Pell 方程

前置知识：连分数、二次域

引入

本文讨论（广义）Pell 方程的求解。广义 Pell 方程是指关于 x 和 y 的不定方程

$$x^2 - Dy^2 = N,$$

其中，D 是正整数且不是完全平方数[1]，N 是非零整数。狭义的 Pell 方程特指 $N = 1$ 或 $N = \pm 1$ 的特殊情形，有时也包括 $N = \pm 4$ 的情形。广义 Pell 方程与在实二次整数环内寻找范数为 N 的二次整数紧密相关，而常常称作（狭义）Pell 方程的这些情形可以看作是寻找实二次整数环内的单位数。

当本文提及 Pell 方程时，特指 $N = 1$ 的情形。相应地，$N = -1$ 的情形称为负 Pell 方程[2]（negative Pell's equation）。

解的结构

广义 Pell 方程的整数解 (x, y) 和二次整数 $x + y\sqrt{D}$ 联系密切，因此文献中 Pell 方程的解常常写作 $x + y\sqrt{D}$ 的形式。因为二次整数的范数

$$N(x + y\sqrt{D}) = x^2 - Dy^2,$$

所以，广义 Pell 方程大致相当于在求解范数为 N 的二次整数。但是，两者确实有细微的区别。当 x 和 y 都是整数时，$x + y\sqrt{D}$ 一定是二次整数；反过来，二次整数未必要求 x 和 y 都是整数——在 $D \equiv 1 \pmod 4$ 的情形，x 和 y 还可以同时是半整数[3]。

这个区别在求解基本单位数时格外重要。因为二次整环中的单位数是指范数为 ± 1 的二次整数。对于 $D \equiv 2, 3 \pmod 4$，要找到这样的单位数，只需要求解广义 Pell 方程在 $N = \pm 1$ 的情形即可；但是对于 $D \equiv 1 \pmod 4$，还需要考虑 $N = \pm 4$ 的情形。下文 会讨论单位数的求解方法。

要理解广义 Pell 方程解的结构，需要从 Brahmagupta 恒等式 入手：

$$(x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = (x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2.$$

它相当于二次整数的范数保持乘法，即

$$\begin{aligned} N\left(x_1 + y_1\sqrt{D}\right) N\left(x_2 + y_2\sqrt{D}\right) &= N\left((x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D})\right) \\ &= N\left((x_1x_2 + Dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{D}\right). \end{aligned}$$

利用这一恒等式，可以利用方程 $x^2 - Dy^2 = N_1$ 和方程 $x^2 - Dy^2 = N_2$ 的整数解复合出方程 $x^2 - Dy^2 = N_1N_2$ 的整数解。当然，从二次整数的角度看，解的复合就是二次整数的乘法，这就体现了将 Pell 方程的解记作二次整数形式的方便之处。特别地，取 $N_1 = N$ 和 $N_2 = 1$ 就可以发现，如果已知 $x^2 - Dy^2 = N$ 的一组解和相应的 Pell 方程 $x^2 - Dy^2 = 1$ 的全体解，就可以得到 $x^2 - Dy^2 = N$ 更多的解。当然，这种方法未必能够生成全部的解。但是，这至少说明理解 Pell 方程的解的结构对理解广义 Pell 方程的解的结构有重要作用。

Pell 方程

方程 $x^2 - Dy^2 = 1$ 的几何意义是实轴在 x 轴、虚轴在 y 轴的双曲线。双曲线上的每个点都唯一对应了 $x + y\sqrt{D}$ 的一个非零取值：双曲线的左支对应着 $x + y\sqrt{D}$ 的负值，右支则对应正值。而且，在每一支上，双曲线自下而上对应的 $x + y\sqrt{D}$ 的取值是严格递增的。二次整数的取值给 Pell 方程的解赋予了自然的顺序。

双曲线同时关于 x 轴和 y 轴对称，因此讨论 Pell 方程的解只需要考虑在第一象限内的那一段即可，其余解可以通过对称性获得。这相当于只考虑 $x + y\sqrt{D} > 1$ 的解。如果方程除了 $(\pm 1, 0)$ 之外还存在不平凡的解，那么一定在第一象限内存在 $x + y\sqrt{D}$ 取值最小的解 (x_1, y_1)，这也是第一象限内（不含坐标轴）横纵坐标都最小的整点，它称为 Pell 方程的基本解（fundamental solution）[4]。根据前文的讨论，满足 $x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k$ 的整数对 (x_k, y_k) 都是 Pell 方程的解，而且都在第一象限。反过来，这也的确是 Pell 方程在第一象限内的全部解。再利用对称性，就可以得到如下结论：

定理

设 Pell 方程 $x^2 - Dy^2 = 1$ 的基本解是 (x_1, y_1)。那么，它的全部解就是

$$\{(x, y) : x + y\sqrt{D} = \pm(x_1 + y_1\sqrt{D})^k, k \in \mathbf{Z}\}.$$

证明

首先证明第一象限中不存在其他解。不妨设存在其他解 $x + y\sqrt{D}$ 且对于某个 $k \geq 0$ 有

$$x_k + y_k\sqrt{D} < x + y\sqrt{D} < x_{k+1} + y_{k+1}\sqrt{D}.$$

几何意义上，这相当于说整点 (x, y) 落入了双曲线上 (x_k, y_k) 和 (x_{k+1}, y_{k+1}) 之间（不含端点）。将不等式同时乘以 $x_k - y_k\sqrt{D} = (x_k + y_k\sqrt{D})^{-1}$ 就得到

$$1 < (x + y\sqrt{D})(x_k - y_k\sqrt{D}) = (xx_k - Dyy_k) + (x_k y - xy_k)\sqrt{D} < x_1 + y_1\sqrt{D}.$$

根据前文提到的单调性，这个不等式就说明 $(xx_k - Dyy_k, x_k y - xy_k)$ 是位于 $(1, 0)$ 和 (x_1, y_1) 之间的整点。这与 (x_1, y_1) 的选取矛盾。

将第一象限的解扩展到整个平面时，指数 k 取相反数（即整体取倒数）就是关于 x 轴对称，整体取相反数则是关于原点对称。再加上 $k = 0$ 时的平凡解，就得到 Pell 方程的全部解。

前文的讨论只是假设了基本解的存在。现在要说明的是，Pell 方程总是存在非平凡的解。

定理

Pell 方程 $x^2 - Dy^2 = 1$ 总是存在除了 $(\pm 1, 0)$ 之外的整数解。

证明

首先，Dirichlet 定理 表明存在无数对正整数 (x, y) 使得

$$\left|\frac{x}{y}-\sqrt{D}\right| \leq \frac{1}{y^2}$$

成立，它们都满足不等式

$$|x^2-Dy^2| = y^2\left|\frac{x}{y}-\sqrt{D}\right|\left|\frac{x}{y}+\sqrt{D}\right| \leq \frac{1}{y^2}+2\sqrt{D} < 1+2\sqrt{D}.$$

因而，必然存在整数 $m \in (-1-2\sqrt{D}, 1+2\sqrt{D})$ 使得有无数对 (x, y) 都满足 $x^2-Dy^2=m$。将这些 (x, y) 根据对 m 的余数分类，就知道对某一对整数 (x_0, y_0)，一定存在无数对 (x, y) 使得 $x \equiv x_0 \pmod{m}$ 以及 $y \equiv y_0 \pmod{m}$ 成立。任取满足这些条件的两对互异的 (x_1, y_1) 和 (x_2, y_2)，则

$$\frac{x_1+y_1\sqrt{D}}{x_2+y_2\sqrt{D}} = \frac{x_1x_2-Dy_1y_2}{m}+\frac{x_2y_1-x_1y_2}{m}\sqrt{D}.$$

因为根据同余关系有

$$\begin{aligned} x_1x_2-Dy_1y_2 \equiv x_0^2-Dy_0^2 = m \equiv 0 \pmod{|m|},\\ x_2y_1-x_1y_2 \equiv x_0y_0-x_0y_0 = 0 \pmod{|m|}, \end{aligned}$$

