

浅谈 Pell 方程

尔濯

2023 年 7 月 7 日

摘要

本文通过 Dirichlet 单位定理分析了 Pell 方程解的结构，总结了一些基本单位的判定方法，并给出了一些 Pell 方程实例的计算.

目录

1	解的结构	2
2	基本单位的判定	7
3	广义 Pell 方程	8
4	例题分析	9

1 解的结构

Definition 1. *Pell 方程*是指形如

$$x^2 - dy^2 = \pm 1$$

的不定方程, 其中 $d > 1$ 且无平方因子, 而形如

$$x^2 - dy^2 = N$$

的不定方程一般称为*广义 Pell 方程*.

本文完全剖析了 Pell 方程的解的结构, 并就实二次域类数为 1 的情况刻画了广义 Pell 方程解的结构, 而给出这种刻画最犀利的工具自然是 Dirichlet 单位定理, 因为其对一个数域 K 的代数整数环 O_K 的单位给出了一种精确的描述.

Theorem 2 (Dirichlet 单位定理,[4]). 设 K 为 n 次数域, K 到 \mathbb{C} 有 r_1 个实嵌入, r_2 对复嵌入, $r_1 + 2r_2 = n$, 则 K 的代数整数环 O_K 的单位构成的乘法群 U_k 可以表为:

$$U_k = W_k \times V_k$$

其中 W_k 为数域 K 的单位根群, 且为一个有限循环群, V_k 为秩为 $r_1 + r_2 - 1$ 的自由 Abel 群.

Dirichlet 单位定理的证明是复杂的, 但其对 O_K 单位群 U_k 给出的描述是易懂的, 该定理告诉我们可以从 U_k 中找到 $r = r_1 + r_2 - 1$ 个元素 u_1, u_2, \dots, u_r , 使得 U_k 中每个元素 u 可以表示为

$$u = w \prod_{i=1}^r u_i^{a_i}$$

且这种表法在相差一个单位根的意义下唯一, 此时将这组单位 $\{u_1, \dots, u_r\}$ 称为*基本单位组*, 将每个 u_i 称为*基本单位*.

而我们知道, 对于代数整数环 O_K 中的元素 u , $u \in U_k$ 等价于 $N_{K/\mathbb{Q}}(u) = \pm 1$, 而且一个基本的事实是, 对于实二次域 $K = \mathbb{Q}(\sqrt{d})$, 其代数整数环

$$O_k = \begin{cases} k_1 + k_2\sqrt{d} & k_1, k_2 \in \mathbb{Z} \quad \text{当 } d \equiv 2, 3 \pmod{4} \\ k_1 + k_2 \frac{1+\sqrt{d}}{2} & k_1, k_2 \in \mathbb{Z} \quad \text{当 } d \equiv 1 \pmod{4} \end{cases}$$

对于实二次域 $K = \mathbb{Q}(\sqrt{d})$, 其只有两个实嵌入, 没有复嵌入, 且单位根群为 $\{1, -1\}$ 构成的乘法群, 因此取其中一个基本单位 $\epsilon = a + b\omega$, 则所有单位可以表示为

$$U_k = \{\pm \epsilon^n : n \in \mathbb{Z}\} \quad (1)$$

其中

$$\omega = \begin{cases} \sqrt{d} & \text{当 } d \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{当 } d \equiv 1 \pmod{4} \end{cases}$$

而对于 $d \equiv 2, 3 \pmod{4}$ 的实二次域而言, $k_1 + k_2\sqrt{d}$ 为单位等价于 k_1, k_2 为 Pell 方程 $x^2 - dy^2 = \pm 1$ 的解. 不难看出在 U_k 能作为基本单位的只有 $\pm \epsilon, \pm \epsilon^{-1}$, 这四个数中有且仅有一个写成 $k_1 + k_2\sqrt{d}$ 的形式后满足 $k_1, k_2 > 0$, 此后对于 $d \equiv 2, 3 \pmod{4}$ 的情况我们都取这样的元素作为基本单位, 并不妨记为 ϵ , 不难验证这个基本单位 $\epsilon > 1$.

