整数

2010/6/15 更新

この章では，とくに断らなくても文字は整数.

A 整数の除法

任意の整数 a, b (ただし $b>0$) に対し

$$a=bq+r \quad (0 \leqq r < b)$$

をみたす整数 q，r がただ1組存在する. $\cdots$🎀

このような q，r を，a を b で割ったときの**商**，**余り**という.

〈例〉 $-28=5\cdot(-6)+2$

より，-28 を 5 で割ったときの商と余りは

商：-6，余り：2.

B 約数・倍数

(1) 2つの整数 a，b ($b \neq 0$) に対して

$$a=bq$$

をみたす整数 q（負でもかまわない）が存在するとき，a は b で**割り切れる**（b は a を整除する）といい，記号

$b \mid a$ （例：$3 \mid 9$, $25 \mid 100$, $5 \nmid 8$）

で表す. またこのとき，a を b の**倍数**，b を a の**約数**という.

〈注1〉$-6=3\cdot(-2)$ であるから，-6(負) は 3 の倍数である. 3 の倍数を列記すると

$\ldots,\ -9,\ -6,\ -3,\ 0,\ 3,\ 6,\ 9,\ \ldots.$

また，$6=(-2)\cdot(-3)$ だから，-2 は6の約数である. 6 の約数を全部書くと

$1,\ 2,\ 3,\ 6,\ -1,\ -2,\ -3,\ -6.$

〈注2〉$\underline{0}=2\cdot 0$, $\underline{0}=6\cdot 0$, $\underline{0}=2007\cdot 0$, $\ldots$

であるから，$\underline{0}$ は任意の整数の倍数 (任意の整数は 0 の約数) である. すなわち，

(任意の整数) $\mid 0$.

(2) 2つ（以上）の整数 a, b $(,\cdots)$ に共通な倍数，約数を，それぞれ a, $b(,\ \cdots)$ の**公倍数**，**公約数**という. 正なる最小の公倍数を**最小公倍数** (L.C.M.：least common multiple) という. また，最大なる公約数を**最大公約数** (G.C.D.：greatest common divisor) といい，

記号 $(a,\ b,\ \cdots)$

で表すことがある.

一般に,「公倍数は最小公倍数の倍数」であり,「公約数は最大公約数の約数」である.

C 素数

ちょうど2つの正の約数をもつ正整数，すなわち，1と自分自身以外に約数をもたない正整数から1を除いたものを，**素数**という. 1でも素数でもない正整数を**合成数**という.

(1) 素因数分解の一意性 (初等整数論の基本定理)

1を除く任意の正整数 n は，異なる素数 p，q，r，$\cdots$ と正整数 α, β, γ, $\cdots$ を用いて

$$n=p^{\alpha}q^{\beta}r^{\gamma}\cdots \qquad \cdots(*)$$

の形に（現れる素数の順序を除いて）ただ1通りに表される. $(*)$ の右辺を n の**素因数分解**という.

〈例〉 $\begin{cases} 60=2^2\cdot 3\cdot 5, \\ 24=2^3\cdot 3 \end{cases}$ ← 60,24 の素因数分解

より，60 と 24 について

G.C.D. $=2^2\cdot 3=12$, ←（各素因数の最小次数を選ぶ）

L.C.M. $=2^3\cdot 3\cdot 5=120$. ←（各素因数の最大次数を選ぶ）

(2) 素数の基本性質

以下において，p は素数とする.

ⓐ $ab=p$ $(a,\ b>0)$ ならば $(a,\ b)=(1,\ p)$ or $(p,\ 1)$.

ⓑ $p \mid ab$ ならば $p \mid a$ or $p \mid b$.

〈例〉$3 \mid a^2(=a\cdot a)$ ならば，$3 \mid a$.

〈注〉$9 \mid a^2(=a\cdot a)$ でも，$\underset{3^2}{9} \mid a$ とは限らない!

D 互いに素

2つ（以上）の整数 a，b（，$\cdots$）が1以外に正の公約数をもたないとき，これらの整数は**互いに素**であるという. この用語については，次の2通りの言い換えができる.

