アルゴリズム B 演習 No. 10 2013 年 12 月 20 日配布

10. 合同式

- a, b を整数，n を自然数とする．$a - b$ が n で割り切れるとき，a と b は n を法として合同であるといい，$a \equiv b \pmod{n}$ と表す．
- 上で定義した関係 $\equiv \pmod{n}$ は $\mathbb{Z}$ 上の同値関係であり，この同値関係による $\mathbb{Z}$ の商集合を $\mathbb{Z}/n\mathbb{Z}$ で表す．$a \in \mathbb{Z}$ が属する同値類を $a \bmod n$ で表す．
- $\mathbb{Z}/n\mathbb{Z}$ に演算 $+, \cdot \colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ を次のように定める．

  $$(a \bmod n) + (b \bmod n) = (a + b) \bmod n, \quad (a \bmod n) \cdot (b \bmod n) = ab \bmod n.$$

  このとき，演算 $+, \cdot$ によって $\mathbb{Z}/n\mathbb{Z}$ は可換環となる．
- 以上の議論は次のように言い換えられる．$n\mathbb{Z}$ を n の倍数全体がなす $\mathbb{Z}$ のイデアルとすると，$\mathbb{Z}/n\mathbb{Z}$ は $\mathbb{Z}$ の $n\mathbb{Z}$ による剰余環である．
- $x \in \mathbb{Z}/n\mathbb{Z}$ が**単元**または**可逆元**であるとは，$y \in \mathbb{Z}/n\mathbb{Z}$ が存在して，$xy = 1 \bmod n$ となることをいう．y を x の**逆元**という．$\mathbb{Z}/n\mathbb{Z}$ の単元全体を $(\mathbb{Z}/n\mathbb{Z})^\times$ で表す．$(\mathbb{Z}/n\mathbb{Z})^\times$ は乗法に関して可換群をなす．
- a を整数，n を自然数とする．$a \bmod n$ が $\mathbb{Z}/n\mathbb{Z}$ の単元であることと，a と n が互いに素であることは同値である．$a \bmod n$ が単元であるとき，その逆元は次のように計算できる．$ax + ny = 1$ を満たす整数 x, y を拡張ユークリッドの互除法 (No. 9) により求める．このとき，$a \bmod n$ の逆元は $x \bmod n$ である．
- $(\mathbb{Z}/n\mathbb{Z})^\times$ の元の個数を $\varphi(n)$ で表すと，関数 $\varphi \colon \mathbb{N} \to \mathbb{N}$ が定まる．これを**オイラーの φ 関数**という．$\varphi(1) = 1$ であることに注意する．
- m, n を互いに素な自然数とする．このとき，写像

  $$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z};$$
  $$a \bmod mn \mapsto (a \bmod m, a \bmod n)$$

  は well-defined であり，環同型である．これを**中国剰余定理**という．

問題

解答に際して，その問題より前にある問題の結果を用いてもよい．

10-1. 拡張ユークリッドの互除法を用いて，$\mathbb{Z}/60\mathbb{Z}$ における $13 \bmod 60$ の逆元を求めよ．

10-2. $20x \equiv 13 \pmod{47}$ を満たす整数 x で，$0 \leq x \leq 46$ を満たすものを求めよ．

10-3. n を自然数とし，a を $1 \leq a < n$, $\gcd(a, n) = 1$ を満たす整数とする．このとき，$a \bmod n$ の逆元を求める計算は $O\big((\log n)^3\big)$ のビット演算量でできることを示せ．ただし，四則演算のビット演算量は No. 8 のものを用いるとする[*1]．

10-4. $m_1, m_2, \ldots, m_r$ をどの 2 つも互いに素な自然数とし，$a_1, a_2, \ldots, a_r$ を整数とする．連立合同式

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned} \tag{$*$}$$

を考える．$M_i = m_1 m_2 \cdots m_r / m_i$ とし，$M_i N_i \equiv 1 \pmod{m_i}$ となる整数 N_i を取る．このとき，$x = \sum_{i=1}^{r} a_i M_i N_i$ は連立合同式 $(*)$ の解であることを示せ．

10-5. $x \equiv 7 \pmod{12}$, $x \equiv 8 \pmod{17}$ となるような整数 x を一つ求めよ．

10-6. l, m, n をどの 2 つも互いに素な自然数とする．写像 $f\colon \mathbb{Z}/lmn\mathbb{Z} \to \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ を

$$f(a \bmod lmn) = (a \bmod l, a \bmod m, a \bmod n)$$

で定めると，f は well-defined であり，環同型であることを示せ．

10-7. ある人の年齢は 3 で割ると 2 余り，5 で割ると 4 余り，7 で割ると 5 余るという．この人の年齢は何歳か求めよ．

10-8. m, n を互いに素な自然数とする．このとき，$\varphi(mn) = \varphi(m)\varphi(n)$ であることを示せ．

10-9. n を 2 以上の自然数とし，$n = \prod_{i=1}^{r} p_i^{e_i}$ と素因数分解されているとする．ただし，$p_1, \ldots, p_r$ は相異なる素数である．このとき，次の式が成り立つことを示せ．

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

10-10. $\varphi(120)$ の値を求めよ．

10-11. a を整数，n を自然数とする．a と n が互いに素ならば，$a^{\varphi(n)} \equiv 1 \pmod{n}$ が成り立つことを示せ．

10-12. 3^{2013} を 20 で割った剰余を求めよ．

[*1] （筆算による）除算のビット演算量に関する評価をより精密にすることで，実際には $O\big((\log n)^2\big)$ のビット演算量で十分であることが証明できる．