1 合同式

整数 $a,\ b,\ m$ **に対して** $a-b$ **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」あるいは「**a **と** b **は** modulo m **で等しい」などと言い** $a \equiv b \pmod{m}$ **と書く。**

$m = 0$ **のときは** $a \equiv b \pmod{m} \iff a = b$ **であるから，以下では** $m \neq 0$ **のときに考える。このときは** $a \equiv b \pmod{m}$ **は** $a-b$ **が** m **で割り切れると言うことに他ならない。**

例 1.1 $8 \equiv 5 \pmod{3}$, $2 \equiv -4 \pmod{3}$, $2 \equiv -4 \pmod{2}$

$8-5=3,\ 2-(-4)=6$ **はいずれも** 3 **の倍数である。**$2-(-4)=6$ **は** 2 **の倍数でもある。** //

合同式の基本性質をまとめておこう。

定理 1.1 a, b, c, d, m **を整数とするとき，次が成り立つ。**

(1) $a \equiv a \pmod{m}$

(2) $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$

(3) $a \equiv b \pmod{m},\ b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$

(4) $\begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases} \Longrightarrow \begin{cases} a+c \equiv b+d \pmod{m} \\ ac \equiv bd \pmod{m} \end{cases}$

(5) k **が整数のとき**

$$a \equiv b \pmod{m} \Longrightarrow \begin{cases} ka \equiv kb \pmod{m} \\ ka \equiv kb \pmod{km} \end{cases}$$

(6) n **が自然数のとき**

$a \equiv b \pmod{m} \Longrightarrow a^n \equiv b^n \pmod{m}$

☞ **加法・乗法については** $\equiv$ **は** $=$ **と同じ性質をもつということが分かる。除法に関しては次の例を参照。**

(1) $a-a=0$ **で，**0 **は** m **の倍数であるから** $a \equiv a \pmod{m}$

(2) $a \equiv b \pmod{m}$ **より** $a-b=um$ **と書ける。そうすると** $b-a=-um$ **となるから** $b \equiv a \pmod{m}$ **である。**

(3) 仮定より $a-b=um \cdots ①, b-c=vm \cdots ②$ **である。** ① **より** $a=b+um$ **であり** ② **より** $c=b-vm$ **であるから** $a-c=(b+um)-(b-vm)=(u+v)m$ **となるので** $a \equiv c \pmod{m}$ **である。**

(4) 仮定より $a-b=um,\ c-d=vm$ であるから $a=b+um,\ c=d+vm$ と書ける。そうすると $a+c=(b+um)+(d+vm)=(b+d)+(u+v)m$ であるから $(a+c)-(c+d)=(u+v)m$ は m の倍数となり $a+c\equiv c+d \pmod m$ である。また $ac=(b+um)(d+vm)=bd+(bv+ud+uvm)m$ であるあから $ac-bd=(bv+ud+uvm)m$ となり $ac-bd$ は m の倍数であるから $ac\equiv bd \pmod m$ である。

(5) 仮定より $a-b=um$ であるから，両辺に k をかけると $k(a-b)=ukm$ となる。よって $ka-kb$ は m の倍数であるから $ka\equiv kb \pmod m$ である。また $ka-kb$ は km の倍数でもあるから $ka\equiv kb \pmod{km}$ でもある。

(6) $\left.\begin{array}{l} a\equiv b \pmod m \\ a\equiv b \pmod m \\ \quad\vdots \\ a\equiv b \pmod m \end{array}\right\} n$ 個　辺々をかけると (4) より $a^n\equiv b^n \pmod m$ を得る。■

例 1.2 a, x, y, m を整数とし a と m の最大公約数を d とする。このとき

$$ax\equiv ay \pmod m \Longrightarrow x\equiv y \left(\mathrm{mod}\ \frac{m}{d}\right)$$