这说明上式右侧得到的是整数解。而且，因为 $(x_1, y_1) \neq (x_2, y_2)$，它并不平凡。这就说明 Pell 方程的确存在非平凡解。

当然，本节提供的是非构造性的证明，在下文讨论 Pell 方程的解法时，会直接利用连分数的渐近分数构造出 Pell 方程的解，因而提供了 Pell 方程存在非平凡解的另一种证明。另外，尽管本节得到的 Pell 方程解的结构与实二次整数环的单位数的结构是一致的，但是对于 $D \equiv 1 \pmod{4}$ 的情形，本节并没有完全解决相应的二次整数环的单位数的结构问题，下文将进一步讨论。

广义 Pell 方程

广义 Pell 方程 $x^2-Dy^2=N$ 的图像同样是平面上的双曲线，同样以 x 轴和 y 轴为对称轴。前文已经指出，方程 $x^2-Dy^2=N$ 的部分解可能只相差一个 Pell 方程解的因子，这意味着可以将方程 $x^2-Dy^2=N$ 的解划分为等价类。对于方程 $x^2-Dy^2=N$ 的两个解 (x_1, y_1) 和 (x_2, y_2)，如果存在 Pell 方程的解 (u, v) 使得 $x_2+y_2\sqrt{D} = (x_1+y_1\sqrt{D})(u+v\sqrt{D})$ 成立，那么称解 (x_1, y_1) 和 (x_2, y_2) 等价。两个解等价的充分必要条件是

$$N \mid (x_1x_2-Dy_1y_2),\ N \mid (x_2y_1-x_1y_2).$$

因为 Pell 方程的解相对容易求出，一个自然的想法是在上述的每个等价类中各求出一个解。只要知道这些解，就可以利用相应的 Pell 方程的解得到所要求的广义 Pell 方程的全部解。在广义 Pell 方程的解的等价类中，由于对称性，每个等价类都存在纵坐标 y 非负但是尽可能小的解：如果这样的解唯一，它就称为该等价类的基本解；否则，该等价类必然有两个 y 非负且最小的解，而且它们关于 y 轴对称，此时选择 $x>0$ 的那个作为基本解。由此，求解广义 Pell 方程 $x^2-Dy^2=N$，就相当于求解它的基本解集 U。设它对应的 Pell 方程的基本解是 (r, s)，则广义 Pell 方程的全部解的集合是

$$\{(x, y) : x+y\sqrt{D} = \pm(r+s\sqrt{D})^k(u+v\sqrt{D}), k \in \mathbf{Z}, u+v\sqrt{D} \in U\}.$$

广义 Pell 方程的基本解必然是有限的。这是因为从上面的通解表达式可知，绝对值 $|u+v\sqrt{D}|$ 必然位于 $r-s\sqrt{D}$ 和 $r+s\sqrt{D}$ 之间。文末的参考文献中提供了关于基本解的坐标的范围的更严格的估计。当然，与 Pell 方程的情形不同，广义 Pell 方程可能没有解。

利用广义 Pell 方程的一个解 (u, v) 和 Pell 方程的基本解 (r, s) 得到同一个等价类中的全部解的方法，除了利用解的复合之外，还可以利用如下递推关系

$$x_k = 2rx_{k-1} - x_{k-2},\ y_k = 2ry_{k-1} - y_{k-2},$$

其中，$x_k + y_k\sqrt{D} = (r + s\sqrt{D})^k(u + v\sqrt{D})$。这是因为 x_n 和 y_n 都可以对某一对实数 (A, B) 写成 $A(r + s\sqrt{D})^k + B(r - s\sqrt{D})^k$ 的形式，而根据 Vieta 定理，$r \pm s\sqrt{D}$ 是方程 $x^2 - 2rx + 1 = 0$ 的两个实根，进而 x_n 和 y_n 都满足上述的二阶常系数递推关系。相较于解的复合，该递推公式有更少的乘法次数。

求解方法

Pell 方程和广义 Pell 方程的求解都可以基于连分数进行。

PQa 算法

本文讨论的算法都基于 PQa 算法，它可以用于求出特定的二次无理数的连分数展开。

设整数 P_0, Q_0, D 满足 $Q_0 \neq 0$，$D > 0$ 且不是完全平方数，以及 $P_0^2 \equiv D \pmod{Q_0}$。那么，二次无理数

$$\omega = \frac{P_0 + \sqrt{D}}{Q_0}$$

的连分数展开 $[a_0, a_1, \cdots]$ 可以通过如下 递推公式 求得：

$$a_k = \left\lfloor \frac{P_k + \sqrt{D}}{Q_k} \right\rfloor,\ P_{k+1} = a_kQ_k - P_k,\ Q_{k+1} = \frac{D - P_{k+1}^2}{Q_k}.$$

进而，ω 的第 k 个渐近分数的分子和分母 A_k 和 B_k 由如下 递推公式 给出：

$$A_k = a_kA_{k-1} + A_{k-2},\ B_k = a_kB_{k-1} + B_{k-2}$$

且 $A_{-1} = 1$，$A_{-2} = 0$，$B_{-1} = 0$，$B_{-2} = 1$。

这些公式的正确性已经在连分数一文中得到证明。那里也说明了，因为二次无理数是 循环连分数，所以，三元组 (P_k, Q_k, a_k) 最终将进入循环，算法总可以在有限步内终止。不妨设循环节的最小长度是 ℓ，且循环的最早的起始位置是 k_0，则二次无理数的连分数展开可以写作

$$\omega = [a_0, \cdots, a_{k_0-1}, \overline{a_{k_0}, \cdots, a_{k_0+\ell-1}}].$$

利用 PQa 算法解决 Pell 方程，需要建立如下结论：

定理

继续上述记号。设 $G_k = Q_0A_k - P_0B_k$，则整数对 (G_{k-1}, B_{k-1}) 满足关系式

$$G_{k-1}^2 - DB_{k-1}^2 = (-1)^kQ_0Q_k,$$

且它们的最大公因数 $\gcd(G_{k-1}, B_{k-1})$ 整除 Q_k。

证明

设 ω 的连分数展开中，第 k 个余项（完全商）为 ω_k，即

$$\omega = [a_0, a_1, \cdots, a_{k-1}, \omega_k] = \frac{\omega_k A_{k-1} + A_{k-2}}{\omega_k B_{k-1} + B_{k-2}}.$$

将 $\omega = (P_0 + \sqrt{D})/Q_0$ 和 $\omega_k = (P_k + \sqrt{D})/Q_k$ 代入上式，就得到

$$\frac{P_0 + \sqrt{D}}{Q_0} = \frac{(P_k + \sqrt{D})A_{k-1} + Q_k A_{k-2}}{(P_k + \sqrt{D})B_{k-1} + Q_k B_{k-2}}.$$

消去左右两侧的分母并比较有理部分和无理部分的系数，再代入 G_k 的表达式，就得到如下等式：

$$\begin{aligned} G_{k-1} &= P_k B_{k-1} + Q_k B_{k-2}, \\ DB_{k-1} &= P_k G_{k-1} + Q_k G_{k-2}. \end{aligned}$$

因此，将一式乘以 G_{k-1} 减去二式乘以 B_{k-1}，就有

$$\begin{aligned} G_{k-1}^2 - DB_{k-1}^2 &= (B_{k-2}G_{k-1} - B_{k-1}G_{k-2})Q_k \\ &= (A_{k-1}B_{k-2} - B_{k-1}A_{k-2})Q_0 Q_k \\ &= (-1)^k Q_0 Q_k. \end{aligned}$$

最后一步利用了渐近分数的 差分公式。这就证明了第一个结论。

为了证明第二个结论，将 G_k 的表达式代入第一个结论，有

$$(Q_0 A_{k-1} - P_0 B_{k-1})^2 - DB_{k-1}^2 = (-1)^k Q_0 Q_k.$$

所以，利用 $Q_0 \mid (P_0^2 - D)$ 有

$$Q_0 A_{k-1}^2 + \left(\frac{P_0^2 - D}{Q_0} B_{k-1} - 2P_0 A_{k-1}\right) B_{k-1} = (-1)^k Q_k.$$

故而，$\gcd(G_{k-1}, B_{k-1}) = \gcd(Q_0 A_{k-1}, B_{k-1})$ 整除 Q_k。

这个结论提供了一种寻找方程 $x^2 - Dy^2 = N$ 的解的方法。如果合理地选择 $Q_0 > 0$ 并选择 P_0 为同余方程 $P_0^2 \equiv D \pmod{Q_0}$ 的解，那么通过对 $(P_0 + \sqrt{D})/Q_0$ 执行 PQa 算法，直到找到 $(-1)^k Q_0 Q_k = N$，此时 (G_{k-1}, B_{k-1}) 就成为原方程的一组解。而且，如果 $Q_k = \pm 1$，那么这样得到的解一定是本原解，也就是说 G_{k-1} 和 B_{k-1} 一定是互素的。

