Exercise

Chapter 1. 整數的基本性質

(1) 假設 $a, b, c \in \mathbb{Z}$ 且 $c \neq 0$, 試證明以下有關於整除的基本性質.
   (a) 若 $c \mid a+b$ 且 $c \mid a$, 則 $c \mid b$.
   (b) $a \mid b$ 若且唯若 $ac \mid bc$.
   (c) 若 $a \mid b$, 則對任意 $n \in \mathbb{N}$ 皆有 $a^n \mid b^n$.
   (d) 若 $a > 1$ 且 $a-1 \mid b-1$ 以及 $a-1 \mid bc-1$, 則 $a-1 \mid c-1$.

(2) 假設 $a, m, n \in \mathbb{N}$ 且 $a > 1$, 以下我們要證明 $a^m - 1 \mid a^n - 1$ 若且唯若 $m \mid n$.
   (a) 利用因式分解 $x^h - 1 = (x-1)(x^{h-1} + x^{h-2} + \cdots + x + 1)$ (其中 $h \in \mathbb{N}$), 證明若 $m \mid n$, 則 $a^m - 1 \mid a^n - 1$.
   (b) 證明若 $a^m - 1 \mid a^{m'+r} - 1$ (其中 $m', r \in \mathbb{Z}$ 且 $m', r \geq 0$) 且 $a^m - 1 \mid a^{m'} - 1$, 則 $a^m - 1 \mid a^r - 1$. 依此證明若 $a^m - 1 \mid a^n - 1$, 則 $m \mid n$.

(3) 以下我們介紹兩種不同形式的 division algorithm (除法原理). 這裡我們僅假設 $a, b \in \mathbb{Z}$ 且 $b \neq 0$ (不必假設 $b \in \mathbb{N}$).
   (a) 證明存在唯一的 $h, r \in \mathbb{Z}$ 滿足
   $$a = bh + r \text{ 且 } 0 \leq r < |b|.$$
   (b) 證明存在唯一的 $h, r \in \mathbb{Z}$ 滿足
   $$a = bh + r \text{ 且 } -\frac{|b|}{2} < r \leq \frac{|b|}{2}.$$

(4) 假設 $a, b \in \mathbb{Z}$ 且 d 是集合 $\{ma + nb \mid m, n \in \mathbb{Z}\}$ 中最小的正整數. 試證明若 $r \in \mathbb{N}$, 則 rd 是集合 $\{mra + nrb \mid m, n \in \mathbb{Z}\}$ 中最小的正整數. 依此證明 $\gcd(ra, rb) = r \gcd(a, b)$.

(5) 假設 $a, b, c \in \mathbb{Z}$, 試利用定理：

「$\gcd(a, b) = 1$ 若且唯若存在 $r, s \in \mathbb{Z}$ 使得 $ra + sb = 1$」

證明以下有關於互質的性質.

(a) 假設 $\gcd(a, b) = 1$ 且 $c \mid a + b$. 試證明 $\gcd(a, c) = \gcd(b, c) = 1$.

(b) 假設 $m, n \in \mathbb{N}$. 試證明 $\gcd(a, b) = 1$ 若且唯若 $\gcd(a^m, b^n) = 1$.

(6) 假設 $a, b \in \mathbb{Z}$ 且 $d = \gcd(a + b, a - b)$.

(a) 試證明 $d \mid 2a$ 且 $d \mid 2b$.

(b) 若已知 $\gcd(a, b) = 1$ 試證明當 a, b 同為奇數或同為偶數時 $d = 2$; 而當 a, b 為一奇一偶時 $d = 1$.

