整数論と代数の初歩

廣瀬勝一

準備

整数の集合 $\mathbb{Z} \stackrel{\text{def}}{=} \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

床関数　$\lfloor x \rfloor = \max\{b \in \mathbb{Z} \,|\, b \leq x\}$

天井関数　$\lceil x \rceil = \min\{b \in \mathbb{Z} \,|\, b \geq x\}$

例）$\lfloor 3.14 \rfloor = 3$ and $\lceil 3.14 \rceil = 4$.

整数 a と正整数 b について

$$a = q \cdot b + r \quad \text{かつ} \quad 0 \leq r \leq b - 1$$

を満たす整数 q, r が一意に決まる．q は商，r は剰余.

例）$a = 68, b = 7$ のとき，$67 = 9 \times 7 + 4$

合同

a, b を整数とし，n を正整数とする．n が $a - b$ を割り切るとき，a は n を法として b と合同であると言う．これは以下のように表記される．

$$a \equiv b \pmod{n}$$

注意）$a \bmod n$ は a を n で割ったときの剰余を表す二項演算

- $13 \equiv 4 \pmod{9}$
- $13 \bmod 9 = 4$

最大公約数と最小公倍数

a, b を正整数とする.

$\gcd(a, b)$ は a, b の最大公約数を表す.

$\gcd(a, b) = 1$ のとき，a, b は互いに素であるという.

例)

- $\gcd(45, 12) = 3$
- 56 と 15 は互いに素.

$\mathrm{lcm}(a, b)$ は a, b の最小公倍数を表す.

$$\mathrm{lcm}(a, b) = \frac{a \cdot b}{\gcd(a, b)}$$

ユークリッドの互除法

与えられた二つの正整数 a_0, a_1 の最大公約数を計算するアルゴリズム

以下の一連の除算を行う（$a_0 > a_1$ が仮定されている）

$$
\begin{aligned}
a_0 &= a_1\, q_1 + a_2 \\
a_1 &= a_2\, q_2 + a_3 \\
&\vdots \\
a_{k-2} &= a_{k-1}\, q_{k-1} + a_k \\
a_{k-1} &= a_k\, q_k
\end{aligned}
$$

$a_0, a_1, \ldots, a_k$ について

$$
\gcd(a_0, a_1) = \cdots = \gcd(a_{k-1}, a_k) = a_k
$$

拡張されたユークリッドの互除法

$\alpha_0, \alpha_1, \ldots, \alpha_k$ と $\beta_0, \beta_1, \ldots, \beta_k$ を以下のように定義する

$$\begin{aligned} \alpha_0 &= 1 & \beta_0 &= 0 \\ \alpha_1 &= 0 & \beta_1 &= 1 \\ \alpha_j &= \alpha_{j-2} - q_{j-1}\alpha_{j-1} & \beta_j &= \beta_{j-2} - q_{j-1}\beta_{j-1} \end{aligned}$$

このとき，$\alpha_j\, a_0 + \beta_j\, a_1 = a_j$ が成立するので，

$$\alpha_k\, a_0 + \beta_k\, a_1 = a_k = \gcd(a_0, a_1)$$

例

$a_0 = 770, a_1 = 336$

$$
\begin{aligned}
770 &= 336 \times 2 + 98 \\
336 &= 98 \times 3 + 42 \\
98 &= 42 \times 2 + 14 \\
42 &= 14 \times 3
\end{aligned}
\qquad
\begin{aligned}
\alpha_0 &= 1 & \beta_0 &= 0 \\
\alpha_1 &= 0 & \beta_1 &= 1 \\
\alpha_2 &= 1 & \beta_2 &= -2 \\
\alpha_3 &= -3 & \beta_3 &= 7 \\
\alpha_4 &= 7 & \beta_4 &= -16
\end{aligned}
$$

