Diophantine Equations

Florian Luca

Universidad Nacional Autónoma de México

Introduction

This is a very gentle introduction on how to solve certain Diophantine equations.

In the first chapter, we recall the aspects of the continued fractions that will be useful in the subsequent chapters. We shall insist in the property of convergents of an irrational α as being "the best" approximations of α by rationals and we shall show the connection between this property and the resolution of Pell equations.

In the second chapter, we take a brief tour of the theory of linear recurrent sequences of order 2. We define the Lucas sequences and observe that the sequence of Fibonacci numbers is an example of such a sequence. The most important result here is the Theorem of Primitive Divisors which will be formulated in its most general form, but will be proved only for Lucas sequences with real roots. We present some applications, in particular related to the largest prime factor of $x^2 - 1$ when x tends to infinity in the set of natural numbers.

In the third chapter, we give various specific statements of which belong to what is known as the theory of lower bounds for linear forms in logarithms of algebraic numbers. To illustrate the importance of this machinery, we give three examples. We shall see, for example, that the largest Fibonacci number having only one repeated digit in its decimal expansion is 55. We shall also see that $d = 120$ is the largest positive integer such that $d + 1$, $3d + 1$ and $8d + 1$ are all three perfect squares.

There are certain little computations along the way which can be done with either Maple or Mathematica.

Florian Luca Bordeaux, January 23, 2009

Contents

Chapter 1

Continued Fractions

1.1 Definitions

In this chapter, we recall those aspects of the continued fractions that will be useful later on.

Definition 1.1.1. *(i) A finite continued fraction is an expression of the form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} \tag{1}$$

where $a_0 \in \mathbb{R}$ and $a_i \in \mathbb{R}_{>0}$ for all $1 \leq i \leq n$. We shall use the notation $[a_0, a_1, \ldots, a_n]$ for the above expression.

(ii) The continued fraction $[a_0, \ldots, a_n]$ is called simple if $a_0, \ldots, a_n \in \mathbb{Z}$.

(iii) The continued fraction $C_k = [a_0, \ldots, a_k]$ with $0 \leq k \leq n$ is called the k-th convergent of $[a_0, \ldots, a_n]$.

It is clear that every simple continued fraction is a rational number. Conversely, using the Euclidean algorithm, every rational number can be represented as a simple continued fraction. In fact, if p and $q > 0$ are coprime and we write

$$\begin{array}{lll} p & = r_0 a_0 + r_1, & 1 \leq r_1 < r_0 := q; \\ r_0 & = r_1 a_1 + r_2, & 1 \leq r_2 < r_1; \\ \ldots & = \ldots, & \\ r_{n-1} & = r_n a_n, & \end{array}$$

where $n \geq 0$ is maximal such that $r_n \geq 1$, then we see easily that the expression (1) is p/q.

1.2 Properties

For each continued fraction $[a_0, \ldots, a_n]$ we define $p_0, \ldots, p_n$ and $q_0, \ldots, q_n$ via

$$\begin{array}{llll} p_0 & = a_0, & q_0 & = 1; \\ p_1 & = a_0 a_1 + 1, & q_1 & = a_1; \\ p_k & = a_k p_{k-1} + p_{k-2}, & q_k & = a_k q_{k-1} + q_{k-2}; \end{array}$$

for all $k = 2, \ldots, n$.

Proposition 1.2.1. *With the previous notation, we have:*

(i) $C_k = p_k/q_k$;

(ii) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ *for all* $k \geq 1$;

(iii)
$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}} \qquad \text{for } 1 \leq k \leq n;$$

(iv)
$$C_k - C_{k-2} = \frac{(-1)^k a_k}{q_k q_{k-2}} \qquad \text{for } 2 \leq k \leq n.$$

Proof. (i) We use induction over k.
If $k = 0$, then $C_0 = [a_0] = p_0/q_0$.
If $k = 1$, then

$$C_1 = [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}.$$

If $k = 2$, then

$$\begin{aligned} C_2 &= [a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_2(a_0 a_1 + 1) + a_0}{a_2 a_1 + 1} \\ &= \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0} = \frac{p_2}{q_2}. \end{aligned}$$

