv b^n \pmod{p}$ である．

別 3 が成り立つことから $a \cdot a \equiv c \cdot c \pmod{p}$ すなわち $a^2 \equiv b^2 \pmod{p}$

さらに $a^2 \cdot a \equiv b^2 \cdot b \pmod{p}$ すなわち $a^3 \equiv b^3 \pmod{p}$

これを繰り返して $a^n \equiv b^n \pmod{p}$ である．

合同式と割り算

a，b，k を整数，p を 2 以上の整数，n を自然数とする．

$ka \equiv kb \pmod{p}$ かつ k と p が互いに素 であるとき

$$a \equiv b \pmod{p}$$

考 $ka \equiv kb \pmod{p}$ ならば $ka - kb = k(a-b)$ は p の倍数である．
k と p が互いに素なので $a-b$ は p の倍数である．

合同式の準公式

a，b は整数，p は 2 以上の整数とする．

1 $a \equiv 1 \pmod{p}$ ならば $a^n \equiv 1 \pmod{p}$

2 $a \equiv -1 \pmod{p}$ ならば $a^n \equiv (-1)^n \pmod{p}$

3 $a^2 \equiv a \pmod{p}$ ならば $a^n \equiv a \pmod{p}$

考 1 合同式の和・差・積・累乗 4 より
$a \equiv 1 \pmod{p}$ ならば $a^n \equiv 1^n \equiv 1 \pmod{p}$
2 合同式の和・差・積・累乗 4 より
$a \equiv -1 \pmod{p}$ ならば $a^n \equiv (-1)^n \pmod{p}$
3 $a^2 \equiv a \pmod{p}$ ならば $a \equiv a \pmod{p}$ も成り立つことから
$a^2 \cdot a \equiv a \cdot a \pmod{p}$
すなわち $a^3 \equiv a^2 \equiv a \pmod{p}$
これを繰り返して $a^n \equiv a \pmod{p}$

倍数と剰余

a，p が互いに素な整数とするとき

$$a,\ 2a,\ 3a,\ \cdots,\ (p-1)a$$

の $(p-1)$ 個の整数は p で割ったときの余りがすべて異なる．

㊟ ある 2 つの整数 m，n が存在し $1 \leqq n < m \leqq p-1$ を満たすもとで
ma と na が p で割ったときの余りが等しいと仮定すると
$ma \equiv na \pmod{p}$ すなわち $(m-n)a \equiv 0 \pmod{p}$
ところが $0 < m-n \leqq p-1 < p$ より $(m-n)$ は p の倍数ではない．
a，p が互いに素であることから $(m-n)a$ は p で割り切れることはないので矛盾．
よって 2 つの整数は存在しないので示された．

フェルマーの小定理

a を自然数，p を素数 とするとき

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

とくに

$$a \text{ と } p \text{ が互いに素ならば } \ a^{p-1} \equiv 1 \pmod{p}$$

㊟ $a,\ 2a,\ 3a,\ \cdots,\ (p-1)a$ は p で割ったときの余りがすべて異なるので
$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a = (p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$
$(p-1)!$ と p は互いに素であるから $a^{p-1} \equiv 1 \pmod{p}$