这个思想是解决 Pell 方程和广义 Pell 方程的核心。理解了这一思想后，下面就着手处理算法的一些细节，并证明所有的解都可以通过该方式得到。

Pell 方程

要解决 Pell 方程 $x^2 - Dy^2 = 1$，只需要对 $(P_0, Q_0, D) = (0, 1, D)$ 运行 PQa 算法，直到出现 $(-1)^k Q_k = 1$，此时 (A_{k-1}, B_{k-1}) 就是 Pell 方程的一组解（因为 G_{k-1} 此时就是 A_{k-1}）。当然，对于 Pell 方程，对该过程可以进行更精确的描述。

首先，解一定出现在循环节的末尾处。上述过程相当于对 $\sqrt{D}$ 做连分数展开。对此，已经有 结论：

$$\sqrt{D} = [\lfloor \sqrt{D} \rfloor, \overline{a_1, \cdots, a_{\ell-1}, 2\lfloor \sqrt{D} \rfloor}].$$

此处，循环节长度为 ℓ，且起始位置是第 1 项（下标从 0 开始）。而且，它的第 ℓ 项余项等于 $\lfloor \sqrt{D} \rfloor + \sqrt{D}$，这说明 $Q_\ell = 1$。因此，如果 ℓ 是偶数，那么 $(A_{\ell-1}, B_{\ell-1})$ 就是 Pell 方程的一组非平凡解；如果 ℓ 是奇

数，那么 $(A_{2\ell-1}, B_{2\ell-1})$ 就是 Pell 方程的一组非平凡解。

接下来要说明，刚刚得到的这组解一定是基础解。这个结论基于两点理由：第一，Pell 方程的所有正整数解 (x, y) 对应的分数 x/y 都出现在 $\sqrt{D}$ 的渐近分数中，这就保证了 (x, y) 必定是 PQa 算法过程中的某个 (A_k, B_k)；第二，除了循环节末尾，不会再出现其他位置有 $Q_k = 1$，因为 A_k 和 B_k 的递推关系保证了它们的大小随着下标增加而增加，所以最小的正整数解（即基础解）必然出现在刚刚指明的位置。这两点理由可以分别从如下的两条定理得出：

定理

设方程 $x^2 - Dy^2 = N$ 有正整数解 (x, y)，如果 $|N| < \sqrt{D}$，那么 $\dfrac{x}{y}$ 一定等于 $\sqrt{D}$ 的渐近分数。

证明

当 $N > 0$ 时，因为 $x^2 - Dy^2 > 0$，所以 $x > y\sqrt{D}$。故而，有

$$\left|\frac{x}{y} - \sqrt{D}\right| = \frac{N}{y(x + y\sqrt{D})} < \frac{N}{2y^2\sqrt{D}} < \frac{1}{2y^2}.$$

根据 Legendre 判别法 可知，$\dfrac{x}{y}$ 是 $\sqrt{D}$ 的渐近分数。

当 $N < 0$ 时，$x > y\sqrt{D}$ 不再成立。所以，转而考虑方程 $y^2 - \dfrac{1}{D}x^2 = -\dfrac{N}{D}$ 的解。因为 $\dfrac{|N|}{D} < \sqrt{\dfrac{1}{D}}$，所以上面的论证依然成立。这说明 $\dfrac{y}{x}$ 是 $\dfrac{1}{\sqrt{D}}$ 的渐近分数。根据 倒数定理 可知，$\dfrac{x}{y}$ 也是 $\sqrt{D}$ 的渐近分数。

定理

在对 $(P_0, Q_0, D) = (0, 1, D)$ 运行上述 PQa 算法的过程中，$Q_k = 1$ 必然推出 $\ell \mid k$。

证明

在 $\sqrt{D}$ 的连分数展开中，除了第 0 个余项，所有其他余项都是 纯循环连分数。设 $Q_k = 1$。根据 Galois 的结论，必然有余项 $\omega_k = P_k + \sqrt{D} > 1$，且它的共轭 $-1 < P_k - \sqrt{D} < 0$，这说明 $P_k = \lfloor\sqrt{D}\rfloor$。因此，余项 ω_k 就等于 ω_ℓ。但是，余项的重复意味着连分数的循环，如果 k 不是 ℓ 的整数倍，就与 ℓ 是最小正周期相矛盾。所以，必然有 $\ell \mid k$。

综合本节的讨论可知，只要对 $\sqrt{D}$ 做连分数展开，亦即以 $(P_0, Q_0, D) = (0, 1, D)$ 为起点做 PQa 算法，当首次得到 $Q_\ell = 1$ 时，就到达了第一个循环节的末尾。此时，如果 ℓ 是偶数，那么 $(A_{\ell-1}, B_{\ell-1})$ 就是 Pell 方程的基本解；否则，$(A_{2\ell-1}, B_{2\ell-1})$ 是 Pell 方程的基本解。对于循环节长度 ℓ 为奇数的情形，并不需要继续 PQa 算法到两倍的循环节处，马上就会说明 $A_{2\ell-1} + B_{2\ell-1}\sqrt{D} = (A_{\ell-1} + B_{\ell-1}\sqrt{D})^2$，因而可以直接从 $(A_{\ell-1}, B_{\ell-1})$ 直接计算出 Pell 方程的基本解。Pell 方程所有其他解都可以通过 Pell 方程的基本解计算。

示例

1. 求解方程 $x^2 - 14y^2 = 1$。

   对 $(P_0, Q_0, D) = (0, 1, 14)$ 运行 PQa 算法结果如下：（标红部分为第一个循环节）

k	P	Q	a	A	B	G	$G^2 - DB^2$
0	0	1	3	3	1	3	-5
1	3	5	1	4	1	4	2
2	2	2	2	11	3	11	-5
3	2	5	1	15	4	15	1
4	3	1	6	101	27	101	-5
5	3	5	1	116	31	116	2

   循环节长度 $\ell = 4$ 为偶数。方程的最小正整数解为 $(G_3, B_3) = (15, 4)$。

2. 求解方程 $x^2 - 41y^2 = 1$。

   对 $(P_0, Q_0, D) = (0, 1, 41)$ 运行 PQa 算法结果如下：（标红部分为第一个循环节）

k	P	Q	a	A	B	G	$G^2 - DB^2$
0	0	1	6	6	1	6	-5
1	6	5	2	13	2	13	5
2	4	5	2	32	5	32	-1
3	6	1	12	397	62	397	5
4	6	5	2	826	129	826	-5
5	4	5	2	2049	320	2049	1
6	6	1	12	25414	3969	25414	-5
7	6	5	2	52877	8258	52877	5

   循环节长度 $\ell = 3$ 为奇数。方程的最小正整数解为 $(G_5, B_5) = (2049, 320)$。它也可以通过 $(G_2, B_2) = (32, 5)$ 计算得出：

$$(32+5\sqrt{41})^2 = 2049 + 320\sqrt{41}.$$

负 Pell 方程

根据上一节的讨论可知，负 Pell 方程的解也必然对应于 $\sqrt{D}$ 的渐近分数，而且只能出现在 $(-1)^k Q_k = -1$ 处。这只能出现在循环节的末尾。因此，负 Pell 方程有解，当且仅当循环节长度 ℓ 是奇数。当解存在时，$(A_{\ell-1}, B_{\ell-1})$ 就是负 Pell 方程的基本解。它的求解方法和上一节是一致的。

利用前文对于 Pell 方程解的结构的证明相仿的思路，可以证明如下结论：

定理

设方程 $x^2 - Dy^2 = -1$ 有解，且基本解是 (x_1, y_1)。那么，$x^2 - Dy^2 = \pm 1$ 的所有整数解都属于集合

$$\{(x, y) : x + y\sqrt{D} = \pm(x_1 + y_1\sqrt{D})^k, k \in \mathbf{Z}\}.$$

特别地，满足 $x_2 + y_2\sqrt{D} = (x_1 + y_1\sqrt{D})^2$ 的整数解 (x_2, y_2) 正是 $x^2 - Dy^2 = 1$ 的基本解。

