2023 年春数论课程笔记

整理者：子綦 • 子游

2023 年 3 月 31 日

目录

1 授课老师信息

名字：栗慧曦
办公室：数院 414
分为：初等数论解析数论代数数论
网课推荐：Core Topics in Modern number theory

2 初等数论

以下事实将被默认：

命题 2.0.1 (良序原理) *任何非空的正整数集合都包含一个最小的元素。*

推论 2.0.1 *数 $\sqrt{5}$ 不是有理数。*

证明 考虑 $S = \{b : b \in \mathbb{Z}_+, there\ \ exists\ \ an\ \ integral\ \ a\ \ such\ \ that\ \ \frac{a}{b} = \sqrt{5}\}$。我们假定 S 非空。则根据良序原理，S 有最小的元素 y，设 $\frac{x}{y} = \sqrt{5}$，$x \in \mathbb{Z}$.

于是 $x^2 = 5y^2$。$x^2 - 2xy = 5y^2 - 2xy, x(x-2y) = y(5y-2x)$. 于是 $\frac{x}{y} = \frac{5y-2x}{x-2y}$。

显然 $x - 2y = (\sqrt{5}-2)y > 0$，并且 $x - 2y < y, \sqrt{5} < 3$。于是矛盾于 y 最小！因此 S 是空集，这意味着 $\sqrt{5}$ 是无理数。 □

2.1 费马-欧拉定理及其应用

定理 2.1.1 (费马-欧拉) 设 a,n 是两个互素的正整数，即 $(a,n)=1$。那么下式成立：

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

证明 考虑群 $\mathbb{Z}/n\mathbb{Z}$ 有阶数 $\varphi(n)$，证毕。 □

例 2.1.1 $2^{12} \equiv 1(\mathrm{mod}13)$。

$3^6 \equiv 1(\mathrm{mod}14)$。

推论 2.1.2 (费马小定理) 给定一个素数 p 和一个整数 a, 且 (a,p) 互素。则 $a^{p-1} \equiv 1(\mathrm{mod}p)$。

推论 2.1.3 (费马小定理 · 形式 2) 设 p 是一个素数，则 $a^p \equiv a(\mathrm{mod}p)$。

对于一个较大的奇整数 n, 若 2^n 模 n 不等于 2，则 n 是一个合数。这一点可以用于判定一个数是否是素数。这被称为 Fermat's primality test to base 2.

素数是正整数，且必须严格大于 1. 这一点很容易搞错。

判定一个数是否是素数，如果使用蛮力计算，事实上可以在 $C\sqrt{n}$ 步内计算 n 的素因数分解。而 Fermat's primality test 仅需要 O($log(n)$) 步。

定义 2.1.1 如果一个数 n 能够通过所有的费马素数测试法, 则称其为 Carmichael 数。事实上,Carmichael 数的个数是无穷多个。

我们继续介绍 Miller test 方法来判定一个数是否是素数。

对于奇数 n，我们首先将 $n-1$ 写为 $2^r s$，$r \geq 1$,s 是一个基数。我们验证 $a^s \equiv 1(\mathrm{mod}n)$,$a^s \equiv -1(\mathrm{mod}n), \ldots, a^{2^{r-1}s} \equiv -1(\mathrm{mod}n)$

如果都不成立，则 n 是一个合数。

如果合数 n 通过了 Miller 测试，说明其伪装的很好。我们称之为在底 a 下的强 pseudoprime（伪素数）。

例 2.1.2 对 25 使用 2 为基的 *Miller* 测试：

$25-1=2^3 \times 3.2^3 \equiv 8,2^{2\times 3} \equiv 14,2^{2^2\times 3} \equiv 21$。所以 25 未通过，是合数。

注解 一个合数至多能通过 1/4 的 *Miller* 测试。因而如果一个数通过了很多底的 *Miller* 测试, 从概率上讲其非常可能是一个素数。比如, 若其通过了 10 个测试, 则不是素数的可能性仅为 $(1/4)^10$。