$$7 \times 770 + (-16) \times 336 = 14$$

剰余演算（加算，減算）

n を法とする加算の結果 $=$ 通常の加算の結果を n で割った剰余

減算 $x - y = x + (-y)$

例）$n = 7$ を法とする加減算

$x+y$	y						
	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x

y	$-y$
0	0
1	6
2	5
3	4
4	3
5	2
6	1

剰余演算（乗算，除算）

n を法とする乗算の結果 = 通常の乗算の結果を n で割った剰余

除算 $x/y = x \cdot y^{-1}$

例）$n = 7$ を法とする乗除算

$x \cdot y$	y					
	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

y	y^{-1}
1	1
2	4
3	5
4	2
5	3
6	6

剰余演算の性質

n を法とする剰余演算について，$a > n$, $b > n$ のとき

- $a + b \bmod n = (a \bmod n) + (b \bmod n) \bmod n$
- $a \cdot b \bmod n = (a \bmod n) \cdot (b \bmod n) \bmod n$
- $-a \bmod n = -(a \bmod n) \bmod n$
- $a^{-1} \bmod n = (a \bmod n)^{-1} \bmod n$

例）

- $8 \cdot 9 \bmod 5 = 3 + 4 \bmod 5 = 2$
- $8 \cdot 9 \bmod 5 = 3 \cdot 4 \bmod 5 = 2$
- $-9 \bmod 5 = -4 \bmod 5 = 1$

$$9 + (-9) \bmod 5 = 9 + 1 \bmod 5 = 10 \bmod 5 = 0$$

- $7^{-1} \bmod 5 = 2^{-1} \bmod 5 = 3$

$$7 \cdot 7^{-1} \bmod 5 = 7 \cdot 3 \bmod 5 = 21 \bmod 5 = 1$$

剰余演算の性質

例）n を法とする剰余乗算について，$a > n$, $b > n$ のとき

$a = q \cdot n + r, b = q' \cdot n + r'$（$0 \leq r \leq n-1, 0 \leq r' \leq n-1$）とすると

$$\begin{aligned} a \cdot b \bmod n &= (q \cdot n + r)(q' \cdot n + r') \bmod n \\ &= (q \cdot q' \cdot n^2 + (q \cdot r' + q' \cdot r)n + r \cdot r') \bmod n \\ &= r \cdot r' \bmod n \\ &= (a \bmod n) \cdot (b \bmod n) \bmod n \end{aligned}$$

孫子定理 (Chinese Remainder Theorem) (1/2)

正整数 $n_1, n_2, \ldots, n_k$ はどの二つも互いに素であるとし，$N = \prod_{i=1}^{k} n_i$ とする．このとき，整数 $c_1, c_2, \ldots, c_k$ について

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \quad \cdots \\ x \equiv c_k \pmod{n_k} \end{cases}$$

は $\{0, 1, \ldots, N-1\}$ に唯一の解

$$x = \sum_{i=1}^{k} c_i \, N_i \, y_i \bmod N$$

を持つ．ここで，$1 \leq i \leq k$ について

$$N_i = N/n_i \ , \qquad y_i = {N_i}^{-1} \bmod n_i$$

である．

例

$$\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 6 \pmod 8 \\ x \equiv 7 \pmod{11} \end{cases}$$

について

$$N = 7 \times 8 \times 11 = 616$$

であり

$$\begin{aligned} N_1 &= 88 \ , & y_1 &= 88^{-1} \bmod 7 = 4^{-1} \bmod 7 = 2 \\ N_2 &= 77 \ , & y_2 &= 77^{-1} \bmod 8 = 5^{-1} \bmod 8 = 5 \\ N_3 &= 56 \ , & y_3 &= 56^{-1} \bmod 11 = 1^{-1} \bmod 11 = 1 \end{aligned}$$

したがって

$$x = \sum_{i=1}^{3} c_i \, N_i \, y_i \bmod N = 590$$

オイラー関数 (Euler Totient Function)

整数 $n \geq 1$ に対し，オイラー関数は以下のように定義される．

$$\phi(n) \stackrel{\text{def}}{=} |\{x \,|\, x \in \mathbb{Z} \wedge 1 \leq x \leq n \wedge \gcd(x, n) = 1\}|$$

