浅谈 Pell 方程

尔濯

2023 年 5 月 3 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

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在 U_k 中找到 $r = r_1 + r_2 - 1$ 个元素 $u_1, u_2, \ldots, u_r$，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 $\{u_1, \ldots, u_r\}$ 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

$$O_k = \begin{cases} k_1 + k_2\sqrt{d} & k_1, k_2 \in \mathbb{Z} \quad \text{当} d \equiv 2, 3 (\mathrm{mod}\, 4) \\ k_1 + k_2\dfrac{1+\sqrt{d}}{2} & k_1, k_2 \in \mathbb{Z} \quad \text{当} d \equiv 1 (\mathrm{mod}\, 4) \end{cases}$$

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

$$U_k = \{\pm\epsilon^n : n \in \mathbb{Z}\} \tag{1}$$

其中

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

而对于 $d \equiv 2, 3 (\mathrm{mod}\, 4)$ 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 $d \equiv 2, 3 (\mathrm{mod}\, 4)$ 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，$d\equiv 2,3(mod 4), \epsilon=a+b\sqrt{d}$ 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) 刻画的单位群 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 $y=1,2,\ldots$ 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 $d\equiv 1(\mathrm{mod}\,4)$ 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 $u=a+b\dfrac{1+\sqrt{d}}{2}$,$u$ 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

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

和集合

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

通过映射

$$\varphi : A \to B \quad (x,y) \to (2x+y, y) \tag{2}$$

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

显然

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

与

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

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

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

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

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

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：

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

方程 $(2x+y)^2 - dy^2 = -4$ 全部整数解为：

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

从而 $x^2 - dy^2 = 4$ 的全体整数解可表示为

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

$x^2 - dy^2 = -4$ 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，我么可以刻画 $x^2 - dy^2 = \pm 1$ 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 $m \equiv n \equiv 0(mod 2)$ 时，全部整数解为

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

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

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

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 $m \equiv n \equiv 0(mod 2)$ 时，全部整数解为

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

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

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

Pell 方程 $x^2 - dy^2 = 1$ 分下列两种情况讨论:

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

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

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

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

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:

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

所有 $m \equiv n \equiv 0(\mathrm{mod}\, 2)$ 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 $\forall n > 0$

$$\epsilon^{-n} = a_{-n} + b_{-n}\omega = \frac{c_{-n} + d_{-n}\sqrt{d}}{2}$$

$$(\epsilon^n)^{-1} = a_n + b_n\omega = (\frac{c_n + d_n\sqrt{d}}{2})^{-1} = \pm(\frac{c_n - d_n\sqrt{d}}{2})$$

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 $m \equiv n \equiv 1(\mathrm{mod}\, 2)$ 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：

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

不难看出

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

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 $c_k - d_k \equiv c_{k-3} - d_{k-3}(mod\, 4)$*

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

$k = 2$ 时，

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

因此 $k = 2$ 成立，又因为

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

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：

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

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

$$c_k \equiv \frac{m}{2}c_{k-1} + \frac{nd}{2}d_{k-1} \equiv \frac{m}{2}c_{k-4} + \frac{nd}{2}d_{k-4} \equiv c_{k-3} (\mathrm{mod}\, 2)$$

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 $(\mathrm{mod}\, 2)$ 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.* $d \equiv 2, 3 (mod 4)$ 时，基本单位 $\epsilon = a + b\sqrt{d}$ 可以通过将 $y = 1, 2, \ldots$ 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. $d \equiv 1 (mod 4)$ 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 $y = 1, 2 \ldots$, 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 $p \equiv 1 (mod 4)$ 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，$(\mathrm{mod}\, 4)$ 知 $x_0 \equiv 1(\mathrm{mod}\, 2), y_0 \equiv 0(\mathrm{mod}\, 2)$, 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

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

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. *$d \equiv 3(mod 4)$ 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 $(\mathrm{mod}\, 4)$ 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