2.2 中国剩余定理

命题 2.2.1 方程 $ax \equiv b \pmod{m}$ 是可解的，当且仅当 $d|b$，其中 $d=(a,m)$. 当 $d|b$，方程有 d 个不同的解：

$$x_0, x_0+m/d, \ldots, x_0+(d-1)m/d$$

定理 2.2.1 (CRT) 设 $m_1, \ldots, m_s$ 是两两互素的，其中 $s \geq 2$. 假设 $(a_i,m_i)=1,1 \leq i \leq s$, 那么方程组：

$$a_i x \equiv b_1 (\mathrm{mod} \quad m_i)$$

在 $\mathrm{mod}M = m_1 \ldots m_n$ 的要求下具有唯一的解。

证明 定理的证明充满着比较繁琐的构造。这里省略。但是为了解方程，又不得不说明怎么来的。因此我直接截取讲义的一部分：

Theorem 14. *The system of linear congruence equation*

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \cdots \\ x \equiv c_s \pmod{m_s} \end{cases}$$

where $m_1, m_2, \ldots, m_s$ are pairwise relatively prime, $s \geqslant 2$,has a unique solution mod $M = m_1 m_2 \ldots m_s$

Proof. (Existence) Let $n_i = \frac{M}{m_i}$. Since $m_1, m_2, \cdots, m_j$ are pairwise relatively prime, we know (n_i, m_i)=1 for $1 \leq i \leq s$.So $n_i y_i \equiv 1 \pmod{m_i}$has a unique solution $y_i \equiv n_i^{-1} \pmod{m_i}$.
We can verify $x_0 \equiv C_1 n_1 y_1 + C_2 n_2 y_2 + \cdots + C_s n_s y_s \pmod{M}$ satisfies the system of linear congruences. For example $X_0 \equiv C_1 n_1 y_1 + 0 + \cdots + 0 \equiv C_1 n_1 y_1 \equiv \pmod{m_i}$.
(Uniqueness)If x and y both satisfy the system of linear congruences, then

$$\begin{cases} x - y \equiv 0 \pmod{m_1} \\ x - y \equiv 0 \pmod{m_2} \\ \cdots \\ x - y \equiv 0 \pmod{m_s} \end{cases}$$

Since $m_1, m_2, \cdots, m_s$are pairwise relatively prime,we know $m_1 m_2 \cdots m_s | (x - y)$, i.e., $x \equiv y \pmod{M}$ □

3 代数数论

定义 3.0.1 *设正整数 a, b, c 满足:*

$$a^2 + b^2 = c^2 \quad (a, b, c) = 1 \tag{1}$$

则称 (a, b, c) 是互素的毕达哥拉斯三元数组。

定理 3.0.1 *(a, b, c) 是互素的毕达哥拉斯三元数组，则存在一个偶数且:*

$$a = 2st,\ b = t^2 - s^2,\ c = t^2 + s^2, \text{where } 0 < s < t,\ (s, t) = 1 \tag{2}$$

使得 s, t 一奇数一偶数。

证明 $a^2 = c^2 - b^2$，于是:

$$(a/2)^2 = (c + d)/2(c - d)/2 \tag{3}$$

我们断言 $\frac{c+d}{2}$ 和 $\frac{c-d}{2}$ 都是平方数。若不然，则两者有公共的素因子。显然不能是 2，则 c 和 b 不互素。

设 $t^2=\frac{c+d}{2}$,$s^2=\frac{c-d}{2}$。显然 $s<t$ 且 $(s,t)=1$。且 s,t 之中一奇数一偶数。

若 a,b,c 满足等式。我们只需要验证 (a,b,c) 互素。这也是显然的。 □

费马大定理说明当 $n\geq 3$ 的时候，上述方程没有非平凡的整数解。我们之后将会证明:$n=3$ 时，$x^3+y^3=z^3$ 没有非平凡的解，其中 $x,y,z\in\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$

