

---

# 數論

高晔竣

December 2, 2018

底下若沒有特別說明，所有  $n, m$  等英文字母都是代表正整數或整數， $p, q$  則代表質數 (prime)。

## 1 同餘

**定義 1.** 對整數  $a, b$  和正整數  $m$ ，我們說  $a \equiv b \pmod{m}$  若且唯若  $m \mid a - b$ 。

**性質 2.** 同餘的基本運算規則：

(1) 若  $a \equiv b \pmod{m}$ ,  $c \equiv d \pmod{m}$ ，則  $a \pm c \equiv b \pm d \pmod{m}$ 。

(2) 若  $a \equiv b \pmod{m}$ ,  $c \equiv d \pmod{m}$ ，則  $ac \equiv bd \pmod{m}$ 。

(3) 若  $ca \equiv cb \pmod{m}$ ，則  $a \equiv b \pmod{\frac{m}{(c, m)}}$ 。

(4) 若  $ab \equiv 0 \pmod{p}$ ，則  $a \equiv 0$  或  $b \equiv 0 \pmod{p}$ 。

**例題 1.** 令  $P(x)$  為整係數多項式，則  $P(a+n) \equiv P(a) \pmod{n}$ 。

**定理 3.** (Bézout Lemma) 不定方程  $ax + by = c$  有整數解若且唯若  $\gcd(a, b) \mid c$ 。

**推論 3.1.** 對  $a \in \mathbb{Z}$ ，存在  $b$  使得  $ab \equiv 1 \pmod{m}$  若且唯若  $(a, m) = 1$ 。此時  $b$  被稱為  $a$  的模反元素，記為  $a^{-1}$ 。

**例題 2.**  $p > 3$ ，證明： $p^2 \mid (p-1)! \left( \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1} \right)$ 。

**例題 3.** 證明： $(a+b)^p \equiv a^p + b^p \pmod{p}$ 。

**定理 4.** (Lucas) 令  $\overline{n_k \cdots n_1 n_0}$ ,  $\overline{m_k \cdots m_1 m_0}$  為  $n, m$  的  $p$  進位表示式，則

$$\binom{n}{m} \equiv \binom{n_k}{m_k} \binom{n_{k-1}}{m_{k-1}} \cdots \binom{n_1}{m_1} \binom{n_0}{m_0} \pmod{p}$$