Theorem 3. 设 $K = \mathbb{Q}(\sqrt{d})$, $d > 0$ 且无平方因子, $d \equiv 2, 3 \pmod{4}$, $\epsilon = a + b\sqrt{d}$ 为基本单位, 令 $\epsilon^n = a_n + b_n\sqrt{d}$, 则

1. 当 $N_{K/\mathbb{Q}}(\epsilon) = 1$ 时, Pell 方程 $x^2 - dy^2 = -1$ 无整数解, Pell 方程 $x^2 - dy^2 = 1$ 整数解解为 $\{(\pm a_n, \pm b_n) : n \in \mathbb{Z}_{\geq 0}\}$
2. 当 $N_{K/\mathbb{Q}}(\epsilon) = -1$ 时, Pell 方程 $x^2 - dy^2 = -1$ 整数解为 $\{(\pm a_{2n+1}, \pm b_{2n+1}) : n \in \mathbb{Z}_{\geq 0}\}$, Pell 方程 $x^2 - dy^2 = 1$ 整数解为 $\{(\pm a_{2n}, \pm b_{2n}) : n \in \mathbb{Z}_{\geq 0}\}$

Proof: 由于 Pell 方程的解关于原点对称, 我们只需求出所有非负整数解, 则其所有解只差一对正负号. 注意到由 (1) 刻画单位群 U_k 的结构, 方程 $x^2 - dy^2 = \pm 1$ 的非负整数解为: $\{(a_n, b_n) : n \in \mathbb{Z}_{\geq 0}\}$. 当 $N_{K/\mathbb{Q}}(\epsilon) = 1$ 时, 所有 U_k 中元素的范数均为 1, 化作不定方程的语言就是说: Pell 方程 $x^2 - dy^2 = -1$ 无非负整数解, Pell 方程 $x^2 - dy^2 = 1$ 非负整数解为 $\{(a_n, b_n) : n \in \mathbb{Z}_{\geq 0}\}$, 情况 1 证毕.

对于情况 2, $N_{K/\mathbb{Q}}(\epsilon) = -1$, 此时单位根群中元素的范数按奇偶呈正负交替的形式排列, 从而 Pell 方程 $x^2 - dy^2 = -1$ 非负整数解为 $\{(a_{2n}, b_{2n}) : n \in \mathbb{Z}_{\geq 0}\}$, $x^2 - dy^2 = 1$ 非负整数解为 $\{(a_{2n+1}, b_{2n+1}) : n \in \mathbb{Z}_{\geq 0}\}$, 从而得到全体解的表达形式.

Theorem 4 (解的递推关系). $x^2 - dy^2 = \pm 1$ 的所有正整数解 $\{(a_n, b_n) : n \in \mathbb{Z}_{\geq 1}\}$ 可以由基本单位 $\epsilon = a + b\sqrt{d}$ 按递推关系:

$$\begin{bmatrix} a_n \\ b_n \end{bmatrix} = \begin{bmatrix} a & bd \\ b & a \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

得到, 且序列 $\{a_n : n \in \mathbb{Z}_{>0}\}, \{b_n : n \in \mathbb{Z}_{>0}\}$ 均为严格单调递增的序列.

Proof: 注意到:

$$a_{n+1} + b_{n+1}\sqrt{d} = (a_n + b_n\sqrt{d})(a + b\sqrt{d}) = (aa_n + bdb_n) + (ba_n + ab_n)\sqrt{d}$$

从而

$$\begin{bmatrix} a_{n+1} \\ b_{n+1} \end{bmatrix} = \begin{bmatrix} a & bd \\ b & a \end{bmatrix} \begin{bmatrix} a_n \\ b_n \end{bmatrix} = \cdots = \begin{bmatrix} a & bd \\ b & a \end{bmatrix}^n \begin{bmatrix} a \\ b \end{bmatrix}$$

而序列的递增性可以由递推关系轻松得到, 因而一种求取 Pell 方程基本单位的计算方法是依次取 $y = 1, 2, \dots$ 直到 $x^2 - dy^2 = \pm 1$ 对 x 有解, 此时求出的 x 的正值解就得到了基本单位, 也顺便得到了基本单位的范数.

下面我们讨论 $d \equiv 1 \pmod{4}$ 时解的结构, 由于此时代数整数环里元素的范数并非与该形式 Pell 方程一一对应, 因此我们需要对命题进行一定转化.

考虑 $K = \mathbb{Q}(\sqrt{d})$ 的代数整数环

$$O_K = \left\{ k_1 + k_2 \frac{1 + \sqrt{d}}{2} : k_1, k_2 \in \mathbb{Z} \right\}$$

中的元素 $u = a + b \frac{1 + \sqrt{d}}{2}$, u 为单位等价于 $N_{K/\mathbb{Q}}(u) = \pm 1$ 也就是

$$(2a + b)^2 - db^2 = \pm 4$$

容易验证集合

$$A = \{(x, y) \in \mathbb{Z}^2 : (2x + y)^2 - dy^2 = 4\}$$

和集合

$$B = \{(x, y) \in \mathbb{Z}^2 : x^2 - dy^2 = 4\}$$

通过映射

$$\varphi : A \rightarrow B \quad (x, y) \rightarrow (2x + y, y) \quad (2)$$

建立一一对应. (单射显然, 双射只需 $(\bmod 4)$ 证明右边的解 (x, y) 同奇偶)

显然

$$C = \{(x, y) \in \mathbb{Z}^2 : (2x + y)^2 - dy^2 = -4\}$$

与

$$D = \{(x, y) \in \mathbb{Z}^2 : x^2 - dy^2 = -4\}$$

也有相同的对应关系.