(7) 假設 $n \in \mathbb{N}$, $n > 2$ 且 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

(a) 對任意 $t \in \mathbb{N}$ 且 $1 \leq t \leq n - 1$, 試證明

$$\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_t), \gcd(a_{t+1}, \ldots, a_n)).$$

(b) 對任意 $t_1, \ldots, t_r \in \mathbb{N}$ 其中 $t_0 = 0 < t_1 < t_2 < \cdots < t_r < n = t_{r+1}$, 若對 $0 \leq i \leq r$, 令 $d_i = \gcd(a_{t_i+1}, \ldots, a_{t_{i+1}})$. 試證明

$$\gcd(a_1, \ldots, a_n) = \gcd(d_0, d_1, \ldots, d_r).$$

(8) 假設 $n \in \mathbb{N}$, $n > 2$ 且 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

(a) 對任意 $t \in \mathbb{N}$ 且 $1 \leq t \leq n - 1$, 試證明

$$\operatorname{lcm}(a_1, \ldots, a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_t), \operatorname{lcm}(a_{t+1}, \ldots, a_n)).$$

(b) 對任意 $t_1, \ldots, t_r \in \mathbb{N}$ 其中 $t_0 = 0 < t_1 < t_2 < \cdots < t_r < n = t_{r+1}$, 若對 $0 \leq i \leq r$, 令 $l_i = \operatorname{lcm}(a_{t_i+1}, \ldots, a_{t_{i+1}})$. 試證明

$$\operatorname{lcm}(a_1, \ldots, a_n) = \operatorname{lcm}(l_0, l_1, \ldots, l_r).$$

(9) 假設 $a_1, a_2, \ldots, a_n \in \mathbb{N}$. 試證明 $\operatorname{lcm}(a_1, a_2, \ldots, a_n) = a_1 a_2 \cdots a_n$ 若且唯若 $a_1, a_2, \ldots, a_n$ 兩兩互質 (pairwise relatively prime).

(10) 假設 $a, b, c \in \mathbb{Z}$ 且 $d = \gcd(a, b)$.

(a) 試證明方程式 $ax + by = c$ 有整數解若且唯若 $d \mid c$.

(b) 假設 $d \mid c$ 且 $x = m_0, y = n_0$ 是 $ax + by = d$ 的一組整數解, 試寫下 $ax + by = c$ 的所有整數解 (用 a, b, c, d, m_0, n_0 表示).

(11) 試寫出以下 diophantine equations 的所有整數解.

(a) $18x + 27y = 15$.

(b) $17x + 29y = 10$.

(12) 假設 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ 且 $d = \gcd(a_1, a_2, \ldots, a_n)$.

(a) 若 $c \in \mathbb{Z}$ 且 $d \nmid c$, 試證明方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

無整數解.

(b) 若 $c \in \mathbb{Z}$ 且 $d \mid c$, 試證明方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

有無限多組整數解.

(13) 試寫出以下 diophantine equations 的所有整數解.

(a) $9x_1 + 12x_2 + 16x_3 = 13$.

(b) $8x_1 - 4x_2 + 6x_3 = 6$.

(14) 假設 $a, b \in \mathbb{Z}$, 試證明 $\gcd(a, b) = 1$ 若且唯若 $\gcd(a + b, ab) = 1$.

(Hint: 利用 Euclid 的 Lemma 以及大於 1 的整數皆有質因數處理)

(15) 試找出可能的一組 $a, b \in \mathbb{N}$ 滿足 $\gcd(a,b) = 12$ 且 $\operatorname{lcm}(a,b) = 360$.

(16) 假設 $a, b, n \in \mathbb{N}$ 若已知 $ab = n^2$ 且 $\gcd(a,b) = 1$, 試證明存在 $c, d \in \mathbb{N}$ 滿足 $a = c^2$ 且 $b = d^2$.

(17) 假設 $m \in \mathbb{N}$ 且 p 是質數, 如果 $p^a \mid m$ 且 $p^{a+1} \nmid m$, 則我們稱 p^a 恰整除 m 且用 $p^a || m$ 表示之. 現假設 $p^a || m$ 且 $p^b || n$.

(a) 若已知 $a < b$, 試求 r 滿足 $p^r || m + n$.

