第4講 整数

1 基本用語

A 除法の原理，商と余り

整数 a，b（$b>0$）が与えられたとき，

$$\boldsymbol{a=bq+r,\quad 0\leqq r<b}$$

を満たす整数 q，r がただ1組存在する（**整数の除法の原理**）．このとき，q を「a を b で割ったときの**商**」，r を「a を b で割ったときの**余り**（**剰余**）」という．

B 約数と倍数

整数 a，b（$b\neq 0$）に対して，

$$a=bq$$

を満たす整数 q が存在するとき，「a は b で割り切れる」，「a は b の**倍数**である」または，「b は a の**約数**である」という．

ここで，$0=b\cdot 0$ より，0 は 0 以外の任意の整数の倍数であり，$a=1\cdot a$ より，1 は任意の整数の約数である．

例1　等式 $(x+1)(y+2)=5$ を満たす整数の組 $(x,\ y)$ をすべて求めよ．

解　x，y が整数であるとき，$x+1$，$y+2$ はともに整数となるので，5 の約数を考えて，

$$(x+1,\ y+2)=(1,\ 5),\ (5,\ 1),\ (-1,\ -5),\ (-5,\ -1)$$

よって，求める整数の組 $(x,\ y)$ は，

$$(x,\ y)=(0,\ 3),\ (4,\ -1),\ (-2,\ -7),\ (-6,\ -3)$$

C 素数

2 以上の整数のうち，1 とそれ自身以外に正の約数をもたないものを**素数**という．素数を小さい方からあげると，

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \cdots$$

となる．

D 公約数と公倍数

整数 a, b, c, … に共通な約数を**公約数**, 公約数のうちで最大のものを**最大公約数**という. また, 整数 a, b, c, … に共通な倍数を**公倍数**, 正の公倍数のうちで最小のものを**最小公倍数**という.

2 つの整数 a, b の最大公約数が 1 であるとき, a と b は**互いに素**であるという.

2 剰余による類別と合同式

A 剰余による整数の分類

2 つの整数 a, b の平方の和 a^2+b^2 を 3 で割ったときの余りについて考えてみよう.

すべての整数は 3 で割ったときの余りによって分類すると,

$$3k, \quad 3k+1, \quad 3k+2 \quad (k \text{ は整数})$$

のいずれかの形で表すことができる. いま,

$$(3k)^2=3\cdot 3k^2,$$
$$(3k+1)^2=3(3k^2+2k)+1,$$
$$(3k+2)^2=3(3k^2+4k+1)+1$$

となるから, a^2+b^2 を 3 で割ったときの余りは,

a \ b	3 の倍数	3 で割った余りが 1	3 で割った余りが 2
3 の倍数	0	1	1
3 で割った余りが 1	1	2	2
3 で割った余りが 2	1	2	2

である.

上述の議論によって, 例えば $a^2+b^2=c^2$ を満たす 3 つの整数 a, b, c については,

- a と b の少なくとも一方は 3 の倍数である
- c が 3 の倍数 $\Longrightarrow$ a, b はともに 3 の倍数である

などがわかる.

ある整数が正の整数 m の倍数であることを示したり, ある整数を m で割ったときの余りを求めたりする場合は, 整数全体を m で割ったときの余り 0, 1, …, $m-1$ により分類しておくと考えやすくなることがある.