现在设 $\epsilon = a + b\omega$ 为基本单位, 则由 (1) 能作为基本单位的只有 $\pm\epsilon^{-1}, \pm\epsilon$, 这四者中存在唯一一个 > 1 , 从而不妨设 $\epsilon = a + b\omega > 1, \epsilon^n = a_n + b_n\omega$.

当 $N_{K/\mathbb{Q}}(\epsilon) = 1$ 时, 方程 $(2x + y)^2 - dy^2 = 4$ 全部整数解为

$$\{(a_n, b_n) : n \in \mathbb{Z}\} \cup \{(-a_n, -b_n) : n \in \mathbb{Z}\} \quad (3)$$

方程 $(2x + y)^2 - dy^2 = -4$ 无整数解. 由 (2) 我们得到: $x^2 - dy^2 = -4$ 无整数解. 为了表示 $x^2 - dy^2 = 4$ 的正整数解, 我们引入一组新的序列

$$\{c_n = 2a_n + b_n : n \in \mathbb{Z}\}, \{d_n = b_n : n \in \mathbb{Z}\}$$

则 $x^2 - dy^2 = 4$ 的全体整数解可表示为

$$\{(c_n, d_n) : n \in \mathbb{Z}\} \cup \{(-c_n, -d_n) : n \in \mathbb{Z}\} \quad (4)$$

当 $N_{K/\mathbb{Q}}(\epsilon) = -1$ 时, 类比 Theorem 3 我们得到, 方程 $(2x + y)^2 - dy^2 = 4$ 全部整数解为:

$$\{(a_{2n}, b_{2n}) : n \in \mathbb{Z}\} \cup \{(-a_{2n}, -b_{2n}) : n \in \mathbb{Z}\} \quad (5)$$

方程 $(2x + y)^2 - dy^2 = -4$ 全部整数解为:

$$\{(a_{2n-1}, b_{2n-1}) : n \in \mathbb{Z}\} \cup \{(-a_{2n-1}, -b_{2n-1}) : n \in \mathbb{Z}\} \quad (6)$$

从而 $x^2 - dy^2 = 4$ 的全体整数解可表示为

$$\{(c_{2n}, d_{2n}) : n \in \mathbb{Z}\} \cup \{(-c_{2n}, -d_{2n}) : n \in \mathbb{Z}\} \quad (7)$$

$x^2 - dy^2 = -4$ 的全体整数解可表示为:

$$\{(c_{2n-1}, d_{2n-1}) : n \in \mathbb{Z}\} \cup \{(-c_{2n-1}, -d_{2n-1}) : n \in \mathbb{Z}\}$$

有了上述分析, 我们可以刻画 $x^2 - dy^2 = \pm 1$ 的解的结构了, 记 $m = c_1, n = d_1$, 则定理表述如下:

Theorem 5. 当 $N_{K/\mathbb{Q}}(\epsilon) = 1$ 时, Pell 方程 $x^2 - dy^2 = -1$ 无整数解, Pell 方程 $x^2 - dy^2 = 1$ 分下列两种情况,

1. 当 $m \equiv n \equiv 0(\text{mod } 2)$ 时, 全部整数解为

$$\left\{ \left(\frac{1}{2}c_n, \frac{1}{2}d_n \right) : n \in \mathbb{Z} \right\} \cup \left\{ \left(-\frac{1}{2}c_n, -\frac{1}{2}d_n \right) : n \in \mathbb{Z} \right\}$$

2. 当 $m \equiv n \equiv 1(\text{mod } 2)$ 时, 全部整数解为

$$\left\{ \left(\frac{1}{2}c_{3n}, \frac{1}{2}d_{3n} \right) : n \in \mathbb{Z} \right\} \cup \left\{ \left(-\frac{1}{2}c_{3n}, -\frac{1}{2}d_{3n} \right) : n \in \mathbb{Z} \right\}$$

当 $N_{K/\mathbb{Q}}(\epsilon) = -1$ 时, Pell 方程 $x^2 - dy^2 = -1$ 分下列两种情况讨论:

1. 当 $m \equiv n \equiv 0(\text{mod } 2)$ 时, 全部整数解为

$$\left\{ \left(\frac{1}{2}c_{2n+1}, \frac{1}{2}d_{2n+1} \right) : n \in \mathbb{Z} \right\} \cup \left\{ \left(-\frac{1}{2}c_{2n+1}, -\frac{1}{2}d_{2n+1} \right) : n \in \mathbb{Z} \right\}$$

