
講義就是 1% 的排版，加上 99% 的前人講義

趙庭偉

June 13, 2019

1 同餘

定義 1 若 $n|a-b$ ，我們記做 $a \equiv b \pmod{n}$ (a 同餘 b 模 n)

性質 1 若 $a \equiv b \pmod{n}, b \equiv c \pmod{n}$ ，則 $a \equiv c \pmod{n}$

性質 2 若 $a \equiv b \pmod{n}$ ，則 $a \pm c \equiv b \pm c \pmod{n}$

性質 3 若 $a \equiv b \pmod{n}$ ，則 $ac \equiv bc \pmod{n}$

性質 4 若 $a \equiv b \pmod{n}$ ，且 $c|a, c|b$ ，則 $\frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{n}{\gcd(n,c)}}$

性質 5 若 $a \equiv b \pmod{n}$ ，則 $a^k \equiv b^k \pmod{n}$

性質 6 若 $\gcd(a, n) = 1$ ，則存在 b 使得 $ab \equiv 1 \pmod{n}$ ，而且這個 b 在模 n 下唯一，我們記做 a^{-1} 。

定義 2 若 $\gcd(b, n) = 1$ ，則我們定義 $\frac{a}{b} \equiv ab^{-1} \pmod{n}$

附註 注意到此時上述的性質們依舊成立，而性質四則不再要求 $c|a, c|b$ 。

性質 7 $x^2 \equiv 0, 1 \pmod{3}$

$x^2 \equiv 0, 1 \pmod{4}$

$x^2 \equiv 0, 1, 4 \pmod{8}$

$x^3 \equiv 0, \pm 1 \pmod{7}$

$x^3 \equiv 0, \pm 1 \pmod{9}$

練習 1 有個數列滿足 $a_{n+1} = a_n^3 + 103$ ，試證明這個數列最多只有一項是完全平方數

練習 2 試求出最小的正整數 n ，使得存在 $x_1^3 + x_2^3 + \dots + x_n^3 = 2002^{2002}$

練習 3 $p \geq 5$ 求證 $\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$

2 中國剩餘定理

先來點噁心的東西：

定理 1 Let R be a ring, I_1, I_2, \dots, I_k are ideals of R s.t. they are pairwise coprime, then we have

$$R/I \cong R/I_1 \times R/I_2 \times \dots \times R/I_k$$

where $I = I_1 I_2 \dots I_k$.

看完噁心的東西之後，來點故事吧 (?)

古時候孫子算經就提出了線性同餘方程，也就是一次式 mod 不同數時的共同解：

有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物幾何？

換成剛剛學到的話就是：

$$x \in \mathbb{N}, x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}$$

那這要怎麼解呢？所有解會長怎樣呢？秦九韶在算數九章中給出了完整的解法，而上面那題的解法被編成了一個口訣：

三人同行七十希，五樹梅花廿一支，七子團圓正半月，除百零五使得知

說的是把模 3 的餘數乘以 70，模 5 的餘數乘以 21，模 7 的餘數乘以 15，然後加起來，得到的數 mod 105 就是所有解了。

$$70 \times 2 + 21 \times 3 + 15 \times 2 = 233 \equiv 23 \pmod{105}$$

再來我們就好奇拉，如果不是 mod 3,5,7，而是其他數的話呢？會不會一定有解，上面的 70,21,15 怎麼來的？諸如此類的問題，而中國剩餘定理就給出了這些問題的答案：

定理 2 (中國剩餘定理)
$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}, \text{ 且 } m_1, m_2, \dots, m_n \text{ 兩兩互質, 這個同餘}$$

方程必定有解，且如果我們令 $M_i = m_1 m_2 \dots m_{i-1} m_{i+1} \dots m_n$ (除了 m_i 之外其他乘起來)， x_i 為 M_i 在 $(\text{mod } m_i)$ 下的倒數 (任取一個整數) 的話，則 $x \equiv a_1 x_1 M_1 + \dots + a_n x_n M_n \pmod{m_1 m_2 \dots m_n}$ 為所有解。

練習 4 (歐拉 φ 函數) 令 $\varphi(n)$ 代表小於等於 n 且與 n 互質的正整數個數。如果 $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ ，則

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right)$$

3 一些走在路上都會聽到的定理

定理 3 (費馬小定理) 若 p 是質數, 且 $\gcd(a, p) = 1$, 則

$$a^{p-1} \equiv 1 \pmod{p}$$

定理 4 (歐拉定理) 若 $\gcd(a, n) = 1$, 則

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

定理 5 (威爾森定理) 若 p 是質數, 則

$$(p-1)! \equiv -1 \pmod{p}$$

定理 6 (迪利克雷定理) 若 $\gcd(a, b) = 1$, 則 $ak + b$ 型的質數有無窮多個。

定義 3 (p -adic valuation) 給定質數 p , 若 $n = p^\alpha t, \gcd(p, t) = 1$, 則我們定義

$$v_p(n) = \alpha$$

定理 7 (Lifting The Exponent, LTE) 當 $p|a-b$ 且 $\gcd(p, a) = \gcd(p, b) = 1$ 時, 我們有:

1. 若 $p \neq 2$: $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$
2. 若 $p = 2, 4|a-b$: $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$
3. 若 $p = 2, 4 \nmid a-b, 2|n$: $v_p(a^n - b^n) = v_p(a - b) + v_p(a + b) + v_p(n) - 1$

練習 5 試求出所有質數 p 以及正整數 a, b 使得 $a^p - b^p = 1$

練習 6 $k > 1$, 試證明存在無窮多個 n 使得 $n|1^n + 2^n + 3^n + \dots + k^n$

練習 7 設 4444^{4444} 的各位數字和為 A , A 的各位數字和為 B , B 的各位數字和為 C , 求 $C = ?$

練習 8 求 $7^{7^{\dots^7}}$ (k 次) 的末兩位數

練習 9 設 p 為奇質數, a_1, \dots, a_p 與 b_1, \dots, b_p 都是模 p 的完全剩餘系, 試證明: $a_1 b_1, \dots, a_p b_p$ 不可能是模 p 的完全剩餘系

4 一些長得奇奇怪怪的定理

定理 8 (費馬大定理) 當 $n \geq 3$ 時,

$$x^n + y^n = z^n$$

沒有 $xyz \neq 0$ 的整數解。

定理 9 (Bertrand-Chebyshev 定理) 對於所有正整數 $n \geq 3$ ，存在質數 p 使得 $n < p < 2n - 2$

定理 10 (Catalan 猜想, Mihăilescu's 定理)

$$x^a - y^b = 1$$

在 $a, b > 1$ 時的正整數解只有 $(x, y, a, b) = (3, 2, 2, 3)$ 。

定理 11 (Kobayashi 定理) 若 $\{a_i\}_{i=1}^{\infty}$ 的質因數集有限 (也就是 $\{p \in \mathbb{P} | p | a_i \text{ for some } i\}$ 是有限集)，則對於所有整數 $t \neq 0$ ， $\{a_i + t\}_{i=1}^{\infty}$ 的質因數集無限。

定理 12 (Green-Tao 定理) 對於任意的正整數 k ，存在長度是 k 的質數等差數列。

練習 10 求所有整數 a, b, c 使得

$$(a - b)(a^2 - b^2)(a^3 - b^3) = 3c^3$$

練習 11 證明可以把 $1, 2, \dots, 2n$ 兩兩配對分成 n 組，使得每一組和都是質數。

練習 12 對於所有正整數 $n \geq 3$ ，證明存在 n^2 個相異質數構成的 n 階幻方。