

09-03-NumberTheory

Created on 20220605.

Last modified on 2023 年 4 月 2 日.

目录

Chapter 1 Introduction

1.1 Contents

- a: 初等数论
- b: 解析数论
- c: 代数数论
- d: 超越数论
- e: 丢番图逼近
- f: 数的几何 (几何数论)
- g: 概率数论
- h: 计算数论
- i: 组合数论
- j: 算术代数几何
- k: 数论其他学科

1.2 Symbol

Definition 1.1. 模 m 后余数相同: $a \equiv b \pmod{m}$

Chapter 2 初等数论

2.1 整数的整除性

2.1.1 因数和倍数

2.1.2 质数和合数

2.1.3 质数分布

不大于 x 的质数的个数 $\pi(x)$

Proposition 2.1. 质数定理

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \log(x)} = 1$$

Proposition 2.2. *Goldbach* 猜想: 大于 4 的偶数都是 2 个奇质数的和。

是否存在无数个形如 $2^p - 1$ 的数是质数

Fermat 数: $F_n = 2^{2^n} - 1$, F_5 不是质数

2.1.4 最大公因数和最小公倍数

最大公因数: (a, b)

最小公倍数: $\{a, b\}$

a 能被 b 除尽, 即 a 是 b 的整数倍: $b|a$

辗转相除法

$a = q \cdot b + r$, prove that: $(a, b) = (r, b)$, which means that $(r + qb, b) = (r, b)$.

Mark as to prove $L = R$, Prove:

$$\begin{aligned}
 (1) \\
 & \because L|a, L|b \\
 & \because r = a - qb \\
 & \therefore L|r \\
 & \because L|b \\
 & \therefore L|(r, b) \Rightarrow L|R; \\
 (2) \\
 & \because R|b, R|r \\
 & \because a = qb + r \\
 & \therefore R|a \\
 & \because R|b \\
 & \therefore R|(a, b) \Rightarrow R|L; \\
 & \because (1) \text{ and } (2) \\
 & \therefore L = R
 \end{aligned} \tag{2.1}$$

Proposition 2.3. $ab = (a, b) \cdot \{a, b\}$

Proposition 2.4. $(a, b) = 1, a|bc \Rightarrow a|c$

Proposition 2.5. $a|\prod a_i, (a, a_1) = \cdots = (a, a_{n-1}) = 1, \Rightarrow a|a_n$

Proposition 2.6. 算术基本定理：不计质因数的次序，正整数分解成质数连乘的形式是唯一的。 $a = \prod p_i = L = \prod q_i = R, \because p_1|R, \text{ set } p_1 = q_1, \text{ let } L = L/p_1, R = R/q_1, \text{ keep doing, } \therefore p_i = q_i$
 $a = \prod p_i^{n_i}$

Proposition 2.7. 任意 4 个连续整数的乘积加 1 是一个平方数 $a(a+1)(a+2)(a+3) + 1 = qq \Rightarrow a(a+3) \cdot (a+1)(a+2) = (q-1)(q+1)$

Proposition 2.8. a 是整数, $6|a(a-1)(2a-1)$. *Proof* $a = 2m \Rightarrow a(a-1)(2a-1) = 2m(9m^2 - 6m - (m-1)(m+1)), a = 2m+1 \Rightarrow a(a-1)(2a-1) = 2m(9m^2 + 6m - (m-1)(m+1))$

Proposition 2.9. $a \nmid 2, a \nmid 3, \Rightarrow 24|a^2 + 23$. *Proof*, 分类讨论即可。

Proposition 2.10. $(a^n, b^n) = (a, b)^n$

$(na, nb) = n(a, b)$

Proposition 2.11. $a, b \in \mathbb{Z}_+, \sqrt[n]{b}$ 如果不是整数，则不是有理分数。

Proposition 2.12. 代数方程 $\prod a_i x^i = 0, a_i \in \mathbb{Z}$ 如果有有理数根, 根一定是整数。

证明, 设 $x = \frac{p}{q}$, 即需要证明 $q = 1$. 带入 x , 有 $\sum \frac{a_i p^i}{q^i} = 0$, 两边乘以 q^n , $\sum a_i p^i q^{n-i} = 0, \therefore p^n = q \times T \Rightarrow q | p^n, \therefore q = 1$