とくに a と m が互いに素のときは $x\equiv y \pmod m$ となる。

仮定より $ax-ay=sm\cdots①$ である。a と m の最大公約数が d であるから $a=a_1d,\ m=m_1d$ (a_1 と m_1 は互いに素) と書ける。これを ① に代入すると $a_1dx-a_1dy=sm_1d$ であるから，両辺を d で割ると $a_1(x-y)=sm_1\cdots②$ となる。② より a_1 は sm_1 を割り切るが，a_1 と m_1 は互いに素であるから a_1 は s を割り切る。$s=a_1s_1$ とおくと ② は $a_1(x-y)=a_1s_1m_1$ となるので両辺を a_1 で割ると $x-y=s_1m_1$ となる。よって $x\equiv y \pmod{m_1}$ である。ここで $m_1=\dfrac{m}{d}$ であったから $x\equiv y \left(\mathrm{mod}\ \dfrac{m}{d}\right)$ を得る。//

例 1.3 自然数 N が 9 で割り切れるための条件は，N の各位の数字の和が 9 の倍数となることである。

$$\begin{cases} N=a_n\times 10^n+a_{n-1}\times 10^{n-1}+\cdots+a_1\times 10+a_0 \\ 0\leqq a_j\leqq 9\ \ (j=0,1,\cdots,n-1) \\ 1\leqq a_n\leqq 9 \end{cases}$$ とする。

$10 \equiv 1 \pmod 9$ であるから $10^k \equiv 1 \pmod 9$ である。この両辺に a_k をかけると $a_k \times 10^k \equiv a_k \pmod 9$ である[注1]。従って

$$\begin{aligned} N &= a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0 \\ &\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9 \end{aligned}$$

$N \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9$ である。N が 9 で割り切れるということは $N \equiv 0 \pmod 9$ ということである。よって N が 9 で割り切れるための条件は $a_n + a_{n-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 9$ つまり 各位の数字の和が 9 で割り切れることである。//

1 次方程式の整数解は合同式を用いると簡単に解ける場合もある。

例 1.4　$7x + 9y = 1 \cdots$ ① の整数解は $(x, y) = (-5 - 9t,\ 4 + 7t)$ (t は任意の整数) である。

① を　mod 7 で考えると $9y \equiv 1 \pmod 7$ であるが $9 \equiv 2 \pmod 7$ であるから $2y \equiv 1 \pmod 7$ となる。この両辺に 4 をかけると $8y \equiv 4 \pmod 7$ である。ここで $8 \equiv 1 \pmod 7$ であるから $y \equiv 4 \pmod 7$ である。よって $y = 4 + 7t$ と書けるのでこれを ① に代入すると $7x + 9(4 + 7t) = 1$ つまり $7x = -35 - 9 \cdot 7t$ となるので，両辺を 7 で割って $x = -5 - 9t$ となる。以上で $(x, y) = (-5 - 9t,\ 4 + 7t)$ //

2　剰余の問題

a を整数，m を自然数とするとき，$a = mh + r$ かつ $0 \leqq r < m$ となる整数の組 (h, r) がただひと組存在する。そこで h を，a を m で割った商，r を余り (剰余) と言う[注2]。

$a,\ b$ を整数，m を自然数とする。このとき $a \equiv b \pmod m$ は $a - b$ が m で割り切れるということである。これは言い換えると a を m で割った余りと b を m で割った余りが等しいと言うことになる[注3]。従って，余りを計算するときに合同式が役立つ。

[注1] 今後は，mod 9 で考えるときは 10^k と 1 が等しいのだから　mod 9 で考えるときは，10^k を 1 で置き換えてよい，と考える方が便利である。

[注2] m の倍数を考えると，$mh \leqq a < m(h+1)$ となる整数 h がある。そこで $r = a - mh$ とおけば $0 \leqq r < m$ かつ $a = mh + r$ となる。

