フェルマの小定理

p を素数とし，a と p は互いに素であるとする。

まず，p 個の整数 $a, 2a, 3a, \cdots\cdots, (p-1)a, pa$ を p で割ったときの余りはすべて異なることを示そう。

k, l を $1 \leqq k < l \leqq p$ を満たす整数とし，ka と la を p で割ったときの余りが等しいとする。

このとき，

$ka = mp + r$（$0 \leqq m < a$, $0 \leqq r < p$），$la = np + r$（$0 \leqq n \leqq a$, $0 \leqq r < p$）

とおける。

$r = ka - mp$，$r = la - np$ より　$(l-k)a = (m-n)p$

となり，a, p は互いに素な整数だから，$l-k$ は p の倍数であるが，$0 < l-k \leqq p-1$ であるから，これを満たす k, l は存在しない。

よって，ka と la を p で割ったときの余りは等しくない。

pa は p で割り切れるから，$p-1$ 個の整数 $a, 2a, 3a, \cdots\cdots, (p-1)a$ を p で割ると，余りは $1, 2, 3, \cdots\cdots, p-1$ のいずれかである。すなわち，p を法として，

$\{a, 2a, 3a, \cdots\cdots, (p-1)a\} \equiv \{1, 2, 3, \cdots\cdots, p-1\}$　（mod p）

これらの積を作ると，

$a \times 2a \times 3a \times \cdots\cdots \times (p-1)a \equiv 1 \times 2 \times 3 \times \cdots\cdots \times (p-1)$

$(p-1)! \times a^{p-1} \equiv (p-1)!$　（mod p）

$(p-1)!$ と p は互いに素であるから，$a^{p-1} \equiv 1$　（mod p）

中国の剰余定理（Chinese remainder theorem）

m, n を互いに素な正の整数とする。任意の整数 a, b に対して，連立合同式

$$x \equiv a \ (\mathrm{mod}\ m), \qquad x \equiv b \ (\mathrm{mod}\ n)$$

を満たす整数 x が mn を法として一意的に存在する。

注　この定理を一般化したものが中国の剰余定理（または孫子の剰余定理）である。

〔証明〕(i)　まず，連立合同式の解が存在することを示そう。

m, n が互いに素だから，　$mu + nv = 1$

を満たす整数 u, v が存在する。ここで，$y_1 = nv = 1 - mu$，$y_2 = mu = 1 - nv$ とおくと，

$y_1 \equiv 1$（mod m），$y_2 \equiv 0$（mod m）

$y_1 \equiv 0$（mod n），$y_2 \equiv 1$（mod n）

となる。このとき，$x = ay_1 + by_2$ とおくと，この x が，連立合同式の解である。

(ii)　次に，一意性について示そう。

x', x''がともに連立合同式の解であるとする。すなわち，

$x' \equiv x''$（$\equiv a$）（mod m），$x' \equiv x''$（$\equiv b$）（mod n）

とする。$x' - x''$ は m の倍数であり，かつ n の倍数である。m, n は互いに素だから m, n の最小公倍数は mn だから，$x' - x''$ は mn の倍数である。

よって，$x' \equiv x''$（mod mn）だから，mn を法として解は一意的に存在する。