アルゴリズム B 演習 No. 9 2012 年 12 月 14 日配布

9. 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．
- $\mathbb{Z}/n\mathbb{Z}$ が体であるのは，$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z}) \setminus \{0 \bmod n\}$ となるときであり，そのときに限る．
- $(\mathbb{Z}/n\mathbb{Z})^\times$ 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．

9-1. 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ことを示せ．

9-2. 拡張ユークリッドの互除法を用いて，$\mathbb{Z}/105\mathbb{Z}$ における $64 \bmod 105$ の逆元を求めよ．

9-3. $20x \equiv 17 \pmod{41}$ を満たす整数 x で，$0 \le x \le 40$ を満たすものを求めよ．

9-4. m, n を互いに素な自然数，b, c 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，$a = brn + csm$ とおくと，$a \equiv b \pmod{m}$ かつ $a \equiv c \pmod{n}$ となることを示せ．

9-5. $x \equiv 2 \pmod{11}$, $x \equiv 5 \pmod{13}$ となるような整数 x を一つ求めよ．

9-6. ある人の年齢は 3 で割ると 1 余り，5 で割ると 3 余り，7 で割ると 4 余るという．この人の年齢は何歳か？

9-7. m, n を自然数とし，a を $0 \leq a < n$ を満たす整数とする．繰り返し二乗法を用いて $a^m \bmod n$ を計算するときのビット演算量が $O\big((\log m)(\log n)^2\big)$ であることを示せ．ただし，k ビットの自然数と l ビットの自然数の乗算は，高々 kl のビット演算量ででき，k ビットの自然数を l ビットの自然数で割って剰余を求める計算は，高々 kl のビット演算量でできるとする．

9-8. 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．

9-9. 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．

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

9-10. $\varphi(300)$ の値を求めよ．

9-11. 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．

9-12. 3^{2012} を 103 で割った剰余を求めよ．