Theorem 1

n の素因数分解を $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ とすると

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

表記法

- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
- $\mathbb{Z}_n^* = \{x \,|\, x \in \mathbb{Z}_n \wedge \gcd(x, n) = 1\}$

注意　$n \geq 2$ について，$\phi(n) = |\mathbb{Z}_n^*|$

例

$$\phi(5) = |\{1,2,3,4\}| = 5\left(1-\frac{1}{5}\right) = 4$$

$$\phi(9) = |\{1,2,4,5,7,8\}| = 9\left(1-\frac{1}{3}\right) = 6$$

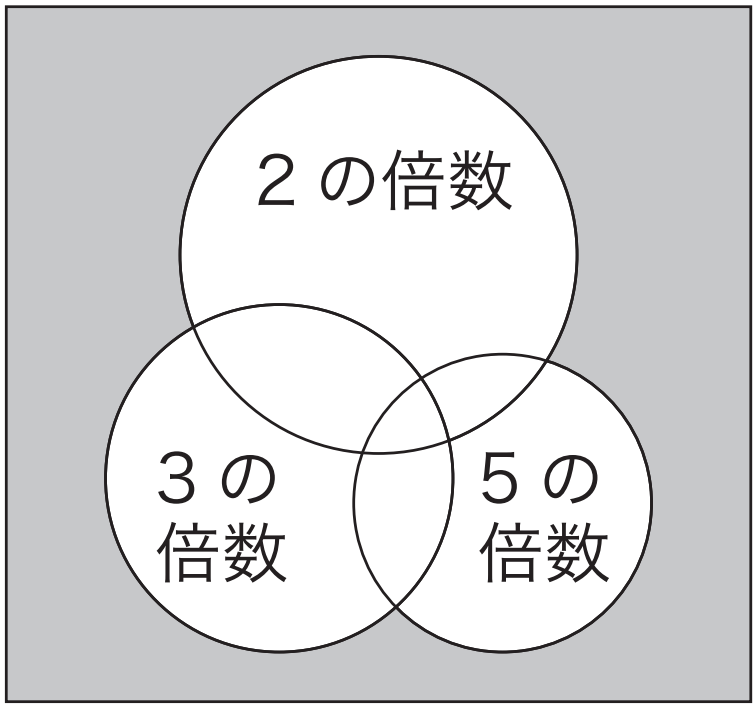
$$\phi(12) = |\{1,5,7,11\}| = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 4$$

$$\phi(30) = |\{1,7,11,13,17,19,23,29\}|$$
$$= 30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 8$$

例

$$\mathbb{Z}_{30}^* = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

$$\begin{aligned}
\phi(30) &= 30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) \\
&= 30\left(1-\left(\frac{1}{2}+\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{2\times 3}+\frac{1}{2\times 5}+\frac{1}{3\times 5}\right)-\frac{1}{2\times 3\times 5}\right) \\
&= 30-(15+10+6)+(5+3+2)-1=8
\end{aligned}$$



オイラーの定理

Theorem 2

a, n を正整数とする．

$$\gcd(a, n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

証明　関数 $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ を $f(x) = ax \bmod n$ と定義する．$\gcd(a, n) = 1$ ならば，a は $\mathbb{Z}_n^*$ に逆元を持つので，f は 1 対 1 関数である．
$\mathbb{Z}_n^* = \{b_1, b_2, \ldots, b_{\phi(n)}\}$ と表記すると，

$$\prod_{i=1}^{\phi(n)} b_i \equiv \prod_{i=1}^{\phi(n)} (ab_i) \equiv a^{\phi(n)} \prod_{i=1}^{\phi(n)} b_i \pmod{n}$$

であり，これより $a^{\phi(n)} \equiv 1 \pmod{n}$ であることが導かれる． □

例

$n = 15$, $a = 4$

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, $\phi(15) = 8$

$f : \mathbb{Z}_{15}^* \to \mathbb{Z}_{15}^*$

$$f(x) = 4x \bmod 15$$

x	1	2	4	7	8	11	13	14
$f(x)$	4	8	1	13	2	14	7	11

$\mathbb{Z}_{15}^* = \{b_1, b_2, \ldots, b_8\}$ と表記すると,

$$\prod_{i=1}^{8} b_i \equiv \prod_{i=1}^{8} (4b_i) \equiv 4^8 \prod_{i=1}^{8} b_i \pmod{n}$$

であり，これより $4^8 \equiv 1 \pmod{n}$.