- 「**共通素因数をもたない.**」
- 「最大公約数 $(a,\ b,\ \cdots)=1$」

a, b が互いに素であることの基本用法として，次の3つがある.

ⓐ：$ax=by$ ならば $b \mid x$ かつ $a \mid y$. $\cdots$☼

ⓑ：$ab \mid n \Longleftrightarrow a \mid n$ かつ $b \mid n$.

ⓒ：$ab=n^2$ ならば a, b はいずれも平方数.

(☼が成立する理由は $\boxed{\text{F}}$(1) の解答で.)

$\boxed{\text{E}}$ 整数の特性→攻め方 ♦

↑ぶっちゃけ入試問題の解き方

有理数にはない，整数独自の 2 つの特性に注目！

(1) “余り”を用いた独自の除法
→「余り」「約数」など，整数固有の概念に注目する．

(2) 有限区間には有限個しか要素をもたない．
→値の範囲を絞り込む．

$\boxed{\text{F}}$ 不定方程式

$x,\, y$ に関する次の各方程式は，未知数が複数個あるのに対して条件が 1 つしかない．このような「不定方程式」を $x,\, y$ が整数であるという付帯条件のもとに解いてみよう．

(1) $5x = 4y$

(2) $x^2 - 4y^2 = 5$

(3) $x^2 + 4y^2 = 5$

〔解答〕

(1) 5 と 4 が互いに素であることに注目する．

- $4 \mid 4y$ (右辺).
- よって $4 \mid 5x$ (左辺).
- しかるに，$5{\cdot}x$ のうち，5 の方は $4 (= 2^2)$ と互いに素，つまり共通素因数をもたない．
- したがって，$5{\cdot}x$ のうち，x の方が 4 で割り切れる，すなわち $4 \mid x$.

よって $x = 4k\ (k \in \mathbb{Z})$ と表せる．これを与式に代入すると

$$5{\cdot}4k = 4y \ \text{ i.e. } 5k = y.$$
$$\therefore (x,\, y) = (4k,\, 5k)\ (k \in \mathbb{Z}).$$

(2) 左辺を因数分解すると

$$(x + 2y)(x - 2y) = 5.$$

$x + 2y,\, x - 2y$ はいずれも整数であるから，5 の約数である．したがって，次表．

↑$\boxed{\text{E}}$(1)

$x+2y$	1	5	−1	−5
$x-2y$	5	1	−5	−1
x	3	3	−3	−3
y	−1	1	1	−1

(3) $x \in \mathbb{Z}$ より $x \in \mathbb{R}$ だから $x^2 = 5 - 4y^2 \geqq 0$ が必要．よって $y^2 \leqq \dfrac{5}{4}$ より ←$\boxed{\text{E}}$(2)

$$y = -1,\, 0,\, 1$$

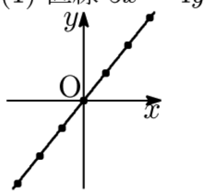
に絞られ，右表を得る．したがって

y	−1	0	1
x^2	4	5	4
x	±2	なし	±2

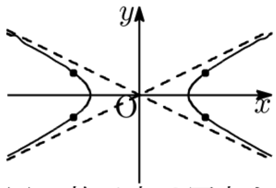
$$(x,\, y) = (2,\, -1),\, (-2,\, -1),\, (2,\, 1),\, (-2,\, 1).$$

〈注〉上記 (1)，(2)，(3) は，それぞれ次の図形上にある**格子点**(両座標とも整数である点) を求める問題に他ならない．

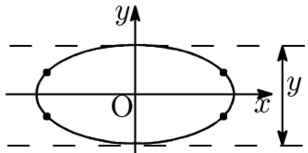
(1) 直線 $5x = 4y$



(2) 双曲線 $x^2 - 4y^2 = 5$



(3) 楕円 $x^2 + 4y^2 = 5$



(1) 格子点は原点を基点として等間隔で並ぶ．

(2) 双曲線において，$x,\, y$ の変域は有限ではない．そこで，$\boxed{\text{E}}$(1) を用いた．

(3) 楕円において，$x,\, y$ の変域は有限である．そこで，$\boxed{\text{E}}$(2) を用いた．

$\boxed{\text{G}}$ 合同式

2 つの整数 a，b を正整数 n で割ったときの余りが等しいならば，

$$n \mid a - b \leftarrow \left(\begin{array}{l}\text{差をとると}\\ n\text{ の倍数}\end{array}\right)$$