Proposition 2.13. $A: \{4t - 1, t \in \mathbb{Z}\}$, 证 A 中有无限质数。

假设最多有 k 个, 尝试推出矛盾。

(step1) 记质数分解 $m = \prod^n p_i \in A, \therefore (4T + 1)(4U - 1) = 4\alpha - 1, (4T + 1)(4U + 1) = 4\beta + 1, \therefore$

$\exists p_i \in A$, 设 A 中最多有 k 个质数, 考察 $a = \prod^k p_i - 1$

(step2) 设 a 是质数, $\therefore 1 = \prod^k p_i - a, \therefore p_i \nmid a, \therefore a$ 是第 $k+1$ 的质数, 矛盾;

设 a 不是质数, a 一定有质数 $b \in A, b \notin \{p_i\}$, 所以存在第 $k+1$ 的质数, 矛盾。

综上, 有无限个。

Proposition 2.14. 证明 $F_5 = 2^32 + 1 = 641 \times 6700417$ 不是质数?

2.2 进制

二进制的加减乘除

2.3 不定方程

2.3.1 一元不定方程

$\prod_{i=0} a_i x^i = 0, a_i \in \mathbb{Z}$, 对于整数解 α , we have $a_0 = -\prod_{i=1} a_i \alpha^i \Rightarrow \alpha | a_0$

2.3.2 二元一次不定方程

$ax + by = c, a \neq 0, b \neq 0, a, b, c \in \mathbb{Z}$. 方程总可化简, 直到 $(a, b) = 1$ 该型方程找到特解 x_1, y_1 后, 通解: $x = x_1 + bu, y = y_1 + au, u \in \mathbb{Z}$

Proposition 2.15. $(a, b) = 1 \Rightarrow \exists x, y \in \mathbb{Z}, ax + by = 1$

Prove:

(step1) for set $A: \{ax + by | a, b \text{ is fixed}\}$, we have $c_1, c_2 \in A \Rightarrow c_1 + c_2 \in A$.

(step2) $a > b$, let $b = r_0$, we have

$$\left[\begin{array}{ccc} a = q_1 r_0 + r_1 & (a, r_0) = (r_0, r_1) & r_1 = a - q_1 r_0 \\ r_0 = q_2 r_1 + r_2 & (r_0, r_1) = (r_1, r_2) & r_2 = r_0 - q_2 r_1 \\ \vdots & \vdots & \vdots \\ r_n = q_{n+2} r_{n+1} + r_{n+2} & (r_n, r_{n+1}) = (r_{n+1}, r_{n+2}) & r_{n+2} = r_n - q_{n+2} r_{n+1} \\ r_{n+1} = q_{n+3} r_{n+2} + 0 & (r_{n+1}, r_{n+2}) = r_{n+2} & 0 = r_{n+1} - q_{n+3} r_{n+2} \end{array} \right] \quad (2.2)$$

from column 2, we have $(a, r_0) = r_{n+2} = 1$. From cloumn 3, and $\because a, b \in A, \therefore r_i \in A, \therefore \exists x, y, ax + by = r_{n+2} = 1$

2.3.3 勾股数

$x^2 + y^2 = z^2$, 做如下限定后 $x, y, z \in \mathbb{Z}_+, (x, y) = 1, 2|x$, 有: $x = 2ab, y = a^2 - b^2, z = a^2 + b^2, a > b, (a, b) = 1, 2 \nmid (a + b)$

Proposition 2.16. 整数边长的直角三角形, 斜边与一直角边长差 1, 3 个边可表示成: $2b + 1, 2b^2 + 2b, 2b^2 + 2b + 1, b \in \mathbb{Z}$

Proof $x^2 + y^2 = z^2$, 改写成等式集合 $Ax = 2ab, y = a^2 - b^2, z = a^2 + b^2$, let $z = x + 1$, so $a^2 + b^2 - 2ab = 1 \Rightarrow a = b + 1$, 带入等式集合 A , 即得。