(b) 試舉一個 $a = b$ 的例子使得 $p^r || m + n$ 且 $r > a$.

(c) 試求 s 滿足 $p^s || mn$.

Chapter 2. Arithmetic Function

(1) 我們定義一個 arithmetic function ρ 為 $\rho(1) = 1$ 且對 $n > 1$ 定義 $\rho(n) = 2^m$ 其中 m 為 n 的相異質因數個數.

(a) 試證明 ρ 是 multiplicative 且說明 ρ 不是 completely multiplicative.

(b) 令

$$f(n) = \sum_{d|n, d\in\mathbb{N}} \rho(d).$$

若 $n = p_1^{n_1} \cdots p_r^{n_r}$ 為 n 的質因數分解, 試求 $f(n)$.

(2) 所謂的 Liouville λ-function 是一個 arithmetic function λ 其定義如下: $\lambda(1) = 1$ 且對 $n > 1$ 若 n 的質因數分解為 $n = p_1^{n_1} \cdots p_r^{n_r}$, 則

$$\lambda(n) = (-1)^{n_1 + \cdots + n_r}.$$

(a) 試證明 λ 是 completely multiplicative.

(b) 令

$$F(n) = \sum_{d|n, d\in\mathbb{N}} \lambda(d),$$

試證明如果存在 $a \in \mathbb{N}$ 使得 $n = a^2$, 則 $F(n) = 1$; 否則 $F(n) = 0$.

(3) 以下是幾個關於 Euler ϕ-function 的性質. 此處 $m, n \in \mathbb{N}$.
   (a) 假設 $n = p_1^{n_1} \cdots p_r^{n_r}$ 是 n 的質因數分解. 試證明
   $$\phi(n) = \big(p_1^{n_1-1} \cdots p_r^{n_r-1}\big)\big((p_1-1)\cdots(p_r-1)\big).$$
   並依此證明 $\sqrt{n}/2 \le \phi(n) \le n$.
   (b) 試證明若 n 為奇數則 $\phi(2n) = \phi(n)$, 而若 n 為偶數則 $\phi(2n) = 2\phi(n)$.
   (c) 假設 n 有 m 個相異奇質因數, 試證明 $2^m \mid \phi(n)$.
   (d) 試證明 $\phi(n^m) = n^{m-1}\phi(n)$.
   (e) 假設 $m \mid n$, 試證明 $\phi(m) \mid \phi(n)$ 且 $\phi(mn) = m\phi(n)$.

(4) 已知 f, g 皆為 multiplicative arithmetic function. 且知對任意質數 p 以及 $m \in \mathbb{N}$ 皆有 $f(p^m) = p+1$ 且 $g(p^m) = p^{m-1}$.
   (a) 若 $f * g$ 表示 f 和 g 的 convolution, 試求 $f * g(100)$ 之值.
   (b) 若對任意 $n \in \mathbb{N}$ 皆有 $g(n) = \sum_{d|n, d\in\mathbb{N}} h(d)$. 試求 $h(100)$ 之值.

Chapter 3. Congruences

(1) 假設 $a, b, c, d \in \mathbb{Z}$ 且 $m \in \mathbb{N}$ 其中 $c \equiv d \pmod m$.
   (a) 已知 $\gcd(c, m) = 1$, 若 $ac \equiv bd \pmod m$, 試證明 $a \equiv b \pmod m$.
   (b) 若 c 和 m 不互質, 試找出一反例 $ac \equiv bd \pmod m$ 但 $a \not\equiv b \pmod m$.

(2) 假設 $n \in \mathbb{N}$ 且 n 的 10 進位表示為 $abcabc$, 其中 $a, b, c \in \mathbb{N}$ 且 $1 \le a \le 9$ 以及 $0 \le b, c \le 9$ (例如 $n = 123123$). 試證明 $7 \mid n$.