证明

由于对称性，只需要考虑正整数解，即 $x + y\sqrt{D} > 1$ 的情形。但是由于 $x^2 - Dy^2 = \pm 1$ 是两段双曲线，所以 $x + y\sqrt{D}$ 无法和 (x, y) 建立一一对应。为了处理这种困难，首先证明上述的 (x_2, y_2) 是 $x^2 - Dy^2 = 1$ 的基本解。

显然，(x_2, y_2) 是 $x^2 - Dy^2 = 1$ 的解。如果设 (z, w) 是 $x^2 - Dy^2 = 1$ 的基本解，那么必然有 $1 < z + w\sqrt{D} \le x_2 + y_2\sqrt{D}$。如果右侧的不等式不含有等号，那么将不等式同除以 $x_1 + y_1\sqrt{D}$ 就得到 $-x_1 + y_1\sqrt{D} < (z + w\sqrt{D})(-x_1 + y_1\sqrt{D}) < x_1 + y_1\sqrt{D}$。将该不等式的中间项的表达式展开就能得到 $x' + y'\sqrt{D}$ 的形式，它的范数是 -1 且 (x', y') 也是整数解。将该不等式取倒数，就发现 $-x' + y'\sqrt{D}$ 同样落入 $-x_1 + y_1\sqrt{D}$ 和 $x_1 + y_1\sqrt{D}$ 之间。二次整数 $\pm x' + y'\sqrt{D}$ 互为倒数，必然有一个大于 1。但是 1 和 $x_1 + y_1\sqrt{D}$ 不应该再出现别的范数为 -1 的二次整数，这与 $x_1 + y_1\sqrt{D}$ 的最小性矛盾。所以，必然成立 $x_2 + y_2\sqrt{D} = z + w\sqrt{D}$，即 (x_2, y_2) 是方程 $x^2 - Dy^2 = 1$ 的基本解。

基于此，如果出现方程 $x^2 - Dy^2 = \pm 1$ 的解 (x, y) 不对应某个 $(x_1 + y_1\sqrt{D})^k$，那么必然存在 k 使得 $(x_1 + y_1\sqrt{D})^{2k} < x + y\sqrt{D} < (x_1 + y_1\sqrt{D})^{2k+2}$，消去因子 $(x_1 + y_1)^{2k+1}$，就说明存在位于 $-x_1 + y_1\sqrt{D}$ 和 $x_1 + y_1\sqrt{D}$ 之间的范数为 ± 1 的二次整数 $x' + y'\sqrt{D} \ne 1$。重复上一段利用倒数的论证可知，这与 $x_1 + y_1\sqrt{D}$ 的最小性矛盾。因而原命题得证。

因为 $(A_{\ell-1}, B_{\ell-1})$ 是负 Pell 方程的最小正整数解，而 $x^2 - Dy^2 = \pm 1$ 的所有正整数解都出现在集合

$$\{(x, y) : x + y\sqrt{D} = (A_{\ell-1} + B_{\ell-1}\sqrt{D})^k, k \in \mathbf{N}_+\}$$

中，又因为这些正整数解必然对应 $\sqrt{D}$ 的在循环节末尾（前一位）处的渐近分数，而且渐近分数的分子和分母是严格单调递增的，所以对所有 $k \in \mathbf{N}_+$ 总是有

$$(A_{\ell-1} + B_{\ell-1}\sqrt{D})^k = A_{k\ell-1} + B_{k\ell-1}\sqrt{D}.$$

在所有这些正整数解中，k 为奇数时就是负 Pell 方程的解，k 为偶数时就是 Pell 方程的解，两者交替出现。

判断负 Pell 方程是否有解，需要计算 $\sqrt{D}$ 连分数展开的循环节的长度，这并不容易计算，因此希望能够找到更简单的判断方法。但是，目前并没有条件简明、容易计算的判断方法[5]。此处仅仅提供一个简单的结

论。

定理

方程 $x^2 - Dy^2 = -1$ 有解，则 4 不能整除 D 且 D 不含有 $4k+3$ 型的素因子。反过来，如果 $D = 2$ 或 D 是 $4k+1$ 型的素数，那么方程必然有解。

证明

首先，负 Pell 方程有解，就意味着 -1 是 D 的二次剩余，因而 -1 也是 D 的任意一个因子 d 的二次剩余，故而 $d \neq 4$ 且 d 不是 $4k+3$ 型素数。反过来，方程 $x^2 - 2y^2 = -1$ 的解有非平凡解 $(1,1)$。剩下的就是 D 是 $4k+1$ 型素数的情形。

设 D 是 $4k+1$ 型素数，要证明方程 $x^2 - Dy^2 = -1$ 有解。思路是通过 Pell 方程 $x^2 - Dy^2 = 1$ 的基本解 (u, v) 入手，构造出 $x^2 - Dy^2 = -1$ 的解 (α, β)。如果 u 是偶数，将 $u^2 - Dv^2 = 1$ 两侧对 4 取模，就得到 $v^2 \equiv -1 \pmod 4$，但是 -1 并不是模 4 的二次剩余。这个矛盾说明 u 是奇数。考察等式 $Dv^2 = u^2 - 1 = (u+1)(u-1)$。因为 u 是奇数，所以 $\gcd(u+1, u-1) = \gcd(u+1, 2) = 2$。根据这一事实，将 Dv^2 的因子分给 $u+1$ 和 $u-1$，必然一个是 $2\alpha^2$，另一个是 $2D\beta^2$，其中，α 和 β 是互素的正整数而且 $v = 2\alpha\beta$。将 $u = \alpha^2 + D\beta^2$ 和 $v = 2\alpha\beta$ 代入 $u^2 - Dv^2 = 1$ 就得到 $\alpha^2 - D\beta^2 = \pm 1$。因为 (u, v) 是 Pell 方程的基本解而且 (α, β) 是比 (u, v) 更小的正整数对，这个等式右侧不能是 $+1$，故而只能是 -1。这就证明 $x^2 - Dy^2 = -1$ 存在解 (α, β)。

如果 D 是合数，那么不含有 $4k+3$ 型素因子且没有平方因子也不能保证方程 $x^2 - Dy^2 = -1$ 有解，例如 $x^2 - 34y^2 = -1$ 就没有解。

示例

利用上面的示例中的计算结果可知，方程 $x^2 - 14y^2 = -1$ 无解，且方程 $x^2 - 41y^2 = -1$ 的最小正整数解为 $(G_2, B_2) = (32, 5)$。

范数为 ±4 的情形

接下来讨论方程 $x^2 - Dy^2 = \pm 4$ 的解。此时，解的性态取决于 $D \bmod 4$ 的大小。

有些情形是容易的。如果 $D \equiv 0 \pmod 4$，那么 x 是偶数，因而 $(x/2, y)$ 是方程 $u^2 - (D/4)v^2 = \pm 1$ 的解。其余的情形，必然有 x, y 同时是奇数或者同时是偶数。如果 x, y 同时是奇数，方程两侧对 4 取模就得到 $D \equiv 1 \pmod 4$。所以，如果 $D \equiv 2, 3 \pmod 4$，那么 x, y 只能同时是偶数，因而 $(x/2, y/2)$ 是方程 $u^2 - Dv^2 = \pm 1$ 的解。因此，除了 $D \equiv 1 \pmod 4$ 的情形，方程 $x^2 - Dy^2 = \pm 4$ 的解都可以通过相应的（负）Pell 方程的解得到。

现在讨论 $D \equiv 1 \pmod 4$ 的情形，它不能简单地转化为已经解决的情形。为了找到基本解，可以对 $(P_0, Q_0, D) = (1, 2, D)$ 应用 PQa 算法，当首次得到 $Q_\ell = 2$ 时，就到达了第一个循环节的末尾。如果循环节长度 l 是偶数，那么 $(G_{\ell-1}, B_{\ell-1})$ 就是方程 $x^2 - Dy^2 = 4$ 的基本解；否则，$(G_{\ell-1}, B_{\ell-1})$ 就是方程 $x^2 - Dy^2 = -4$ 的基本解。从 $(G_{\ell-1}, B_{\ell-1})$ 出发，可以得到方程 $x^2 - Dy^2 = \pm 4$ 的所有解：

$$\left\{(x, y) : \frac{x + y\sqrt{D}}{2} = \pm\left(\frac{G_{\ell-1} + B_{\ell-1}\sqrt{D}}{2}\right)^k, k \in \mathbf{Z}\right\}.$$