フェルマーの小定理 (Fermat's Little Theorem)

Corollary 3

a, p を正整数とする．p が素数でありかつ $\gcd(a, p) = 1$ ならば，

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

証明　$\phi(p) = p - 1$ だから，オイラーの定理より明らか． □

群 (Group)

以下の条件が満たされるとき，G は演算 $\circ$ に関して**群**をなすと言う．

- $\circ$ は閉じている．即ち，すべての $a, b \in G$ について $a \circ b \in G$
- $\circ$ は**結合則**を満たす．即ち，すべての $a, b, c \in G$ について $(a \circ b) \circ c = a \circ (b \circ c)$
- すべての $a \in G$ について $a \circ I = I \circ a = a$ を満たす $I \in G$ が存在する．I は**単位元 (identity)** と呼ばれる．
- すべての $a \in G$ について，$a \circ a^{-1} = a^{-1} \circ a = I$ を満たす $a^{-1} \in G$ が存在する．a^{-1} は a の**逆元 (inverse)** と呼ばれる．

さらに交換則が満たされるとき，可換群と呼ばれる．

$$\text{すべての } a, b \in G \text{ について } a \circ b = b \circ a$$

演算 $\circ$ が加法のとき，G は**加法群 (additive group)** と呼ばれる．
演算 $\circ$ が乗法のとき，G は**乗法群 (multiplicative group)** と呼ばれる．

加法群の例

例 1）$\mathbb{Z}$ は加法に関して（可換）群をなす.

- 単位元は 0 である.
- すべての $a \in \mathbb{Z}$ について，a の逆元は $-a$ である.

例 2）任意の正整数 n について，$\mathbb{Z}_n$ は n を法とする加法に関して（可換）群をなす.

- 単位元は 0 である.
- すべての $a \in \mathbb{Z}_n$ について，a の逆元は $n - a$ である.

乗法群に関する例

例 1）$\mathbb{Q} \setminus \{0\}$ は乗法に関して（可換）群をなす.

例 2）$\mathbb{Z} \setminus \{0\}$ は乗法に関して群をなさない.

例 3）任意の正整数 n について，$\mathbb{Z}_n^*$ は n を法とする乗法に関して（可換）群をなす.

- 単位元は 1 である.
- すべての $a \in \mathbb{Z}_n^*$ について，逆元 $a^{-1} \in \mathbb{Z}_n^*$ が存在する.

拡張ユークリッドの互除法より $\alpha\, a + \beta\, n = 1$ を満たす整数 α, β が存在し

$$\alpha\, a \equiv 1 \pmod{n}$$

である．したがって，$a^{-1} = \alpha \bmod n$ である.

例）$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

$$-10 \times 2 + 1 \times 21 = 1$$

したがって

$$2^{-1} \equiv -10 \equiv 11 \pmod{21}$$

$\mathbb{Z}_{21}^*$ の乗算表

	1	2	4	5	8	10	11	13	16	17	19	20
1	1	2	4	5	8	10	11	13	16	17	19	20
2	2	4	8	10	16	20	1	5	11	13	17	19
4	4	8	16	20	11	19	2	10	1	5	13	17
5	5	10	20	4	19	8	13	2	17	1	11	16
8	8	16	11	19	1	17	4	20	2	10	5	13
10	10	20	19	8	17	16	5	4	13	2	1	11
11	11	1	2	13	4	5	16	17	8	19	20	10
13	13	5	10	2	20	4	17	1	19	11	16	8
16	16	11	1	17	2	13	8	19	4	20	10	5
17	17	13	5	1	10	2	19	11	20	16	8	4
19	19	17	13	11	5	1	20	16	10	8	4	2
20	20	19	17	16	13	11	10	8	5	4	2	1

幾つかの性質

G を有限の (乗法) 群とする.