(3) 假設 $a \in \mathbb{Z}$ 且 $2 \nmid a$.
   (a) 試證明 $a^2 \equiv 1 \pmod 8$.
   (b) 試說明並列出 a^2 在 modulo 24 之下所有可能的同餘類.
   (c) 若再假設 $3 \nmid a$, 試證明 $a^2 \equiv 1 \pmod{24}$.

(4) 已知 $\gcd(58, 63) = 1$, 故知 58 在 modulo 63 之下有乘法反元素 (即存在 $a \in \mathbb{Z}$ 使得 $58 \times a \equiv 1 \pmod{63}$). 以下是有關乘法反元素之問題.
   (a) 試利用輾轉相除法找出 $58x + 63y = 1$ 的一組整數解. 並依此找出 58 在 modulo 63 之下的乘法反元素.
   (b) 試找出 $b \in \mathbb{Z}$ 且滿足 $1 \le b \le 63$, 使得 $58 \times b \equiv 47 \pmod{63}$.

(5) 假設 $p \geq 5$ 是一個質數, 試證明

$$\{\frac{-(p-1)}{2}, \frac{-(p-3)}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-3}{2}, \frac{p-1}{2}\}$$

是一個 reduced residue system modulo p.

(6) 以下是有關 Euler's Theorem 的應用.

(a) 試求 99^{999999} 除以 26 的餘數.

(b) 假設 $n \in \mathbb{Z}$ 且 $3 \nmid n$. 試證明 $9 \mid n^7 - n$ 並依此證明 $n^7 \equiv n \pmod{63}$.

(c) 假設 $m, n \in \mathbb{N}$ 且 $\gcd(m, n) = 1$. 試證明 $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

(7) 以下是有關 Fermat's Little Theorem 的應用.

(a) 試證明 11 整除 $456^{654} + 123^{321}$.

(b) 假設 p 是一質數且 $a, b \in \mathbb{Z}$ 滿足 $p \nmid a$ 以及 $p \nmid b$. 試證明若 $a^p \equiv b^p \pmod{p}$ 則 $a \equiv b \pmod{p}$, 並依此證明若 $a^p \equiv b^p \pmod{p}$ 則 $a^p \equiv b^p \pmod{p^2}$.

(c) 假設 p, q 是相異質數且滿足 $p - 1 \mid q - 1$. 試證明若 $a \in \mathbb{Z}$ 且 $\gcd(a, pq) = 1$, 則 $a^{q-1} \equiv 1 \pmod{pq}$.

(8) 試利用 Fermat's Little Theorem 找出 11 在 modulo 29 的乘法反元素, 並依此解 $11x \equiv 15 \pmod{29}$.

(9) 假設 p 是一個奇質數.

(a) 試證明若 $a \in \mathbb{N}$ 滿足 $(p-1)/2 < a < p$, 則存在 $b \in \mathbb{N}$ 滿足 $1 \leq b \leq (p-1)/2$ 使得 $a \equiv -b \pmod{p}$. 依此以及 Wilson's Theorem 證明

$$(\frac{p-1}{2}!)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

(b) 試證明若 a 是奇數滿足 $1 \leq a < p-1$, 則存在偶數 b 滿足 $1 < b \leq p-1$ 使得 $a \equiv -b \pmod{p}$. 依此以及 Wilson's Theorem 證明

$$1^2 3^2 5^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

(c) 利用前兩小題結果證明當 $p \equiv 1 \pmod{4}$ 時 congruence equation $x^2 \equiv -1 \pmod{p}$ 有解.

(10) 假設 $m \in \mathbb{N}$ 且 $m > 2$. 若 $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ 是一個 modulo m 之下的 reduced residue system, 試證明 $r_1 + r_2 + \cdots + r_{\phi(m)} \equiv 0 \pmod{m}$.