(例)

$$\begin{array}{rl} a = & 5{\cdot}8 + 3 \\ -)\ b = & 5{\cdot}6 + 3 \\ \hline a - b = & 5{\cdot}(8 - 6) \end{array}$$

が成り立つ (逆も成立)．このとき，a，b は n を**法として合同**であるといい，

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

と表す．

〈例 1〉 $17 \equiv 2 \pmod{3}$. $\quad \bigl(3 \mid 17 - 2\bigr)$

$29 \equiv 15 \pmod{7}$. $\quad \bigl(7 \mid 29 - 15\bigr)$

〈例 2〉 n^3 と n を 6 で割った余りが等しいこと，すなわち $n^3 \equiv n \pmod{6}$ を示そう．

$n^3 - n = n(n^2 - 1) = (n - 1)n(n + 1)$ であり，$n,\, n + 1$ の一方は 2 の倍数．また，$n - 1,\, n,\, n + 1$ のいずれかは 3 の倍数．2 と 3 は互いに素であるから，$n^3 - n$ は $2{\cdot}3 = 6$ の倍数 $(6 \mid n^3 - n.)$．すなわち，$n^3 \equiv n \pmod{6}$.
□

〈注〉合同式を使うと,「余りが等しい」という日本語を書かなくて済むので手の負担が軽くなる．頭の負担は変わらない．変わってはならない！

H 剰余類

整数を 3 で割ったときの商と余りのうち，商は無視して余りだけに注目し，余りが等しい整数からなる集合，つまり 3 を法として互いに合同である整数の集合を作ることにより，整数全体を次のような 3 つの集合に分類することができる．

$\{3k|k\in\mathbb{Z}\}=\{\ldots-3,\ 0,\ 3,\ 6,\ \ldots\}$ ←余りが 0
$\{3k+1|k\in\mathbb{Z}\}=\{\ldots-2,\ 1,\ 4,\ 7,\ \ldots\}$ ←余りが 1
$\{3k+2|k\in\mathbb{Z}\}=\{\ldots-1,\ 2,\ 5,\ 8,\ \ldots\}$ ←余りが 2

上記 3 つの集合の各々を，法 3 の**剰余類**という．

〈注 1〉$\{3k+2|k\in\mathbb{Z}\}$ は $\{3k-1|k\in\mathbb{Z}\}$ と表すこともできる．

〈注 2〉一般に，整数全体は a を法として

$$\{ak\},\ \{ak+1\},\ \{ak+2\},\ \ldots,\ \{ak+(a-1)\}$$
(いずれも $k\in\mathbb{Z}$)

の a 個の剰余類に分けられる．

〈例 1〉整数全体は 2 を法とする 2 つの剰余類：

$\ldots-4,\ -2,\ 0,\ 2,\ 4,\ \ldots$ ←偶数
$\ldots-3,\ -1,\ 1,\ 3,\ \ldots$ ←奇数

に分けられる．

〈例 2〉**平方数** n^2 を 5 で割ったときの余りを考える．n を，5 を法とする 5 つの剰余類に分け，それぞれの場合に n^2 を計算すると

$$(5k)^2=5\cdot5k^2,$$
$$(5k\pm1)^2=5\cdot(5k^2\pm2k)+1,$$
$$(5k\pm2)^2=5\cdot(5k^2\pm4k)+4.$$