[注3] $a = mh_1 + r_1,\quad b = mh_2 + r_2$ とする。$a - b = m(h_1 - h_2) + (r_1 - r_2)$ であるが，$m(h_1 - h_2)$ は m で割り切れるから，$a - b$ が m で割り切れるための条件は $r_1 - r_2$ が m で割り切れることである。しかし，$r_1,\ r_2$ は m で割った余りであるから $0 \leqq r_1 < m,\ 0 \leqq r_2 < m$ である。よって $-m < r_1 - r_2 < m$ となる。従って $r_1 - r_2$ が m で割り切れるのは $r_1 - r_2 = 0$ つまり $r_1 = r_2$ のときである。

例 2.1　2^{100} **を** 13 **で割った余りは** 3 **である。**

$2^4 = 16 \equiv 3 \pmod{13}$ **であるから両辺に** 2 **をかけて** $2^5 \equiv 6 \pmod{13}$**。更に両辺に** 2 **をかけると** $2^6 \equiv 12 \equiv -1 \pmod{13}$ **である。従って両辺を** 2 **乗すると** $2^{12} \equiv 1 \pmod{13}$ **と分かる。そうすると**

$$2^{100} = 2^{12\times 8+4} = \left(2^{12}\right)^8 \cdot 2^4 \equiv 1^8 \cdot 3 \pmod{13}$$

となり $2^{100} \equiv 3 \pmod{13}$ **である。従って** 2^{100} **を** 13 **で割った余りは** 3 **である。**//

p **が素数のとき，**a **が** p **と互いに素なら** $a^{p-1} \equiv 1 \pmod{p}$ **となることが知られている (付録の「**Fermat **の小定理」参照)。この定理を使えば** $2^{12} \equiv 1 \pmod{13}$ **がただちに分かる。また，**Fermat **の小定理の拡張である** Euler **の定理を用いると** m **が素数でないときも** $a^n \equiv 1 \pmod{m}$ **となる** n **を容易に見つけることができる。**

自然数 m **と** n **は互いに素とする。整数** N **を** m **で割った余りと，**N **を** n **で割った余りが分かれば，**N **を** mn **で割った余りが分かる（中国の剰余定理参照)。合同式を利用して** N **を** mn **で割った余りを求めてみよう。**

例 2.2　**整数** N **を** 5 **で割ると** 3 **余り，**7 **で割ると** 2 **余るとき，**N **を** 35 **で割った余りは** 23 **である。**

仮定より $\begin{cases} N \equiv 3 \pmod{5} & \cdots ① \\ N \equiv 2 \pmod{7} & \cdots ② \end{cases}$ **である。**

①×7 **より** $7N \equiv 21 \pmod{35} \cdots ③$**。** ②×5 **より** $5N \equiv 10 \pmod{35} \cdots ④$**。** $3\times ④ - 2\times ③$ **より** $N \equiv -12 \equiv 23 \pmod{35}$ **である。よって** N **を** 35 **で割った余りは** 23 **である。**//

mod m **で考えるということは，**m **で割った余りが等しい数は同じものと見なすことに他ならない。**m **で割った余りは** $0, 1, \cdots, m-1$ **の** m **通りしかない。従って** mod m **で考えるとき有限個の場合分けですべての場合を尽くすことができる。これを利用して命題を証明する例を示そう。**

例 2.3　**整数** x, y, z **が** $x^2 + y^2 = z^2$ **を満たすとき，**x, y **のうち少なくともひとつは** 3 **の倍数である。**

$x^2+y^2=z^2$ **より** $x^2+y^2\equiv z^2 \pmod 3$ $\cdots$ ①**である。いま仮に** x, y **はともに** 3 **の倍数ではないとする。**

mod 3 **で考えると**

$t \pmod 3$	0	1	-1
$t^2 \pmod 3$	0	1	1

となる。いま， x, y **は** 3 **の倍数ではないとしているので，表より** $x^2\equiv y^2\equiv 1 \pmod 3$ **である。従って** ① **から** $z^2\equiv 2 \pmod 3$ **となるが，表より** $2 \pmod 3$ **は平方数ではないので矛盾である。**

以上で x, y **のうち少なくともひとつは** 3 **の倍数であることが示された。**//