Let now $k > 2$ and assume that $C_i = p_i/q_i$ for all $i = 0, \ldots, k$. Observe that $p_{k-2}, q_{k-2}, p_{k-1}$ and q_{k-1} depend only on $a_0, \ldots, a_{k-1}$. Thus,

$$\begin{aligned} C_{k+1} &= \left[a_0, a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right] = \frac{(a_k + 1/a_{k+1})p_{k-1} + p_{k-2}}{(a_k + 1/a_{k+1})q_k + q_{k-1}} \\ &= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}. \end{aligned}$$

(ii) If $k = 1$, then

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1)1 - a_0 a_1 = 1.$$

By induction, if $k \geq 2$, then

$$\begin{aligned} p_k q_{k-1} - p_{k-1} q_k &= (a_k p_{k-1} + p_{k-2})q_{k-1} - p_{k-1}(a_k q_{k-1} + q_{k-2}) \\ &= -(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) = -(-1)^{k-2} = (-1)^{k-1}. \end{aligned}$$

(iii) By (i) and (ii), we have that

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{p_k q_{k-1} - p_{k-1} q_k}{q_k q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}.$$

(iv) Finally,

$$C_k - C_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - q_k p_{k-2}}{q_k q_{k-2}},$$

where

$$\begin{aligned} p_k q_{k-2} - q_k p_{k-2} &= (a_k p_{k-1} + p_{k-2})q_{k-2} - (a_k q_{k-1} + q_{k-2})p_{k-2} \\ &= a_k(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) = (-1)^{k-2}a_k. \end{aligned}$$

□

1.3 Infinite continued fractions

Proposition 1.2.1 shows that $C_k < C_{k-2}$ if $k \geq 3$ is odd and $C_k > C_{k-2}$ if $k \geq 2$ is even. Thus,

$$C_1 > C_3 > C_5 > \cdots \qquad \text{and} \qquad C_2 < C_4 < C_6 < \cdots.$$

Furthermore,

$$C_{2m} - C_{2m-1} = \frac{(-1)^{2m-1}}{q_{2m}q_{2m-1}} < 0,$$

therefore,

$$C_1 > C_3 > C_5 > \cdots > C_6 > C_4 > C_2.$$

In particular, if $(a_n)_{n\geq 0}$ is an infinite sequence of integers with $a_n > 0$ for all $n \geq 1$, then setting $C_k = [a_0, \ldots, a_k]$, we infer that:

(i) the sequence $(C_{2n+1})_{n\geq 0}$ is decreasing and bounded, in particular convergent;

(ii) the sequence $(C_{2n})_{n\geq 0}$ is increasing and bounded, in particular convergent;

(iii) the sequence $C_{2n} - C_{2n+1}$ tends to zero.

In particular, $(C_n)_{n\geq 0}$ is convergent. This fact will help us define correctly the infinite continued fractions.

Definition 1.3.1. *Let $(a_n)_{n\geq 0}$ be an infinite sequence of integers with $a_n > 0$ for all $n \geq 1$. Define the infinite continued fraction as the limit of the finite continued fraction*

$$[a_0, a_1, \ldots] := \lim_{n\to\infty} C_n.$$

It is easy to see that the infinite continued fractions always represent irrational numbers. Conversely, every irrational number α can be developed in an infinite continued fraction.

Proposition 1.3.2. *Given $\alpha = \alpha_0 \in \mathbb{R}\backslash\mathbb{Q}$, let $(a_n)_{n\geq 0}$ be defined as*

$$a_k = \lfloor \alpha_k \rfloor, \qquad \alpha_{k+1} = \frac{1}{\alpha_k - a_k} \qquad \text{for all } k \geq 0.$$

Then $\alpha = [a_0, a_1, \ldots]$.