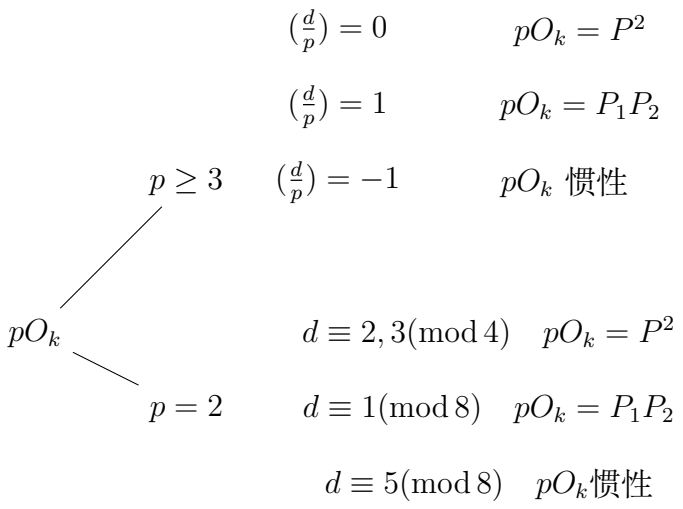
本小节将讨论广义 Pell 方程的部分情况，即形如

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

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 $K = \mathbb{Q}(\sqrt{d}), d \equiv 2, 3(\mathrm{mod}\, 4), d > 1$ 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 $d\equiv 1(\mathrm{mod}\,4), h(K)=1$ 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 $\det B=1$, 所以我们只需要求出 $a^2-ab-b^2=1$ 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 $\dfrac{1+\sqrt{5}}{2}$, 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

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

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 $n\equiv 0(\mathrm{mod}\,2)$，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:*

$$x_1,x_2,\ldots,x_k$$

均给定且为整数的递推数列:

$$x_{n+k}=a_1x_n+a_2x_{n+1}+\cdots+a_kx_{n+k-1}$$

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

Proof: 考虑数列 u_n 满足下列条件:

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

易知这样的 u_n 存在且唯一，再考虑:

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

由抽屉原理必有 s,t 使得 $U_s=U_t$，从而有:

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

从而 $s-t$ 是该数列 $modm$ 的一个周期.

Exercise 17. 方程

$$x^4 - 2y^2 = 17$$

在 $\mathbb{Q}$ 上无解，但在所有 $\mathbb{Q}_p$ 其中 $p \leq \infty$ 上有解.

Proof: 在 $\mathbb{R} = \mathbb{Q}_\infty$ 上该方程有解显然，考虑在 $\mathbb{Q}_2$ 上方程的解.

Lemma 18 (Hensel,[2])**.** 考虑多项式 $f(x) \in \mathbb{Z}_p[x]$ 和 p 进整数 α_1 满足:

$$|f(\alpha_1)|_p < |f^{'}(\alpha_1)|_p^2$$

则存在 $\alpha \in \mathbb{Z}_p$ 和正整数 n 使得

$$\alpha_1 \equiv \alpha (mod p^n \mathbb{Z}_p)$$

且满足 $f(\alpha) = 0$.

根据引理，我们考虑 $f(x) = x^4 - 17 \in \mathbb{Z}_2[x]$ 和 $\alpha_1 = 3$, 容易验证 α_1 满足引理所需条件，从而有 $\alpha \in \mathbb{Z}_p$ 使得 $f(\alpha) = 0$，因此 $x = \alpha, y = 0$ 是原方程在 $\mathbb{Q}_2$ 上的解.

再考虑 $\mathbb{Q}_p$ 其中 p 为奇素数，分两种情况讨论，当 $(\frac{2}{p}) = 1$ 时，不难证明有 x_0 使得:

$$x_0^2 \equiv 32 (\mathrm{mod}\, p)$$

从而得到 $\alpha \in \mathbb{Z}_p$ 使得 $\alpha^2 - 32 = 0$，从而 $x = 3, y = \alpha$ 为 $\mathbb{Q}_p$ 的上方程的解. 当 $(\frac{-2}{p}) = 1$ 时，不难证明有 y_0 使得:

$$2y_0^2 \equiv -1 (\mathrm{mod}\, p)$$

从而得到 $\beta \in \mathbb{Z}_p$ 使得 $2\beta^2 + 1 = 0$，从而 $x = 2, y = \beta$ 为 $\mathbb{Q}_p$ 的上方程的解. 综合上面两种情况，我们证明了 $p \equiv 3 (\mathrm{mod}\, 4)$ 时局部解一定存在，当 $p \equiv 1 (\mathrm{mod}\, 4)$ 时，$(\frac{-1}{p}) = 1$(不难看出 $p = 17 = 2 \times 8 + 1$ 也属于上面两种情况，因此我们后续不讨论 $p = 17$ 的情况), 从而有

$$y_0^2 \equiv -1 (\mathrm{mod}\, p)$$

如果我们能证明方程

$$x^4 - 17z^4 = -2 (\mathrm{mod}\, p)$$

有解 (x_0, z_0), 此时如果 $z_0 \equiv 0 (\mathrm{mod}\, p)$ 则回到前面的情况，因此我们取 $(x_1, y_1) = (\frac{x_0}{z_0}, \frac{y_0}{z_0^2})$(除法按取逆元理解)，得到了:

$$x_1^4 - 17 = y_1^2 (\mathrm{mod}\, p)$$

不难验证此时 $p \nmid y_1^2$，因此由 Hensel 引理得到一个局部解. 因此对于局部解的情况最终只需证明

$$x^4 - 17z^4 = -2 (\mathrm{mod}\, p)$$

有解，这需要一些雅可比和相关的知识.

我们称有限域乘法群 $\mathbb{F}_p^*$ 到 $\mathbb{C}^*$ 的同态 χ 为一个特征标, 平凡的特征标称为主特征，一般记作 ε, 非主特征补充在 0 处的定义为 0，主特征补充为 1.

Proposition 19. 当素数 $p \nmid a$ 时，方程 $x^n - a \equiv 0 (mod p)$ 的解数为

$$\sum_{\chi^n = \varepsilon} \chi(a)$$

当素数 $p | a$ 时，方程 $x^n - a \equiv 0 (mod p)$ 的解数为 1.

Proof: 后者显然，前者只需考虑特征标的生成元, 计算得到两者均为 $(n, p-1)$.

Proposition 20. 定义雅克比和为

$$J(\chi,\lambda)=\sum_{a+b=1}\chi(a)\lambda(b)\quad a,b\in\mathbb{F}_p$$

1. χ 为非主特征，则 $J(\chi,\chi^{-1})=-\chi(-1)$
2. $J(\varepsilon,\varepsilon)=p$
3. $J(\varepsilon,\chi)=0,\chi\neq\varepsilon$
4. $|J(\lambda,\chi)|=\sqrt{p},\lambda,\chi,\lambda\chi\neq\varepsilon$

Proof: 详见 [1, page93]

记 $(\mathrm{mod}\,p)$ 的所有四次特征为 $\varepsilon,\chi_i,i=1,2,3$,$N()$ 表示该方程解数, 则由上述两条性质我们得知

$$x^4-17y^4=-2(\mathrm{mod}\,p)$$

的解数为

$$\begin{aligned}&\sum_{a-17b\equiv-2(\mathrm{mod}\,p)}N(x^4=a)N(y^4=b)\\=&\sum_{a-17b\equiv-2(\mathrm{mod}\,p)}(\varepsilon+\chi_1+\chi_2+\chi_3)(a)(\varepsilon+\chi_1+\chi_2+\chi_3)(b)\\=&\sum_{a+b\equiv1(\mathrm{mod}\,p)}(\varepsilon+\chi_1+\chi_2+\chi_3)(\frac{a}{-2})(\varepsilon+\chi_1+\chi_2+\chi_3)(\frac{b}{-34})\\\geq&p-3-6\sqrt{p}\end{aligned}$$

考虑所有形如 $8k+5$ 的素数，当 $p\geq53$ 时,$p-3-6\sqrt{p}>0$，因此只需证明 $p=5,13,29,37$ 的情况, 但此时只需在方程

$$x^4-2y^2=17$$

中考虑，我们通过 C++ 简单计算知这四种情况均成立.

因此我们证明了局部解的存在性，下面证明全局解不存在.

