情報基礎数学 I 演習問題

2012, 吉原

(1) m, n の最大公約数を (m, n)，最小公倍数を $[m, n]$ と表すとき，次の性質を証明せよ。
  (a) $m|n$ かつ $n|m$ ならば，$m = n$ または $m = -n$。
  (b) 正の整数 m, n に対して，$(m, n) = [m, n]$ ならば $m = n$ である。

(2) na と nb がともに k で割り切れて、かつ $(a, b) = 1$ のとき、n は k で割り切れることを示せ。

(3) 次の数の最大公約数をユークリッドの互除法を用いて求めよ。
  (a) 1365 と 2184,
  (b) 2940 と 16731

(4) 方程式 $390x + 231y = 6$ の整数解について考察する。
  (a) 390 と 231 の最大公約数をユークリッドの互除法を用いて求めよ。
  (b) この方程式の一組の解を求めよ。
  (c) この方程式のすべての整数解を求めよ。

(5) 一次不定方程式 $119x + 105y = 28$ について：
  (a) 一組の特殊解をユークリッドの互除法を用いて求めよ。
  (b) 次に一般解も求めよ。

(6) 次の一次不定方程式の整数解をすべて求めよ。
  (a) $273x + 110y = 1$
  (b) $238x + 273y = 7$
  (c) $2174x + 2156y = 66$

(7) ある自然数 x を 3 で割ったら 1 余り，7 で割ったら 5 余り，11 で割ったら 3 余ったという。この自然数を次の手続きに従って求めよ。（暗算で求めたのは不可である）
  (a) x の連立 1 次合同方程式を書け。
  (b) それを解け。

(8) 次の問いに答えよ。
  (a) 集合 $S = \{\ 245m + 168n \mid m, n \in \mathbb{Z}\}$ に含まれる最小の正の数 a を求めよ。さらに、集合 S はどのような数でできているか答えよ。
  (b) $245x + 168y = b$ が解をもつための b の条件を述べよ。
  (c) (a) で求めた a に対して $245x + 168y = a$ の解をすべて求めよ。

(9) 方程式 $1092x + 715y = n,\ n \in \mathbb{Z}$ の整数解について考察する。

(a) 1092 と 715 の最大公約数 d をユークリッドの互除法を用いて求めよ。
(b) (1) で求めた d に対して $n = 3d$ のとき、この方程式の一組の解を求めよ。
(c) $n = 3d$ のとき、この方程式のすべての整数解を求めよ。

(10) a, b は整数で同時には 0 でないとする。$ax + by$ （$x, y \in \mathbb{Z}$）の形の最小の正数を $d = ax_0 + by_0$ とすると、$d = (a, b)$ であることを証明せよ。

(11) 25^{1000} を 13 で割った余りを求めよ。

(12) 次の問いに答えよ。
(a) n を自然数とするとき，$10^{6n} - 1$ は 7 と 13 で割り切れることを証明せよ。
(b) a と b を自然数として a を b で割った余りを r とするとき，a と b の最大公約数は b と r の最大公約数に等しいことを証明せよ。

(13) $2^n - 1$ が素数ならば n は素数であることを示せ。この逆の主張は成立するか？

(14) $n,\ a,\ b$ を正の整数で、$(a, b) = 1$ とする。このとき $(a^n, b^n) = 1$ を示せ。

(15) $n,\ a,\ b$ を整数とするとき，$(n, a) = 1, (n, b) = 1$ ならば $(n, ab) = 1$ を示せ。

(16) $n,\ a,\ b$ を整数とするとき，$(a, b) = 1, ab = n^2$ ならば $a,\ b$ は平方数であることを示せ。

(17) 小学校以来使われてきた、「ある数が 3 の倍数である判定法で、各桁の数の和が 3 の倍数であること」があるが、このことを証明してみよう。以下の問いに答えよ。
(a) 任意の自然数 m に対して、$10^m \equiv 1 \pmod 3$ であることを示せ。
(b) 10 進法で表した数 n の各桁の数字の和が 3 の倍数である必要十分条件は、n が 3 の倍数であることを証明せよ。

(18) $a_0,\ a_1, \cdots, a_n$ を整数で、$a_0 \neq 0,\ a_n \neq 0$ とする。このとき、方程式
$$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$
が有理数の解 b/c $((b, c) = 1)$ をもつならば、c は a_0 の約数であり、b は a_n の約数であることを示せ。

