11

・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
>
> $a \equiv b \pmod{m}$ （モッド）
>
> で表す。

(例1) $3 \equiv 1 \pmod{2}$ ← 余り1

$98 \equiv 14 \pmod{7}$ ← 余り0

$80 \equiv -1 \pmod{3}$ ← 余り2

> $a \equiv c \pmod{m}$、$b \equiv d \pmod{m}$ 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 $a^k \equiv c^k \pmod{m}$
>
> 等式の計算と同じ
>
> aとmが互いに素のとき
>
> 5 $ax \equiv ay \pmod{m} \Rightarrow x \equiv y \pmod{m}$ （aで割る）

(証明)

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

$$\begin{cases} a = mq_1 + r_1 \\ c = mq_1' + r_1 \end{cases} \quad \begin{cases} b = mq_2 + r_2 \\ d = mq_2' + r_2 \end{cases}$$
（$q_1, q_1', r_1, q_2, q_2', r_2$ は整数）

とおける。

$a+b = (mq_1 + r_1) + (mq_2 + r_2)$

$= m(q_1 + q_2) + r_1 + r_2$

$c+d = (mq_1' + r_1) + (mq_2' + r_2)$

$= m(q_1' + q_2') + r_1 + r_2$

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。

$ab = (mq_1 + r_1)(mq_2 + r_2)$

$= m^2 q_1 q_2 + mq_1 r_2 + mr_1 q_2 + r_1 r_2$

$= m(mq_1 q_2 + q_1 r_2 + r_1 q_2) + r_1 r_2$

$cd = (mq_1' + r_1)(mq_2' + r_2)$

$= m^2 q_1' q_2' + mq_1' r_2 + mr_1 q_2' + r_1 r_2$

$= m(mq_1' q_2' + q_1' r_2 + r_1 q_2') + r_1 r_2$

よって

$ab \equiv cd \pmod{m}$

また、これをくり返し用いると

$a^k \equiv c^k \pmod{m}$ ← $a \equiv c \pmod{m}$ に $a \equiv c \pmod{m}$ をくり返しかける

$ax \equiv ay \pmod{m}$ より

$$\begin{cases} ax = mq_3 + r_3 \\ ay = mq_3' + r_3 \end{cases}$$
（q_3, q_3', r_3 は整数）

とおける。

$ax - ay = (mq_3 + r_3) - (mq_3' + r_3)$

$a(x-y) = m(q_3 - q_3')$

aとmは互いに素なので、$x-y$はmの倍数である

よって

$x \equiv y \pmod{m}$ □

(例2) 37^{100}を6で割ったときの余りを求めよ。

$37 \equiv 1 \pmod{6}$ であるから

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

(例3) 11^{111}を3で割ったときの余りを求めよ。

> point
>
> $a^n \equiv \pm 1 \pmod{m}$
>
> となるようなnを見つける

$11 \equiv 2 \pmod{3}$

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

であるから

$11^{111} \equiv 2^{111} \pmod{3}$

$= 2 \cdot (2^2)^{55}$

$\equiv 2 \cdot 1^{55} \pmod{3}$

$\equiv 2 \pmod{3}$

(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。

$n \equiv 4 \pmod{5}$ であるから

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

$= 20$

$\equiv 0 \pmod{5}$