**習題 1.** 求所有質數  $p, q, r$  使得  $p \mid qr - 1, q \mid rp - 1, r \mid pq - 1$ 。

**習題 2.** (12N1) 給定兩個相異的非零整數  $a, b$ ，構造滿足以下條件的集合  $A$ ：

---

(1)  $a, b \in A$  。

(2) 對所有  $x, y \in A$  和整數  $k$ ， $x^2 + kxy + y^2 \in A$ 。

求所有數對  $(a, b)$  使得唯一滿足以上條件的集合  $A$  就是整數集  $\mathbb{Z}$ 。

**習題 3.** (2006APMO3)  $p \geq 5$ ，證明  $p^5 \mid \binom{p^2}{p} - p$ 。

## 2 基本的數論定理

**定義 5.** 在模  $m$  下， $a$  的同餘類是指所有模  $m$  和  $a$  同餘的整數形成的集合。

$$\bar{a} = \{b \mid a \equiv b \pmod{m}\} = \{a + km \mid k \in \mathbb{Z}\}$$

**定義 6.** 在所有同餘類中各選一個數，形成的集合稱為模  $m$  的完全剩餘系。

**定義 7.** 在所有跟  $m$  互質的同餘類中各選一個數，形成的集合稱為模  $m$  的既約剩餘系，其元素個數計為  $\varphi(m)$  (歐拉函數)。

**定理 8.** (費馬小定理)  $(a, p) = 1$ ，則  $a^{p-1} \equiv 1 \pmod{p}$ 。

**例題 4.** (歐拉定理)  $(a, m) = 1$ ，則  $a^{\varphi(m)} \equiv 1 \pmod{m}$ 。

**例題 5.**  $(a, b) = 1$ ，證明： $a^2 + b^2$  的奇質因數都是  $4k + 1$  的形式。

**定理 9.** (拉格朗日)  $f(x)$  是一個整係數多項式且首項不為  $p$  的倍數。則同餘方程式  $f(x) \equiv 0 \pmod{p}$  (模  $p$  下) 的解數最多有  $\deg f(x)$  個。

**推論 9.1.**  $x^p - 1 \equiv x(x-1)\cdots(x-(p-1)) \pmod{p}$ 。

**定理 10.** (Wilson 定理)  $(p-1)! \equiv -1 \pmod{p}$ 。

**定理 11.** (中國剩餘定理) 如果  $m_1, \dots, m_r$  兩兩互質，則同餘方程組

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

在模  $m$  底下恰有一解 (解為一個模  $m$  的同餘類)。

**性質 12.** 計算歐拉函數  $\varphi(n)$ ：

(1)  $\varphi(1) = 1$ 。

---

(2)  $\varphi(p^k) = (p-1)p^{k-1}$ 。

(3) 如果  $(n, m) = 1$ ，則  $\varphi(nm) = \varphi(n)\varphi(m)$ 。

**定理 13.** 若  $n$  的質因數分解為  $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ ，其中  $p_1, \dots, p_r$  為相異質數， $\alpha_i > 0$ ，則

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)。$$

**例題 6.** 證明： $\sum_{d|m} \varphi(d) = m$ 。

**例題 7.** 求所有正整數  $n$  使得  $\varphi(n) \mid n$ 。

**例題 8.**  $\{a_1, a_2, \dots, a_m\}, \{b_1, b_2, \dots, b_m\}$  是模  $m$  下的兩組完全剩餘系。

(1)  $\{a_1 + b_1, a_2 + b_2, \dots, a_m + b_m\}$  有沒有可能是一組完全剩餘系？

(2)  $\{a_1 b_1, a_2 b_2, \dots, a_m b_m\}$  有沒有可能是一組完全剩餘系？

**習題 4.**  $m > 4$  是合數，證明： $(m-1)! \equiv 0 \pmod{m}$ 。

**習題 5.** (05N1) 定義數列  $a_n = 2^n + 3^n + 6^n - 1$ 。求所有正整數  $m$  使得  $(m, a_n) = 1 \ \forall n \in \mathbb{N}$ 。

**習題 6.** 求所有正整數  $k, m$  使得  $k! + 48 = 48(k+1)^m$ 。

### 3 數論技巧

最簡單的數論技巧：

(1) 亂炸一通

(2) 取 mod(通常是模質數)

(3) 壓大小

(4) 無窮遞降法

**例題 9.** 求不定方程  $x^2 + y^2 = z^2$  的所有整數解。

**例題 10.** 求不定方程  $x^4 + y^4 = z^2$  的所有整數解。

**例題 11.** (2011APMO1) 證明：不存在正整數  $a, b, c$  使得  $a^2 + b + c, a + b^2 + c, a + b + c^2$  都是完全平方數。

**例題 12.** (02N1) 求最小的正整數  $k$ ，使得存在  $k$  個整數  $a_1, \dots, a_k$  滿足  $a_1^3 + \dots + a_k^3 = 2002^{2002}$ 。

---

**例題 13.**  $a, b$  為正整數使得  $ab + 1 \mid a^2 + b^2$ 。證明  $\frac{a^2 + b^2}{ab + 1}$  是完全平方數。

**習題 7.** 求所有正整數  $x$  使得  $x^4 + x^3 + x^2 + x + 1$  是完全平方數。

**習題 8.** 求所有正整數  $n$  使得  $2^n + n \mid 8^n + n$ 。

**習題 9.** (06N1) 求所有整數  $x, y$  使得  $1 + 2^x + 2^{2x+1} = y^2$ 。

**習題 10.** 求不定方程  $12^x - 5^y = 7$  的正整數解。

**習題 11.** (14N2) 求所有正整數  $x, y$  使得  $\sqrt[3]{7x^2 - 13xy + 7y^2} = x - y + 1$ 。

**習題 12.**  $a, b$  為正整數使得  $ab - 1 \mid a^2 + b^2$ 。證明  $\frac{a^2 + b^2}{ab - 1} = 5$ 。

## 4 指數、原根

**定義 14.**  $(a, m) = 1$ 。若  $d$  為最小的正整數使得  $a^d \equiv 1 \pmod{m}$ ，則稱  $d$  為  $a$  在模  $m$  下的指數 (order)，記為  $d = \text{Ord}_m(a)$ 。