Chapter 4. Congruence Equations

(1) 令 p 為一質數.
   (a) 假設 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 其中 $a_i \in \mathbb{Z}$. 若存在 $r_1, \ldots, r_{n+1} \in \mathbb{Z}$ 滿足 $f(r_i) \equiv 0 \pmod{p}$ 且對任意 $i \neq j$ 皆有 $r_i \not\equiv r_j \pmod{p}$, 試證明對所有 $0 \leq i \leq n$ 皆有 $p \mid a_i$.
   (b) 考慮 $g(x) = (x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1)$. 試證明 $g(x) = a_{p-2}x^{p-2} + \cdots + a_1 x + a_0$, 其中對所有 $0 \leq i \leq p-2$ 皆有 $p \mid a_i$.
   (c) 試利用 (b) 之結果證明 Wilson's Theorem.

(2) 解 congruence equation 的方法也可推廣到多變數多項式的情況.
   (a) 假設 $f(x,y) \in \mathbb{Z}[x,y]$ 為以 x, y 為變數的整係數多項式. 試證明若 $m' \mid m$ 且 $f(x,y) \equiv 0 \pmod{m'}$ 無整數解, 則 $f(x,y) \equiv 0 \pmod{m}$ 無整數解.
   (b) 試證明 congruence equation $3x^2 - 7y^2 \equiv 2 \pmod{525}$ 無整數解.

(3) 試解以下的 congruence equation.
   (a) 求 $9x \equiv 21 \pmod{30}$ 在 modulo 30 之下的所有解.
   (b) 求 $18x \equiv 15 \pmod{27}$ 在 modulo 27 之下的所有解.

(4) 解一次的 congruence equation 的方法也可推廣到解多變數的一次 congruence equation.
   (a) 考慮 congruence equation $a_1 x + a_2 y \equiv b \pmod{m}$. 令 $d = \gcd(a_1, a_2, m)$. 試證明若 $d \nmid b$, 則此 congruence equation 無解, 而若 $d \mid b$, 則此 congruence equation 在 modulo m 之下共有 dm 組解.
   (b) 試解以下的 congruence equation:

   (1) $2x + 3y \equiv 4 \pmod{7}$; (2) $3x + 6y \equiv 2 \pmod{9}$.

   (c) 試將 (a) 的結果推廣到 n 個變數的一次 congruence equation.

(5) 試解: (a) $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$ (b) $\begin{cases} 5x \equiv 3 \pmod{7} \\ 2x \equiv 4 \pmod{8} \\ 3x \equiv 6 \pmod{9} \end{cases}$ (c) $x^2 \equiv x \pmod{525}$.

(6) 中國剩餘定理也可推廣到不互質的情況.
   (a) 試證明 $\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$ 有聯立解若且唯若 $\gcd(m_1, m_2) \mid b_1 - b_2$. 並證明若有解則其解在 modulo $\operatorname{lcm}(m_1, m_2)$ 之下唯一.
   (b) 試求以下聯立解: (a) $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 1 \pmod{6} \end{cases}$ (b) $\begin{cases} x \equiv 7 \pmod{16} \\ x \equiv 3 \pmod{24} \end{cases}$
   (c) 試將 (a) 的結果推廣到 n 個聯立式的情形.

Chapter 5. 二次的 Congruence Equations

(1) 試利用配方法解以下二次的 congruence equations.
   (a) $x^2 + x \equiv 3 \pmod{13}$
   (b) $2x^2 + x \equiv 3 \pmod{39}$
   (c) $3x^2 + x \equiv 3 \pmod{39}$

(2) 試解以下二次的 congruence equations.
   (a) $x^2 \equiv 21 \pmod{4}$
   (b) $x^2 \equiv 21 \pmod{32}$
   (c) $x^2 \equiv 33 \pmod{64}$
   (d) $x^2 \equiv 40 \pmod{64}$
   (e) $2x^2 \equiv 40 \pmod{32}$
   (f) $2x^2 \equiv 40 \pmod{64}$

(3) 試解以下二次的 congruence equations.
   (a) $x^2 \equiv 21 \pmod{9}$
   (b) $x^2 \equiv 18 \pmod{27}$
   (c) $x^2 \equiv 31 \pmod{81}$