(19) a を正の有理数とするとき，a^2 が整数なら a も整数であるこを示せ。

(20) n が平方数でないとき，$\sqrt{n}$ は無理数であるこを示せ。

(21) $a, b, c, d \in \mathbb{Z}$ でかつ c, d が互いに素とする。このとき、

$$\frac{a}{c} + \frac{b}{d} \in \mathbb{Z}$$

なら、

$$\frac{a}{c} \in \mathbb{Z}, \quad \frac{b}{d} \in \mathbb{Z}$$

であることを証明せよ。

(22) 次の S_n は整数でないことを証明せよ。

$$S_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \quad (n > 1)$$

(23) 合成数 n は $\sqrt{n}$ を超えない素因数をもつことを示せ。

(24) 任意の自然数 $n \geq 2$ に対して，方程式 $x^n - x - 1 = 0$ は有理数の解を持たないことを示せ。

(25) 次の問いに答えよ。

(a) $\sqrt{6}$ は無理数であることを証明せよ。

(b) 方程式 $x^3 + 3x + 3 = 0$ は有理数の解をもたないことを証明せよ。

(26) a, b を整数，p を素数とするとき，$(a+b)^p \equiv a^p + b^p (\mathrm{mod}\ p)$ が成立することを証明せよ。

(27) $10^{6n} - 1$ は 7, 9, 11, 13 で割りきれるこを証明せよ。

(28) 以下の問いに答えよ。

(a) すべての自然数 $n (< 91)$ に対して、n^{13} は 91 で割ると n 余ることを証明せよ。

(b) 方程式 $x^3 + 3x + 2 = 0$ は有理数の解を持たないことを証明せよ。

(29) 一次合同式 $66x \equiv 2 \ (\mathrm{mod}\ 17)$ を解け。

(30) 次の連立一次合同式を解け.

$$\left\{ \begin{array}{lllll} x & \equiv & 4 & (\mathrm{mod} & 9) \\ x & \equiv & 3 & (\mathrm{mod} & 7) \\ x & \equiv & 5 & (\mathrm{mod} & 11) \end{array} \right.$$

(31) 次の連立一次合同式を解け。

$$\begin{cases} x & \equiv & 2 & \pmod{5} \\ x & \equiv & 5 & \pmod{7} \\ x & \equiv & 7 & \pmod{13} \end{cases}$$

(32) 次の連立一次合同方程式を解け。

$$x \equiv 2 \pmod 5,\ x \equiv 3 \pmod 6,\ x \equiv 4 \pmod 7.$$

(33) ある自然数 x は、3 で割ると 2 余り、7 で割ると 3 余り、11 で割ると 4 余るという。このとき以下の問に答えよ。
(1) この条件を合同方程式で表せ。
(2) それを解いて x を求めよ。

(34) ある自然数 n は、5 で割ると 2 余り、6 で割ると 3 余り、7 で割ると 4 余るという。このとき以下の問に答えよ。
(a) この条件を合同方程式で表せ。
(b) それを解いて n を求めよ。

(35) $\varphi(n) = 6$ をみたす自然数 n を求めよ。

(36) 次の問いに答えよ。
(a) 自然数 n に対して，$1, 2, \ldots, n$ の中で n と互いに素なものの個数が 4 となるような n をすべて求めよ。
(b) 自然数 n に対して，$1, 2, \ldots, n$ の中で n と互いに素なものの個数が 5 となるような n をすべて求めよ。

(37) $(m, n) \neq 1$ のとき $\varphi(mn) = \varphi(m)\varphi(n)$ が成立するか？

(38) n が偶数のとき，$\varphi(2n) = 2\varphi(n)$ であり，n が奇数のとき，$\varphi(2n) = \varphi(n)$ が成立することを証明せよ。

(39) $n \geq 3$ のとき，$\varphi(n)$ は常に偶数であることを示せ。

(40) オイラー関数 $\varphi(n)$ について以下の問いに答えよ。
(a) $\varphi(n) = 4$ の解を求めよ。
(b) p を素数とするとき $\varphi(n) = p$ に解があればすべて求めよ。

(41) 暗号化鍵 $(n, e) = (35, 13)$ をもつ暗号文 $y = 16$ を解読せよ。すなわち，暗号化鍵 $(35, 13)$ から復号化鍵 d を求め，暗号文 y を復号化し，もとの文 x を求めよ。

(42) 暗号化鍵 $(n, e) = (21, 7)$ をもつ暗号文 $y = 19$ を解読せよ。すなわち，暗号化鍵 $(21, 7)$ から復号化鍵 d を求め，暗号文 y を復号化し，もとの文 x を求めよ。

(43) 暗号化鍵 $(n, e) = (55, 7)$ をもつ暗号文 $y = 27$ を解読せよ。すなわち，暗号化鍵 $(55, 7)$ から復号化鍵 d を求め，暗号文 y を復号化し，もとの文 x を求めよ。

(44) 次の暗号化鍵 (n, e) をもつ暗号文 y を解読せよ：$(n, e) = (91, 5)$, $y = 75$

(45) $n = 26646163$, $e = 127$ として，この公開鍵暗号により次の平文を 2 個づつの文字にブロック化した暗号文にせよ。

Heisaspy