

古谷数学教室第 25 回

整数の性質 1

2025 年 11 月 5 日

1 基礎事項

1.1 約数と倍数

2つの整数 a 、 b について、ある整数 k を用いて、 $a = bk$ と表されるとき、 b は a の**約数**であるといい、 a は b の**倍数**であるという。

一般に、整数 a 、 b 、 n について、次のことが成り立つ：

「 a 、 b が n の倍数」 \implies 「 $a + b$ 、 $a - b$ は n の倍数である」。

ある自然数 n について、次の有名な倍数判定法がある：

「 n の一の位が 0」 \implies 「 n は 10 の倍数」。

「 n の一の位が 0, 2, 4, 6, 8 のいずれかである」 \implies 「 n は 2 の倍数」。

「 n の一の位が 0, 5 のいずれかである」 \implies 「 n は 5 の倍数」。

「 n の各位の数の和が 3 の倍数である」 \implies n は 3 の倍数である。

「 n の各位の数の和が 9 の倍数である」 \implies n は 9 の倍数である。

2 以上の自然数で、正の約数が 1 とその数自身のみである数を**素数**という。素数は無数にあることが知られている。2 以上の自然数で、素数でない数を**合成数**という¹⁾。

$15 = 3 \cdot 5$ のように、整数がいくつかの整数の積で表されるとき、そのそれぞれの整数をもとの**因数**という。

素数である因数を**素因数**といい、自然数を素数だけの積の形に表すことを**素因数分解**するという。

一般に、次のことが成り立つ：

1) 合成数は、必ず素因数分解できる。また、1 つの合成数の素因数分解は、積の順序を考えなければ、1 通りであることが知られている。このことを、素因数分解の一意性という。

約数の個数

自然数 N の素因数分解が $N = p^a \cdot q^b \cdot r^c \cdots$ となる時、 N の正の約数の個数は $(a+1)(b+1)(c+1)\cdots$ である。

1.2 最大公約数・最小公倍数

2 つ以上の整数について、共通する約数をそれらの**公約数**といい、公約数のうち最大のものを**最大公約数**という。また、2 つ以上の整数について、共通する倍数をそれらの**公倍数**といい、正の公倍数のうち最小のものを**最小公倍数**という。

一般に、次のことがいえる：

公約数は、最大公約数の約数、公倍数は最小公倍数の倍数である。

2 つの整数 a, b について、共通な素因数がないとき、 a と b の最大公約数は 1 である。2 つの整数 a, b の最大公約数が 1 であるとき、 a, b は**互いに素**であるという。

a, b, c は整数で、 a, b は互いに素であるとする。このとき、一般に、次のことが成り立つ：

1. ac が b の倍数であるとき、 c は b の倍数である。
2. a の倍数であり、 b の倍数でもある整数は、 ab の倍数である。

1.3 整数の割り算と商・余り

整数 a と正の整数 b について、次の式を満たす整数 q, r は 1 通りに定まる：

整数の割り算

$$a = bq + r, \quad 0 \leq r < b.$$

上の等式 $a = bq + r$ において、 q は a を b で割ったときの**商**、 r は a を b で割ったときの**余り**という。 $r = 0$ のとき a は b で**割り切れる**といい、 $r \neq 0$ のときは a は b で**割り切れない**という。

整数を正の整数 m で割ったときの余りに着目すると、すべての整数は、整数 k を用いて、次のいずれかの形に表される：

$$mk, mk + 1, \dots, mk + (m - 1).$$

例えば、整数 3 で割ったときの余りは 0、1、2 のいずれかである。したがって、すべての整数は、整数 k を用いて

$$3k, 3k + 1, 3k + 2.$$

2 おあそび

2.1 最大公約数・最小公倍数の性質

2つの自然数 a 、 b の最大公約数を g 、最小公倍数を l とし、 $a = ga'$ 、 $b = gb'$ であるとする。一般に、次のことがいえる：

1. a' 、 b' は互いに素である。
2. $l = ga'b'$.
3. $ab = gl$.