2.3.4 费马问题

$x^n + y^n = z^n$, 这个不定方程没有正整数解。

Proposition 2.17. $x^4 + y^4 = z^4$ 没有整数解

证明 $x^4 + y^4 = z^4$ 没有整数解。令 $u = z^2$, 即证 $x^4 + y^4 = u^2$ 没有整数解。

step1) 设存在解, 即最小的正解为 u_1 , 证明 $(x, y) = 1$

设 $(x, y) = d > 1, \because d^4 | x^4, d^4 | y^4, \Rightarrow (\frac{x}{d})^4 + (\frac{y}{d})^4 = (\frac{u_1}{d^2})^2, \because \frac{u_1}{d^2} < u_1$, 矛盾, 即证。

step2) $(x, y) = 1$, so x, y 是 2 个奇数, 或是 1 奇 1 偶。分类讨论都是不可能的。

step2.1) 证明不可能是 2 个奇数。

假设是 2 个奇数, $x = 2m + 1, y = 2n + 1, L = x^4 + y^4 = (2m + 1)^4 + (2n + 1)^4 = 4T + 2$, so $2|L = R = u^2, 4 \nmid L = R = u^2$, 不存在这样的 u , 所以不能是 2 个奇数。

step2.2) 证明不可能是 1 奇 1 偶。

$x^4 + y^4 = u_1^2$ 改写为 $(x^2)^2 + (y^2)^2 = u_1^2$, 可进一步改为: $x^2 = 2ab, y^2 = a^2 - b^2, u_1 = a^2 + b^2, a > b, (a, b) = 1, 2 \nmid (a + b)$

step2.2.1) 设 $a = 2n, b = 2m + 1$

$y^2 = a^2 - b^2 \Rightarrow a^2 = b^2 + y^2 = 4U + 2, \therefore 4 \nmid a^2$, 与 $a = 2n$ 矛盾。

step2.2.2) 设 $a = 2m + 1, b = 2n$

$\because (a, b) = 1, \therefore (a, m) = 1$, and $\because x^2 = 2ab, \therefore (\frac{x}{2})^2 = am$, 因为 a 和 m 互质, 所以 a 需要能分解为 $a = c^2$, 即 $am = c^2 d^2, (c, d) = 1, \therefore 2 \nmid c, b = 2m = 2d^2$,

$y^2 = a^2 - b^2 \Rightarrow b^2 + y^2 = a^2 \Rightarrow (2d^2)^2 + y^2 = (c^2)^2$, 可改写为 $2d^2 = 2kl, y = k^2 - l^2, c^2 = k^2 + l^2, (k, l) = 1, d^2 = kl$

$d^2 = kl$, 所以 k 和 l 可分解为 $k = K^2, l = L^2, \therefore c^2 = K^4 + L^4$

$c \leq c^2 = a \leq a^2 < a^2 + b^2 = u_1$, 与 u_1 最小的正整数解矛盾。

step3) 综上, 即证不存在。

Proposition 2.18. 证明整数方程没有整数解: $x^4 - 4y^4 = z^2, x, y, z \in \mathbb{Z}$

Proof: 两边平方, 有 $z^4 = (x^4 + 4y^4)^2 - 16x^4y^4 \Rightarrow (2xy)^4 + z^4 = (x^4 + 4y^4)^2$, 此式无解, 所以原式无解。

2.4 一次同余式

2.4.1 同余

同余性质

Proposition 2.19. *reflection:* $a \equiv a \pmod{m}$

symmetry: $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

transitivity: $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ *Proof:* $a - b = q_1m, b - c = q_2m, \therefore a - c = tm$

Proposition 2.20. $(m, n) = 1, ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$ *Proof:* $ac - bc = qm, \therefore a - b = tm$

Proposition 2.21. $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ *Proof:* $a - b = qm$, and $a^n = (b + qm)^n \therefore a^n - b^n = tm$

应用

Proposition 2.22. $10^n \pmod{9} \equiv 1$, for example, $5874192 \pmod{9} = (5 + 8 + 7 + 4 + 1 + 2) \pmod{9} = 0$

Proposition 2.23. $(a \times b) \pmod{9} = ((a \pmod{9}) \times (b \pmod{9})) \pmod{9}$

$28997 \times 39459 \neq 1144192613, L = 8 \times 3 = 6 \neq 5 = R$, 不相等一定没有算对, 但是相等却不一定算对。

