中国の剰余定理

$m,\ n$ を互いに素な自然数，$a,\ b$ を $0 \leqq a < m,\ 0 \leqq b < n$ となる整数とするとき，m で割った余りが a で，n で割った余りが b であるような整数が必ず存在する。しかも，そのような整数を mn で割った余りはすべて等しい。これを中国の剰余定理と呼ぶ。ここでは，合同式を用いてこれを定式化し証明する。

定理（中国の剰余定理）

$m,\ n$ を互いに素な自然数とし，$a,\ b$ を任意の整数とする。このとき，$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ となる整数 x が存在する。そして $\bmod mn$ で考えれば，このような x はただひとつに決まる。

まず，$m,\ n$ は互いに素であるから，整数論の基本定理より

$$sm + tn = 1 \cdots ①$$

となる整数 $s,\ t$ がある。そこで $x = atn + bsm$ とおく。そうすると

$$\begin{aligned} x &\equiv atn + bsm \pmod{m} \\ &\equiv atn \pmod{m} \end{aligned}$$

となるが，① より $asm + atn = a$ であるから $atn \equiv a \pmod{m}$ である。よって $x \equiv atn \equiv a \pmod{m}$ となり，確かに $x \equiv a \pmod{m}$ である。

全く同様にして $x \equiv b \pmod{n}$ となることも示される。

今度は一意性を示すために，

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \quad \begin{cases} y \equiv a \pmod{m} \\ y \equiv b \pmod{n} \end{cases}$$

とする。そうすると

$$\begin{cases} x - y \equiv 0 \pmod{m} \\ x - y \equiv 0 \pmod{n} \end{cases}$$

となる。従って $x - y$ は m でも n でも割り切れるが，$m,\ n$ は互いに素なので mn で割り切れることになる。よって $x - y \equiv 0 \pmod{mn}$ つまり $x \equiv y \pmod{mn}$ となり，x を mn で割った余りと y を mn で割った余りは等しい。■

［例］5 で割って 3 余り，13 で割って 7 余るような整数を N とする。このとき N を 65 で割った余りを求めよう。

N という数はいろいろあるが，65 で割った余りはすべて一致することは中国の剰余定理から分かっている。

$$N \equiv 3 \pmod 5 \cdots ①$$
$$N \equiv 7 \pmod{13} \cdots ②$$

①×13 より $13N \equiv 39 \pmod{65} \cdots ③$ である。
一方，②×5 より $5N \equiv 35 \pmod{65} \cdots ④$ である。そうすると ③×2 − ④×5 より

$$N \equiv -97 \pmod{65}$$

となるが，$-97 \equiv 33 \pmod{65}$ であるから

$$N \equiv 33 \pmod{65}$$

となる。従って，N を 65 で割った余りは 33 である。
また，5 で割って 3 余り，13 で割って 7 余るような整数の全体は $33 + 65t$ (t は任意の整数) であることも分かった。