Proof. Clearly,

$$\alpha = \alpha_0 = a_0 + \frac{1}{\alpha_1} = [a_0, \alpha_1] = [a_0, a_1, \alpha_2] = \cdots = [a_0, a_1, \ldots, a_k, \alpha_{k+1}].$$

By (i) of Proposition 1.2.1,

$$\alpha = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}},$$

therefore

$$\begin{aligned} |\alpha - C_k| &= \left|\frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k}\right| = \left|\frac{-(p_kq_{k-1} - q_kp_{k-1})}{(\alpha_{k+1}q_k + q_{k-1})q_k}\right| \\ &= \frac{1}{(\alpha_{k+1}q_k + q_{k-1})q_k} < \frac{1}{q_k^2}. \end{aligned} \tag{2}$$

Since $q_k \geq k$ for $k \geq 1$, we have that $1/q_k^2 \to 0$ as $k \to \infty$, which completes the proof. □

1.4 Convergentes

In this section, we prove that the convergents p_k/q_k of an irrational α give the best approximations of α by rationals.

Proposition 1.4.1. *(i) Let α be an irrational number and let $C_k = p_k/q_k$ for $k \geq 0$ be the convergents of the continued fraction of α. If $r,\ s \in \mathbb{Z}$ with $s > 0$ and k is a positive integer such that*

$$|s\alpha - r| < |q_k\alpha - p_k|,$$

then $s \geq q_{k+1}$.

(ii) If α is irrational and r/s is a rational number with $s > 0$ such that

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2},$$

then r/s is a convergent of α.

Proof. (i) Suppose that $1 \leq s < q_{k+1}$. The system of equations

$$\begin{aligned} p_kx + p_{k+1}y &= r \\ q_kx + q_{k+1}y &= s \end{aligned}$$

gives

$$(p_{k+1}q_k - p_kq_{k+1})x = sp_{k+1} - rq_{k+1}, \qquad (p_kq_{k+1} - p_{k+1}q_k)y = sp_k - rq_k.$$

Using Proposition 1.2.1 (ii), we get that

$$x = (-1)^k(sp_{k+1} - rq_{k+1}), \qquad y = (-1)^k(rq_k - sp_k).$$

We now prove that x and y are nonzero and have opposite signs. If $x = 0$, then $r/s = p_{k+1}/q_{k+1}$. Since p_{k+1} and q_{k+1} are coprime (see Proposition

1.2.1 (ii), for example), we have that $q_{k+1} \mid s$, which contradicts the hypothesis that $1 \leq s < q_{k+1}$. If $y = 0$, then $r = p_k x,\ s = q_k x$, and therefore

$$|s\alpha - r| = |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|,$$

which again leads to a contradiction. Thus, $xy \neq 0$.

Assume now that $y < 0$. Since $q_k x = s - q_{k+1}y$, we have that $x > 0$. If $y > 0$, we then get that $q_{k+1}y \geq q_{k+1} > s$, and therefore $q_k x = s - q_{k+1}y < 0$, which implies that $x < 0$. We already know that

$$\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}} \qquad \text{if } k \equiv 0 \pmod 2,$$

and

$$\frac{p_{k+1}}{q_{k+1}} < \alpha < \frac{p_k}{q_k} \qquad \text{if } k \equiv 1 \pmod 2.$$

In both cases, $q_k\alpha - p_k$ and $q_{k+1}\alpha - p_{k+1}$ have opposite signs, therefore $x(q_k\alpha - p_k)$ and $y(q_{k+1}\alpha - p_{k+1})$ have the same sign. We now get

$$\begin{aligned} |s\alpha - r| &= |(q_k x + q_{k+1}y)\alpha - (p_k x + p_{k+1}y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})| \\ &= |x||q_k\alpha - p_k| + |y||q_{k+1}\alpha - p_{k+1}| \\ &> |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|, \end{aligned}$$

which leads to the desired contradiction.

