

# Solving Diophantine Equations via Lucas-Lehmer Theory

R. A. Mollin

Department of Mathematics and Statistics  
University of Calgary, Canada  
ramollin@math.ucalgary.ca

## Abstract

In this work we look at an approach to solving Pell's equation using continued fractions and fundamental units in real quadratic orders. We demonstrate that there is an underlying general approach using Lucas-Lehmer methods for solving Pell and other quadratic Diophantine equations that is often overlooked in the literature.

**Mathematics Subject Classification:** Primary: 11D09; 11A55; Secondary: 11R11; 11R29

**Keywords:** Pell's equation; continued fractions; Lucas-Lehmer theory; Fibonacci

## 1 Introduction

Continued fractions play a vital role in the solutions of Pell's equations  $x^2 - Dy^2 = \pm 1$ . Moreover, the theory of E. Lucas and D.H. Lehmer together with the interplay between quadratic orders is often disregarded in discussions of such solutions. In this work we highlight the aforementioned interplay in a presentation of how to solve Pell's equations via a generalization of what Ayoub [1] calls the  $k$ -Fibonacci sequences. We uncover not only the continued fraction connection, mentioned in [1], but also the critical role, absent from [1], of Lucas-Lehmer theory and its role in the interplay between the fundamental units of related real quadratic orders.

## 2 Notation and Preliminaries

Herein, we will be concerned with the simple continued fraction expansions of  $\sqrt{D}$ , where  $D$  is a positive integer that is not a perfect square. We denote

this expansion by,

$$\sqrt{D} = \langle q_0; \overline{q_1, q_2, \dots, q_{\ell-1}, 2q_0} \rangle,$$

where  $\ell = \ell(\sqrt{D})$  is the period length,  $q_0 = \lfloor \sqrt{D} \rfloor$  (the *floor* of  $\sqrt{D}$ ), and  $q_1, q_2, \dots, q_{\ell-1}$  is a palindrome.

The  $k$ th convergent of  $\alpha$  for  $k \geq 0$  is given by,

$$\frac{A_k}{B_k} = \langle q_0; q_1, q_2, \dots, q_k \rangle,$$

where

$$A_k = q_k A_{k-1} + A_{k-2},$$

$$B_k = q_k B_{k-1} + B_{k-2},$$

with  $A_{-2} = 0$ ,  $A_{-1} = 1$ ,  $B_{-2} = 1$ ,  $B_{-1} = 0$ . Also, for any  $k \in \mathbb{N}$ ,

$$A_{k-1}^2 - B_{k-1}^2 D = (-1)^k.$$

In particular,

$$A_{k\ell-1}^2 - B_{k\ell-1}^2 D = (-1)^{k\ell}.$$

In the next section, we will be considering what are typically called the standard Pell equations (2.1)–(2.2), given below. The *fundamental solution* of such an equation means the (unique) least positive integers  $(x, y)$  satisfying it. The following result shows how all solutions of the Pell equations are determined from continued fractions.

**Theorem 2.1** *Suppose that  $\ell = \ell(\sqrt{D})$  and  $k$  is any positive integer. Then if  $\ell$  is even, all positive solutions of*

$$x^2 - y^2 D = 1 \tag{2.1}$$

are given by

$$x = A_{k\ell-1} \text{ and } y = B_{k\ell-1},$$

whereas there are no solutions to

$$x^2 - y^2 D = -1. \tag{2.2}$$

If  $\ell$  is odd, then all positive solutions of Equation (2.1) are given by

$$x = A_{2k\ell-1} \text{ and } y = B_{2k\ell-1},$$

whereas all positive solutions of Equation (2.2) are given by

$$x = A_{(2k-1)\ell-1} \text{ and } y = B_{(2k-1)\ell-1}.$$

*Proof.* This appears in many introductory number theory texts possessing an in-depth section on continued fractions. For instance, see [3, Corollary 5.7, p. 236].  $\square$

We highlight the following fact which will be used throughout.