Proposition 2.24. $(a, m) \nmid b \Rightarrow (ax + b) \pmod{m} \neq 0$. *Prove:* suppose $\exists c, m \mid (ac + b), \therefore \exists \alpha, \alpha m = ac + b \Rightarrow b = \alpha m - ac, \therefore (a, m) = L, \therefore b = \alpha L, \therefore L \mid b$, 矛盾, 即证。

例: $2x \equiv 179 \pmod{562}$ 没有整数解

Proposition 2.25. $(a, m) = 1, m \nmid a \Rightarrow \exists x, m \mid (ax + b)$, 证明 $\exists ax + my = z, z = -b$

例: $256x \equiv 179 \pmod{337}$ 有整数解

Proposition 2.26. $ad \equiv bd \pmod{md} \Rightarrow a \equiv b \pmod{m}$, 证明, 改写一下即显然 $md \mid (ad - bd) \Rightarrow m \mid (a - b)$

Proposition 2.27. $1935 \mid (1296x - 1125) \Rightarrow 215 \mid 144x - 125, x = 80, 295, 510, 725, 940, 1155, 1370, 1585, 1800?$

2.4.2 孙子定理

解同余式组

Proposition 2.28. $x \equiv a \pmod{3}, x \equiv b \pmod{5}, x \equiv c \pmod{7} \Rightarrow x = 70a + 21b + 15c \pmod{105}$

Proposition 2.29. $\{m_k\}, \forall i, j, (m_i, m_j) = 1, \prod m_i = m_i M_i$, 方程组 $x \equiv b_i \pmod{m_i}$ 的解为 $x = (\sum b_i M'_i M_i) \pmod{\prod m_i}, M'_i M_i \equiv 1 \pmod{m_i}$.

Prove: $i = j, (m_i, M_j) = 1, \therefore \exists n_i, M'_j, n_i m_i + M'_j M_j = 1 \Rightarrow M'_j M_j \equiv 1 \pmod{m_i}$

$i \neq j, m_i \mid M_j, \therefore \exists b_j, b_j M'_j M_j \equiv 0 \pmod{m_i}, \therefore \sum b_j M'_j M_j \equiv b_i M'_i M_i \equiv b_i \pmod{m_i}$

例: $1 = x \pmod{2}, 2 = x \pmod{5}, 3 = x \pmod{7}, 4 = x \pmod{9}$, 解 $M = 2 \times 5 \times 7 \times 9 = 630, M_i = [315, 126, 90, 70], M'_i = [1, 1, 6, 4], \therefore x = 315 + 2 \times 126 + 3 \times 6 \times 90 + 4 \times 4 \times 70 = 157 \pmod{630}, \therefore x = 157 + 630k, k \in \mathbb{Z}$

Proposition 2.30. $a \equiv x \pmod{m_1} \equiv x \pmod{m_2}$, 所有解是 $x \equiv a \pmod{\{m_1, m_2\}}$, 证明的话, 两边改写一下即可 $m_1 \mid (a - x), m_2 \mid (a - x), \{m_1, m_2\} \mid (a - x)$

Proposition 2.31. $(m_1, m_2) = d, d \mid (b_1, b_2)$, 方程组 $Ax \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}$, 解为 $x \equiv x_0 \pmod{(\{m_1, m_2\})}$, 其中 x_0 是方程组 A 的解。

Proposition 2.32. $(n_i, n_j) = 1, n_i \mid m_i, \{n_1, \dots, n_k\} = \{m_1, \dots, m_k\}, \therefore$ 方程组 $x \equiv b_i \pmod{m_i}$ 与方程组 $x \equiv b_i \pmod{n_i}$ 同解

2.5 剩余系

2.5.1 完全剩余系

Complete residue system

Proposition 2.33. m 的完全剩余系 $\forall k \in \mathbb{Z}, \varphi_m(k) = k \pmod{m} = \alpha \in A = \{0, 1, \dots, m - 1\}$, a set B , that $\varphi_m(B) = A$ *Proof:* $a - b = qm$, and $a^n = (b + qm)^n \therefore a^n - b^n = tm$