命题 3.0.1 *方程 $x^4+y^4=z^2$ 没有非平凡的解。*

证明 显然不妨设 $(x,y)=1$。我们考虑 $x^4+y^4=z^2$。此时 (x^2,y^2,z) 是毕达哥拉斯互素的三元对。于是存在 $0<n<m$ 一奇数一偶数满足:$x^2=2mn,y^2=m^2-n^2,z=m^2+n^2$。

如果 m 是偶数，n 是奇数，则 y^2 模 4 余 3。矛盾！

于是 $n^2+y^2=m^2$。于是 $m=a^2$,a 是奇数。$2n=b$，b 是偶数。设 $b=2c$，则 $n=2c^2$。于是:

$$a^4=m^2=n^2+y^2=4c^2+y^2 \tag{4}$$

因此 $(2c^2,y,a^2)$ 是毕达哥拉斯互素的三元对。因此:

$$2c^2=2m_1n_1\quad y=m_1^2-n_1^2\quad a^2=m_1^2+n_1^2\ldots \tag{5}$$

因此 $m_1=a_1^2$,$n_1=b_1^2$. 此时 $a^2=a_1^4+b_1^4$。因此 (a_1,b_1,a) 也是一个非平凡的解 $x^4+y^4=z^2$。但是 $z=m^2+n^2>a\ldots$。根据良序引理容易导出矛盾。 □

为了证明费马最后一个定理, 我们只需要说明 $x^p+y^p=z^p$，p 是一个素数。我们考虑 $p=3$ 的情况，但是此时 $x,y,z\in\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$.

定义 3.0.2 *一个复数 ξ 被称为一个代数数，若存在一个首项为 1 的多项式 $f(x)\in\mathbb{Z}[x]$ 使得 $f(\xi)=0$。*

定理 3.0.2 *$\mathbb{Q}$ 中的代数数只有 $\mathbb{Z}$。*

我们称 $K/\mathbb{Q}$ 是一个数域，若 $[K:Q]<\infty$。我们用 $\mathcal{O}_K$ 表示所有的 K 中的代数数。则 $\mathcal{O}_{\mathbb{Q}}=\mathbb{Z}$。

我们将会关心 $K=\mathbb{Q}[\sqrt{-m}]$ 其中 m 是一个正的非平方数。根据抽象代数的知识，我们有:

$$\mathcal{O}_{\mathbb{Q}[\sqrt{-m}]}=\mathbb{Z}[-\sqrt{-m}],m\equiv 1(\mod 4);=\mathbb{Z}[\frac{1+\sqrt{-m}}{2}],m\equiv 3(\mod 3) \tag{6}$$

定义映射 N:

$$N:\mathcal{O}_{\mathbb{Q}[\sqrt{-m}]}\to\mathbb{Z}\quad ;a+b\sqrt{-m}\mapsto a^2+mb^2\ a,b\in\mathbb{Q} \tag{7}$$

可以验证 $N(ab)=N(a)N(b).N(a)=0$ 当且仅当 $a=0$。$N(a)=1$ 当且仅当 a 是一个单位。

命题 3.0.2 *整环 $\mathcal{O}_{\mathbb{Q}[\sqrt{-3}]}=\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ 是一个欧几里得环，即我们可以在环里面做带余除法。*

引理 3.0.3 *设 $\alpha\in\mathcal{O}_{\mathbb{Q}[-\sqrt{3}]}$。若 $N(\alpha)$ 是一个有理素数则 α 是 $\mathcal{O}_{\mathbb{Q}[\sqrt{-3}]}$ 上的素元。*

证明 显然。 □

推论 3.0.4 *考虑 $N(\sqrt{-3})=3$ 是 $\mathbb{Z}$ 中的素数，则 $\sqrt{-3}$ 是素元素。*

接下来我们考虑方程 $x^3+y^3=z^3$ 在模 $\sqrt{-3}$ 下的解。$\sqrt{-3}$ 的伴随是 $\sqrt{-3}$,$-\sqrt{-3}$,$\omega-1$,....