2. 当 $m \equiv n \equiv 1(\text{mod } 2)$ 时, 全部整数解为

$$\left\{ \left(\frac{1}{2}c_{6n+3}, \frac{1}{2}d_{6n+3} \right) : n \in \mathbb{Z} \right\} \cup \left\{ \left(-\frac{1}{2}c_{6n+3}, -\frac{1}{2}d_{6n+3} \right) : n \in \mathbb{Z} \right\}$$

Pell 方程 $x^2 - dy^2 = 1$ 分下列两种情况讨论:

1. 当 $m \equiv n \equiv 0(\text{mod } 2)$ 时, 全部整数解为

$$\left\{ \left(\frac{1}{2}c_{2n}, \frac{1}{2}d_{2n} \right) : n \in \mathbb{Z} \right\} \cup \left\{ \left(-\frac{1}{2}c_{2n}, -\frac{1}{2}d_{2n} \right) : n \in \mathbb{Z} \right\}$$

2. 当 $m \equiv n \equiv 1(\text{mod } 2)$ 时, 全部整数解为

$$\left\{ \left(\frac{1}{2}c_{6n}, \frac{1}{2}d_{6n} \right) : n \in \mathbb{Z} \right\} \cup \left\{ \left(-\frac{1}{2}c_{6n}, -\frac{1}{2}d_{6n} \right) : n \in \mathbb{Z} \right\}$$

Proof: 显然这里方程的所有解就是前文分析的 $x^2 - dy^2 = \pm 4$ 解的两项皆为偶数的部分同时除以 2, 所以我们只需判断何时 $\{c_n : n \in \mathbb{Z}\}, \{d_n : n \in \mathbb{Z}\}$ 同为奇数, 何时同为偶数. 注意到:

$$\frac{c_{n+1} + d_{n+1}\sqrt{d}}{2} = a_{n+1} + b_{n+1}\frac{1 + \sqrt{d}}{2} = (a_n + b_n \frac{1 + \sqrt{d}}{2})(a + b \frac{1 + \sqrt{d}}{2}) = (\frac{c_n + d_n\sqrt{d}}{2})(\frac{m + n\sqrt{d}}{2})$$

从而:

$$\begin{bmatrix} c_{n+1} \\ d_{n+1} \end{bmatrix} = \begin{bmatrix} \frac{m}{2} & \frac{nd}{2} \\ \frac{n}{2} & \frac{m}{2} \end{bmatrix} \begin{bmatrix} c_n \\ d_n \end{bmatrix} \quad (8)$$

所有 $m \equiv n \equiv 0(\text{mod } 2)$ 的情况时平凡的, 因为由递推关系所有 $n \in \mathbb{Z}_{\geq 0}$ 的项皆同为偶数, 而且 $\forall n > 0$

$$\begin{aligned} \epsilon^{-n} &= a_{-n} + b_{-n}\omega = \frac{c_{-n} + d_{-n}\sqrt{d}}{2} \\ (\epsilon^n)^{-1} &= a_n + b_n\omega = \left(\frac{c_n + d_n\sqrt{d}}{2} \right)^{-1} = \pm \left(\frac{c_n - d_n\sqrt{d}}{2} \right) \end{aligned}$$

故正项与负项只差正负号, 因此 $\{c_n : n \in \mathbb{Z}\}, \{d_n : n \in \mathbb{Z}\}$ 皆为偶数. 因此我们只讨论 $m \equiv n \equiv 1(\bmod 2)$ 的情况, 首先当 $N_{K/\mathbb{Q}}(\epsilon) = 1$ 时, 根据 m, n 的定义:

$$m^2 - dn^2 = 4$$

按递推式 (8) 计算 $c_0, d_0, c_1, d_1, c_2, d_2, c_3, d_3$ 有:

$$\begin{aligned} c_{-1} &= m, d_{-1} = -n \\ c_0 &= 2, d_0 = 0 \\ c_1 &= m, d_1 = n \\ c_2 &= \frac{m^2 + dn^2}{2}, d_2 = mn \\ c_3 &= \frac{m^3 + 3mdn^2}{4}, d_3 = \frac{3m^2n + n^3d}{4} \end{aligned}$$

不难看出

$$\begin{aligned} c_{-1} \equiv d_{-1} &\equiv 1(\bmod 2), c_0 \equiv d_0 \equiv 0(\bmod 2), c_1 \equiv d_1 \equiv 1(\bmod 2) \\ c_2 \equiv d_2 &\equiv 1(\bmod 2), c_3 \equiv d_3 \equiv 0(\bmod 2) \end{aligned}$$

我们猜测奇偶性可以呈现出模 3 周期性, 只需证明下面两个引理, 这两个引理是对 [4] 中该讨论过程的补充:

Lemma 6. 任意 $k \in \mathbb{Z}, k \geq 2$, 有 $c_k - d_k \equiv c_{k-3} - d_{k-3}(\bmod 4)$

