ウィルソンの定理

定理 (Wilson). p を 2 以上の整数とする．このとき，次が成り立つ．

$$p \text{ は素数} \iff (p-1)! \equiv -1 \mod p$$

証明．まず，$p=2$ とすると，p は素数であり，$(2-1)! = 1 \equiv -1 \mod 2$ が成り立つので，この場合は良い．以下では，$p \geqq 3$ とする．

$(\Rightarrow)$ p を奇素数とする．$1 \leqq a \leqq p-1$ を満たす自然数 a を 1 つとると，a と p は互いに素なので，フェルマーの小定理[1]より，

$$a \cdot a^{p-2} = a^{p-1} \equiv 1 \mod p$$

が成り立つ．a に対して，

$$b \equiv a^{p-2} \mod p, \quad 1 \leqq b \leqq p-1$$

を満たす整数 b をとると，a と b は，

$$a \cdot b \equiv 1 \mod p \tag{1}$$

を満たす．また，

$$b^{p-2} \equiv \left(a^{p-2}\right)^{p-2} = a^{(p-2)^2} = a^{(p-3)(p-1)+1} = \left(a^{p-1}\right)^{p-3} \cdot a \equiv a \mod p$$

が成り立つことから，a に対して b を定めたのと同様にして，b に対して定まる自然数は，a に他ならない．このようにして，合同式 (1) を満たす 1 以上，$p-1$ 以下の自然数の組 (a, b) を作ることができる．

$a \neq b$ となるための必要十分条件を考える．これは，

$$\begin{aligned} a^2 \equiv 1 \mod p &\iff a^2 - 1 \equiv 0 \mod p \\ &\iff (a-1)(a+1) \equiv 0 \mod p \\ &\iff a \equiv \pm 1 \mod p \\ &\iff a = 1,\ p-1 \end{aligned}$$

が成り立つことと，

$$a^2 \equiv 1 \mod p \iff a \equiv a^p = a^{p-2} \cdot a^2 \equiv a^{p-2} \equiv b \mod p$$

が成り立つことから，

$$a \neq 1,\ p-1 \iff a \neq b$$

であることが分かる．

以上から，$p-1$ 個の自然数 $1, \cdots, p-1$ から，1 と $p-1$ を除いた $p-3$ 個の自然数は，合同式 (1) を満たすような $\frac{p-3}{2}$ 個の組にすることができる．よって，

$$(p-1)! \equiv 1 \cdot 1^{\frac{p-3}{2}} \cdot (p-1) \equiv -1 \mod p$$

が従う．

$(\Leftarrow)$ 対偶を示す．$p \geqq 3$ が合成数であると仮定すると，ある自然数 n, m $(2 \leqq n, m \leqq p-1)$ が存在して，$p = nm$ と書ける．よって，$(p-1)!$ は，p の倍数となり，$(p-1)! \equiv 0 \mod p$ が従う．よって，

$$(p-1)! \not\equiv 0 \mod p \implies p \text{ は素数} \tag{2}$$

が成り立つ．ここで，上の証明と合わせて，p を法として，$(p-1)!$ は，-1 か 0 のいずれかなので，$(p-1)! \not\equiv 0 \mod p$ であることと，$(p-1)! \equiv -1 \mod p$ であることは同じである．以上から，主張が従う． □

[1] p を素数，a を p と互いに素な整数とすると，$a^{p-1} \equiv 1 \mod p$ が成り立つ．