(4) 試解以下二次的 congruence equations.
   (a) $x^2 + 7x \equiv 15 \pmod{216}$
   (b) $x^2 + 11x \equiv 18 \pmod{216}$

(5) 試分別利用 Euler's Criterion 以及 Gauss's Lemma 計算以下 Legendre symbols:

$$\text{(a) } \left(\frac{11}{23}\right) \qquad \text{(b) } \left(\frac{-6}{11}\right).$$

(6) 假設 p 是一奇質數, 試利用 Gauss's Lemma 證明 $\left(\frac{-1}{p}\right) = 1$ 若且唯若 $p \equiv 1 \pmod 4$.

(7) 假設 p 是一奇質數, $a, b \in \mathbb{Z}$ 且 $p \nmid a, p \nmid b$. 試證明 $ax^2 \equiv b \pmod p$ 有解若且唯若 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$.

(8) 假設 p 是一奇質數.

(a) 假設 $a, b \in \mathbb{Z}$ 試證明 $a^2 \equiv b^2 \pmod p$ 若且唯若 $a \equiv \pm b \pmod p$.

(b) 試證明 $\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = 0$.

(c) 試證明當 $p \equiv 1 \pmod 4$ 時 $\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{(p-1)/2}{p}\right) = 0$.

(9) 以下我們要用反證法證明 $4k+1$ 形式的質數有無窮多個. 假設 $p_1, \ldots, p_r$ 是所有 $4k+1$ 形式的質數, 試證明若 q 是一質數且 $q | 4p_1^2 \cdots p_r^2 + 1$, 則 $q \equiv 1 \pmod 4$ (即 q 亦為 $4k+1$ 形式). 依此得矛盾而得證 $4k+1$ 形式的質數有無窮多個.

(10) 試計算以下的 Legendre symbols.

$$\text{(a) } \left(\frac{-79}{101}\right) \qquad \text{(b) } \left(\frac{91}{127}\right) \qquad \text{(c) } \left(\frac{2817}{4177}\right).$$

(11) 假設 p, q 皆為奇質數.

(a) 試證若 $p = 4q + 1$, 則 $x^2 \equiv q \pmod{p}$ 有解.

(b) 假設 $p \equiv q \equiv 3 \pmod{4}$. 試證 $x^2 \equiv p \pmod{q}$ 有解若且唯若 $x^2 \equiv -q \pmod{p}$ 有解.

(c) 試證 $\left(\frac{-2}{p}\right) = 1$ 若且唯若 $p \equiv 1, 3 \pmod{8}$.

(d) 試證 $\left(\frac{3}{p}\right) = 1$ 若且唯若 $p \equiv \pm 1 \pmod{12}$.

(e) 試找出使得 $\left(\frac{-5}{p}\right) = 1$ 的奇質數的充要條件.

Chapter 6. Primitive Roots

(1) 試求以下之 order: (a) $\mathrm{ord}_{15}(8)$ (b) $\mathrm{ord}_{17}(9)$

(2) 試說明在 modulo 15 和 16 之下無 primitive roots.

(3) 假設 $\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$. 試證明 $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.

(4) 試證明若 $\mathrm{ord}_m(a) = m - 1$, 則 m 必為質數.

(5) 假設 $a, n \in \mathbb{N}$ 且 $a > 1$. 試證明 $\mathrm{ord}_{a^n-1}(a) = n$, 並依此得證 $n \mid \phi(a^n - 1)$.

(6) 假設 $m, n \in \mathbb{N}$ 且 $\gcd(a, mn) = 1$.
   (a) 試證明 $\operatorname{lcm}(\operatorname{ord}_m(a), \operatorname{ord}_n(a)) \mid \operatorname{ord}_{mn}(a)$.
   (b) 若又假設 $\gcd(m, n) = 1$, 試證明 $\operatorname{ord}_{mn}(a) \mid \operatorname{lcm}(\operatorname{ord}_m(a), \operatorname{ord}_n(a))$. 並依此得證當 $\gcd(m, n) = 1$ 時 $\operatorname{ord}_{mn}(a) = \operatorname{lcm}(\operatorname{ord}_m(a), \operatorname{ord}_n(a))$.

