Therefore, in finitely many steps, we reach an equation of the form $x^2 - dy^2 = M'$ with $|M'| < \sqrt{d}$, which can be solved by using continued fractions (Proposition 10.22).

Example 10.16. *Prove that the equation $x^2 - 13y^2 = 53$ has solutions.*

Solution: Consider the congruence $k^2 \equiv 13 \pmod{53}$. It has solutions $k = \pm 15$. The corresponding $M = (k^2 - d)/N$ is equal to 4, and the corresponding equation is $X^2 - 13Y^2 = 4$. We know that this equation has solutions and the least solution is $X + Y\sqrt{d} = 11 + 3\sqrt{13}$. Hence, also the initial equation has solutions. By using formulas (10.39), we obtain one solution (x, y) given by

$$x = \left|\frac{13 \cdot 3 + 15 \cdot 11}{4}\right| = 51, \quad y = \left|\frac{11 + 15 \cdot 3}{4}\right| = 14. \qquad \diamondsuit$$

10.6 Squares in the Fibonacci sequence

Diophantine equations which we have studied so far were polynomial. We will now consider one polynomial-exponential Diophantine equation. We will consider the problem of determining all Fibonacci numbers F_n which are perfect squares. In other words, we will solve the equation

$$F_n = x^2,$$

where n and x are integers. This equation has some obvious solutions: $F_0 = 0$, $F_1 = F_2 = 1$, $F_{12} = 144$. The question is whether those are all solutions. In 1951, Ljunggren [278] proved that the answer to this question is affirmative. His result has been rediscovered by Cohn [84] in 1965.

The idea of the proof uses the simple fact that if a positive integer m is a square, then m is a quadratic residue modulo any positive integer. This means that the Legendre symbol $(\frac{m}{p})$ is equal to 1 for any prime number p, which does not divide m. Moreover, the Jacobi symbol $(\frac{m}{Q})$ is also equal to 1 for any odd positive integer Q, which is relatively prime to m. Hence, if we find an odd positive integer Q such that $(\frac{m}{Q}) = -1$, then we know that m cannot be a square.

In the proof, we will use properties of the Legendre and Jacobi symbols and formulas for Fibonacci and Lucas numbers, which we proved earlier in the book. We begin by proving some auxiliary statements, which will be used in proving the main result of this section.

Lemma 10.26. *Let k be an even positive integer which is not divisible by 3. Then*

$$F_{m+2k} \equiv -F_m \pmod{L_k}, \tag{10.40}$$

$$L_{m+2k} \equiv -L_m \pmod{L_k}. \tag{10.41}$$

Proof: By (1.7), we have

$$F_{m+2k} = F_{m-1}F_{2k} + F_mF_{2k+1}, \quad F_{m+2k} = F_mF_{2k-1} + F_{m+1}F_{2k}.$$

By adding these two equalities, we obtain $2F_{m+2k} = L_mF_{2k} + F_mL_{2k}$. Now from $F_{2k} = F_kL_k$ and $L_{2k} = L_k^2 - 2(-1)^k$ (see (1.11) and (1.19)), we obtain

$$2F_{m+2k} = L_mF_kL_k + F_m(L_k^2 - 2) \equiv -2F_m \pmod{L_k}.$$

Since k is not divisible by 3, the number L_k is odd, so we can divide the last congruence by 2 to obtain (10.40).

Similarly, by adding equalities

$$L_{m+2k} = F_{m-1}L_{2k} + F_mL_{2k+1}, \quad L_{m+2k} = F_mL_{2k-1} + F_{m+1}L_{2k},$$

which are obtained from (1.15), it follows that

$$2L_{m+2k} = L_mL_{2k} + F_m(L_{2k-1} + L_{2k+1}) = L_mL_{2k} + 5F_mF_{2k}. \tag{10.42}$$

From this, we have

$$2L_{m+2k} = L_m(L_k^2 - 2) + 5F_mF_kL_k \equiv -2L_m \pmod{L_k},$$

so, since k is not divisible by 3, we obtain (10.41). □

Theorem 10.27. *If n and x are integers such that $L_n = x^2$, then $n = 1$ or 3, i.e. $x = \pm 1$ or ± 2.*

Proof: The number n cannot be even. Indeed, if $n = 2k$, then $L_{2k} = L_k^2 \pm 2 = x^2$, which is impossible because the number 2 is not a difference of two squares. Thus, n is odd, so we further distinguish between two cases depending on the remainder of n in the division by 4.