2.2 合同式

以下では、 a 、 b 、 c 、 d は整数、 m 、 k は正の整数とする。

一般に、 a 、 b を m で割った余りを、それぞれ r 、 r' とすると、次のことが成り立つ：

1. $a + b$ を m で割った余りは、 $r + r'$ を m で割った余りに等しい。
2. $a - b$ を m で割った余りは、 $r - r'$ を m で割った余りに等しい。
3. ab を m で割った余りは、 rr' を m で割った余りに等しい。
4. a^k を m で割った余りは、 r^k を m で割った余りに等しい。

a を m で割ったときの余りと、 b を m で割ったときの余りが等しいとき、 $a - b$ は m の倍数である。このとき、 a と b は m を法として合同であるという。このことを

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

と表す。このような式を合同式という。

合同式について、次のことが成り立つ：

1. $a \equiv a \pmod{m}$,
2. $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$,
3. $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$.

ただし、 \wedge は「かつ」を意味する。

$a \equiv c \pmod{m}$ 、 $b \equiv d \pmod{m}$ のとき、次が成り立つ：

1. $a \pm b \equiv c \pm d \pmod{m}$,

2. $ab \equiv cd \pmod{m}$,

3. $a^k \equiv c^k \pmod{m}$.

3 例題

1. 次の命題の真偽を定めよ。

(1) 66 は 6 の倍数である。

(2) -12 は 6 の倍数である。

(3) 6 の約数はちょうど 8 個ある。

(4) 0 はすべての整数の倍数である。

(5) 1 はすべての整数の約数である。

(6) 1230 は 2 の倍数である。

(7) 1230 は 3 の倍数である。

(8) 1230 は 4 の倍数でない。

(9) 1230 は 5 の倍数である。

(10) 1230 は 6 の倍数である。

(11) 整数 a 、 b が 3 の倍数ならば、 $a+b$ と $a-b$ も 3 の倍数である。

(12) 1 は素数でない。

2. 3 桁の自然数 N について、3 の倍数判定法と 9 の倍数判定法が正しいことを確認せよ。

3. 2つの整数 a 、 b を m で割った余りを、それぞれ r 、 r' とすると、 $a+b$ を m で割った余りは、 $r+r'$ を m で割った余りに等しいこと、 $a-b$ を m で割った余りは、 $r-r'$ を m で割った余りに等しいこと、 ab を m で割った余りは、 rr' を m で割った余りに等しいことを示せ。

4. a^k を m で割った余りは、 r^k を m で割った余りに等しいことを示せ。

5. 5^{100} を 4 で割った余りを求めよ。

6. n は整数とする。 n^2 を 3 で割ったときの余りは、2 ではない。

4 演習問題

1. a と b は整数とする。 a と $a+b$ がともに 7 の倍数ならば、 b は 7 の倍数であることを示せ。
2. y が 9 の倍数であるとき、 x をすべて求めよ。ただし、 x は 0 から 9 までの 10 個の整数であるとする。
 - (1) $y = 9670 + x$
 - (2) $y = 4038 + 100x$
3. $y = 6230 + x$ を満たす y が 6 の倍数であるとき、 x を求めよ。ただし、 x は 0 から 9 までの 10 個の整数であるとする。
4. 540 を素因数分解せよ。
5. 24 の正の約数をすべて求めよ。
6. 500 の正の約数の個数を求めよ。
7. 次の数の組の最大公約数と最小公倍数を求めよ。
 - (1) 140、525
 - (2) 30、126、140
8. 次の 2 つの整数が互いに素であるかどうかを答えよ。
 - (1) 26 と 39
 - (2) 45 と 76
9. 縦 90cm、横 168cm の板がある。次のものを求めよ。
 - (1) 同じ大きさのこの板を同じ向きにすき間なく敷き詰めて正方形を作るとき、最も小さい正方形の 1 辺の長さとのそのときに必要な板の枚数

(2) この板 1 枚に、同じ大きさの正方形のタイルをすき間なく敷き詰めるとき、最も大きい正方形のタイルの 1 辺の長さとそのときに必要なタイルの枚数（タイル 1 辺の長さは整数とする）

10. 2 つの整数 a 、 b を 9 で割った余りがそれぞれ 4、6 であるとき、次の数を 9 で割ったときの余りを求めよ。

(1) $2a + 7b$

(2) $a^2 - 5ab$