アルゴリズム B 演習 No. 10　　2015 年 12 月 11 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

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

  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．四則演算のビット演算量として，No. 8 で与えたものを使うものとする．

10-1. 拡張ユークリッドの互除法を用いて，$\mathbb{Z}/57\mathbb{Z}$ における 26 mod 57 の逆元を求めよ．

10-2. $31x \equiv 55 \pmod{58}$ を満たす整数 x で，$0 \leq x \leq 57$ 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のビット演算量は $O\big((\log n)^3\big)$ であることを示せ．

10-4. m, n を互いに素な自然数，a, b を整数とする．r, s を $rn + sm = 1$ を満たす整数とする．このとき，$x = arn + bsm$ とおくと，$x \equiv a \pmod{m}$ かつ $x \equiv b \pmod{n}$ となることを示せ．

10-5. $x \equiv 12 \pmod{47}$, $x \equiv 11 \pmod{50}$ を満たす整数 x を一つ求めよ．

10-6. 有限集合 $A_1, \ldots, A_r$ に対して，次の式が成り立つことを示せ．

$$\begin{aligned}\#(A_1 \cup \cdots \cup A_r) = \sum_{i=1}^{r} \#A_i - \sum_{1 \leq i < j \leq r} \#(A_i \cap A_j) \\ + \sum_{1 \leq i < j < k \leq r} \#(A_i \cap A_j \cap A_k) \\ - \cdots + (-1)^r \#(A_1 \cap \cdots \cap A_r).\end{aligned}$$

10-7. n を 2 以上の自然数として，$n = \prod_{i=1}^{r} p_i^{e_i}$ 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り，$e_1, \ldots, e_r \geq 1$ とする．このとき，次の式が成り立つことを示せ．

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

10-8. $\varphi(819)$ の値を求めよ．

10-9. 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．

10-10. $2^{2015} \bmod 35$ を計算せよ．