Proposition 2.34. m 的完全剩余系 $K, \forall a, b \in K, a \not\equiv b \pmod{m}$

给定集合 $T, \forall a, b \in T, a \not\equiv b \pmod{m}$, therefore T 是 m 的完全剩余系 K

Proposition 2.35. m 的完全剩余系 K, K 的每个元素加 a , 得到的集合仍是完全剩余系。

相当于平移 $a \pmod{m}$

m 的完全剩余系 $K, (b, m) = 1, K$ 的每个元素乘以 b , 得到的集合仍是完全剩余系。证明参考 2.20。

应用

Proposition 2.36. m_1, m_2 的完全剩余系记为 $R_{m_1}, R_{m_2}, (m_1, m_2) = 1, \therefore R_{m_1 m_2} = \{m_2 x_1 + m_1 x_2 | x_1 \in R_{m_1}, x_2 \in R_{m_2}\}$

Proof, 即证明这 $m_1 m_2$ 个数对 $m_1 m_2$ 不同余。 $m_2 x_1 + m_1 x_2 \equiv m_2 y_1 + m_1 y_2 \pmod{m_1 m_2}$, therefore $m_2(x_1 - y_1) = m_1 m_2 q - m_1(x_2 - y_2)$, therefore $m_1 | m_2(x_1 - y_1) \Rightarrow m_1 | (x_1 - y_1)$, therefore $x_1 \equiv y_1 \pmod{m_1}$, 即证。

Proposition 2.37. $\{m_i\}$ 是 k 个互质的正整数, $x_i \in R_{m_i}, \prod m_i = m_i M_i$, therefore $\{\sum M_i x_i\} = R_{\prod m_i}$. 证明如 2.36

$\{m_i\}$ 是 k 个互质的正整数, $x_i \in R_{m_i}$, therefore

$$\{x_1 + m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 m_2 \cdots m_{k-1} x_k\} = R_{\prod m_i}$$

证明如 2.36

2.5.2 简化剩余系

Proposition 2.38. m 的简化剩余系: m 的完全剩余系中, 挑出与 m 互质的, 包括 $1+mk$ 不包括 km 。

m 的简化剩余系 $K, (b, m) = 1, K$ 的每个元素乘以 b , 得到的集合仍是简化剩余系。

2.5.3 欧拉函数、欧拉定理、费马定理

欧拉函数

Definition 2.1. 欧拉函数 $\varphi(m)$: 不大于 m 的和 m 互质的正整数的个数。

对于质数 p , 有 $\varphi(p^l) = p^l - p^{l-1}$ *Proof*: $1p, 2p, \cdots, p^{l-1}p$ 是 p 的倍数, 即证。

Proposition 2.39. $a = \prod p_i^{a_i} \Rightarrow \varphi(a) = \prod p_i^{a_i-1}(p_i - 1)$

Proof: $n=1$, is obvious. $n=2$, p_1 的倍数 $1p_1, 2p_1, \cdots, \frac{a}{p_1}p_1$, 有 $\frac{a}{p_1}$ 个, 考虑 $p_1 p_2$ 的倍数, 所以 $\varphi(a) = a(1 - \frac{a}{p_1} - \frac{a}{p_1} + \frac{a}{p_1 p_2}) = a(1 - \frac{a}{p_1})(1 - \frac{a}{p_2})$, 继续考虑下去可以证明。

It is easy to see that $(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$

Proposition 2.40. $\forall m > 2, 2|\varphi(m)$

Proof: 如果 m 因数分解后, 若 m 的因数含有 2, 易知成立; m 的因数没有 2 则肯定有一个奇数 p , $p-1$ 是偶数, 即证。

因而, 不大于 m 的和 m 互质的正整数, 之和是 $\frac{m\varphi(m)}{2}$, 证明: 从小到大排列后, $\{n_k\}$, $(n_i, n_{\varphi(m)-i}) = 1$, 求和即证。 m 等于 1 的时候也成立。

Proposition 2.41. 质数 p

$$\sum_0 \varphi(p^i) = p^n$$

欧拉定理

Definition 2.2. 欧拉定理: $(a, m) = 1, a^{\varphi(m)} \equiv 1 \pmod{m}$

Proof: 对于 m 的简化剩余系中的元素 a_i , we have $aa_i = a_j \Rightarrow \prod_{\varphi(m)} aa_i = \prod_{\varphi(m)} a_i$, 即证。

