



・合同式

m を正の整数とする。

2つの整数 a, b を m で割ったときの余りが等しいとき

a と **b は m を法として合同**といい

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

と表す。

$$(例1) \quad 3 \equiv 1 \pmod{2} \quad \leftarrow \text{余り } 1$$

$$98 \equiv 14 \pmod{7} \quad \leftarrow \text{余り } 0$$

$$80 \equiv -1 \pmod{3} \quad \leftarrow \text{余り } 2$$

$$ax \equiv ay \pmod{m} \text{ とする}$$

$$\begin{cases} ax = m g_3 + r_3 \\ ay = m g'_3 + r_3 \end{cases} \quad (g_3, g'_3, r_3 \text{ は整数})$$

とおける。

$$ax - ay = (mg_3 + r_3) - (mg'_3 + r_3)$$

$$a(x-y) = m(g_3 - g'_3)$$

a と m は互いに素なので、 $x-y$ は m の倍数である

よって

$$x \equiv y \pmod{m} \quad \square$$

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

- 1 $a+b \equiv c+d \pmod{m}$
- 2 $a-b \equiv c-d \pmod{m}$
- 3 $ab \equiv cd \pmod{m}$
- 4 $a^k \equiv c^k \pmod{m}$

a と m が互いに素のとき

$$5 \quad ①x \equiv ②y \pmod{m} \quad \leftarrow \text{aで割る} \Rightarrow x \equiv y \pmod{m}$$

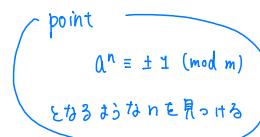
等式の計算
と同じ

(例2) 37^{100} を 6 で割ったときの余りを求めよ。

$$37 \equiv 1 \pmod{6} \text{ であるから}$$

$$37^{100} \equiv 1^{100} \equiv 1 \pmod{6}$$

(例3) 11^{100} を 3 で割ったときの余りを求めよ。



$$11 \equiv 2 \pmod{3}$$

$$2^2 \equiv 1 \pmod{3}$$

であるから

$$11^{100} \equiv 2^{100} \pmod{3}$$

$$= 2 \cdot 2^{99}$$

$$= 2 \cdot 1^{99} \pmod{3}$$

$$= 2 \pmod{3}$$

(例4) n を 5 で割った余りが 4 のとき、 n^2+n を 5 で割ったときの余りを求めよ。

$$n \equiv 4 \pmod{5} \text{ であるから}$$

$$n^2 + n \equiv 4^2 + 4 \pmod{5}$$

$$= 20$$

$$\equiv 0 \pmod{5}$$

(証明)

$$a \equiv c \pmod{m}, b \equiv d \pmod{m} \text{ とする}$$

$$\begin{cases} a = mg_1 + r_1 \\ c = mg'_1 + r_1 \end{cases} \quad \begin{cases} b = mg_2 + r_2 \\ d = mg'_2 + r_2 \end{cases} \quad (g_1, g'_1, r_1, g_2, g'_2, r_2 \text{ は整数})$$

とおける。

$$a+b = (mg_1 + r_1) + (mg_2 + r_2)$$

$$= m(g_1 + g_2) + \underline{r_1 + r_2}$$

$$c+d = (mg'_1 + r_1) + (mg'_2 + r_2)$$

$$= m(g'_1 + g'_2) + \underline{r_1 + r_2}$$

よって、

$$a+b \equiv c+d \pmod{m}$$

また、2についても同様に証明できる。

$$ab = (mg_1 + r_1)(mg_2 + r_2)$$

$$= m^2 g_1 g_2 + mg_1 r_2 + mr_1 g_2 + r_1 r_2$$

$$= m(mg'_1 g'_2 + g'_1 r_2 + r_1 g'_2) + \underline{r_1 r_2}$$

$$cd = (mg'_1 + r_1)(mg'_2 + r_2)$$

$$= m^2 g'_1 g'_2 + mg'_1 r_2 + mr_1 g'_2 + r_1 r_2$$

$$= m(mg'_1 g'_2 + g'_1 r_2 + r_1 g'_2) + \underline{r_1 r_2}$$

よって

$$ab \equiv cd \pmod{m}$$

また、これをくり返し用いると

$$a^k \equiv c^k \pmod{m} \quad \leftarrow \begin{cases} a \equiv c \pmod{m} \text{ に} \\ a \equiv c \pmod{m} \text{ を} \\ \text{くり返し用いる} \end{cases}$$