Lemma 7. 任意 $k \in \mathbb{Z}, k \geq 2$, 有 $c_k \equiv c_{k-3}(\bmod 2)$

$k = 2$ 时,

$$\frac{m^2 + dn^2}{2} - mn - m - n \equiv -(m+1)(n+1) \equiv 0(\bmod 4)$$

因此 $k = 2$ 成立, 又因为

$$c_3 - d_3 - 2 = \frac{m(4 + 4dn^2) + n(4m^2 - 4)}{4} - 2 \equiv 0(\bmod 4)$$

因此 $k = 3$ 时成立, 对 $k > 3$ 的情况, 我们同时对这两个引理进行归纳:

$$\begin{aligned} c_k - d_k &= \frac{m}{2}(c_{k-1} - d_{k-1}) + \frac{n}{2}(dd_{k-1} - c_{k-1}) \\ &= \frac{m}{2}(c_{k-1} - d_{k-1}) + \frac{n}{2}((4s+1)d_{k-1} - c_{k-1}) \\ &= 2nsd_{k-1} + \frac{m-n}{2}(c_{k-1} - d_{k-1}) \\ &\equiv 2nsd_{k-4} + \frac{m-n}{2}(c_{k-4} - d_{k-4}) \\ &\equiv c_{k-3} - d_{k-3}(\bmod 4) \end{aligned}$$

从而:

$$c_k = \frac{m}{2}c_{k-1} + \frac{nd}{2}d_{k-1} = \frac{m}{2}c_{k-4} + \frac{nd}{2}d_{k-4} + \frac{m}{2}(c_{k-1} - c_{k-4}) + \frac{nd}{2}(d_{k-1} - d_{k-4})$$

由归纳假设: $\frac{c_{k-1} - c_{k-4}}{2}, \frac{d_{k-1} - d_{k-4}}{2}$ 均为整数且同奇偶, 因此

$$c_k \equiv \frac{m}{2}c_{k-1} + \frac{nd}{2}d_{k-1} \equiv \frac{m}{2}c_{k-4} + \frac{nd}{2}d_{k-4} \equiv c_{k-3} \pmod{2}$$

由此判定了 $n \in \mathbb{Z}_{\geq -1}$ 的 c_n, d_n 奇偶的周期性, 由于正项负项只差正负号, 因此奇偶性不变, 从而通过中国剩余定理解出上述的方程的解的情况, 因此 $N_{K/\mathbb{Q}}(\epsilon) = 1$ 的情况证毕, 而 $N_{K/\mathbb{Q}}(\epsilon) = -1$ 的情况可完全类比上述证明. 不过事实上我们可以直接通过递推数列证明:

$$c_{n+2} = mc_{n+1} - c_n$$

从而上述结论在该递推数列 $(\bmod 2)$ 的意义下是平凡的.

2 基本单位的判定

本节我们总结几个常用的基本单位的判定.

Proposition 8. 1. $d \equiv 2, 3 \pmod{4}$ 时, 基本单位 $\epsilon = a + b\sqrt{d}$ 可以通过将 $y = 1, 2, \dots$ 依次代入 $dy^2 \pm 1$ 看其是否为完全平方数, 如果 $dy^2 - 1$ 为完全平方数 $x^2, x > 0$, 则此时基本单位为 $x + y\sqrt{d}$, 范数为 -1 , 如果 $dy^2 + 1$ 为完全平方数 $x^2, x > 0$, 则此时基本单位为 $x + y\sqrt{d}$, 范数为 1 .

2. $d \equiv 1 \pmod{4}$ 时, 且 $d \neq 5$, 基本单位 $\epsilon = a + b\omega = \frac{m + n\sqrt{d}}{2} > 1$, 可以依次用 $y = 1, 2, \dots$, 代入 $dy^2 \pm 4$ 看其是否为完全平方数, 如果 $dy^2 - 4$ 为完全平方数 $x^2, x > 0$, 则基本单位为 $\frac{x + y\sqrt{d}}{2}$, 范数为 -1 , 如果 $dy^2 + 4$ 为完全平方数 $x^2, x > 0$, 则基本单位为 $\frac{x + y\sqrt{d}}{2}$, 范数为 1 .

3. $d = 5$ 时, 基本单位为 $\frac{1 + \sqrt{5}}{2}$

Proof: 1 的证明已经在 Theorem 4 给出, 只证明 2, 3.

先证明 3, 由于 $\epsilon > 1$, 所以 ϵ 为 $\pm\epsilon^{-1}, \pm\epsilon$ 中最大者, 因此 $m > 0, n > 0$, 而 $\frac{1 + \sqrt{5}}{2} > 1$, 因此有 $\epsilon^k = \frac{1 + \sqrt{5}}{2}, k > 0$, 但是如果 $k > 1$, 则有

$$\frac{m + n\sqrt{d}}{2} = \epsilon < \epsilon^k = \frac{1 + \sqrt{5}}{2}$$

与 $m > 0, n > 0$ 矛盾, 因此 $k = 1$.