**Remark 2.1** The *fundamental solution* of  $x^2 - Dy^2 = (-1)^\ell$  is given by  $A_{\ell-1} + B_{\ell-1}\sqrt{D}$ . This is the solution with least positive  $x, y$ . Moreover, as stated in Theorem 2.1, all solutions of (2.1) are powers of  $A_{\ell-1} + B_{\ell-1}\sqrt{D}$  and all solutions of (2.2) are *odd powers* of  $A_{\ell-1} + B_{\ell-1}\sqrt{D}$ . Thus, (2.2), called the *negative Pell equation*, is solvable if and only if  $\ell = \ell(\sqrt{D})$  is odd, whereas (2.1), called the *positive Pell equation*, is always solvable with its fundamental solution being  $A_{\ell-1} + B_{\ell-1}\sqrt{D}$  when  $\ell$  is even and  $A_{2\ell-1} + B_{2\ell-1}\sqrt{D}$  when  $\ell$  is odd.

Now for the balance of the discussion in this section, we need to define general orders in which we will work. If  $D_0 > 1$  is a squarefree integer, then a *fundamental discriminant with radicand  $D$*  is given by

$$\Delta_0 = \begin{cases} D_0 & \text{if } D_0 \equiv 1 \pmod{4}, \\ 4D_0 & \text{if } D_0 \equiv 2, 3 \pmod{4}. \end{cases}$$

Now suppose that  $\Delta = f_\Delta^2 \Delta_0$  for given positive integer  $f_\Delta$ . If we set

$$\sigma_0 = \begin{cases} 2 & \text{if } \Delta_0 \equiv 1 \pmod{4}, \\ 1 & \text{if } \Delta_0 \equiv 0 \pmod{4}, \end{cases}$$

then for  $g = \gcd(\sigma_0, f_\Delta)$ , and  $\sigma = \sigma_0/g, \Delta = 4D/\sigma^2$  is called a *discriminant* with *associated radicand*  $D = (f_\Delta/g)^2 D_0$  (and underlying fundamental discriminant  $\Delta_0$  having fundamental radicand  $D_0$ ). Set

$$\omega_{\Delta_0} = \begin{cases} (1 + \sqrt{D_0})/2 & \text{if } \Delta_0 \equiv 1 \pmod{4}, \\ \sqrt{D_0} & \text{if } \Delta_0 \equiv 0 \pmod{4}, \end{cases}$$

then  $\omega_\Delta = f_\Delta \omega_{\Delta_0} + h$  where  $h \in \mathbb{Z}$  is called the *principal surd associated with the discriminant  $\Delta$* . Thus, if  $\omega'_\Delta$  is the algebraic conjugate of  $\omega_\Delta$ , then  $\Delta = (\omega_\Delta - \omega'_\Delta)^2$ , and

$$\mathcal{O}_\Delta = [1, f_\Delta \omega_{\Delta_0}] = [1, \omega_\Delta] = \mathbb{Z}[\omega_\Delta] = \mathbb{Z} + \omega_\Delta \mathbb{Z}$$

is called an order in  $\mathbb{Q}(\sqrt{D_0})$  having *conductor*  $f_\Delta$  with discriminant  $\Delta$  and associated radicand  $D$ .

The fundamental unit of  $\mathcal{O}_\Delta$  is denoted by  $\varepsilon_\Delta$ , that is the smallest positive unit in  $\mathcal{O}_\Delta$ . When  $\sigma = 2$ , then  $\varepsilon_\Delta = (a + b\sqrt{\Delta})/2$  where  $a$  and  $b$  have the same parity.

### 3 Lucas-Lehmer Theory and Pell's Equation

Let  $\alpha$  and  $\beta$  be the roots of

$$x^2 - \sqrt{R}x + Q = 0,$$

where  $R, Q \in \mathbb{Z}$ , with  $\gcd(R, Q) = 1$ . It follows that

$$\alpha + \beta = \sqrt{R}, \quad \alpha\beta = Q, \quad \text{and} \quad \alpha - \beta = \sqrt{R - 4Q}.$$

Set

$$\sqrt{\Delta} = \sqrt{R - 4Q}$$

from which it follows that

$$2\alpha = \sqrt{R} + \sqrt{\Delta} = \sqrt{R} + \sqrt{R - 4Q},$$

and

$$2\beta = \sqrt{R} - \sqrt{\Delta} = \sqrt{R} - \sqrt{R - 4Q}.$$

#### Definition 3.1 Lucas Functions

Let  $n \geq 0$  be an integer. Then the following are called *Lucas functions*:

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta),$$

and

$$V_n = \alpha^n + \beta^n.$$

The above were dubbed functions rather than sequences by Lucas, then later extended by D.H. Lehmer. They satisfy the Diophantine equation;

$$V_n^2 - \Delta U_n^2 = 4Q^n, \tag{3.3}$$

and the recurrence relations

$$U_{n+1} = R^{1/2}U_n - QU_{n-1}, \tag{3.4}$$

and

$$V_{n+1} = R^{1/2}V_n - QV_{n-1},$$

—see [2, Exercise 3.1.5, pp. 73–75].

**Remark 3.1** If we let  $Q = -1$  and  $R = k^2$  then we get Ayoub’s  $k$ -Fibonacci sequence  $a_{n+1} = ka_n + a_{n-1}$ . In [1] it is stated that the following formula can be derived via the techniques of homogeneous second order difference equations:

$$a_n = U_n = \frac{(k + \sqrt{k^2 + 4})^n - (k - \sqrt{k^2 + 4})^n}{2^n \sqrt{k^2 + 4}}$$

for any nonnegative integer  $n$ . However, this is just a direct application of (3.4) in the Lucas-Lehmer theory. He looked into this in [1] from the perspective of solutions to

$$x^2 - (k^2 + 4)y^2 = \pm 1,$$

for which he chooses as solutions  $(x_n, y_n) = ((U_{n+1} + U_{n-1})/2, U_n/2)$  and goes on to explain that certain  $k$ -Fibonacci sequences such as for  $k = 2$  will yield rational solutions. However, we know from (3.4) that when  $k = 2$ , for instance,  $(x_n, y_n) = (U_n + U_{n-1}, U_n/2)$  where  $U_n$  is even if and only if  $n$  is even, which follows from the fact that  $U_2 = 2 \mid U_n$  for even  $n$  and  $\gcd(U_m, U_n) = U_{\gcd(m,n)}$  so this is no surprise. Indeed, via (3.3), we have that  $(x_n, y_n) = (V_n/2, U_n/2)$  is the solution of  $x_n^2 - (k^2 + 4)y_n^2 = (-1)^n$ , so for  $k = 2$ , we have  $(V_1/2, U_1/2) = (1, 1/2)$  but his masks the fact that since  $\Delta = 8$ , then taking  $U_1\sqrt{\Delta} = 2\sqrt{2}$  we get  $1 + \sqrt{2}$  which is the fundamental unit of  $\mathbb{Z}[\sqrt{2}]$ . To get solutions of  $x^2 - 8y^2 = 1$ , we look at  $(1 + \sqrt{2})^2 = 3 + 2\sqrt{2} = 3 + \sqrt{8}$  which is the fundamental unit of the order  $\mathbb{Z}[\sqrt{8}]$ . Here we have the interaction between the orders  $\mathbb{Z}[\sqrt{2}]$  and  $\mathbb{Z}[\sqrt{8}]$ . The odd  $k$  case, for instance, using Ayoub’s example with  $k = 3$  we have that  $V_n/2 + U_n/2\sqrt{13} = ((3 + \sqrt{13})/2)^n$ , so in particular for  $n = 3$  we have that  $((3 + \sqrt{13})/2)^3 = 18 + 5\sqrt{13}$  so all *integral* solutions of  $x^2 - 13y^2 = (-1)^n$  are powers of  $18 + 5\sqrt{13}$  and this holds since the latter is the fundamental unit of  $\mathbb{Z}[\sqrt{13}]$  whereas  $(3 + \sqrt{13})/2$  is the fundamental unit of  $\mathbb{Z}[(1 + \sqrt{13})/2]$ . Hence, what is missed in [1] is this interplay between these two quadratic orders. Indeed Ayoub says: “Note that in the first example (where  $k$  is even) alternate solutions are integral, while in the second (where  $k$  is odd), every third solution is integral. It turns out his is no coincidence.” Then he spends the balance of the paper demonstrating this fact. However, as seen above this is an immediate consequence of Lucas-Lehmer theory.