**定義 15.** 若  $\text{Ord}_m(g) = \varphi(m)$ ，則稱  $g$  為  $m$  的原根 (primitive root)。

**性質 16.** 指數的一些性質：

- (1)  $(a, m) = 1$ ， $d$  為指數，則  $a^c \equiv 1 \pmod{m}$  若且唯若  $d \mid c$ 。
- (2) 若  $g$  是  $m$  的原根，則  $\{1, g, g^2, \dots, g^{\varphi(m)-1}\}$  是模  $m$  下的一組既約剩餘系。
- (3)  $(m, n) = 1$ ，則  $\text{Ord}_{mn}(a) = [\text{Ord}_m(a), \text{Ord}_n(a)]$ 。

**性質 17.** 若  $m$  的原根存在，則  $m$  的原根有  $\varphi(\varphi(m))$  個。

**定理 18.** 質數都有原根。

事實上，對一個正整數  $m$ ， $m$  有原根若且唯若  $m = 1, 2, 4$  或  $p^\alpha, 2p^\alpha$  的形式，其中  $p$  是奇質數。

**例題 14.** 證明： $n \mid \varphi(2^n - 1)$ 。

**例題 15.** 證明： $n^4 + 1$  的質因數都是 2 或  $8k + 1$  的形式。

**例題 16.** 證明： $1^n + 2^n + \dots + (p-1)^n \equiv \begin{cases} -1, & p-1 \mid n \\ 0, & p-1 \nmid n \end{cases} \pmod{p}$ 。

**習題 13.** 求所有質數  $p, q$  使得  $pq \mid p^p + q^q + 1$ 。

---

**習題 14.**  $p$  和  $2p+1$  都是質數。證明存在一個  $2p+1$  的倍數，各位數字和不超過 3。

**習題 15.** 證明： $n^4 - n^2 + 1$  的質因數都是  $12k+1$  的形式。

**習題 16.** (06N5) 求不定方程  $\frac{x^7-1}{x-1} = y^5 - 1$  的所有整數解。

## 5 LTE

**定義 19.** 若  $p^\alpha \mid n$  且  $p^{\alpha+1} \nmid n$ ，則稱作  $p^\alpha$  恰整除  $n$ ，記為  $p^\alpha \parallel n$  或  $v_p(n) = \alpha$ 。

**定理 20.** (Lifting the exponent lemma)  $a \equiv b \not\equiv 0 \pmod{p}$ ，則有：

- (1)  $p$  是奇質數： $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$ 。
- (2)  $p = 2, 2 \mid n$ ： $v_p(a^n - b^n) = v_p(a - b) + v_p(a + b) + v_p(n) - 1$ 。
- (3)  $p = 2, 2 \nmid n$ ： $v_p(a^n - b^n) = v_p(a - b)$ 。

**例題 17.** 求所有正整數  $n$  使得  $n^2 \mid 2^n + 1$ 。

**例題 18.** 若正整數  $a, b$  和正奇數  $c$  滿足  $c \mid a^c + b^c$ ，則  $c \mid \frac{a^c + b^c}{a + b}$ 。

**習題 17.** (2012APMO3) 求所有正整數  $n$  和質數  $p$  使得  $p^n + 1 \mid n^p + 1$ 。

**習題 18.** (14N5) 求所有質數  $p$  和正整數  $x, y$  使得  $x^{p-1} + y, y^{p-1} + x$  皆為  $p$  的冪次。