(ii) Assume that r/s is not a convergent of the continued fraction of α; that is, $r/s \neq p_k/q_k$ for all k. Let k be the largest nonnegative integer such that $s \geq q_k$. Since $q_0 = 1$ and $q_k \to \infty$ as $k \to \infty$, it follows that this integer exists. Since $q_k \leq s < q_{k+1}$, by (i), we have that

$$|q_k\alpha - p_k| \leq |s\alpha - r| = s\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s},$$

and so

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2sq_k}.$$

Since $r/s \neq p_k/q_k$, we have that $|sp_k - rq_k| \geq 1$, therefore

$$\frac{1}{sq_k} \leq \frac{|sp_k - rq_k|}{sq_k} = \left|\frac{p_k}{q_k} - \frac{r}{s}\right| \leq \left|\frac{p_k}{q_k} - \alpha\right| + \left|\alpha - \frac{r}{s}\right| < \frac{1}{2sq_k} + \frac{1}{2s^2},$$

which implies that

$$\frac{1}{2sq_k} < \frac{1}{2s^2},$$

therefore $q_k > s$, which is a contradiction. □

Part (ii) of Proposition 1.4.1 is known as Legendre's criterion for a rational r/s to be a convergent of α. This result was generalized by several authors. We give a couple of examples in what follows.

Let $C_k = p_k/q_k$ be a convergent of the continued fraction of α. For each $n \geq 0$ we define

$$p_{k,n} = np_{k+1} + p_k, \qquad q_{k,n} = nq_{k+1} + q_k.$$

If $n = 0$, then $p_{k,n} = p_k$ and $q_{k,n} = q_k$. If $n = a_{k+2}$, then $p_{k,n} = p_{k+2}$ and $q_{k,n} = q_{k+2}$. If $1 \leq n \leq a_{k+2} - 1$, then the amount

$$\frac{p_{k,n}}{q_{k,n}} = \frac{np_{k+1} + p_k}{nq_{k+1} + q_k}$$

is called an *intermediary convergent* of $\alpha = [a_0, a_1, \ldots]$.

We have the following results.

Proposition 1.4.2. *If $r,\ s > 0$ are integers such that*

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^2},$$

then r/s is either a convergent or an intermediary convergent of α. In fact, $r/s = p_{k,n}/q_{k,n}$ with $n = 0,\ 1$ or $a_{k+2} - 1$.

For the proof, see either [38], or Theorem 1.10 in [40].

Proposition 1.4.3. *Let α be an irrational and let $r,\ s \geq 2$ be integers such that*

$$\left|\alpha - \frac{r}{s}\right| < \frac{2}{s^2}.$$

Then

$$\frac{r}{s} \in \left\{ \frac{p_k}{q_k}, \frac{p_{k+1} \pm p_k}{q_{k+1} \pm q_k}, \frac{2p_{k+1} \pm p_k}{2q_{k+1} \pm q_k}, \frac{3p_{k+1} \pm p_k}{3q_{k+1} \pm q_k}, \frac{p_{k+1} \pm 2p_{k+1}}{q_{k+1} \pm 2q_k}, \frac{p_{k+1} - 3p_k}{q_{k+1} - 3q_k} \right\}$$

for some $k \geq 0$.

For a proof of Proposition 1.4.3 above, see either [26] or [81]. The following result is a variation of a lemma of Baker and Davenport [3] and is due to Dujella and Pethő [27]. For a real number x we use $\|x\| = \min\{|x - n| : n \in \mathbb{Z}\}$ for the distance from x to the nearest integer.

Lemma 1.4.4. *Let M be a positive integer and p/q be a convergent of the continued fraction of the irrational γ such that $q > 6M$ and let μ be some real number. Let $\varepsilon = \|\mu q\| - M\|\gamma q\|$. If $\varepsilon > 0$, then there is no solution to the inequality*

$$0 < m\gamma - n + \mu < AB^{-m}$$

in positive integers m and n with

$$\frac{\log(Aq/\varepsilon)}{\log B} \leq m \leq M.$$

Proof. Suppose that $0 \leq m \leq M$. Then

$$m(\gamma q - p) + mp - nq + \mu q < qAB^{-m}.$$

Thus,

$$qAB^{-m} > |\mu q - (nq - mp)| - m\|\gamma q\| \geq \|\mu q\| - M\|\gamma q\| := \varepsilon,$$