如果循环节长度 ℓ 是偶数，所有这些都是方程 $x^2 - Dy^2 = 4$ 的解；否则，当 k 是奇数时，(x, y) 是方程 $x^2 - Dy^2 = -4$ 的解，而当 k 是偶数时，(x, y) 是方程 $x^2 - Dy^2 = 4$ 的解。

这个算法的正确性依赖于如下事实：

定理

设方程 $x^2 - Dy^2 = \pm 4$ 有正整数解 (x, y)。如果 $D \equiv 1 \pmod 4$，那么，$\dfrac{(x+y)/2}{y}$ 一定是 $\dfrac{1+\sqrt{D}}{2}$ 的渐近分数。

证明

首先注意到，此时 x, y 必然奇偶性相同，所以 $(x+y)/2$ 是整数。如果 (x, y) 是方程 $x^2 - Dy^2 = 4$ 的解，那么 $x > y\sqrt{D} > 2y$，所以，

$$\left| \frac{(x+y)/2}{y} - \frac{1+\sqrt{D}}{2} \right| = \frac{2}{y(x+y\sqrt{D})} < \frac{1}{2y^2}.$$

根据 Legendre 判别法 可知，$\dfrac{(x+y)/2}{y}$ 是 $\dfrac{1+\sqrt{D}}{2}$ 的渐近分数。

如果 (x, y) 是方程 $x^2 - Dy^2 = -4$ 的解，那么要建立上述不等式，只需要证明 $4y < x + y\sqrt{D}$。这至少对于除了 $D = 5, 13$ 之外的情形都成立。对于 $D = 5, 13$ 的情形，将 $x = \sqrt{Dy^2 - 4}$ 代入该不等式可知，它等价于 $2(\sqrt{D} - 2)y^2 > 1$ 成立。除了 $(D, y) = (5, 1)$ 之外，该不等式对于所有 $D = 5, 13$ 和正整数 y 都成立。剩下的就是验证 $(D, y) = (5, 1)$ 的情形，此时，方程 $x^2 - 5y^2 = -4$ 的解是 $(x, y) = (1, 1)$，需要验证的是 $\dfrac{1}{1}$ 是 $\dfrac{1+\sqrt{5}}{2} = [\overline{1}]$ 的渐近分数，而这是显然成立的。

定理

设 D 是正整数但不是完全平方数。二次无理数 $\omega = \dfrac{1+\sqrt{D}}{2}$ 的连分数展开具有形式

$$\omega = [\lfloor \omega \rfloor, \overline{a_1, \cdots, a_{\ell-1}, 2\lfloor \omega \rfloor - 1}],$$

其中，ℓ 为循环节长度，且 $a_k = a_{\ell-k}$ 对任何 $1 < k < \ell$ 都成立。

证明

因为 $\lfloor\omega\rfloor-1+\omega>1$，而且它的共轭等于 $\lfloor\omega\rfloor-\omega$，位于 -1 和 0 之间，所以根据 Galois 的结论 可知，$\lfloor\omega\rfloor-1+\omega$ 是纯循环连分数，可以写成

$$\lfloor\omega\rfloor-1+\omega=[\overline{2\lfloor\omega\rfloor-1,a_1,\cdots,a_{\ell-1}}].$$

而 Galois 关于倒数负共轭的结论说明

$$\frac{1}{\omega-\lfloor\omega\rfloor}=[\overline{a_{\ell-1},\cdots,a_1,2\lfloor\omega\rfloor-1}].$$

因此，根据连分数的定义，有

$$\lfloor\omega\rfloor-1+\omega=2\lfloor\omega\rfloor-1+\frac{1}{\dfrac{1}{\omega-\lfloor\omega\rfloor}}=[2\lfloor\omega\rfloor-1,\overline{a_{\ell-1},\cdots,a_1,2\lfloor\omega\rfloor-1}].$$

连分数展开的唯一性就说明 $a_k=a_{\ell-k}$ 对所有 $1<k<\ell$ 都成立，因而要证明的展开式也成立。

定理

设 $D\equiv 1\pmod 4$。在对 $(P_0,Q_0,D)=(1,2,D)$ 运行上述 PQa 算法的过程中，$Q_k=2$ 必然推出 $\ell\mid k$。

证明

在 $\dfrac{1+\sqrt{D}}{2}$ 的连分数展开中，除了第 0 个余项，所有其他余项都是 纯循环连分数。设 $Q_k=2$。根据 Galois 的结论，必然有余项 $\omega_k=\dfrac{P_k+\sqrt{D}}{2}$ 的共轭 $-1<\dfrac{P_k-\sqrt{D}}{2}<0$，亦即 $\sqrt{D}-2<P_k<\sqrt{D}$。因为 PQa 算法中总有 $Q_k\mid P_k^2-D$（见 算法正确性证明），所以 P_k 一定是奇数，这就说明 P_k 取值唯一，即 $P_k=P_0+2(\lfloor\omega\rfloor-1)$，也就是说余项 $\omega_k=\omega\ell$。但是，余项的重复意味着连分数的循环，如果 k 不是 ℓ 的整数倍，就与 ℓ 是最小正周期相矛盾。所以，必然有 $\ell\mid k$。

定理

设方程 $x^2-Dy^2=\pm 4$ 的最小正整数解为 (x_1,y_1)。那么，它的全部解就是

$$\left\{(x,y):\frac{x+y\sqrt{D}}{2}=\pm\left(\frac{x_1+y_1\sqrt{D}}{2}\right)^k,k\in\mathbf{Z}\right\}.$$

证明

根据对称性，只需要考虑正整数解 (x,y) 即可。此处需要证明的只有集合中的实数对 (x,y) 确实是方程 $x^2-Dy^2=\pm 4$ 的整数解。剩下的事情只需要复述对方程 $x^2-Dy^2=\pm 1$ 的解的结构的证明即可。

实际上要证明的是，对于方程 $x^2-Dy^2=\pm 4$ 的任何整数解 (x_1,y_1) 和 (x_2,y_2)，如下定义的正实数对 (x_3,y_3) 仍然是整数解：

$$\frac{x_3+y_3\sqrt{D}}{2}=\frac{x_1+y_1\sqrt{D}}{2}\frac{x_2+y_2\sqrt{D}}{2}.$$

展开右侧，比较有理项和无理项的系数可知

$$x_3=\frac{x_1x_2+Dy_1y_2}{2},\ y_3=\frac{x_1y_2+x_2y_1}{2}.$$

因为对 $i=1,2$ 有 $x_i\equiv x_i^2\equiv Dy_i^2\equiv Dy_i\pmod 2$，所以

$$\begin{aligned}2x_3=x_1x_2+Dy_1y_2\equiv D^2y_1y_2+Dy_1y_2=D(D+1)y_1y_2\equiv 0\pmod 2,\\ 2y_3=x_1y_2+x_2y_1\equiv Dy_1y_2+Dy_2y_1=2Dy_1y_2\equiv 0\pmod 2.\end{aligned}$$

这说明 x_3 和 y_3 都是整数。再利用范数保持乘法的性质可知，(x_3,y_3) 是 $x^2-Dy^2=\pm 4$ 的解。

综合这些事实，重复前文几节的论述，就可以说明用于解决方程 $x^2-Dy^2=\pm 4$ 的上述算法的正确性。这些结果说明，方程 $x^2-Dy^2=\pm 4$ 具有和方程 $x^2-Dy^2=\pm 1$ 类似的简单的解的结构：它的所有解都可以通过其最小正整数解表示出来，而无需求解其它方程。

其实，方程 $x^2-Dy^2=\pm 1$ 的所有解都可以在方程 $x^2-Dy^2=\pm 4$ 的解中找到，因而从这个角度看，方程 $x^2-Dy^2=\pm 4$ 更为基础。显然，(x,y) 是方程 $x^2-Dy^2=\pm 1$ 的解，当且仅当 $(2x,2y)$ 是方程 $x^2-Dy^2=\pm 4$ 的解。前文的分析指出，当 $D\equiv 2,3\pmod 4$ 时，方程 $x^2-Dy^2=\pm 4$ 的所有解都一定同为偶数，因而对应于 $x^2-Dy^2=\pm 1$ 的解。