如果该方程在 $\mathbb{Q}$ 上有解，显然我们能得到方程 $x^4-17z^4=2y^2$ 的一组整数解，因此我们只需证明方程

$$x^4-17z^4=2y^2$$

无整数解，反证法，假设有整数解 $(x,y,z)=(a,b,c)$ 不妨设 a,c 互素，且均为奇数.

Lemma 21. 实二次域 $K=\mathbb{Q}(\sqrt{17})$ 类数为 1.

Proof: 注意到 K 的 Minkowski 常数为 $\dfrac{\sqrt{17}}{2}<3$，所以 K 的理想类群可以由

$$2\mathcal{O}_K=P_1P_2$$

中的 $[P_1],[P_2]$ 生成, 又因为 $[P_2]=[P_1]^{-1}$，所以理想类群平凡，即类数为 1.

根据 (8) 我们知道 K 基本单位为 $\epsilon = 4+\sqrt{17}$ 且范数为 -1，注意到

$$\frac{a^2-c^2\sqrt{17}}{2}\frac{a^2+c^2\sqrt{17}}{2} = 2(\frac{b}{2})^2$$

我们想证明 $s = \dfrac{a^2-c^2\sqrt{17}}{2}, t = \dfrac{a^2+c^2\sqrt{17}}{2}$ 两者互素，只需证明他们生成的理想为 (1)，首先显然有 $a^2 \in (s,t), 17c^2 \in (s,t)$ 由因为 $(a,c)=1$ 所以不难证明 $(a^2, 17c^2)=1$，从而 s,t 互素, 由代数整数环的唯一分解性和 $N_{K/\mathbb{Q}}(t) = 2(\dfrac{b}{2})^2$ 得到

$$t = \frac{a^2+c^2\sqrt{17}}{2} = \frac{5\pm\sqrt{17}}{2}u\mu^2$$

其中 u 为单位,$\mu \in \mathcal{O}_K$. 注意到无论那种情况，左边作用 $\mathrm{Gal}(K/\mathbb{Q})$ 的元素不改变正负，因此右边也不改变正负, 从而单位 $u = \epsilon^{2n}$，我们不妨将两项合并起来有

$$\frac{a^2+c^2\sqrt{17}}{2} = \frac{5\pm\sqrt{17}}{2}\mu^2 = \frac{5\pm\sqrt{17}}{2}(\frac{\alpha+\beta\sqrt{17}}{2})^2$$

其中 $\alpha \equiv \beta (\mathrm{mod}\, 2)$，从而由线性无关性进行比较系数得到

$$4a^2 = 5(\alpha^2+17\beta) \pm 34\alpha\beta$$

$(\mathrm{mod}\, 17)$ 得到矛盾，证毕.

Exercise 22 (三元有理系数二次型)**.** *设 a,b,c 是三个两两互素且无平凡因子的整数，不定方程*

$$ax^2+by^2+cz^2 = 0$$

在 $\mathbb{Q}$ 有非平凡解 (指的 $xyz \neq 0$ 的解) 当且仅当其系数 a,b,c 满足下列四个条件:

1. *a,b,c 不能均为非负或者非正.*
2. *对于奇素数 $p|a$，有 $(\dfrac{-bc}{p}) = 1$，与之对称的两个条件也满足.*
3. *若 a,b,c 均为奇数，则有其中两者之和 $\equiv 0 (mod 4)$*
4. *如果其中有一个为偶数 (不妨设为 a)，则 $8|b+c$ 或 $8|a+b+c$*

Proof: 事实上任意三元有理系数二次型有无非平凡解的判断都可以通过初等的手段转化为系数无平方因子且两两互素的情况.

Lemma 23 (Hasse-Minkowski)**.**

$$F(x_1,x_2,\ldots,x_n) \in \mathbb{Q}[x_1,x_2,\ldots,x_n]$$

为一个有理系数二次型，方程

$$F(x_1,x_2,\ldots,x_n) = 0$$

在 $\mathbb{Q}$ 上有非平凡解当且仅当其在所有 $\mathbb{Q}_p$(其中 $p \leq \infty$) 上有非平凡解.