(7) 已知 $\operatorname{ord}_{101}(10) = 4$, 試找出在 modulo 101 之下所有 order 為 4 的元素並說明理由.

(8) 令 p 為一奇質數且 a 為 modulo p 之下的一個 primitive root.
   (a) 若 $b \in \mathbb{Z}$ 滿足 $ab \equiv 1 \pmod{p}$, 試證明 b 是 modulo p 之下的一個 primitive root. 依此證明當 $p > 3$ 時所有在 modulo p 之下的 primitive root 之乘積在 modulo p 之下為 congruent to 1.
   (b) 試證明 Legendre symbol $\left(\dfrac{a}{p}\right) = -1$.
   (c) 試證明
$$\operatorname{ord}_p(-a) = \begin{cases} p-1, & \text{若 } p \equiv 1 \pmod 4; \\ (p-1)/2, & \text{若 } p \equiv 3 \pmod 4. \end{cases}$$

(9) 試找出一整數使其對任意 $m \in \mathbb{N}$ 在 modulo 13^m 和 $2 \cdot 13^m$ 之下皆為 primitive root.

(10) 試找出在 modulo 486 之下為 primitive root 之最小的正整數.

(11) 試判斷以下 congruence equation 是否有解, 若有解試寫下其所有解.

(a) $x^3 \equiv 11 \pmod{14}$.

(b) $x^4 \equiv 12 \pmod{17}$.

(c) $x^5 \equiv 13 \pmod{18}$.

(d) $x^6 \equiv 7 \pmod{19}$.

(12) 在以下各題中試找出所有可能的整數 a 使其 congruence equation 有解.

(a) $ax^9 \equiv 6 \pmod{13}$.

(b) $7x^9 \equiv a \pmod{13}$.

(c) $ax^{12} \equiv 9 \pmod{17}$.

(d) $8x^{12} \equiv a \pmod{17}$.

(13) 令 $p \geq 5$ 為質數.

(a) 試證明 $x^4 \equiv -1 \pmod{p}$ 有解若且唯若 $p \equiv 1 \pmod{8}$.

(b) 假設 $p \equiv 1 \pmod{6}$ 且 $p \nmid a$ 試證明若 $x^3 \equiv a \pmod{p}$ 有解, 則在 modulo p 之下共有 3 個相異解.

(c) 假設 $p \equiv 5 \pmod{6}$ 試證明 $x^3 \equiv a \pmod{p}$ 在 modulo p 之下有唯一解.

Chapter 7. 略談 Diophantine Equations

(1) 試證明以下 Diophantine equation 無解.
   (a) $3x^2 - 7y^2 = 2$.
   (b) $x^2 + y^2 + 1 = 4z$.

(2) 試找出所有滿足 $z \leq 50$ 的 primitive Pythagorean triples x, y, z.

(3) 假設 x, y, z 是一組 primitive Pythagorean triple.
   (a) 試證明 x, y 中恰有一個是 3 的倍數.
   (b) 試證明 x, y 中恰有一個是 4 的倍數.
   (c) 試證明 x, y, z 中恰有一個是 5 的倍數.
   (d) 試證明 $60 \mid xyz$

(4) 試找出 $x^2 + 4y^2 = z^2$ 的所有正整數解.

(5) 證明 $x^4 - y^4 = z^2$ 沒有正整數解.

(6) 試證明若 x, y, z 是一組 Pythagorean triple 則 x, y, z 中最多僅有一個是整數的平方.

(7) 試說明以下整數是否可以寫成兩個整數的平方和, 若可以試將之寫成兩個整數的平方和.
   (a) 207
   (b) 637
   (c) 522
   (d) 605