当 $D\equiv 0\pmod 4$ 时，方程 $x^2-Dy^2=\pm 4$ 的解 (x,y) 中，x 一定是偶数，但是 y 可能是奇数。如果在方程 $x^2-Dy^2=\pm 4$ 的最小正整数解 (x_1,y_1) 中，y_1 是偶数，那么在所有解中 y 也一定是偶数，此时这些整数解和方程 $x^2-Dy^2=\pm 1$ 的整数解一一对应；但是，如果在最小整数解 (x_1,y_1) 中，y_1 是奇数，那么 y_k 的奇偶性将和 k 一致，交替变化，因而只有当 k 是偶数时，才对应于方程 $x^2-Dy^2=\pm 1$ 的解。如果 $x^2-Dy^2=\pm 4$ 的最小正整数解中 y_1 是奇数而且 $x_1+y_1\sqrt{D}$ 的范数是 -4，那么，对于这样的 D，$x^2-Dy^2=-4$ 有解，但是 $x^2-Dy^2=-1$ 无解。

当 $D\equiv 1\pmod 4$ 时，方程 $x^2-Dy^2=\pm 4$ 的解 (x,y) 可能同时是奇数，也可能同时是偶数。如果最小正整数解 (x_1,y_1) 已经同时是偶数，那么它的所有整数解也一定同时是偶数，所以总是对应于方程 $x^2-Dy^2=\pm 1$ 的整数解。如果最小正整数解 (x_1,y_1) 同时是奇数，那么有如下结论：

定理

设方程 $x^2-Dy^2=\pm 4$ 的最小正整数解是 (x_1,y_1)。如果 x_1 和 y_1 同时是奇数，那么，$D\equiv 5\pmod 8$，且该方程的整数解 (x,y) 同时是偶数，当且仅当

$$\frac{x+y\sqrt{D}}{2}=\pm\left(\frac{x_1+y_1\sqrt{D}}{2}\right)^{3k},k\in\mathbf{Z}.$$

证明

等式 $x_1^2 - Dy_1^2 = \pm 4$ 的两边同时对 8 取模，得到 $D \equiv 5 \pmod 8$。要证明第二个结论，首先证明 (x_3, y_3) 都是偶数，因为

$$\frac{x_3 + y_3\sqrt{D}}{2} = \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^3 = \frac{x_1^3 + 3Dxy_1^2}{8} + \frac{3x_1^2y_1 + Dy_1^3}{8}\sqrt{D},$$

所以，只需要证明右侧是整数。因为奇数的平方模 8 余 1，所以，有

$$\begin{aligned} x_1^3 + 3Dxy_1 &= x_1(x_1^2 + 3Dy_1) \equiv x_1(1 + 3 \times 5 \times 1) = 16x_1 = 0 \pmod 8, \\ 3x_1^2y_1 + Dy_1^3 &= y_1(3x_1^2 + Dy_1^2) \equiv y_1(3 \times 1 + 5 \times 1) = 8y_1 = 0 \pmod 8. \end{aligned}$$

这就说明了 x_3, y_3 都是偶数。进而，对于所有 $k \in \mathbf{Z}$，都有

$$\frac{x + y\sqrt{D}}{2} = \pm\left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{3k} = \pm\left(\frac{x_3 + y_3\sqrt{D}}{2}\right)^k \in \mathbf{Z},$$

所以此时的 (x, y) 都是偶数。反过来，对于 $r = 1, 2$，总有

$$\pm\left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{3k+r} = \pm\left(\frac{x_3 + y_3\sqrt{D}}{2}\right)^k \left(\frac{x_r + y_r\sqrt{D}}{2}\right).$$

要证明相应的 (x, y) 不是整数，只需要证明该式不是整数，也就是右侧的乘积中第二项不是整数。这在 $r = 1$ 时，就是已知条件；在 $r = 2$ 时，因为

$$\frac{x_2 + y_2\sqrt{D}}{2} = \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^2 = \frac{x_1^2 + Dy_1^2}{4} + \frac{x_1y_1}{2}\sqrt{D},$$

而且 $x_1^2 + Dy_1^2 \equiv 1 + 1 \times 1 = 2 \pmod 4$，$x_1y_1 \equiv 1 \pmod 2$，所以该式也不是整数。这就证明了，只有幂次是 3 的倍数的时候，相应的解才都属偶数。

也就是说，方程 $x^2 - Dy^2 = \pm 4$ 的每三个解中就有一个同时是偶数，它对应着 $x^2 - Dy^2 = \pm 1$ 的整数解。这也说明，对于 $D \equiv 1 \pmod 4$，方程 $x^2 - Dy^2 = -4$ 有解，当且仅当方程 $x^2 - Dy^2 = -1$ 有解。

到目前为止的讨论，已经足够计算实二次整数环的基本单位数。设 D 是正整数且不含平方因子。对于 $D \equiv 2, 3 \pmod 4$ 的情形，只需要求出 $x^2 - Dy^2 = \pm 1$ 的最小正整数解；而对于 $D \equiv 1 \pmod 4$ 的情形，只需要求出 $x^2 - Dy^2 = \pm 4$ 的最小正整数解。当得到最小正整数解 (x, y) 时，对于 $D \equiv 2, 3 \pmod 4$，基本单位数就是 $\pm x \pm y\sqrt{D}$；对于 $D \equiv 1 \pmod 4$，基本单位数就是 $\dfrac{\pm x \pm y\sqrt{D}}{2}$。

示例

1. 求解方程 $x^2 - 14y^2 = \pm 4$。

   利用前文的示例中的计算可知，方程 $x^2 - 14y^2 = 4$ 的最小正整数解为 $(30, 8)$，方程 $x^2 - 14y^2 = -4$ 无解。

2. 求解方程 $x^2 - 41y^2 = \pm 4$。

   对 $(P_0, Q_0, D) = (1, 2, 41)$ 运行 PQa 算法结果如下：（标红部分为第一个循环节）

k	P	Q	a	A	B	G	$G^2 - DB^2$
0	1	2	3	3	1	5	-16
1	5	8	1	4	1	7	8
2	3	4	2	11	3	19	-8
3	5	4	2	26	7	45	16
4	3	8	1	37	10	64	-4
5	5	2	5	211	57	365	16
6	5	8	1	248	67	429	-8
7	3	4	2	707	191	1223	8
8	5	4	2	1662	449	2875	-16
9	3	8	1	2369	640	4098	4
10	5	2	5	13507	3649	23365	-16
11	5	8	1	15876	4289	27463	8

   循环节长度 $\ell = 5$ 为奇数。方程 $x^2 - 41y^2 = -4$ 的最小正整数解为 $(G_4, B_4) = (64, 10)$，方程 $x^2 - 41y^2 = 4$ 的最小正整数解为 $(G_9, B_9) = (4098, 640)$。它们之间有如下关系：

$$\frac{4098 + 640\sqrt{41}}{2} = \left(\frac{64 + 10\sqrt{41}}{2}\right)^2.$$

   当然，因为 $D \equiv 1 \pmod 8$，根据前文结论，此时方程 $x^2 - 41y^2 = \pm 4$ 的最小正整数解一定都是偶数，且总是方程 $x^2 - 41y^2 = \pm 1$ 的最小正整数解的 2 倍，所以也可以直接利用前文的示例得出。

3. 求解方程 $x^2 - 13y^2 = \pm 4$。

   对 $(P_0, Q_0, D) = (1, 2, 13)$ 运行 PQa 算法结果如下：（标红部分为第一个循环节）

k	P	Q	a	A	B	G	G^2-DB^2
0	1	2	2	2	1	3	-4
1	3	2	3	7	3	11	4
2	3	2	3	23	10	36	-4
3	3	2	3	74	33	119	4

循环节长度 $\ell=1$ 为奇数。方程 $x^2-13y^2=-4$ 的最小正整数解为 $(G_0,B_0)=(3,1)$，方程 $x^2-13y^2=4$ 的最小正整数解为 $(G_1,B_1)=(11,3)$。