定義　G の要素の個数を G の**位数 (order)** と言う.

定義　$a \in G$ について，$a^m = 1$ を満たす最小の正整数 m を a の**位数 (order)** と言う.

Theorem 4

G の位数を n とする．すべての $a \in G$ について a の位数は n の約数である.

Corollary 5

G の位数を n とする．すべての $a \in G$ について $a^n = 1$ である.

オイラーの定理は Cor. 5 より導かれる.

Th. 4 の証明

$a \in G$ の位数を k とする．$A = \{a^1, a^2, \ldots, a^k\}$ は G の部分群である．

$b_i \notin A \cup b_1 A \cup \cdots \cup b_{i-1} A$ である G の要素が存在する限り，以下の集合を構成する．

$$
\begin{aligned}
b_1 A &= \{b_1 a^1, b_1 a^2, \ldots, b_1 a^k\} \\
b_2 A &= \{b_2 a^1, b_2 a^2, \ldots, b_2 a^k\} \\
&\vdots \\
b_\ell A &= \{b_\ell a^1, b_\ell a^2, \ldots, b_\ell a^k\}
\end{aligned}
$$

このとき，

- $A \cup b_1 A \cup \cdots \cup b_\ell A = G$
- 相異なる $i, j \in \{1, \ldots, \ell\}$ について，$A \cap b_i A = \phi$, $b_i A \cap b_j A = \phi$

が成立する．したがって $(\ell + 1)k = n$ であり，k は n の約数である． □

例

$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

$a = 4$ の位数は 3

$$4^1 \bmod 21 = 4, \quad 4^2 \bmod 21 = 16, \quad 4^3 \bmod 21 = 64 \bmod 21 = 1$$

$$A = \{1, 4, 16\}$$
$$2A = \{2, 8, 11\}$$
$$5A = \{5, 20, 17\}$$
$$10A = \{10, 19, 13\}$$

巡回群 (cyclic group)

定義　群 G にその位数と等しい位数をもつ元が存在するとき，G は**巡回群**と呼ばれる．

定義　G を巡回群とする．$a \in G$ の位数が G の位数と等しいとき，a は**生成元 (generator)** あるいは**原始元 (primitive element)** と呼ばれる．

Theorem 6

p が素数ならば，乗法群 $\mathbb{Z}_p^*$ の位数 d の元の個数は 0 または $\phi(d)$ である．

Theorem 7

p が素数ならば，乗法群 $\mathbb{Z}_p^*$ は巡回群である．

Th. 6 の証明

Lemma 8

任意の正整数 m について，$c_1, c_2, \ldots, c_m$ を整数とし，

$$f(x) = x^m + c_1 x^{m-1} + \cdots + c_{m-1} x + c_m,$$

とする．このとき，p が素数ならば，$f(x) \equiv 0 \pmod{p}$ は $\mathbb{Z}_p$ に属する高々 m 個の解を持つ．

$\mathbb{Z}_p^*$ に位数 d の元 a が存在すると仮定する．このとき Lem. 8 より，
$x^d - 1 \equiv 0 \pmod{p}$ の $\mathbb{Z}_p^*$ に属するすべての解の集合は
$A = \{a^1, a^2, \ldots, a^d\}$ である．したがって，$\mathbb{Z}_p^*$ の位数 d の元はすべて A の元である．
a^k の位数を d_k とする．$(a^k)^{d_k} = a^{k\,d_k} = 1$ なので，$d \,|\, k\,d_k$ である．したがって，$d_k = \mathrm{lcm}(d,k)/k = d/\gcd(d,k)$ である．したがって，$d_k = d$ のとき，かつそのときに限り $\gcd(d,k) = 1$ である．