(i) Let $n \equiv 1 \pmod 4$. We claim that then $n = 1$. Indeed, if $n \neq 1$, then n can be written in the form $n = 1 + 2 \cdot 3^r \cdot k$, where $r \geq 0$, and k is even and it is not divisible by 3 (as in Lemma 10.26.). Now, from (10.41), we obtain

$$\begin{aligned}L_n &\equiv -L_{1+2k(3^r-1)} \equiv (-1)^2 L_{1+2k(3^r-2)} \equiv \cdots \equiv (-1)^{3^r} L_1\\ &\equiv -1 \pmod{L_k}.\end{aligned}$$

Consider the sequence of remainders of numbers L_m, for $m \geq 1$, in the division by 4:

$$1, 3, 0, 3, 3, 2, 1, 3, \ldots$$

We conclude: if k is even and k is not divisible by 3, then $L_k \equiv 3 \pmod 4$. Now, from the property of the Jacobi symbol (Proposition 4.10), it follows that

$$\left(\frac{L_n}{L_k}\right) = \left(\frac{-1}{L_k}\right) = -1,$$

so L_n cannot be a square.

(ii) Let now $n \equiv 3 \pmod 4$. We claim that $n = 3$. Indeed, if $n \neq 3$, then $n = 3 + 2 \cdot 3^r \cdot k$, where r and k are as above. As in (i), we obtain

$$L_n \equiv -L_3 \equiv -4 \pmod{L_k},$$

so from

$$\left(\frac{L_n}{L_k}\right) = \left(\frac{4}{L_k}\right)\left(\frac{-1}{L_k}\right) = 1 \cdot (-1) = -1,$$

we conclude that L_n is not a square. □

Theorem 10.28. *If n and x are integers such that $L_n = 2x^2$, then $n = 0$ or ± 6, i.e. $x = \pm 1$ or ± 3.*

Proof:

(i) Let n be odd. Since L_n is even, $3 \mid n$. Therefore, $n \equiv \pm 3 \pmod{12}$. From (10.42), it follows that

$$2L_{m+12} = 5F_mF_{12} + L_mL_{12} = 720F_m + 322L_m \equiv 2L_m \pmod{16}.$$

Thus, $2L_n \equiv 2L_{\pm 3} \equiv 8 \pmod{16}$. It is clear that if the square of an integer is divisible by 8, then it is also divisible by 16. Hence, $2L_n$ is not a perfect square which means that $L_n \neq 2x^2$.

(ii) Let $n \equiv 0 \pmod 4$. We will show that then $n = 0$. Otherwise, n would be of the form $n = 2 \cdot 3^r \cdot k$, where r and k are as in the proof of Theorem 10.27, so, by the repeated application of relation (10.41), we would obtain

$$2L_n \equiv -2L_0 \equiv -4 \pmod{L_k}.$$

Now from

$$\Big(\frac{2L_n}{L_k}\Big) = \Big(\frac{4}{L_k}\Big)\Big(\frac{-1}{L_k}\Big) = -1$$

it follows that $2L_n$ is not a perfect square, so $L_n \neq 2x^2$.

(iii) Let $n \equiv 6 \pmod 8$. We claim that then $n = 6$. If $n \neq 6$, then we can write it in the form $n = 6 + 2 \cdot 3^r \cdot k$, where $r \geq 0$, and k is divisible by 4 and it is not divisible by 3. Now,

$$2L_n \equiv -2L_6 \equiv -36 \pmod{L_k}.$$

Let us consider the sequence of remainders of numbers L_m, for $m \geq 1$, in the division by 3:

$$1,\ 0,\ 1,\ 1,\ 2,\ 0,\ 2,\ 2,\ 1,\ 0, \ldots$$

We see that $3 \mid L_m$ if and only if $m \equiv 2 \pmod 4$. Thus, 3 does not divide L_k, so the numbers 36 and L_k are relatively prime, and we have

$$\Big(\frac{2L_n}{L_k}\Big) = \Big(\frac{36}{L_k}\Big)\Big(\frac{-1}{L_k}\Big) = -1,$$

so $L_n \neq 2x^2$.

(iv) Finally, if $n \equiv 2 \pmod 8$, then $L_{-n} = L_n$ and $-n \equiv 6 \pmod 8$. According to (iii), we know that $L_n = 2x^2$ if and only if $-n = 6$, i.e. $n = -6$. □

Theorem 10.29. *If n and x are integers such that $F_n = x^2$, then $n = 0, \pm 1, 2$ or 12, i.e. $x = 0, \pm 1$ or ± 12.*

Proof:

(i) If $n \equiv 1 \pmod 4$, then it is necessarily $n = 1$. Namely, if $n \neq 1$, then n is of the form $n = 1 + 2 \cdot 3^r \cdot k$, where $r \geq 0$ and k is an even number which is not divisible by 3. By multiple application of relation (10.40), we obtain

$$F_n \equiv -F_1 \equiv -1 \pmod{L_k},$$

so from

$$\left(\frac{F_n}{L_k}\right) = \left(\frac{-1}{L_k}\right) = -1$$

it follows that F_n is not a square.