因为该方程的最小正整数解都是奇数，所以可以利用第三个循环节末尾处的数对 $(G_2,B_2)=(36,10)$ 得到相应的（负）Pell 方程 $x^2-13y^2=\pm1$ 的最小正整数解 $(18,5)$。它也可以通过直接计算得到：

$$\frac{36+10\sqrt{13}}{2}=\left(\frac{3+\sqrt{13}}{2}\right)^3.$$

而且，这是负 Pell 方程的解。相应的 Pell 方程的最小正整数解是 $(649,180)$。

4. 求解方程 $x^2-52y^2=\pm4$。

   因为方程 $x^2-13y^2=\pm1$ 的最小正整数解分别是 $(18,5)$ 和 $(649,180)$，所以方程 $x^2-52y^2=\pm4$ 的最小正整数解分别是 $(36,10)$ 和 $(1298,360)$。

一般情形

最后，讨论广义 Pell 方程的解法。

对于 $|N|<\sqrt{D}$ 的情形有一个简单的解法。前文的结论说明方程 $x^2-Dy^2=N$ 的解 (x,y) 一定满足 $\frac{x}{y}$ 等于 $\sqrt{D}$ 的某个渐近分数。而且，根据前文讨论的解的结构可知，每个基础解 (x,y) 都满足 $x+y\sqrt{D}$ 小于等于相应的 Pell 方程 $x^2-Dy^2=1$ 的基础解 $x_1+y_1\sqrt{D}$。利用 PQa 算法中分母序列 B_k 的单调性可知，广义 Pell 方程的这些基础解一定出现在相应的 Pell 方程的基础解出现之前。由此，只需要对 $(P_0,Q_0,D)=(0,1,D)$ 运行 PQa 算法，直到 $Q_{\ell'}=1$ 且 ℓ' 为偶数时为止，过程中对出现的每个 (A_k,B_k) 检验是否存在整数 f 使得

$$A_k^2-DB_k^2=(-1)^{k+1}Q_{k+1}=N/f^2$$

成立，如果成立，则记录 (fA_k,fB_k) 是一个最小正整数解。这个过程记录的所有 (fA_k,fB_k) 就是方程 $x^2-Dy^2=N$ 的全部最小正整数解。利用 $(A_{\ell'-1},B_{\ell'-1})$，即相应的 Pell 方程的基本解，就可以根据求出的这些最小正整数解，生成广义 Pell 方程的所有解。注意，取决于循环节长度 ℓ 是偶数还是奇数，上述的 ℓ' 可能是 ℓ 或是 2ℓ。

对于更为一般的 N 的情形，上述方法不再适用。首先，枚举 N 的所有平方因子 f^2，设 $m=N/f^2$，并枚举同余方程 $z^2\equiv D\pmod{|m|}$ 的所有满足 $-|m|/2<z\le|m|/2$ 的解 z。然后，对 $(P_0,Q_0,D)=(z,|m|,D)$ 运行 PQa 算法，直到 $Q_k=\pm1$ 或已经结束了一个循环节。在第二种情形，那么与该组 (f,z) 相关的方程的解并不存在。在第一种情形，需要进一步判断 $(-1)^kQ_k=N/|N|$ 与否。如果符号一致，那么 (fG_{k-1},fB_{k-1}) 就是方程 $x^2-Dy^2=N$ 的解。否则，它是方程 $x^2-Dy^2=-N$ 的解，而且当且仅当相应的负 Pell 方程的解存在时，才可以通过复合它与相应的负 Pell 方程的基本解来得到方程 $x^2-Dy^2=N$ 的

解。当完成对所有组 (f, z) 的遍历之后，就可以得到方程 $x^2 - Dy^2 = N$ 在每个解的等价类中各恰好一个解，且该解为该等价类中的基本解或最小正整数解。利用它们和相应的 Pell 方程的基本解，可以生成该方程的所有整数解。这一算法称为 **Lagrange–Matthews–Mollin 算法**。

该算法的正确性由如下定理保证：

定理

设方程 $x^2 - Dy^2 = N$ 有整数解 (x, y) 且 $x \geq 0, y > 0, \gcd(x, y) = 1$。令 $Q_0 = |N|$，则 $\gcd(Q_0, y) = 1$。设 P_0 是同余方程 $x \equiv -P_0 y \pmod{Q_0}$ 的解且 $-Q_0/2 < P_0 \leq Q_0/2$，并设整数 X 使得 $x = Q_0 X - P_0 y$ 成立。那么，$P_0^2 \equiv D \pmod{Q_0}$，$\dfrac{X}{y}$ 是 $\omega = \dfrac{P_0 + \sqrt{D}}{Q_0}$ 的一个渐近分数 $\dfrac{A_{k-1}}{B_{k-1}}$，且 $Q_k = (-1)^k \dfrac{N}{|N|}$。

证明

利用 $x \equiv -P_0 y \pmod{Q_0}$ 和 $x^2 - Dy^2 = N \equiv 0 \pmod{Q_0}$，显然有 $P_0^2 \equiv D \pmod{Q_0}$。因而，

$$P_0 x + Dy \equiv -P_0^2 y + Dy = (D - P_0^2) y \equiv 0 \pmod{Q_0}.$$

由此，可以考察整系数矩阵

$$\begin{pmatrix} P & R \\ Q & S \end{pmatrix} = \begin{pmatrix} X & \dfrac{P_0 x + Dy}{Q_0} \\ y & x \end{pmatrix}.$$

它的行列式

$$PS - QR = \frac{x(x + P_0 y) - y(P_0 x + Dy)}{Q_0} = \frac{x^2 - Dy^2}{Q_0} = \pm 1.$$

而且，设 $\zeta = \sqrt{D} > 1$，就有

$$\frac{P\zeta + R}{Q\zeta + S} = \frac{(x + P_0 y)\sqrt{D} + (P_0 x + Dy)}{(x + y\sqrt{D})Q_0} = \frac{P_0 + \sqrt{D}}{Q_0} = \omega.$$

下面要证明 $\dfrac{P}{Q}$ 是 ω 的一个渐近分数。不妨设 $\dfrac{P}{Q}$ 有 连分数展开

$$\frac{P}{Q} = [a_0, a_1, \cdots, a_k]$$

且 $PS - QR = (-1)^{k-1}$。如果设 $\dfrac{p_k}{q_k}$ 是它的第 k 个渐近分数，那么 $(p_k, q_k) = (P, Q)$，且根据 渐近分数的差分公式 可知，$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$。这说明

$$p_k(S - q_{k-1}) = q_k(R - p_{k-1}).$$

分情况讨论：

- 如果 $S = 0$，那么容易验证 $Q = R = 1$，因而 $\omega = P + \zeta^{-1} = [P, \zeta]$，故而 $\dfrac{P}{Q} = P$ 是 ω 的第 0 个渐近分数；
- 如果 $Q = S > 0$，那么 $Q = S = 1$ 且 $P - R = \pm 1$。此时，
  - 如果 $P = R + 1$，那么 $\omega = R + \dfrac{1}{1 + \zeta^{-1}} = [R, 1, \zeta]$，故而 $\dfrac{P}{Q} = \dfrac{R+1}{1} = [R, 1]$ 是 ω 的第 1 个渐近分数；
  - 如果 $P = R - 1$，那么 $\omega = R - 1 + \dfrac{1}{1 + \zeta} = [R - 1, \zeta - 1]$，故而 $\dfrac{P}{Q} = R - 1$ 是 ω 的第 0 个渐近分数；
- 如果 $Q \neq S > 0$，那么由于 $Q = q_k \mid (S - q_{k-1})$，总存在整数 κ 使得 $S = \kappa q_k + q_{k-1}$ 和 $R = \kappa p_k + p_{k-1}$ 成立。因为 $q_k \geq q_{k-1}$ 且 $S > 0$，所以 $\kappa \geq 0$。因而，$\omega = \dfrac{(\kappa + \zeta)p_k + p_{k-1}}{(\kappa + \zeta)q_k + q_{k-1}} = [a_0, a_1, \cdots, a_k, \kappa + \zeta]$，故而 $\dfrac{P}{Q}$ 是它的第 k 个渐近分数。

综上所述，总有 $\dfrac{X}{y}$ 是 $\omega = \dfrac{P_0 + \sqrt{D}}{Q_0}$ 的渐近分数，并按照 PQa 算法中的记号记作 $\dfrac{A_{k-1}}{B_{k-1}}$。因为 $A_{k-1}^2 - DB_{k-1}^2 = (-1)^k Q_0 Q_k$，所以 $Q_k = (-1)^k \dfrac{N}{|N|}$。

