フェルマーの小定理

定理 (Fermat). p を素数とする．

- 任意の整数 a に対して，次が成り立つ．
$$a^p \equiv a \mod p$$
- p と互いに素な整数 a に対して，次が成り立つ．
$$a^{p-1} \equiv 1 \mod p$$

証明. • 1 つ目の主張を示す．$a = 0$ のときは明らかなので，$a \neq 0$ とする．

$a > 0$ の場合を示す．下の補題を繰り返し用いることで，a^p は，p を法として，

$$\begin{aligned} a^p &= \{(a-1)+1\}^p \\ &\equiv (a-1)^p + 1 = \{(a-2)+1\}^p + 1 \\ &\equiv (a-2)^p + 2 \equiv \cdots \equiv (a-a)^p + a = a \end{aligned}$$

と計算できる．よって，$a > 0$ のときは主張が従う．

$a < 0$ の場合，$b = -a$ とおけば，$b > 0$ である．よって，上と同様にして，合同式

$$b^p \equiv b \mod p \tag{1}$$

が得られる．$p = 2$ なら，$a \equiv -a \mod 2$ なので，合同式 (1) を用いて，

$$a^2 = (-a)^2 = b^2 \equiv b = -a \equiv a \mod 2$$

と計算でき，主張の合同式が得られる．$p > 2$ なら，p は奇数なので，$b^p = -a^p$ である．よって，合同式 (1) を用いて，

$$-a^p = b^p \equiv b = -a \mod p$$

が得られる．この合同式の両辺を -1 倍することで，主張の合同式が得られる．

• 2 つ目の主張を示す．0 は任意の素数の倍数なので，a と p が互いに素であるという仮定から，$a \neq 0$ であることに注意する．1 つ目の主張から，合同式

$$a(a^{p-1} - 1) \equiv 0 \mod p$$

が得られるが，a と p は互いに素なので，

$$a^{p-1} - 1 \equiv 0 \mod p$$

が成り立つ． □

....

補題. p を素数，n を自然数とする．このとき，

$$(n+1)^p \equiv n^p + 1 \mod p$$

が成り立つ[1]．

---

[1]証明は，https://gleamath.com/binomial-thm-mod-p を参照．