Moreover, these and more general such radicands have been extensively studied from this perspective and the types in this example are special cases of what are called *narrow Richaud-Degert (RD) types*. Indeed, any radicand  $D = k^2 + r$  where  $|r| \mid 4k$  is called an *extended (RD) type* and is called a *narrow R-D type* if  $|r| = 1, 4$ . These are well understood and completely defined from the continued fraction perspective—see [2, Theorem 3.2.1, p. 78]. For  $D = k^2 + 4$ , the continued fraction expansion of  $\sqrt{k^2 + 4}$  has period length 5 when  $k$  is odd, and if  $k$  is even it has period length 2. Moreover, the fundamental unit in the former case is  $(k^3 + 3k)/2 + (k^2 + 1)/2\sqrt{D}$  and in the

latter case it is  $(k^2 + 2)/2 + k/2\sqrt{D}$ . The former follows from the fact that the fundamental unit of  $\mathbb{Z}[\sqrt{k^2 + 4}]$  for odd  $k$  is given by

$$\left(\frac{k + \sqrt{k^2 + 4}}{2}\right)^3 = \frac{k^3 + 3k}{2} + \frac{k^2 + 1}{2}\sqrt{k^2 + 4},$$

where  $(k + \sqrt{k^2 + 4})/2$  is the fundamental unit of  $\mathbb{Z}[(1 + \sqrt{k^2 + 4})/2]$ —see [2, Theorem 2.1.4, p. 53] and [2, Theorem 3.2.1, p. 78].

It is an exercise to verify the following fact—see [2, Exercise 3.2.7, p. 85]. It is the purpose of this work to show how much more general results may be achieved via Lucas-Lehmer theory and extend the intent of Ayoub in [1] to give a complete generalization in an elementary fashion.

**Proposition 3.1** Let  $D_0$  be a fundamental radicand and let  $f$  be the least positive integer such that  $f^2D_0 = k^2 + r$  with  $-k < r \leq k$  and  $r \mid 4k$ . Also, let  $\Delta$  be the discriminant associated with the radicand  $D = f^2D_0$ . Then the fundamental unit of  $\mathcal{O}_\Delta$  is given as follows.

- (a)  $\varepsilon_\Delta = k + f\sqrt{D_0}$  if  $|r| = 1$  unless  $D_0 = 5$  and  $f = 1$ .
- (b)  $\varepsilon_\Delta = (k + f\sqrt{D_0})/2$  for  $|r| = 4$ .
- (c)  $\varepsilon_\Delta = (2k^2 + r + 2kf\sqrt{D_0})/|r|$  if  $|r| \notin \{\pm 1, \pm 4\}$ .

Now let  $\Delta = k^2 \pm 4m^2$  be a discriminant where  $m \mid k$ , which is of RD-type. Thus, we may generalize the  $k$ -Fibonacci sequence discussed in Remark 2.1 as follows:

$$U_{n+1} = kU_n \pm m^2U_{n-1} \text{ for any } n \geq 0 \tag{3.5}$$

may be dubbed the  $(k, \pm m)$ -Fibonacci sequence. In this case,  $Q = \mp m^2$  and  $R = k^2$ . By Proposition 3.1 we have that when  $m > 1$ , then by properties of the Lucas functions, given in [4, Theorem 8.1, p. 272] for instance,

$$\begin{aligned} \left(\frac{V_2 + U_2\sqrt{\Delta}}{2m^2}\right)^n &= \left(\frac{V_{2n} + U_{2n}\sqrt{\Delta}}{2m^{2n}}\right) \\ &= \varepsilon_\Delta^n = \left(\frac{k^2 \pm 2m^2 + k\sqrt{k^2 \pm 4m^2}}{2m^2}\right)^n, \end{aligned}$$

and

$$\frac{V_{2n}^2 - U_{2n}^2(k^2 \pm 4m^2)}{4m^{4n}} = \left(\frac{V_{2n}}{2m^{2n}}\right)^2 - \left(\frac{U_{2n}}{2m^{2n}}\right)^2 (k^2 \pm 4m^2) = 1.$$