Th. 7 の証明

Lemma 9

任意の正整数 n について，以下の式が成り立つ．

$$\sum_{d \mid n} \phi(d) = n$$

Th. 4，Th. 6，Lem. 9 より，$\mathbb{Z}_p^*$ は原始元を持つ．

素数 p についての $\mathbb{Z}_p^*$ の例

$\mathbb{Z}_{11}^*$ について，原始元の個数は $\phi(10) = 4$ である．

$x^e \bmod 11$

x \ e	1	2	3	4	5	6	7	8	9	10	ord.
1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1	10
3	3	9	5	4	1	3	9	5	4	1	5
4	4	5	9	3	1	4	5	9	3	1	5
5	5	3	4	9	1	5	3	4	9	1	5
6	6	3	7	9	10	5	8	4	2	1	10
7	7	5	2	3	10	4	6	9	8	1	10
8	8	9	6	4	10	3	2	5	7	1	10
9	9	4	3	5	1	9	4	3	5	1	5
10	10	1	10	1	10	1	10	1	10	1	2

平方剰余と平方非剰余

n, a を互いに素な正整数とする.

$x^2 \equiv a \pmod{n}$ が $\mathbb{Z}_n$ に属する解を持つとき，a は $\boldsymbol{n}$ **を法とする平方剰余**と呼ばれる.

$x^2 \equiv a \pmod{n}$ が $\mathbb{Z}_n$ に属する解を持たないとき，a は $\boldsymbol{n}$ **を法とする平方非剰余**と呼ばれる.

平方剰余 (quadratic residues, QR)
平方非剰余 (quadratic non-residues, QNR)

平方剰余と平方非剰余

Theorem 10

p を奇素数（3以上の素数）とする．

$$a \text{ は } p \text{ を法とする } QR \text{ である} \Leftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p}$$

証明 $(\Rightarrow)$ a が p を法とする QR ならば，ある $x \in \mathbb{Z}_p^*$ について $x^2 \equiv a \pmod{p}$ が成り立つ．したがって，$a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$．
$(\Leftarrow)$ $a^{(p-1)/2} \equiv 1 \pmod{p}$ と仮定する．g を $\mathbb{Z}_p^*$ の原始元とする．このとき，ある $k \in \mathbb{Z}_{p-1}$ について $a \equiv g^k \pmod{p}$ が成り立つ．
$a^{(p-1)/2} \equiv g^{(p-1)k/2} \equiv 1 \pmod{p}$ で g は原始元なので k は偶数でなければならない（仮に k が奇数であるとすると，$g^{(p-1)/2} \equiv 1 \pmod{p}$ となり g が原始元であることと矛盾する）．したがって a は p を法とする QR である． □

ルジャンドル (Legendre) 記号 (1/2)

p を奇素数とし，a を正整数とする．

ルジャンドル記号は以下のように定義される．

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod{p} \text{ のとき} \\ 1 & a \text{ が } p \text{ を法とする QR であるとき} \\ -1 & a \text{ が } p \text{ を法とする QNR であるとき} \end{cases}$$

ルジャンドル記号 (2/2)

Theorem 11

p を奇素数とする．このとき

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$$

証明　$a \equiv 0 \pmod{p}$ のときは明らか．

$a \not\equiv 0 \pmod{p}$ ならば，$\gcd(a, p) = 1$ で $a^{p-1} \equiv 1 \pmod{p}$．

$$\left(a^{(p-1)/2} + 1\right)\left(a^{(p-1)/2} - 1\right) \equiv 0 \pmod{p}$$

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}.$$

したがって，Th. 10 より

$$a^{(p-1)/2} \equiv 1 \pmod{p} \Leftrightarrow a \text{ は } p \text{ を法とする QR}$$

$$a^{(p-1)/2} \equiv -1 \pmod{p} \Leftrightarrow a \text{ は } p \text{ を法とする QNR}$$

□

ヤコビ (Jacobi) 記号

n, a を正整数とする.
さらに，n は奇数とし，その素因数分解を $n = p_1^{e_1} \cdots p_k^{e_k}$ とする.

ヤコビ記号は以下のように定義される.

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

ヤコビ記号は n を素因数分解しなくても計算できる.
計算時間は $O((\log n)^2)$ である.