该定理保证了方程的所有正解都存在于相应的二次无理数的渐近分数中。因为利用 PQa 算法计算渐近分数时，只要进入循环节，就一定能保证渐近分数总是正的。所以，只要枚举所有定理条件所允许的二次无理

数，计算它的渐近分数直到一个循环节内，就能够找到一个解。因为在同一个二次无理数的渐近分数中出现的两个解，一定是等价的，所以只要得到第一个满足 $(-1)^k Q_k = N/|N|$ 的解，就可以停止继续后面的计算。与前面的所有算法都不同的是，此处满足条件的 k 可能出现在尚未进入循环节时。

示例

1. 求解方程 $x^2 - 157y^2 = 12$。

   因为 $12^2 < 157$，所以对 $(P_0, Q_0, D) = (0, 1, 157)$ 运行 PQa 算法结果如下：（标红部分为第一个循环节）

k	P	Q	a	A	B	G	G
0	0	1	12	12	1	12	
1	12	13	1	13	1	13	
2	1	12	1	25	2	25	
3	11	3	7	188	15	188	
4	10	19	1	213	17	213	
5	9	4	5	1253	100	1253	
6	11	9	2	2719	217	2719	
7	7	12	1	3972	317	3972	
8	5	11	1	6691	534	6691	
9	6	11	1	10663	851	10663	
10	5	12	1	17354	1385	17354	
11	7	9	2	45371	3621	45371	
12	11	4	5	244209	19490	244209	
13	9	19	1	289580	23111	289580	
14	10	3	7	2271269	181267	2271269	
15	11	12	1	2560849	204378	2560849	
16	1	13	1	4832118	385645	4832118	
17	12	1	24	118531681	9459858	118531681	
18	12	13	1	123363799	9845503	123363799	

k	P	Q	a	A	B	G	G
19	1	12	1	241895480	19305361	241895480	
20	11	3	7	1816632159	144983030	1816632159	
21	10	19	1	2058527639	164288391	2058527639	
22	9	4	5	12109270354	966424985	12109270354	
23	11	9	2	26277068347	2097138361	26277068347	
24	7	12	1	38386338701	3063563346	38386338701	
25	5	11	1	64663407048	5160701707	64663407048	
26	6	11	1	103049745749	8224265053	103049745749	
27	5	12	1	167713152797	13384966760	167713152797	
28	7	9	2	438476051343	34994198573	438476051343	
29	11	4	5	2360093409512	188355959625	2360093409512	
30	9	19	1	2798569460855	223350158198	2798569460855	
31	10	3	7	21950079635497	1751807067011	21950079635497	
32	11	12	1	24748649096352	1975157225209	24748649096352	
33	1	13	1	46698728731849	3726964292220	46698728731849	
34	12	1	24	1145518138660728	91422300238489	1145518138660728	
35	12	13	1	1192216867392577	95149264530709	1192216867392577	

循环节长度 $\ell = 17$ 为奇数，所以需要考察两个循环节内 $G_{k-1}^2 - 157B_{k-1}^2$ 与 12 相差一个平方因子的情形，即 $k = 1, 9, 13, 19, 23, 31$ 的情形。它们对应的解就是下表中的 (fG, fB)：

k	f	fG_{k-1}	fB_{k-1}	x	y
1	1	13	1	13	1

k	f	fG_{k-1}	fB_{k-1}	x	y
9	1	10663	851	10663	851
13	2	579160	46222	579160	46222
19	2	483790960	38610722	-579160	46222
23	1	26277068347	2097138361	-10663	851
31	1	21950079635497	1751807067011	-13	1

全体 (fG, fB) 就是方程 $x^2 - 157y^2 = 12$ 的解集的所有等价类中的最小正整数解。要通过这些解得到全部解，可以利用相应的 Pell 方程的基本解 $(46698728731849, 3726964292220)$。比如说，可以将它们转化为该等价类中的基本解 (x, y)，相应的解也一并列于上表中。

2. 求解方程 $x^2 - 157y^2 = 12$。

   这次利用 Lagrange–Matthews–Mollin 算法求解。首先，枚举 $N = 12$ 的平方因子：

   - $f^2 = 1^2$ 时，有 $m = 12$，同余方程 $P^2 \equiv 157 \pmod{12}$ 有解 $z = \pm 1, \pm 5$；
   - $f^2 = 2^2$ 时，有 $m = 3$，同余方程 $P^2 \equiv 157 \pmod{3}$ 有解 $z = \pm 1$。

   对于所有可能的 (f, z) 组合运行初始参数为 $(P_0, Q_0, D) = (z, |m|, D)$ 的 PQa 算法，并找到首个 $(-1)^k Q_k = 1$ 的位置，对应的 (fG_{k-1}, fB_{k-1}) 就是一组解。结果如下表所示：

f	z	m	k	fG_{k-1}	fB_{k-1}
1	1	12	32	21950079635497	1751807067011
1	-1	12	2	13	1
1	5	12	24	26277068347	2097138361
1	-5	12	10	10663	851
2	1	3	20	483790960	38610722
2	-1	3	14	579160	46222

   这就是前文列举的所有等价类中的最小正整数解，可以利用 Pell 方程的基本解将它们转化为基本解。

3. 求解方程 $x^2 - 79y^2 = \pm 101$。

   仍然使用 Lagrange–Matthews–Mollin 算法求解。因为 $N = 101$ 是素数，所以一定有 $f = 1$。此时，$m = 101$，相应的同余方程 $P^2 \equiv 79 \pmod{101}$ 有解 $P = \pm 33$。

   对 $(P_0, Q_0, D) = (33, 101, 79)$ 运行 PQa 算法结果如下：（标红部分为第一个循环节）

k	P	Q	a	A	B	G	G^2-DB^2
0	33	101	0	0	1	-33	1010
1	-33	-10	2	1	2	35	909
2	13	9	2	2	5	37	-606
3	5	6	2	5	12	109	505
4	7	5	3	17	41	364	-303
5	8	3	5	90	217	1929	1010
6	7	10	1	107	258	2293	-707
7	3	7	1	197	475	4222	909
8	4	9	1	304	733	6515	-606
9	5	6	2	805	1941	17252	505

循环节长度 $\ell=6$ 为偶数。直到一个循环节结束，都不存在 $Q_k=\pm1$，因而，该情形无解。相应地，对于 $(P_0,Q_0,D)=(-33,101,79)$ 运行 PQa 算法也可以观察到类似的情况。因此，该方程无解。

习题

- LOJ 6687.「Project Euler 66」解方程
- SPOJ EQU2 - Yet Another Equation
- SPOJ PELL2 - Pell (Mid pelling)
- UVa 12909. Numeric Center
- UVa 10241. Semi-triangular and also Square

参考文献与注释

- Pell's equation - Wikipedia
- John P. Robertson - Solving the generalized Pell equation $x^2-Dy^2=N$
- Keith Matthews - The Diophantine Equation $x^2-Dy^2=N$,$D>0$
- Existence of Solution to Pell's Equation - Suryateja Gavva's Blog
- Calculating the simple continued fraction of a quadratic irrational - Number Theory Web（PQa 算法）

- Solving the diophantine equation x2–Dy2 = N, D > 0 and not a perfect square, N ≠ 0 - Number Theory Web（Lagrange–Matthews–Mollin 算法）

---

1. 当 D 是完全平方数时，直接做因式分解可知，$(x+y\sqrt{D})(x-y\sqrt{D})=N$，因此所有解可以通过遍历 N 的因数得知。特别地，当 $N=1$ 时，方程只有解 $(\pm 1,0)$；当 $N=-1$ 且 $D\neq 1$ 时，方程没有解。 ↩
2. 有些中文文献也称它为第二型 Pell 方程。 ↩
3. 即形如 $n+\frac{1}{2}$ 且 $n\in\mathbf{Z}$ 的有理数。 ↩
4. 注意，Pell 方程中基本解的定义与实二次整数环中的基本单位数的定义并不一致。首先，部分实二次整数环中的基本单位数 $x+y\sqrt{D}$ 中的 x,y 是半整数，因而并非 Pell 方程的解。其次，同一个实二次整数环的基本单位数有四个，但是基本解只有一个，因为基本解要求 x,y 都是正数。 ↩
5. 一个较为实用的判断方法和工具在 这里 及其参考文献。使得方程 $x^2-Dy^2=-1$ 有解的正整数 D 的列表是 OEIS A031396。 ↩