Proof: 详见 [3]

因此原命题等价于探索对所有 $\mathbb{Q}_p$ 原方程有非平凡解的充要条件，我们先证明对奇素数 $p \nmid abc$ 原方程在 $\mathbb{Q}_p$ 上有解. 我们先证明方程

$$ax^2 + by^2 + cz^2 \equiv 0 (\mathrm{mod}\, p)$$

一定有解.

Lemma 24. 定义

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \sum_{t_1 + \cdots + t_l = 0} \chi_1(t_1)\chi_2(t_2)\ldots\chi_l(t_l)$$

有以下性质：

1. $J_0(\epsilon, \epsilon, \ldots, \epsilon) = p^{l-1}$
2. $J_0(\chi_1, \chi_2, \ldots, \chi_l) = 0$, 当 $\chi_1, \ldots, \chi_l$ 中存在平凡特征但不全为平凡特征.
3. $J_0(\chi_1, \chi_2, \ldots, \chi_l) = 0$, 当 $\chi_1, \ldots, \chi_l$ 全为非平凡特征，且它们乘积为非平凡特征.
4. $|J_0(\chi_1, \chi_2, \ldots, \chi_l)| = (p-1)p^{\frac{l-2}{2}}$, 当 $\chi_1, \ldots, \chi_l$ 全为非平凡特征，且它们乘积为平凡特征.

Proof: 详见 [1, page93]

从而方程解数为

$$\begin{aligned}
&\sum_{au+bv+cw \equiv 0 (\mathrm{mod}\, p)} N(x^2 = u)N(x^2 = v)N(x^2 = w) \\
=&\sum_{au+bv+cw \equiv 0 (\mathrm{mod}\, p)} (1 + (\frac{u}{p}))(1 + (\frac{v}{p}))(1 + (\frac{w}{p})) \\
=&\sum_{u+v+w \equiv 0 (\mathrm{mod}\, p)} (1 + (\frac{a^{-1}u}{p}))(1 + (\frac{b^{-1}v}{p}))(1 + (\frac{c^{-1}w}{p})) \\
=&p^2
\end{aligned}$$

因此一定存在一组非平凡的解 (x_0, y_0, z_0)，不妨设其中 $p \nmid x_0$，再对多项式

$$f(x) = ax^2 + (by_0^2 + cz_0^2)$$

用 Hensel 引理即可得到 $\mathbb{Q}_p$ 上的一个解, 我们接下来处理 $p = 2$ 的情况, 这需要一个引理.

Lemma 25. $b \in \mathbb{Z}_2^\times$ 为平方元当且仅当 $b \equiv 1 (mod\, 8\mathbb{Z}_2)$.

Proof: 详见 [2, page73]

当 a, b, c 全为奇数时，假如

$$ax^2 + by^2 + cz^2 = 0$$

在 $\mathbb{Q}_2$ 上有非平凡解 (x_0, y_0, z_0)，不妨设 $\max\{|x_0|_2, |y_0|_2, |z_0|_2\} = 1$，否则两边同时乘以 2 的幂进行调整，$(\mathrm{mod}\, 2\mathbb{Z}_2)$ 知 x_0, y_0, z_0 中恰有两个为 $\mathbb{Z}_2^\times$ 中单位，不妨设为 y_0, z_0 从而由 Lemma 25 并 $(\mathrm{mod}\, 4\mathbb{Z}_2)$ 知

$$b + c \equiv 0 (\mathrm{mod}\, 4)$$

反之，如果系数 a,b,c 满足均为奇数且

$$b+c\equiv 0(\mathrm{mod}\,4)$$

我们想构造一组非平凡的解, 令 $y^2=1+8k_1, z^2=1+8k_2, k_1,k_2\in\mathbb{Z}_2$ 则有 $b+c+8(k_1b+k_2c)=-ax^2$ 当 $b+c\equiv 0(\mathrm{mod}\,8)$ 时，可取 k_1,k_2 使得 $b+c+8(k_1b+k_2c)=-16a$, 则 $x=4$ 为解，当 $b+c\equiv 4(\mathrm{mod}\,8)$ 时，可取 k_1,k_2 使得 $b+c+8(k_1b+k_2c)=-4a$, 则 $x=2$ 为解，从而当系数全为奇数时，$\mathbb{Q}_2$ 上有非平凡解充要条件是两者之和 $\equiv 0(\mathrm{mod}\,4)$.