已经排除了第三种情况, 所以 $dy^2 + 4, dy^2 - 4$ 不能同时为完全平方数, 注意到 $x^2 - dy^2 = \pm 4$ 全体正整数解为 $\{(c_n, d_n) : n \in \mathbb{Z}_{>0}\}$, 因此只需证明递推公式 (8) 中表示的序列 d_n 是递增的, 如果 $m > 1$ 递增是显然的, $m = 1$ 时会回归到 2 情况, 证毕.

上面一个性质是具体计算的角度, 下面的性质都是理论的角度.

Proposition 9. 设 $p \equiv 1 \pmod{4}$ 为素数, 则 $\mathbb{Q}(\sqrt{p})$ 的基本单位的范数为 -1 .

Proof: 由 Theorem 5, 等价于证明 $x^2 - dy^2 = -1$ 有整数解. 反证法, 假设无整数解, 则基本单位范数为 1, 取 (x_0, y_0) 为 $x^2 - dy^2 = 1$ 的一组正整数解使得 x_0 最小, $(\text{mod } 4)$ 知 $x_0 \equiv 1(\text{mod } 2), y_0 \equiv 0(\text{mod } 2)$, 这组解为 $(\frac{1}{2}c_1, \frac{1}{2}d_1)$ 或 $(\frac{1}{2}c_3, \frac{1}{2}d_3)$, 则

$$x_0^2 - py_0^2 = 1 \Rightarrow py_0^2 = (x_0 - 1)(x_0 + 1) \Rightarrow p\left(\frac{y_0}{2}\right)^2 = \frac{x_0 - 1}{2} \frac{x_0 + 1}{2}$$

从而由 $x_1 > 0, x_2 > 0$

$$x_1^2 = \frac{x_0 - 1}{2}, px_2^2 = \frac{x_0 + 1}{2}$$

或者

$$x_1^2 = \frac{x_0 + 1}{2}, px_2^2 = \frac{x_0 - 1}{2}$$

不论是哪种情况通过左式减右式都会矛盾, 前者与方程无解矛盾, 后者与最小性矛盾.

Proposition 10. $d \equiv 3(\text{mod } 4)$ 且无平方因子, 则 $K = \mathbb{Q}(\sqrt{d})$ 基本单位范数为 1.

Proof: 由 Theorem 3, 等价于证明 $x^2 - dy^2 = -1$ 无整数解. 反证法, 假设有解, 则两边 $(\text{mod } 4)$ 得到矛盾.

Proposition 11. 设 $d = t^2 + 4$ 无平方因子, $t > 0$, 则 $\frac{t + \sqrt{d}}{2}$ 为实二次域 $\mathbb{Q}(\sqrt{d})$ 的基本单位.

Proof: $t = 1$ 时为 Proposition 8 的情况 3, $t > 1$ 时, 由 Proposition 8 的情况 2, 可知 $\frac{t + \sqrt{d}}{2}$ 为实二次域的基本单位, 且基本单位的范数为 -1 .

Proposition 12. 设 $d = t^2 - 4$ 无平方因子, $t \geq 5$, 则 $\frac{t + \sqrt{d}}{2}$ 为实二次域 $\mathbb{Q}(\sqrt{d})$ 的基本单位.

Proof: 由 Proposition 8 的情况 2, 可知 $\frac{t + \sqrt{d}}{2}$ 为实二次域的基本单位, 且基本单位的范数为 1.

3 广义 Pell 方程

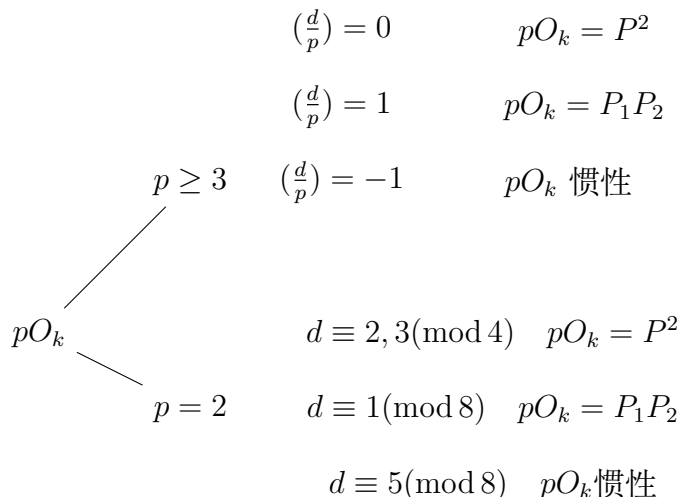
本小节将讨论广义 Pell 方程的部分情况, 即形如

$$x^2 - dy^2 = N$$

的不定方程, 其中 $d > 1$ 且无平方因子, N 为任意整数.