Definition 2.3. 费马定理: 对于质数 p , $p \nmid a, a^{p-1} \equiv 1 \pmod{m}$

Proof: a 整除不了的质数 p 和 a 互质, $\varphi_p = p-1$, 带入欧拉定理, 即证。

应用

Proposition 2.42. 今天周六, $t = a^{b^c}$ 天后是周几呢? *Answer:* $a \equiv a_1 \pmod{7}, 0 \leq a_1 \leq 6, a_1 = 0$ is Saturday too. When $1 \leq a_1 \leq 6$, 费马定理 $\because (a_1, 7) = 1, \therefore a_1^6 \equiv 1 \pmod{7}$.

$$b \equiv b_1 \pmod{6}, b_1 = 0, a_1^{b^c} \equiv 1 \pmod{7}$$

$$b_1 = 1, b^c = 6n + 1, \therefore a_1^{b^c} \equiv a_1 \pmod{7}$$

$$b_2 = 2, b^c = 6n + 2, \text{ or } b^c = 6n + 4 \therefore a_1^2, a_1^4$$

$$b_2 = 3, b^c = 6n + 3 \therefore a_1^3$$

$$b_2 = 4, b^c = 6n + 4 \therefore a_1^4$$

$$b_2 = 5, b^c = 6n + 5 \therefore a_1^5$$

$$\begin{bmatrix} a_1^1 & a_1^2 & a_1^3 & a_1^4 & a_1^5 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 4 & 1 & 2 & 4 \\ 3 & 2 & 6 & 4 & 5 \\ 4 & 2 & 1 & 4 & 2 \\ 5 & 4 & 6 & 2 & 3 \\ 6 & 1 & 6 & 1 & 6 \end{bmatrix} \quad (2.3)$$

例如, $t = 773^{3169^c}, a_1 = 1, b \equiv 1 \pmod{6}, \therefore 3$, 如今天周日则 t 天后是周三

Proposition 2.43. $(a+b)(\text{ mod } m) = [a(\text{ mod } m)+b(\text{ mod } m)](\text{ mod } m) = [a(\text{ mod } m)+b(\text{ mod } m)]^n(\text{ mod } m)$

Proof, compare $(a+b)^2, (tm+a_1+b)^2$, we can see it is true.

Proposition 2.44. $(12371^{56}+34)^{28}(\text{ mod } 111) \equiv (50^{56}+34)^{28} \equiv ((125000^9 \times 50)^2+34)^{28} \equiv ((14^9 \times 50)^2+34)^{28} \equiv ((14^9 \times 50)^2+34)^{28} \equiv ((80^3 \times 50)^2+34)^{28} \equiv ((68 \times 50)^2+34)^{28} \equiv ((70)^2+34)^{28} \equiv ((70)^2+34)^{28} \equiv 70$

$$\varphi(111) = 72 \Rightarrow (12371^{56}+34)^{72c} \equiv 1(\text{ mod } 111)$$

Proposition 2.45. $3^{8232010} - 3^{10} \equiv 0(\text{ mod } 24010000)$ *Proof:* $t = 24010000 = 2^4 \times 5^4 \times 7^4, \therefore \varphi(t) = 8232000, 3^{\varphi(t) \equiv 1(\text{ mod } t)}, \therefore 3^{8232010} \Rightarrow 3^{10}$

Proposition 2.46. $21|(121^6 - 1)$

Proof: $\varphi(21) = 12, \therefore 11^{12} \equiv 1(\text{ mod } 21), \square$

Proposition 2.47. *primer $p, p \neq 2, p \neq 5, p|9 \cdots 9, (p-1)k \uparrow 9$.*

Proof: $(p, 10) = 1, (10^k, p) = 1, \therefore (10^k)^{p-1} \equiv 1(\text{ mod } p), \square$

Proposition 2.48. $641|F_5$

Proof: equals to prove $641|(2^{32}+1) \Rightarrow 640 \equiv -1(\text{ mod } 641) \Rightarrow 5 \times 2^7 \equiv -1(\text{ mod } 641) \Rightarrow 5^4 \times 2^{28} \equiv 1(\text{ mod } 641)$. And $\therefore 5^4 \equiv -2^4(\text{ mod } 641), \therefore -2^{32} \equiv 1(\text{ mod } 641), \square$

Proposition 2.49. *primer $p, (\sum a_i)^p \equiv (\sum(a_i^p))(\text{ mod } p)$*