ヤコビ記号の計算に有用な性質

- $m_1 \equiv m_2 \pmod{n}$ ならば，$\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$ である．
- $\left(\frac{2}{n}\right) = \begin{cases} 1 & n \equiv \pm 1 \pmod{8} \text{ のとき} \\ -1 & n \equiv \pm 3 \pmod{8} \text{ のとき} \end{cases}$
- $\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$ である．

  特に，奇数 t について $m = 2^k t$ とすると，$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{t}{n}\right)$
- m が奇数ならば，$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4} \left(\frac{n}{m}\right)$ である．

素数判定

RSA などの現在広く利用されている公開鍵暗号のセットアップでは，非常に大きな素数をランダムに生成する必要がある．これは通常以下のようにして行われる．

1. 非常に大きな整数を無作為に選択する．
2. それが素数かどうかを判定する．

この方法を何度繰り返せば素数が見つかるか？

素数判定

Theorem 12 (素数定理)

N 以下の素数の個数はおよそ $N/\ln N$ である.

この定理より，k ビットの素数の個数はおよそ以下の通りである.

$$\frac{2^k}{\ln 2^k} - \frac{2^{k-1}}{\ln 2^{k-1}} \approx \frac{2^{k-1}}{\ln 2^{k-1}} \approx \frac{2^{k-1}}{(k-1)\ln 2}$$

したがって k が大きければ

$$\Pr[\text{無作為に選ばれた } k \text{ ビットの整数が素数である}] \approx \frac{1}{0.693\,k}$$

素数判定

素数判定の決定性多項式時間アルゴリズムが存在するかどうかは，長い間未解決問題であった.

決定性多項式時間アルゴリズム
　すべての入力に対して入力長の多項式時間で停止して正答を出力する

2002 年，Agrawal, Kayal, Saxena が決定性多項式時間アルゴリズムを公表した.
しかしこのアルゴリズムは実用的ではない.

素数判定

実用的な確率的多項式時間アルゴリズム

- Solovay-Strassen アルゴリズム
- Miller-Rabin アルゴリズム

上の二つのアルゴリズムは，与えられた整数が

- 素数であれば，常に正しく「素数である」と判定する．
- 合成数であれば，誤って「素数である」と判定する可能性がある．

したがって，与えられた整数 n について

- 答が「合成数である」ならば，n は必ず合成数
- 答が「素数である」ならば，n は素数でない可能性がある．

Solovay-Strassen 素数判定法

n を判定対象の整数とする.

1. $1 \leq a \leq n-1$ を満たす整数 a を無作為に選ぶ.
2. $\left(\frac{a}{n}\right) = 0$ ならば「n は合成数である」と判定して停止する.
3. 以下のように判定して停止する.
   - $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$ のとき,「n は素数である」
   - 上記以外のとき,「n は合成数である」

このアルゴリズムで,

$$n \text{ が合成数のとき「} n \text{ は素数である」と判定される確率} \leq \frac{1}{2}$$

Miller-Rabin 素数判定法

n を判定対象の整数とする.

1. $n-1=2^k m$ となる k, m を計算する．ただし m は奇数である.
2. $1 \leq a \leq n-1$ を満たす整数 a を無作為に選ぶ.
3. $b = a^m \bmod n$ を計算する.
4. $b \equiv 1 \pmod{n}$ ならば「n は素数である」と判定して停止する.
5. $i = 0$ から $k-1$ について，以下の計算を行う.
   1. $b \equiv -1 \pmod{n}$ なら「n は素数である」と判定して停止する.
   2. 上記以外のとき $b = b^2 \bmod n$ を計算する.
6. 「n は合成数である」と判定して停止する.

このアルゴリズムで,

$$n \text{ が合成数のとき「} n \text{ は素数である」と判定される確率} \leq \frac{1}{4}$$

演習問題

1. 孫子定理を証明せよ.
2. Th. 1 を証明せよ.
3. Th. 4 の証明で，$A \cup b_1 A \cup \cdots \cup b_\ell A = G$ であることを証明せよ.
4. Lem. 9 を証明せよ.
5. 与えられた整数 n が素数ならば，Miller-Rabin アルゴリズムが常に「n は素数である」と判定することを証明せよ.