下面讨论 $\mathbb{Q}_2$ 上有一个系数为偶数的情况,不妨设 a 为偶数,若 $\mathbb{Q}_2$ 上有非平凡解 (x_0,y_0,z_0), 通过和上面类似的思路可知只有三者均为单位或者只有 x_0 不是单位两者情况,分别 $(\mathrm{mod}\,8\mathbb{Z}_2)$ 知 $8|a+b+c$ 或 $8|b+c$, 另一方面要找非平凡解按照系数都为奇数时的情况操作即可.

最后是 $p|a$ 时 $\mathbb{Q}_p$ 的情况,

$$ax^2+by^2+cz^2=0$$

在 $\mathbb{Q}_p$ 上有非平凡解 (x_0,y_0,z_0), 不妨设 $\max\{|x_0|_p,|y_0|_p,|z_0|_p\}=1$，否则两边同时乘以 2 的幂进行调整, 分类讨论知 y_0,z_0 此时均为 $\mathbb{Z}_p^\times$ 中单位，从而有 $p\nmid y_1,z_1\in\mathbb{Z}$ 使得

$$by_1^2\equiv -cz_1^2(\mathrm{mod}\,p)$$

因此有 $(\dfrac{-bc}{p})=1$. 另一方面要证明这个条件是充要的，由于 $(\dfrac{-bc}{p})=1$，从而有

$$by_1^2\equiv -c(\mathrm{mod}\,p)$$

考虑多项式 $f(y)=by^2+c$，由 Hensel 引理存在 $y_2\equiv y_1(\mathrm{mod}\,p)$ 使得 $f(y_2)=0$, 从而 $(0,y_2,1)$ 是一组非平凡解, 综合上面所有情况，原命题得证.

Exercise 26. *对任意正整数 $M>0$，存在 $N>0$，使得任意 $n\geq N$ 有*

$$v_2(2+\frac{2^2}{2}+\frac{2^3}{3}+\cdots+\frac{2^n}{n})\geq M$$

其中 $v_2(n)$ 表示有理数 n 写成既约分数后分子 2 的幂次减去分母 2 的幂次.

Proof: 这看上去是一个初等数论问题, 实际上要用 p 进幂级数的方法来解决. 我们在 $\mathbb{Q}_p$ 上定义幂级数

$$\log_p(1+x)=\sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$$

如果我们证明了 $p=2$ 时该幂级数在 $x=-2$ 处收敛于 0 即可得到该命题. 首先我们记该幂级数收敛半径为 ρ，则收敛半径满足

$$f(x)=\frac{1}{\rho}=\limsup\sqrt[n]{\left|\frac{1}{n}\right|_p}=1$$

且 $|x|_p=1$ 时候，由于 $\left|\dfrac{1}{n}\right|_p$ 不趋于 0, 因此该幂级数收敛范围为 $|x|_p<1$，即为 $p\mathbb{Z}_p$. 如果我们证明了对于 $a,b\in 1+p\mathbb{Z}_p$,

$$\log_p(a)+\log_p(b)=\log_p(ab)$$

则取 $p=2, a=b=-1$ 即可证明原命题. 首先我们对该幂级数求导得到

$$f'(x)=\sum_{n=1}^{\infty}(-1)^{n-1}x^{n-1}=\frac{1}{x+1}$$

其次我们取定 $y\in p\mathbb{Z}_p$，定义

$$g(x)=f(y+(1+y)x)$$

由于 $|y+(1+y)x|_p<1\Longleftrightarrow|x|_p<1$, 因此 f,g 有相同的收敛范围，由 [2, Proposition 4.4.2], g 可以在 0 处展开为幂级数，由链式求导法则

$$g'(x)=(1+y)\frac{1}{1+(y+(1+y)x)}=\frac{1}{1+x}$$

由 [2, Corollary 4.4.5],f 和 g 只差常数，取 $x=0$ 知

$$g(0)=c+f(0)$$

则常数 $c=f(y)$，从而有

$$\log_p(a+1)+\log_p(b+1)=\log_p((a+1)(b+1))$$

进行一次变量替换即可得证.

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.