When  $2m^2 \mid k$ , then  $U_2/(2m^2) = k/(2m^2) \in \mathbb{Z}$  and  $V_2/(2m^2) = k^2/(2m^2) \pm 1 \in \mathbb{Z}$  and when  $2m^2$  does not divide  $k$ , then  $U_3/(2m^2) = [(k/m)^2 \pm 1]/2 \in \mathbb{Z}$  and  $V_3/(2m^2) = [k((k/m)^2 \pm 3)]/2 \in \mathbb{Z}$ . (Keep in mind that all of the latter is under the assumption that  $m \mid k$ .) In the former case the fundamental solution of  $x^2 - \Delta y^2 = 1$  is given by  $(V_2 + U_2\sqrt{\Delta})/(2m^2)$  and in the latter it is  $(V_6 + U_6\sqrt{\Delta})/(2m^6)$ .

**Example 3.1** Let  $\Delta = k^2 + 4m^2 = 225^2 + 4 \cdot 3^2 = 50661$ . Then  $2m^2 = 18$  does not divide  $k = 225$  and  $U_2/(2m^2) = k/(2m^2) = 225/18 = 25/2 \notin \mathbb{Z}$ , but  $U_3/(2m^2) = 50634/18 = 2813$ . Moreover, the fundamental solution of  $x^2 - 50661y^2 = 1$  is given by

$$\begin{aligned} \varepsilon_{4 \cdot 50661} &= \frac{V_6 + U_6\sqrt{50661}}{2m^6} = \frac{129884770891458 + 577060507800\sqrt{50661}}{1458} \\ &= 89084205001 + 395789100\sqrt{50661} = \left(\frac{5627 + 25\sqrt{50661}}{2}\right)^3 = \varepsilon_{50661}^3. \end{aligned}$$

Note that the fundamental solution is also given by the values from Theorem 2.1 in the simple continued fraction expansion of  $\sqrt{50661}$  namely for  $\ell = 10$  with  $A_{\ell-1} = A_9 = 89084205001$  and  $B_{\ell-1} = 395789100$ , namely

$$\varepsilon_{4 \cdot 50661} = A_9 + B_9\sqrt{50661}.$$

**Example 3.2** Let  $\Delta = k^2 + 4m^2 = 450^2 + 4 \cdot 3^2 = 202536$ . Then  $2m^2 = 18 \mid k = 450$  with  $U_1/(2m^2) = 450/18 = 25$  and  $V_2/(2m^2) = 202518/18 = 11251$ . Moreover, the fundamental solution of  $x^2 - 202536y^2 = 1$  is given by

$$\varepsilon_{4 \cdot 202536} = \frac{V_2 + U_2\sqrt{202536}}{2m^2} = \frac{202518 + 450\sqrt{202536}}{18} = 11251 + 25\sqrt{202536},$$

which may be obtained as in Example 3.1 via the simple continued fraction expansion of  $\sqrt{202536}$  namely from  $A_{\ell-1} = A_1 = 11251$  and  $B_1 = 25$ .

Note that if  $m = 1$  in (3.5) then we get the  $(k, \pm 1)$ -Fibonacci sequence

$$V_n + U_n\sqrt{\Delta} = \left(\frac{k + \sqrt{k^2 \pm 4}}{2}\right)^n,$$

where  $U_1, V_1 \in \mathbb{Z}$  if  $k$  is even and  $U_3, V_3 \in \mathbb{Z}$  if  $k$  is odd. The  $(k, 1)$ -Fibonacci sequence is that of Ayoub [1].

**Acknowledgements:** The author gratefully acknowledge the support of NSERC Canada grant # A8484.

## References

- [1] A. Ayoub, *Fibonacci-like sequences and Pell equations*, *College Math. J.*, **38** (2007), 49–53.
- [2] R.A. Mollin, **Quadratics**, CRC Press, Boca Raton, New York, London, Tokyo (1996).
- [3] R.A. Mollin, **Fundamental Number Theory with Applications**—Second Edition, Chapman & Hall/CRC, Taylor and Francis Group, Boca Raton, London, New York (2008).
- [4] R.A. Mollin, **Advanced Number Theory with Applications**, Chapman & Hall/CRC, Taylor and Francis Group, Boca Raton, London, New York (2009).

**Received: November, 2009**