よって，平方数 n^2 を 5 で割った余りは

$0,\ 1,\ 4$

の 3 種類しかない！

この例からわかるとおり，一般に平方数 n^2 を何かで割った余りは，n を何かで割った余りに比べて，種類が少ない．(ただし，2 で割った余りに関しては，どちらも 0, 1 の 2 種類である．)

I 互除法

$$a=bq+r$$

のとき，

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

最大公約数

が成り立つ．これを繰り返し用いて，2 つの正整数の最大公約数を求める方法を**互除法**という．

〔(∗) の証明〕

a と b の公約数全体の集合を A，b と r の公約数全体の集合を B とし，

$$A=B,\ \text{すなわち,}\begin{cases}A\subset B\ \text{かつ}\\ B\subset A\end{cases}$$

を示せばよい．

1° $d\in A$ のとき，$\begin{cases}a=da',\\ b=db'\end{cases}$ と表せて，

$$r=a-bq=da'-db'q=d(a'-b'q).$$

よって，d は r の約数でもあるから $d\in B$．すなわち $A\subset B$．

2° $d\in B$ のとき，$\begin{cases}b=db',\\ r=dr'\end{cases}$ と表せて

$$a=bq+r=db'q+dr'=d(b'q+r').$$

よって d は a の約数でもあるから $d\in A$．すなわち $B\subset A$．

1°，2° より，$A=B$.□

〈例〉(1242, 615) (1242 と 615 の最大公約数) を求める．(それぞれを素因数分解するのは少しメンドウ．)

$$1242=615\cdot2+12,$$
$$615=12\cdot51+3,$$
$$12=3\cdot4+0.$$

よって，

$(1242,\ 615)$
$=(615,\ 12)$
$=(12,\ 3)$ ←ここでやめてもわかるが…
$=(3,\ 0)$ ←0 が現れるまで続ける
$=3.$

$\boxed{\text{J}}$ 整数係数方程式の有理数解

$a,\ b,\ c,\ d \in \mathbb{Z}$ とする．x の 3 次方程式

$$ax^3+bx^2+cx+d=0 \qquad \cdots ❀$$

が，仮に有理数解 $\dfrac{p}{q}$ ($p,\ q$ は互いに素で $q>0$) をもつとすれば，

$$a\left(\frac{p}{q}\right)^3+b\left(\frac{p}{q}\right)^2+c\left(\frac{p}{q}\right)+d=0.$$

$$ap^3+bp^2q+cpq^2+dq^3=0. \qquad \cdots ☘$$

初めの 3 項を p でくくると

$$p\cdot(ap^2+bpq+cq^2)=-q^3\cdot d.$$

p と $-q^3$ は互いに素であるから ($\boxed{\text{D}}$☼より)

$$p \mid d.$$

☘において，後ろの 3 項を q でくくると

$$q\cdot(bp^2+cpq+dq^2)=-p^3\cdot a.$$

よって上と同様にして

$$q \mid a.$$

以上より，❀の有理数解は

定数項→ d の約数 / 最高次の係数→ a の約数 以外にはない．(必ず有理数解がある訳ではない)

$$\frac{d\text{ の約数}}{a\text{ の約数}}$$

(3 次以外の整方程式についても同様である．)

$\boxed{\text{K}}$ 約数の個数

たとえば $200=2^3\cdot5^2$ の正の約数は
（$2^3\cdot5^2$：素因数分解）

$$2^a\cdot5^b$$

の形で表され，$a,\ b$ のとりうる値は

$$a=0,\ 1,\ 2,\ 3$$
$$b=0,\ 1,\ 2$$

$a \backslash b$	0	1	2
0	1	5	25
1	2	10	50
2	4	20	100
3	8	40	200

のいずれかである．「素因数分解の一意性」より

$$2^a\cdot5^b \underset{\text{一対一対応}}{\longleftrightarrow} (a,\ b)$$

であるから，正の約数の個数は

$$(3+1)(2+1)=12(\text{個}).$$

正の約数の総和は

$$\begin{aligned}
&1\cdot1+1\cdot5+1\cdot5^2\\
&+2\cdot1+2\cdot5+2\cdot5^2\\
&+2^2\cdot1+2^2\cdot5+2^2\cdot5^2\\
&+2^3\cdot1+2^3\cdot5+2^3\cdot5^2\\
&=1\cdot(1+5+5^2)\\
&+2\cdot(1+5+5^2)\\
&+2^2\cdot(1+5+5^2)\\
&+2^3\cdot(1+5+5^2)\\
&=\underbrace{(1+2+2^2+2^3)}_{\text{等比数列の和}}\underbrace{(1+5+5^2)}_{\text{等比数列の和}}
\end{aligned}$$

