09-03-NumberTheory

Created on 20220605.

Last modified on 2023 年 3 月 19 日.

目录

Chapter 1 Introduction

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

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*

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

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

$a = q \cdot b + r, prove\ that : (a, b) = (r, b)$. Mark as to prove $L = R$, Prove:

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

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。$a = \prod p_i = L = \prod q_i = R, \because p_1|R, set\ p_1 = q_1, let\ L = L/p_1, R = R/q_1, keep\ doing, \therefore p_i = q_i$
$a = \prod p_i^{n_i}$

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. $a, b \in \mathbb{Z}_+, \sqrt[a]{b}$ 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 $m = \prod^n p_i \in A, \because (4T+1)(4U-1) = 4\alpha - 1, (4T+1)(4U+1) = 4\beta + 1, \therefore \exists p_i \in A$, 设 A 中最多有 k 个质数，考察 $a = \prod^k p_i - 1$

(step2) 设 a 是质数,$\because 1 = \prod^k p_i - a, \therefore p_i \nmid a, \therefore a$ 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 $F_5 = 2^3 2 + 1 = 641 \times 6700417$ 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 $A : \{ax + by | a, b \textit{ is fixed}\}$, *we have*$c_1, c_2 \in A \Rightarrow c_1 + c_2 \in A$.

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

$$\begin{bmatrix} a = q_1 r_0 + r_1 & (a, r_0) = (r_0, r_1) & r_1 = a - q_1 r_0 \\ r_0 = q_2 r_1 + r_2 & (r_0, r_1) = (r_1, r_2) & r_2 = r_0 - q_2 r_1 \\ \vdots & \vdots & \vdots \\ r_n = q_{n+2} r_{n+1} + r_2 & (r_n, r_{n+1}) = (r_{n+1}, r_{n+2}) & r_2 = r_n - q_{n+2} r_{n+1} \\ r_{n+1} = q_{n+3} r_{n+2} + 0 & (r_{n+1}, r_{n+2}) = r_{n+2} & 0 = r_{n+1} - q_{n+3} r_{n+2} \end{bmatrix} \tag{2.2}$$

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 $A x = 2ab, y = a^2 - b^2, z = a^2 + b^2$, *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，$x = 2m + 1, n = 2n + 1$, $L = x^4 + y^4 = (2m + 1)^4 + (2n + 1)^4 = 4T + 2$, 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 $am=c^2d^2, (c,d)=1, \therefore 2\nmid c, b=2m=2d^2$,

$y^2=a^2-b^2 \Rightarrow b^2+y^2=a^2 \Rightarrow (2d^2)^2+y^2=(c^2)^2$, 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 $k=K^2, l=L^2, \therefore c^2=K^4+L^4$

$c\leqslant c^2=a\leqslant a^2<a^2+b^2=u_1$, 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

Proposition 2.19. $10^n \mod 9\equiv 1$, *for example,* $5874192 \mod 9=(5+8+7+4+1+2) \mod 9=0$

Proposition 2.20. $(a\times b) \mod 9=((a \mod 9)\times(b \mod 9)) \mod 9$

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

Proposition 2.21. $(a,m)\nmid b \Rightarrow (ax+b) \mod (m)\neq 0$. *Prove:suppose* $\exists c, m|(ac+b), \therefore \exists\alpha, \alpha m=ac+b \Rightarrow b=\alpha m-ac, \because (a,m)=L, \therefore b=\alpha L, \therefore L|b$, 矛盾，即证。

例：$2x\equiv 179(mod 562)$ 没有整数解

Proposition 2.22. $(a,m)=1, m\nmid a \Rightarrow \exists x, m|(ax+b)$，证明 $\exists ax+my=z, z=-b$

例：$256x\equiv 179(mod 337)$ 有整数解

Proposition 2.23. $ad\equiv bd(\mod md) \Rightarrow a\equiv b(\mod m)$, 证明，改写一下即显然 $md|(ad-bd) \Rightarrow m|(a-b)$

Proposition 2.24. $1935|(1296x-1125) \Rightarrow 215|144x-125, x=80,295,510,725,940,1155,1370,1585,1800?$

2.4.2 孙子定理

解同余式组

Proposition 2.25. $x \equiv a(\mod 3), x \equiv b(\mod 5), x \equiv c(\mod 7) \Rightarrow x = 70a + 21b + 15c(\mod 105)$

Proposition 2.26. $\{m_k\}, \forall i, j, (m_i, m_j) = 1, \prod m_i = m_i M_i$, 方程组 $x \equiv b_i(\mod m_i)$ 的解为 $x = (\sum b_i M_i' M_i)(\mod \prod m_i), M_i' M_i \equiv 1(\mod m_i)$.

Prove: $i = j, (m_i, M_j) = 1, \therefore \exists n_i, M_j', n_i m_i + M_j' M_j = 1 \Rightarrow M_j' M_j \equiv 1(\mod m_i)$

$i \neq j, m_i | M_j, \therefore \exists b_j, b_j M_j' M_j \equiv 0(\mod m_i), \therefore \sum b_j M_j' M_j \equiv b_i M_i' M_i \equiv b_i(\mod m_i)$

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

Proposition 2.27. $a \equiv x \mod m_1 \equiv x \mod m_2$, 所有解是 $x \equiv a \mod \{m_1, m_2\}$, 证明的话，两边改写一下即可 $m_1 | (a - x), m_2 | (a - x), \{m_1, m_2\} | (a - x)$

Proposition 2.28. $(m_1, m_2) = d, d | (b_1, b_2)$, 方程组 $Ax \equiv b_1(\mod m_1), x \equiv b_2(\mod m_2)$, 解为 $x = \equiv x_0(\mod (\{m_1, m_2\}))$，其中 x_0 是方程组 A 的解。

Proposition 2.29. $(n_i, n_j) = 1, n_i | m_i, \{n_1, \cdots, n_k\} = \{m_1, \cdots, m_k\}, \therefore$, 方程组 $x \equiv b_i(\mod m_i)$ 与方程组 $x \equiv b_i(\mod n_i)$ 同解

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