例 2 n が整数であるとき，n^3-n は 3 の倍数となることを示せ．

解 整数 n を 3 で割ったときの余りによって分類すると，

$$3k,\ 3k+1,\ 3k+2 \quad (k \text{ は整数})$$

それぞれの場合について，n^3-n の値を求める．

(i) $n=3k$ のとき，

$$n^3-n=(3k)^3-3k=3(9k^3-k)$$

(ii) $n=3k+1$ のとき，

$$n^3-n=(3k+1)^3-(3k+1)=3(9k^3+9k^2+2k)$$

(iii) $n=3k+2$ のとき，

$$n^3-n=(3k+2)^3-(3k+2)=3(9k^3+18k^2+11k+2)$$

以上 (i), (ii), (iii) より，n が整数であるとき，n^3-n は 3 の倍数となる．

(注) (iii) では，n を 3 で割ったときの余りが 2 の場合を，$n=3k-1$ と表して次のように計算してもよい．

$$n^3-n=(3k-1)^3-(3k-1)=3(9k^3-9k^2+2k)$$

B 合同式の定義と演算

a, b は整数とする．a と b の差 $a-b$ が正の整数 m の倍数であるとき，

a は m を法として b と合同である

といい，$\boldsymbol{a \equiv b \pmod{m}}$ と表す．この式を合同式という．

このとき，次が成り立つ．

整数 a, b を正の整数 m で割ったときの余りが等しい $\iff$ $a \equiv b \pmod{m}$

合同式の加法，減法，乗法について，次が成り立つ．

a，b，c，d は整数，m，n は正の整数とする．

$a \equiv b \pmod{m}$，$c \equiv d \pmod{m}$ のとき，

1．$a+c \equiv b+d \pmod{m}$

2．$a-c \equiv b-d \pmod{m}$

3．$ac \equiv bd \pmod{m}$

4．$a^n \equiv b^n \pmod{m}$

例3　n が整数であるとき，n^3-n は 3 の倍数となることを示せ．

解　3 を法とする合同式を用いて考え，以下では $(\mathrm{mod}\ 3)$ の記載は省略する．

n が整数であるとき，

$$n \equiv 0 \text{ または } n \equiv 1 \text{ または } n \equiv 2$$

のいずれかが成り立つ．

$$n \equiv 0 \text{ のとき，} n^3-n \equiv 0^3-0 \equiv 0,$$

$$n \equiv 1 \text{ のとき，} n^3-n \equiv 1^3-1 \equiv 0,$$

$$n \equiv 2 \text{ のとき，} n^3-n \equiv 2^3-2 \equiv 6 \equiv 0$$

となるから，n が整数であるとき，n^3-n は 3 の倍数となる．

3　不等式を利用する整数問題

方程式や不等式の整数解を求める際に，不等式を作って範囲を絞り，その範囲の整数を1つずつ調べていくことで，整数解を求める方法がある．

例4　次の問に答えよ．

(1)　等式 $x^2+y^2=10$ を満たす正の整数の組 $(x,\ y)$ をすべて求めよ．

(2)　不等式 $\dfrac{1}{x}+\dfrac{1}{y} \geqq \dfrac{5}{4}$ を満たす整数の組 $(x,\ y)$ をすべて求めよ．ただし，$1 \leqq x \leqq y$ とする．

解 (1)　$x^2+y^2=10$ より，$x^2=10-y^2$ となる．

$y^2 \geqq 0$ であるから，

$$x^2=10-y^2 \leqq 10$$

x が正の整数であることより，$x=1,\ 2,\ 3$ に限られる．

$$x=1 \text{ のとき，} y^2=9,$$

$$x=2 \text{ のとき，} y^2=6,$$

$$x=3 \text{ のとき，} y^2=1$$

以上より，求める正の整数の組 $(x,\ y)$ は，

$$(x,\ y)=(1,\ 3),\ (3,\ 1)$$

(2)　$1 \leqq x \leqq y$ のとき，$\dfrac{1}{x} \geqq \dfrac{1}{y}$ であるから，

$$\frac{5}{4} \leqq \frac{1}{x}+\frac{1}{y} \leqq \frac{1}{x}+\frac{1}{x}=\frac{2}{x}$$

よって，$x \leqq \dfrac{8}{5}$ となり，$x=1$ に限られる．

$$x=1 \text{ のとき，} \frac{1}{y} \geqq \frac{1}{4} \text{ つまり } y \leqq 4$$

以上より，求める整数の組 $(x,\ y)$ は，

$$(x,\ y)=(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (1,\ 4)$$

4・3 n は正の整数とする．x，y，z に関する方程式

$$x^n + y^n + z^n = xyz \qquad \cdots ①$$

を考える．

(1) $n=1$ のとき，① を満たす正の整数の組 $(x,\ y,\ z)$ で，$x \leqq y \leqq z$ となるものをすべて求めよ．

(2) $n=3$ のとき，① を満たす正の整数の組 $(x,\ y,\ z)$ は存在しないことを示せ．