Proof: we need to prove $L \equiv R(\text{ mod } p)$

$$(\text{step1}) \exists k, p|a_k, L = (\sum_{i \neq k} a_i + a_k)^p = R + Tp$$

(step2) $\forall k, p \nmid a_k, \therefore a_i^{p-1} \equiv 1(\text{ mod } p), \therefore a_i^p \equiv a_i(\text{ mod } p), \therefore R \equiv (\sum a_i)(\text{ mod } p)$, so we need to prove $(\sum a_i)^p \equiv (\sum a_i)(\text{ mod } p)$. Mark $S = \sum a_i$, if $p|S$, is obvious. If $p \nmid S, S^{p-1} \equiv 1(\text{ mod } p), \square$

Proposition 2.50. $1978^m \equiv 1978^n(\text{ mod } 1000), \min(m+n), m \neq n?$

Solve: $1000|1978^{n-m} \Rightarrow (2^3 \times 5^3)|2^m \times 989^m(1978^{n-m} - 1)$.

because $989^m(1978^{n-m} - 1)$ is odd, therefore $m \geq 3$, and therefore $5^3|(1978^{n-m} - 1), \therefore 1978^{n-m} \equiv 1(\text{ mod } 125)$. $\therefore \varphi(125) = 100, \therefore 1978^{100} \equiv 1(\text{ mod } 125)$.

We now prove that $(n-m)|100$. Suppose $(n-m) \neq 100, \therefore 100 = q(n-m) + r, \therefore 1978^r \equiv 1(\text{ mod } 125), \therefore r < n-m$, 矛盾。

For now, we have $(n-m)|100, 125|(1978^{n-m}-1)$. $\therefore 125|(1978^{n-m}-1) \therefore 1|1978^{n-m}$, or $6|1978^{n-m}$. $\therefore (n-m)|100, \therefore 4|(m-n), \therefore m-n = 4, 20, 100$.

For now we test if $1978^4 \equiv 1(\text{ mod } 125)$. $L \equiv (125 \times 15 + 103)^4 \equiv 103^4 \equiv (3 + 4 \times 5^2)^{2+2} \equiv (3^2 + 2 \times 3 \times 4 \times 5^2)^2 \equiv 609^2 \equiv (-16^2) \equiv 6$

For now we test if $1978^{20 \times 5} \equiv 1 \pmod{125}$. $L \equiv 6^{25} \equiv [36 \times (125 + 91)]^5 \equiv (36 \times 91)^5 \equiv 26^5$. We can see that for 20, we have 26, and 100 we have 1. So $m = 3, n = 103$.

Proposition 2.51. 分针目前在 12, 问分针走 a^{b^c} , 是几点。

$$\begin{bmatrix} a_1^1 & a_1^2 & a_1^3 & a_1^4 \\ 0 & \dots & & \\ 1 & \dots & & \\ 2 & 4 & 8 & 4 \dots \\ 3 & 9 & 3 \dots & \\ 4 & 4 \dots & & \\ 5 & 1 \dots & & \\ 6 & 0 \dots & & \\ 7 & 1 \dots & & \\ 8 & 4 & 8 \dots & \\ 9 & 9 \dots & & \\ 10 & 4 & 4 \dots & \\ 11 & 1 \dots & & \end{bmatrix} \quad (2.4)$$

表 2.1: model2

a_1	讨论
1,5,7,11	b is odd: a_1 b is even: 1
2	b = 1: 2 b is even: 4 b is odd and $b > 1$: 8
3	b is odd: 3 b is even: 9
4	4
6	b = 1: 6 b > 1: 0
8	b is odd: 8 b is even: 4
9	9
10	b = 1: 10 b > 1: 4

2.6 小数、分数、实数

2.7 连分数

2.7.1 连分数基本性质

2.7.2 无限连分数

2.7.3 数论函数

2.8 复数和三角和

Chapter 3 解析数论

Chapter 4 代数数论

Chapter 5 超越数论

Chapter 6 丢番图逼近

Chapter 7 数的几何（几何数论）

Chapter 8 概率数论

Chapter 9 计算数论

Chapter 10 组合数论

Chapter 11 算术代数几何

Chapter 12 数论其他学科