高校生のための現代数学講座　　東京大学
「素数の世界」　　玉原国際セミナーハウス
講義 (1)　斎藤秀司　　2009 年 7 月 31 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 0.1 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 0.2 $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11, \}$，よって $\varphi(12) = 4$.

定理 0.3 $n = 2^e p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ を n の素因数分解とすると

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

次の定理は重要である.

定理 0.4 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 0.1 より次が従う.

定理 0.5 (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.

補題 0.6 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.

証明. 前の講義でやったユークリッドの互除法からの帰結である. □

補題 0.7 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.

証明. 補題 0.6 より，整数 x, y で $cx + ny = 1$ となるものが存在する．よって,

$$a = acx + any, \ b = bcx + bny$$

となる．ゆえに, $a - b = (ac - bc)x + (ay - by)n$ となるが, 仮定からこの右辺は n で割り切れる．従って, $a - b$ も n で割り切れる. □

補題 0.8 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．

証明. (1) と (2) は簡単なので演習問題とする．(3) は補題 0.7 の帰結である．□

定理 0.4 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 0.8(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 0.8 による．$(a_i, n) = 1$ $(1 \leq i \leq r)$ より，$(n, a_1 \cdot a_2 \cdot \cdots \cdot a_r) = 1$ であるので，再び補題 0.7 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 0.9 p, q を *2* つの素数とする．$(a, pq) = 1$ ならば,

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

証明. 定理 0.3 より $\varphi(pq) = (p-1)(q-1)$. よって主張は定理 0.4 より従う．□

例 0.10 $p = 71$ は素数, $a = 1666$ は 71 で割り切れない．よって,

$$1666^{70} \equiv 1 \ (mod\ 71)$$

例 0.11 $p = 71, q = 97$ 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.

フェルマーの小定理についての問題

[1] 自然数 n にたいし、$\varphi(n) = 12$ が成り立つとする。

(1) $n = 2^e p^a q^b$ または $n = 2^e p^a$ ($p, q > 2$ は素数) とかけることを示せ。

(2) n は次のいずれかであることを示せ：$3\cdot 7,\ 2\cdot 3\cdot 7,\ 2^2\cdot 3^2,\ 2^2\cdot 7,\ 13,\ 2\cdot 13$

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

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

[2] フェルマーの小定理を使って次の事実を示せ。
x を自然数として、素数 $p > 2$ が $x^2 + 1$ の約数なら $p \equiv 1 \mod 4$ である。

ヒント：仮定より $x^2 \equiv -1 \mod p$ である。これより $x^4 \equiv 1 \mod p$ となる。一方、$t = 1, 2, 3$ にたいしては、$x^t \not\equiv 1 \mod p$ である（なぜなら、たとえば $x \equiv 1 \mod p$ なら $x^2 \equiv 1 \mod p$ となり、$1 \equiv -1 \mod p$ となるが、$p > 2$ ならこれは矛盾である）。ここで、$p - 1$ を 4 で割った商を q、あまりを r ($0 \le r \le 3$) とすれば、$p - 1 = 4q + r$ である。フェルマーの小定理より、

$$(x^4)^q x^r = x^{p-1} \equiv 1 \mod p$$

が成り立つので、$x^4 \equiv 1 \mod p$ とあわせて $x^r \equiv 1 \mod p$ が従う。よって先に注意したことから $r = 0$ でなくてはならない。

[3] [2] を使って次の事実を示せ。
$p \equiv 1 \mod 4$ を満たす素数 p が無限個存在する。

ヒント：背理法により示す。$p \equiv 1 \mod 4$ を満たす素数が有限個しか存在しないと仮定して、それらを $p_1,\ p_2,\ \ldots, p_r$ とする。$x = (2p_1p_2\cdots p_r)^2 + 1$ とおき、q を a の素因子とする。[2] より $q \equiv 1 \mod 4$ が成り立つ。さらに、a が $p_1,\ p_2,\ \ldots, p_r$ で割れないことを示し、よって q はこれらのいずれとも異なるので、$p_1,\ p_2,\ \ldots, p_r$ のとり方に矛盾する。