首先我们假设 $K = \mathbb{Q}(\sqrt{d}), d \equiv 2, 3(\text{mod } 4), d > 1$ 且无平方因子, 且类数 $h(K) = 1$, 即 K 的代数整数环 O_K 为主理想整环. 实二次域麻烦之处在于不定方程 $x^2 - dy^2 = N$ 不一定能和找到一个理想范数为 N 等价, 这不同于虚二次域, 原因是单位的范数有可能取到 -1 , 因此我们需要做一些特殊的处理.

一个代数数论中基本的结论是, 素数 p 生成的理想在 O_K 中分解如下图:



又因为如果理想 A 范数 N , 则 $N \in A$, 从而 $A|(N)$, 因此任何范数为 N 的理想一定是 N 生成的理想的因子, 根据上图, 将 N 在 \mathbb{Z} 上进行素因数分解后, 如果素因子在 O_k 上生成的理想惯性, 则必须取偶数个, 如果分裂为两个不同的理想, 则取法总数为要乘以对应素数的素因子幂次加 1, 如果素数分歧为两个相同理想, 只需将这些理想平分, 因此首先我们能求出所有范数 N 的理想.

先找到这些素理想的生成元, 所有生成元只差一个单位, 通过 N 的正负判断这个生成元该乘以范数为何的单位, 从而得到 $x^2 - dy^2 = N$ 的所有解. 但由于一个基本单位范数为 1 的二次域并不存在范数为 -1 的单位, 因此即使可以找到范数为 N 的理想, 我们也不一定能保证方程 $x^2 - dy^2 = N$ 有解, 但是 $x^2 - dy^2 = \pm N$ 的解通过上述手段是可以很轻松的求出的.

而对于 $d \equiv 1 \pmod{4}$, $h(K) = 1$ 的情况, 我们可以用上述方法求出不定方程

$$x^2 + xy + \frac{1-d}{4}y^2 = N$$

的所有解, 此时我们可以将这个不定方程像前面一样和 $x^2 - dy^2 = 4N$ 的解一一对应起来, 此时 $x^2 - dy^2 = N$ 的解正是将 $x^2 - dy^2 = 4N$ 所有两项均为偶数的解摘出来除以 2, 此时的周期性具体计算时可以归结为二阶线性递推数列本身的周期性, 这个命题将被总结在本文的最后, 利用该方法我们可以从理论上获得 d 有平凡因子时 Pell 方程的全部解.

4 例题分析

Exercise 13 (第十四届 CMC 数学 A 第三题). 设 $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, B 与 A 可交换, 且元素均为正整数且行列式为 1, 求证存在 $k \in \mathbb{Z}_{>0}$ 使得 $B = A^k$

Proof: 设 $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, A, B 可交换知:

$$b = c, d = a - b$$

结合题中所给 $\det B = 1$, 所以我们只要求出 $a^2 - ab - b^2 = 1$ 的正整数解, 并刻画出递推关系即可解决该题.

先求其所有整数解, 这等价于求 $(2a - b)^2 - 5b^2 = 4$ 的整数解, 考虑式 (5), 整数解即为

$$\{(a_{2n}, -b_{2n}) : n \in \mathbb{Z}\} \cup \{(-a_{2n}, b_{2n}) : n \in \mathbb{Z}\}$$

注意到 $\mathbb{Q}(\sqrt{5})$ 的基本单位为 $\frac{1+\sqrt{5}}{2}$, 且

$$a_{n+1} + b_{n+1}\omega = (a_n + b_n\omega)(a + b\omega) = aa_n + b\frac{d-1}{4}b_n + (bb_n + ab_n + ba_n)\omega$$

从而

$$\begin{bmatrix} a_{n+1} \\ b_{n+1} \end{bmatrix} = \begin{bmatrix} a & b\frac{d-1}{4} \\ b & a+b \end{bmatrix} \begin{bmatrix} a_n \\ b_n \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a_n \\ b_n \end{bmatrix}$$

从而

$$\begin{bmatrix} a_{2n+2} \\ -b_{2n+2} \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} a_{2n} \\ -b_{2n} \end{bmatrix} \quad n \in \mathbb{Z}$$

其中 $a_0 = 1, -b_0 = 0$, 现在我们只需求出这两个序列中均为正整数或者均为负整数的部分, 注意到 $\begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, 我们列出 $a_{2n}, -b_{2n}$ 前几项并进行简单的归纳, 我们可以得到所有正整数解为:

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad n \in \mathbb{Z}_{>0}$$

从而存在 $k \in \mathbb{Z}_{>0}$ 使得

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}^k \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

由于 A^k 为对称矩阵, 所以

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}^k = \begin{bmatrix} a & b \\ b & q \end{bmatrix} = \begin{bmatrix} a & b \\ b & a-b \end{bmatrix} = B$$

倒数第二个等号是因为 $\det A^k = 1$ 且 $a^2 - ab - b^2 = 1$

Exercise 14. 求所有三边长为连续自然数的三角形, 其面积为正整数.