同様にして，$\boxed{\text{C}}$(1)($*$) の正の約数の個数は
$(\alpha+1)(\beta+1)(\gamma+1)\cdots.$

正の約数の総和は

$$\left(1+p+p^2+\cdots+p^\alpha\right)\left(1+q+q^2+\cdots+q^\beta\right)\times\left(1+r+r^2+\cdots+r^\gamma\right)\times\cdots.$$

$\boxed{\text{L}}$ $\boxed{\text{A}}$✂の証明

1° $q,\ r$ の存在証明

実数全体を，区間

$$[k,\ k+1)\ (k=\ldots,\ -1,\ 0,\ 1,\ 2,\ \ldots)$$

に分割すると，実数 $\dfrac{a}{b}$ はこのうちいずれか 1 つだけに属する．すなわち

$$q \leqq \frac{a}{b} < q+1,$$

$$\text{i.e. } bq \leqq a < bq+b$$

をみたす $q(\in\mathbb{Z})$ がただ 1 つ存在する．そこで

$r=a-bq(\in\mathbb{Z})$ とおけば $0 \leqq r < b$ であるから

$$a=bq+r\ (0 \leqq r < b)$$

をみたす整数 $q,\ r$ の存在が示された．

2° $q,\ r$ の一意性の証明

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

とすると，辺々引いて

$$0=b(q-q')+(r-r'),$$
$$\text{i.e. } r-r'=b(q'-q).$$

よって $r-r'$ は b の倍数で，$-b<r-r'<b$ であるから

$$r-r'=0 \ \text{ i.e. } r=r'.$$

したがって $b(q-q')=0$ だから $q=q'$.

M C (1) の証明 ←「初等整数論講義」(高木貞治著) より引用

素因数分解が可能であることについては，合成数をその約数どうしの積に次々分解していくことにより自明．以下，数学的帰納法を用いて素因数分解の一意性を示す．

$2,3,4,\ \ldots,n$ については素因数分解の一意性が成り立つと仮定し，$n+1$ についてもそれが言えることを示す．

仮に $n+1$ が，素数 $p,q,r,\ \ldots,p',q',r',\ \ldots$ を用いて

$$(n+1=)pqr\cdots=p'q'r'\cdots \qquad \cdots①$$

と 2 通りに素因数分解されたとする．もしも $p=p'$ とすると

$$qr\cdots\cdots=q'r'\cdots\cdots$$

となり，$n+1$ より小さい正整数が 2 通りに素因数分解されたことになって仮定に反す．よって，$p\neq p'$．同様にして，次が示される．

$$\begin{cases} p\neq p',q',r',\ \ldots, \\ q\neq p',q',r',\ \ldots, \\ r\neq p',q',r',\ \ldots, \\ \qquad\vdots \end{cases} \qquad \cdots②$$

$p>p'$ として①の両辺から $p'qr\cdots$ を引くと

$$(A:=)(p-p')qr\cdots=p'(qr\cdots-q'r'\cdots).$$

②より $p'\neq q,r,\ \ldots$ であるし，$p'\mid p-p'$ とすると $p'\mid p$ となるが，これは p,p' が異なる素数であることより不可能．よって，$n+1$ より小さな正整数 A が 2 通りに素因数分解されたことになって不合理．よって $n+1$ についても素因数分解は一意的．

正整数 2 の素因数分解は一意的であるから，2 以上の任意の整数について素因数分解の一意性が示された．□