㊟ $3^5 \equiv 3 \pmod{5}$
3 と 5 は互いに素であるから $3^4 \equiv 1 \pmod{5}$

㊟ $1^6 \equiv 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \pmod{7}$

互いに素と整数解

互いに素である 2 つの整数 a，b と 2 つの整数 X，Y について

$aX = bY$ が成り立つとき

X は b の倍数 かつ Y は a の倍数 であるから 整数 k を用いて

$$\begin{cases} X = bk \\ Y = ak \end{cases}$$

と表せる．

㋐ X，Y を整数として $2X = 3Y$ が成り立つとき

2 と 3 は互いに素なので X は 3 の倍数 かつ Y は 2 の倍数であるから

$$\begin{cases} X = 3k \\ Y = 2k \end{cases} \quad (k \text{ は整数})$$

と表せる．

1 次不定方程式と整数解

a，b，c は 0 以外の整数とする．

x，y の 1 次不定方程式

$$ax + by = c \quad \cdots\cdots①$$

の整数解 (x, y) は次の手順で求める方法がある．

1 まず，① をみたす整数解を 1 組求める．

つまり

$$ax_0 + by_0 = c \quad \cdots\cdots②$$

となる ① の整数解 $(x, y) = (x_0, y_0)$ を 1 つさがす．

2 ① − ② として

$$a(x - x_0) + b(y - y_0) = 0$$

すなわち $a(x - x_0) = b(y_0 - y)$

3 $x - x_0$，$y_0 - y$ が整数であることから整数解 を求める．

例 $4x - 3y = 1$ ……①

をみたす整数の組 (x, y) をすべて求める．

1 $4 \cdot 1 - 3 \cdot 1 = 1$ ……②

2 ① − ② として

$4(x - 1) - 3(y - 1) = 0$

すなわち $4(x - 1) = 3(y - 1)$

3 3 と 4 は互いに素であるから整数 k を用いて

$$\begin{cases} x - 1 = 3k \\ y - 1 = 4k \end{cases}$$

よって $\boldsymbol{(x, y) = (3k + 1,\ 4k + 1)\ (k = 0, \pm 1, \pm 2, \cdots)}$

1 次不定方程式と整数解の存在 Ⅰ

a，b は 0 以外の整数の定数とする．

a と b が互いに素であるならば

$ax+by=1$ を満たす整数の組 (x, y) が存在する

㊟ a と b が互いに素であるとき

a，$2a$，$3a$，…，$(b-1)a$

の $(b-1)$ 個を b で割ったときの余りはすべて異なる

これより，ka を b で割ると余りが 1 になるような 1 以上 $b-1$ 以下の整数 k が存在し

商を q として　$ka=qb+1$　すなわち　$ak+(-q)b=1$　と表せる．

よって　$(x, y)=(k, -q)$　として　$ax+by=1$　をみたす整数の組 (x, y) が存在する．

1 次不定方程式と整数解の存在 Ⅱ

a，b は 0 以外の整数の定数とする．

$ax+by=1$ を満たす整数の組 (x, y) が存在するならば

a と b は互いに素である．

㊟ a と b が互いに素でないと仮定すると，a と b は 2 以上の公約数 d をもつから

$ax+by$ は d の倍数になるから 1 になることはない．

つまり

「a と b が互いに素でない」ならば

「$ax+by=1$　をみたす整数の組 (x, y) が存在しない」が成り立つ．

対偶を考えて

「$ax+by=1$　をみたす整数の組 (x, y) が存在する」ならば

「a と b は互いに素である」も成り立つ．

10 進法の記数法

10^nの位	10^{n-1}の位	…	10^2の位	10 の位	1 の位
a_n	a_{n-1}	…	a_2	a_1	a_0

（a_n, a_{n-1}, …, a_2, a_1, a_0 は 0 以上の 9 以下の整数で，$a_n \neq 0$）

となる数は，最高位が 0 でなく，各位は 0, 1, …, 9 の 10 個で表せて，

この表記法を **10進法**（しんほう） という．

これは，普段使っている数字であり

$$a_n a_{n-1} \cdots a_2 a_1 a_0$$
$$= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0$$

の形で表せる．

例 $3521 = 3 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10 + 1$

p 進法の記数法

p^nの位	p^{n-1}の位	…	p^2の位	p の位	p^0の位
a_n	a_{n-1}	…	a_2	a_1	a_0

（a_n, a_{n-1}, …, a_2, a_1, a_0 は 0 以上の $p-1$ 以下の整数で，$a_n \neq 0$）

となるような数は，最高位は 0 でなく，各位は 0, 1, …, $p-1$ の p 個で表せて，

この表記法を p **進法**（しんほう） という．

各位の数字を最高位から並べて

$$a_n a_{n-1} \cdots a_2 a_1 a_0\ (p)$$

と表し，これを **位取り記数法**（くらいどりきすうほう） という．

注意として，10 進法のときは $_{(10)}$ を省略する．

$$a_n a_{n-1} \cdots a_2 a_1 a_0\ (p)$$
$$= a_n p^n + a_{n-1} p^{n-1} + \cdots + a_2 p^2 + a_1 p^1 + a_0$$

の形で表せる．

例 $2101_{(3)} = 2 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3 + 1 = 64_{(10)} = 64 = 6 \cdot 10 + 4$

10 進法の小数点以下の記数法

$\frac{1}{10}$ の位	$\frac{1}{10^2}$ の位	$\frac{1}{10^3}$ の位	…
b_1	b_2	b_3	…

（b_1, b_2, b_3, … は 0 以上の 9 以下の整数）

となるような整数部分が 0 の 10 進法の小数は

$$0.b_1b_2b_3\cdots$$
$$= \frac{b_1}{10} + \frac{b_2}{10^2} + \frac{b_3}{10^3} + \cdots$$

の形で表せる．

例 $0.2956 = \frac{2}{10} + \frac{9}{10^2} + \frac{5}{10^3} + \frac{6}{10^4}$

p 進法の小数の記数法

$\frac{1}{p}$ の位	$\frac{1}{p^2}$ の位	$\frac{1}{p^3}$ の位	…
b_1	b_2	b_3	…

（b_1, b_2, b_3, … は 0 以上の $p-1$ 以下の整数）

となるような整数部分が 0 の p 進法の小数は

$$0.b_1b_2b_3\cdots_{(p)}$$
$$= \frac{b_1}{p} + \frac{b_2}{p^2} + \frac{b_3}{p^3} + \cdots$$

の形で表せる．

注意として，10 進法のときは $_{(10)}$ を省略する．

例 $0.2101_{(3)} = \frac{2}{3} + \frac{1}{3^2} + \frac{0}{3^3} + \frac{1}{3^4}$

既約分数が有限小数になる条件

整数でない既約分数 $\frac{n}{m}$ について

m の素因数は 2，5 だけからなる $\iff$ $\frac{n}{m}$ は有限小数で表される

すなわち

分母の素因数が 2 と 5 のみである既約分数であることと有限小数であることは同値である．

㊟ $0.013 = \frac{13}{1000} = \frac{13}{2^3 5^3}$

有限小数を既約分数にすると分母は 2 と 5 のみの素因数になる

㊟ ($\Longrightarrow$ について)

分母 m の素因数は 2，5 だけからなるとすると，0 以上の整数 a，b を用いて

$$|m| = 2^a \cdot 5^b$$

と表せる．このとき

$$\left|\frac{n}{m}\right| = \left|\frac{n}{2^a \cdot 5^b}\right| = \left|\frac{2^b \cdot 5^a \cdot n}{2^a \cdot 5^b \cdot 2^b \cdot 5^a}\right| = \left|\frac{2^b \cdot 5^a \cdot n}{10^{(a+b)}}\right|$$

となる．

よって，$2^b \cdot 5^a \cdot n$ は整数であるから $\frac{n}{m}$ は有限小数である．

($\Longleftarrow$ について)

$\frac{n}{m}$ は有限小数で表されるとすると

$\frac{n \cdot 10^k}{m}$ が整数となるような自然数 k が存在する．

m と n は互いに素なので，m は $10^k = 2^k \cdot 5^k$ の約数である．

よって，分母 m の素因数は 2 と 5 だけからなる．