Proof: (本题源于: <https://www.zhihu.com/question/415377792>)

设三边长分别为 $n-1, n, n+1$, 其面积由海伦公式为

$$m = \frac{\sqrt{3n(n-2)(n+2)}}{4}$$

所以只需求不定方程

$$16m^2 = 3(n-2)(n+2)n^2$$

的正整数解.

注意到 $n \equiv 0 \pmod{2}$, 设 $n = 2x$, 则原方程化为

$$3(x-1)(x+1)x^2 = m^2$$

注意到 $x^2 | m^2$, 令 $m = xk$ 有

$$3(x-1)(x+1) = k^2$$

注意到 $3 | k$ 再令 $k = 3t$ 得到

$$3(x-1)(x+1) = 9t^2$$

即 $x^2 - 3t^2 = 1$, 由 Theorem 4, 所有正整数解可以表示为:

$$\begin{bmatrix} x \\ t \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad n \in \mathbb{Z}_{>0}$$

从而原方程的解为 $(3xt, 2x)$

Exercise 15. 求 $5^a - 3^b = 2$ 的所有正整数解 (a, b) .

Proof: 注意到 $(a, b) = (1, 1)$ 是一组解, 下面证明 a, b 都大于 1 时该方程无解.

反证法, 假设有解 (a, b) , 分别 $(\bmod 3), (\bmod 4)$ 知 a, b 均为奇数, 一个很难注意到的等式是

$$15(3^{\frac{b-1}{2}} 5^{\frac{a-1}{2}})^2 = (3^b + 1)^2 - 1$$

考虑 Pell 方程 $x^2 - 15y^2 = 1$, 其所有正整数解由 Theorem 4 可表示为

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 4 & 15 \\ 1 & 4 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad n \in \mathbb{Z}_{>0}$$

只需证明 y_n 中的素因子不能只出现 3, 5, 由递推式 $(\bmod 3)$ 知:

$$y_{n+1} \equiv y_n + 1 (\bmod 3)$$

从而 $3|y_n \Leftrightarrow 3|n$, 另一方面由于

$$y_{n+1} = x_n + 4y_n = 4x_{n-1} + 15y_{n-1} + 4y_n = 4y_n - 16y_{n-1} + 15y_{n-1} + 4y_n = 8y_n - y_{n-1}$$

将递推式 $(\bmod 7)$ 知

$$y_{n+1} \equiv y_n - y_{n-1} (\bmod 7)$$

因为 $y_1 \equiv y_2 \equiv 1 (\bmod 7)$, 所以 $7|y_n \Leftrightarrow 3|n$, 因此 $3|n \Leftrightarrow 21|y_n$, 这说明 y_n 的素因子不能只出现 3, 5.

上述证明过程中线性递推数列呈现出的周期性并非偶然, 事实上我们有如下定理:

Remark 16. 考虑初值:

$$x_1, x_2, \dots, x_k$$

均给定且为整数的递推数列:

$$x_{n+k} = a_1 x_n + a_2 x_{n+1} + \dots + a_k x_{n+k-1}$$

其中 a_i 也均为整数, 则对任意 m 为正整数, x_n 在 $(\bmod m)$ 下取值呈周期性.

Proof: 考虑数列 u_n 满足下列条件:

1. $1 \leq u_n \leq m$
2. $u_n \equiv x_n (\bmod m)$

易知这样的 u_n 存在且唯一, 再考虑:

$$U_i = (u_{1+i}, u_{2+i}, \dots, u_{k+i}) \in \mathbb{Z}^k, i = 0, \dots, m^k$$

由抽屉原理必有 s, t 使得 $U_s = U_t$, 从而有:

$$x_{s+1} \equiv x_{t+1} (\bmod m), x_{s+2} \equiv x_{t+2} (\bmod m), \dots, x_{s+k} \equiv x_{t+k} (\bmod m)$$

从而 $s - t$ 是该数列 $\bmod m$ 的一个周期.

参考文献

- [1] Michael Rosen Kenneth Ireland. *A Classical Introduction to Modern Number Theory*. Springer, 1990.
- [2] Fernando Q.Gouvea. *p-adic Numbers An Introduction*. Springer, 1997.
- [3] Serre. *A Course in Arithmetic*. Springer-Verlag, 1973.
- [4] 冯克勤. 代数数论. 哈尔滨工业大学出版社, 2018.