初等整数論 (6回目)

6. オイラーの定理

今回は合同式の計算で有用なフェルマーの小定理とその一般化であるオイラーの定理を解説する. 下図は a^n を 7 で割った余りを計算した表である.

$a \setminus n$	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

右端がすべて 1 に気づく. つまり, $a = 1, 2, ..., 6$ に対して, $a^6 \equiv 1 \pmod 7$ が成り立つ. このような性質をフェルマーの小定理という.

定理 6-1 (フェルマーの小定理)
素数 p と整数 a に対して, $\gcd(a, p) = 1$ のとき,

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

次にフェルマーの小定理の使い方をみておく.

例題 6-1.

(1) 2^{45} を 23 で割った余りを求めよ.

(2) 2^{40} を 23 で割った余りを求めよ.

[解答]
(1) フェルマーの小定理より $2^{22} \equiv 1 \pmod{23}$. よって

$$2^{45} \equiv (2^{22})^2 \times 2 \equiv 2 \pmod{23}.$$

従って余りは 2.

(2) まず,

$$16 \times 2^{40} \equiv 2^{44} \equiv 1 \pmod{23} \quad (\clubsuit)$$

に注意する. $\gcd(16,23)=1$ よりユークリッド互除法から次式を得る.

$$(-10)\times 16+7\times 23=1.$$

よって $(-10)\times 16\equiv 1 \pmod{23}$. 式 (♣) を -10 倍すると

$$2^{40}\equiv -10\equiv 13 \pmod{23}.$$

従って余りは 13.

□

問題 6-1

(1) 3^{20} を 17 で割った余りを求めよ.

(2) 3^{15} を 17 で割った余りを求めよ.

(3) 3^{20} を 85 で割った余りを求めよ.

フェルマーの小定理では素数を法として考えるが, これを自然数に一般化したものをオイラーの定理と言う. オイラーの定理を紹介するために記号を一つ準備する.

定義 6-1 (オイラー関数)
自然数 m に対して, $1,2,...,m$ のうち m と互いに素な整数の個数を $\varphi(m)$ で表す. 特に p が素数ならば, $\varphi(p)=p-1$ である. 関数 $\varphi(m)$ を**オイラー関数**という.

$1,2,....,10$ のなかで 10 と互いに素なものは $1,3,7,9$ の 4 つ. よって $\varphi(10)=4$.

定理 6-2 (オイラーの定理)
自然数 m と整数 a に対して, $\gcd(a,m)=1$ のとき,

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

[証明]
整数 x に対し, $R_m(x)$ を x を m で割った余りとする. また $a_1,a_2,...,a_{\varphi(m)}$ を $1,2,....,m$ の中で, m と互いに素なもの全体とする. まず,

$$\{R_m(aa_1),R_m(aa_2),...,R_m(aa_{\varphi(m)})\}=\{a_1,a_2,...,a_{\varphi(m)}\} \quad (\diamondsuit)$$

を示す. $\gcd(aa_i,m)=1$ $(i=1,2,...,\varphi(m))$ より,

$$\{R_m(aa_1),R_m(aa_2),...,R_m(aa_{\varphi(m)})\}\subseteq\{a_1,a_2,...,a_{\varphi(m)}\}. \quad (\spadesuit)$$

また整数 k, j $(1 \leq k \leq j \leq \varphi(m))$ に対し,

$$\begin{aligned} R_m(aa_k) = R_m(aa_j) &\Rightarrow aa_k \equiv aa_j \pmod{m} \\ &\Rightarrow a_k \equiv a_j \pmod{m} \quad (\because \gcd(a,m)=1) \\ &\Rightarrow a_k = a_j \\ &\Rightarrow k = j. \end{aligned}$$

よって $R_m(aa_1),\ R_p(aa_2), ..., R_p(aa_{\varphi(m)})$ は相異なる $\varphi(m)$ 個の元からなる. これと包含関係 (♠) より式 (♢) が成り立つ. 式 (♢) より

$$\prod_{k=1}^{\varphi(m)} a_k = \prod_{k=1}^{\varphi(m)} R_m(aa_k) \equiv \prod_{k=1}^{\varphi(m)} aa_k \equiv a^{\varphi(m)} \prod_{k=1}^{\varphi(m)} a_k \pmod{m}.$$

ここで,

$$\gcd\left(\prod_{k=1}^{\varphi(m)} a_k,\ m\right) = 1$$

より $a^{\varphi(m)} \equiv 1 \pmod{m}$ を得る.

□

定理 6-2 を用いてフェルマーの小定理を示す.

[定理 6-1 の証明]

素数 p に対して $\varphi(p) = p - 1$. 定理 6-2 より

$$a^{p-1} \equiv a^{\varphi(p)} \equiv 1 \pmod{p}.$$

□

定理 6-3.

(1) $\gcd(m,n) = 1$ のとき, $\varphi(mn) = \varphi(m)\varphi(n)$.

(2) 素数 p と自然数 n に対して, $\varphi(p^n) = p^{n-1}(p-1)$.

(3) 自然数 n の素因数分解を $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ とすると,

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

[証明]

(1) 自然数 t に対して

$$S_t = \{x \in \mathbb{N} \mid 1 \leq x \leq t, \quad \gcd(x,t) = 1\}$$

とし, さらに写像

$$\varphi : S_{nm} \to S_m \times S_n \quad (x \mapsto (R_m(x), R_n(x)))$$

を考える. 中国剰余定理から φ は全単射である. 従って $\varphi(mn) = \varphi(m)\varphi(n)$.

(2) 問題 6-2.

(3) (1) を繰り返し用いると,

$$\varphi(n) = \varphi(p_1^{s_1})\varphi(p_2^{s_2}) \cdots \varphi(p_k^{s_k}).$$

さらに (2) から

$$\begin{aligned} \varphi(n) &= (p_1 - 1)p^{s_1 - 1} \cdot (p_2 - 1)p^{s_2 - 1} \cdots (p_k - 1)p^{s_k - 1} \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

□

問題 6-2 素数 p と自然数 n に対して, $\varphi(p^n) = p^{n-1}(p-1)$ を示せ.

例題 6-2.

(1) $\varphi(30)$ を求めよ.

(2) 7^{10} を 30 で割った余りを求めよ.

[**解答**]
(1) $\varphi(30) = \varphi(2)\varphi(3)\varphi(5) = 8$.

(2) オイラーの定理より $7^8 \equiv 1 \pmod{30}$. よって

$$7^{10} \equiv 7^2 \equiv 49 \equiv 19 \pmod{30}.$$

従って余りは 19.

問題 6-3

(1) $\varphi(98)$ を求めよ.

(2) 3^{45} を 98 で割った余りを求めよ.