高校生のための現代数学講座　　東京大学
「素数と暗号」　　玉原国際セミナーハウス
講義 (3)　坂井　秀隆　　2017 年 7 月 15 日

「フェルマーの小定理」

自然数 $n \geq 1$ にたいし

$$\mathbb{Z}/n\mathbb{Z} = \{a \in \mathbb{Z} \mid 0 \leq a \leq n-1\}, \quad (\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1\}$$

として，$\varphi(n)$ を $(\mathbb{Z}/n\mathbb{Z})^*$ の元の個数とする．

例 1. 素数 p にたいし，$(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p-1\}$，よって $\varphi(p) = p - 1$.

例 2. $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$，よって $\varphi(12) = 4$.

定理 1. n を自然数，a を n と互いに素な整数とすれば

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

が成り立つ.

上の定理と例 1 より次が従う．

定理 2 (フェルマー (Fermat) の小定理)**.** a を素数 p で割り切れない整数とすれば

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ.

ちなみに，次の定理が成り立つ．

定理 3. $n = 2^e p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ を n の素因数分解とすると

$$\varphi(n) = 2^{e-1} p_1^{a_1-1} p_2^{a_2-1} \cdots p_r^{a_r-1} (p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

補題 3. a と b は互いに素な整数とする．このとき, 整数 x, y で $ax + by = 1$ となるものが存在する.

補題 4. a, b, c を整数, n を自然数とし, n と c は互いに素であるとする．このとき, $ac \equiv bc \pmod{n}$ ならば, $a \equiv b \pmod{n}$ が成り立つ.

補題 5. 自然数 n を固定して，整数 a にたいし a を n で割ったあまりを $\overline{a}$ で表す．$\overline{a}$ は $\mathbb{Z}/n\mathbb{Z}$ の元である．整数 a, b, c にたいし次が成り立つ.

(1) $a = \overline{a} \pmod{n}$.

(2) $\overline{ab} = \overline{(\overline{a}\overline{b})} = \overline{(a\overline{b})} = \overline{(\overline{a}b)}$.

(3) $(a, n) = 1$ かつ $\overline{ab} = \overline{ac}$ なら $\overline{b} = \overline{c}$ である.

(4) $(a, n) = 1$ かつ $(b, n) = 1$ なら $(ab, n) = 1$ である.

定理 1 の証明：$(\mathbb{Z}/n\mathbb{Z})^*$ の元の集合を

$$\{a_1, a_2, \cdots, a_r\} \quad (r = \varphi(n))$$

とする. $(a, n) = 1$ なので, 補題 5(3) より, 集合として

$$\{a_1, a_2, \cdots, a_{p-1}\} = \{\overline{aa_1}, \overline{aa_2}, \cdots, \overline{aa_r}\}$$

となる. ゆえに,

$$\begin{aligned} a_1 \cdot a_2 \cdot \cdots \cdot a_r &= \overline{aa_1} \cdot \overline{aa_2} \cdot \cdots \cdot \overline{aa_r} \\ &= \overline{a^r a_1 \cdot a_2 \cdot \cdots \cdot a_r} \\ &\equiv a^r (a_1 \cdot a_2 \cdot \cdots \cdot a_r) \pmod{n} \end{aligned}$$

となる. ここで 2 番目の等式と 3 番目の合同式は補題 5 による．$(a_i, n) = 1$ $(1 \le i \le r)$ より，$(n, a_1 \cdot a_2 \cdot \cdots \cdot a_r) = 1$ であるので，再び補題 4 より

$$a^r \equiv 1 \pmod{n}$$

となる. これは求める式にほかならない.

系 6. p, q を *2* つの素数とする. $(a, pq) = 1$ ならば,

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

例 7. $p = 71$ は素数, $a = 1666$ は 71 で割り切れない. よって,

$$1666^{70} \equiv 1 \pmod{71}$$

例 8. $p = 71, q = 97$ とし, $n = pq = 6887$ を考える. このとき, $(p-1)(q-1) = 6720$. $a = 1687$ をとれば, 1687 は 71, 97 で割り切れないから

$$1687^{6720} \equiv 1 \pmod{6887}$$

を得る.

問題 9. 2^{56} を 57 で割ったあまりを計算してみよう.

$56 = 32 + 16 + 8 = 2^5 + 2^4 + 2^3$

$2^2 \equiv 4 \pmod{57}$

$2^{2^2} = 4^2 \equiv 16 \pmod{57}$

$2^{2^3} = 16^2 \equiv$

$2^{2^4} \equiv$

$2^{2^5} \equiv$

例 10. $2^{340} = (2^{10})^{34} = 1024^{34} = (3 \cdot 341 + 1)^{34} \equiv 1^{34} \equiv 1 \pmod{341}$

$3^{340} \equiv 56 \pmod{341}$

例 11. 561 は特別な数で, $2^{560} \equiv 3^{560} \equiv \cdots \equiv 560^{560} \equiv 1 \pmod{561}$ であるが, $561 = 3 \cdot 11 \cdot 17$ で, 素数ではない.