(ii) If $n \equiv 3 \pmod 4$, then $F_{-n} = F_n$, so from (i), it follows that $F_n = x^2$ if and only if $-n = 1$, i.e. $n = -1$.

(iii) The remaining case is when n is even. Let $n = 2m$. Now,

$$x^2 = F_{2m} = F_m L_m. \tag{10.43}$$

We know that $\gcd(F_m, L_m) = 2$ if $3 \mid m$, and $\gcd(F_m, L_m) = 1$ otherwise (Example 4.16). Therefore, we will distinguish between two subcases.

(a) If $3 \mid m$, then from (10.43), it follows that $F_m = 2y^2$ and $L_m = 2z^2$. According to Theorem 10.28, the equality $L_m = 2z^2$ is possible only if $\frac{1}{2}n = m = 0, 6$ or -6. The first two possibilities, $m = 0$ and $m = 6$, also satisfy the condition $F_m = 2y^2$, while the third one $m = -6$ does not. Hence, we have $n = 0$ or $n = 12$.

(b) If $3 \nmid m$, then from (10.43), it follows that $F_m = y^2$ and $L_m = z^2$. According to Theorem 10.27, from $L_m = z^2$, it follows that $\frac{1}{2}n = m = 1$ or 3. The possibility $m = 3$ is discarded because m is not divisible by 3. Therefore, $n = 2$. □

A much more difficult problem is to determine all powers in Fibonacci and Lucas sequences, i.e. the solutions of the equations $F_n = x^k$ and $L_n = x^k$ for $k \geq 2$. In 2006, that problem was solved by Bugeaud, Mignotte and Siksek [70]. By a combination of modern methods for solving Diophantine equations, Baker's theory of linear forms in logarithms of algebraic numbers (see Chapter 14.3) and the modular method used in the Wiles proof of Fermat's Last Theorem (see [214], [319, Chapter 24]), they proved that the only Fibonacci numbers which are powers of a positive integer are $F_1 = F_2 = 1^k$, $F_6 = 8 = 2^3$ and $F_{12} = 144 = 12^2$, while the only Lucas numbers with that property are $L_1 = 1 = 1^k$ and $L_3 = 4 = 2^2$.

10.7 Ternary quadratic forms

In Chapter 10.2, we saw that the equation $x^2 + y^2 - z^2 = 0$ has infinitely many integer solutions. In this section, we will study more general equations of a similar form. We will consider *ternary quadratic forms*

$$Q(x, y, z) = Ax^2 + Bxy + Cxz + Dy^2 + Eyz + Fz^2 \tag{10.44}$$

with rational coefficients (homogenous polynomials of degree 2 in three variables). We are interested in the criteria for determining whether the equation $Q(x, y, z) = 0$ has non-trivial rational solutions (x, y, z) (the solution $(x, y, z) = (0, 0, 0)$ is called the trivial solution). It is clear that for this kind of homogenous equation, the solvability in rational numbers is equivalent to the solvability in relatively prime integers (we multiply by a common denominator and divide by a common divisor).

From the extensive literature dealing with this topic, in the presentation of results in this and the following section, we mostly followed [55, Chapter 1.7], [311, Chapter 7], [363, Chapter 4] and [378, Chapter 4].

Let f be a ternary quadratic form and let $\mathcal{A} = [\alpha_{ij}]$ be a regular 3×3 matrix with rational coefficients. Then we say that the form

$$g(x, y, z) = f(\alpha_{11}x + \alpha_{12}y + \alpha_{13}z, \alpha_{21}x + \alpha_{22}y + \alpha_{23}z, \alpha_{31}x + \alpha_{32}y + \alpha_{33}z)$$

is equivalent to the form f. In this manner, we obtain an equivalence relation. Furthermore, the equation $f(x, y, z) = 0$ has a non-trivial rational solution if and only if the equation $g(x, y, z) = 0$ has a non-trivial rational solution (therefore, we will also call those two equations equivalent). Let us note that, unlike in Chapter 5.4 where the transformation matrix has integer coefficients and determinant equal to 1, here, the transformation matrix has rational coefficients and a non-zero determinant.