from where we get

$$m < \frac{\log(Aq/\varepsilon)}{\log B}.$$

□

1.5 Quadratic Irrationalities

Let α be real quadratic irrational. That is, $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ is a root of an equation of the form

$$Ax^2 + Bx + C = 0 \qquad \text{with} A,\ B,\ C \in \mathbb{Z},\ A \neq 0.$$

Thus, we can write $\alpha = (a + b\sqrt{e})/f$, with integers $a,\ b,\ e,\ f$ such that $e > 0$ is not a perfect square. We can take

$$a = -B, \quad b = 1, \quad e = B^2 - 4AC \quad y \quad f = 2A.$$

Note that

$$\alpha = \frac{a + b\sqrt{e}}{f} = \frac{af + \sqrt{eb^2f^2}}{f^2} = \frac{P_0 + \sqrt{d}}{Q_0}$$

with $P_0 = af,\ Q_0 = f^2$ and $d = eb^2f^2$ is a representation of α with integers $P_0,\ Q_0,\ d$, where d is not a perfect square, and such that $Q_0 \mid d - P_0^2$.

We define recursively

$$\begin{aligned} \alpha_k &= \frac{P_k + \sqrt{d}}{Q_k}, \\ a_k &= \lfloor \alpha_k \rfloor, \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k}, \end{aligned} \tag{3}$$

for $k = 0,\ 1,\ \ldots$. We have the following result.

Proposition 1.5.1. *The continued fraction* $[a_0, a_1, \ldots]$ *defined in* (3) *above is the continued fraction of* α.

Proof. Let $k \geq 0$ and assume that P_k and Q_k are integers with $Q_k \mid d - P_k^2$. Then $P_{k+1} = a_k Q_k - P_k$ is an integer and

$$d - P_{k+1}^2 = d - (a_k Q_k - P_k)^2 = (d - P_k^2) + Q_k(2a_k P_k - a_k^2 Q_k) \equiv 0 \pmod{Q_k}.$$

Thus, $Q_{k+1} = (d - P_{k+1}^2)/Q_k$ is an integer which clearly satisfies $Q_{k+1} \mid d - P_{k+1}^2$. Since d is not a perfect square, the sequences $(P_k)_{k\geq 0}$ y $(Q_k)_{k\geq 0}$ are well-defined. Finally,

$$\begin{aligned} \alpha_k - a_k &= \frac{P_k + \sqrt{d}}{Q_k} - a_k = \frac{\sqrt{d} - (a_k Q_k - P_k)}{Q_k} = \frac{\sqrt{d} - P_{k+1}}{Q_k} \\ &= \frac{d - P_{k+1}^2}{Q_k(\sqrt{d} + P_{k+1})} = \frac{Q_k Q_{k+1}}{Q_k(\sqrt{d} + P_{k+1})} = \frac{1}{\alpha_{k+1}}. \end{aligned}$$

In particular, $\alpha_{k+1} > 0$. Moreover, $\alpha_k = [a_k, \alpha_{k+1}]$. Applying the above formula with $k = 0, 1, \ldots$, we have that

$$\alpha = \alpha_0 = [a_0, \alpha_1] = [a_0, a_1, \alpha_1] = \ldots = [a_0, a_1, \ldots].$$

□

The continued fraction $[a_0, a_1, \ldots]$ is called *periodic* if there exist h and n such that $a_m = a_{m+h}$ holds for all $m \geq n$. If h and n are minimal with the above property, then we write

$$[a_0, a_1, \ldots] = [a_0, a_1, \ldots, a_{n-1}, \overline{a_n, a_{n+1}, \ldots, a_{n+h-1}}] \tag{4}$$

Proposition 1.5.2. *An irrational* α *is quadratic if and only if its continued fraction is periodic.*

Proof. Assume that α is quadratic. We use the notations (3). By Proposition 1.5.1, for each $k \geq 2$ we have that

$$\alpha = [a_0, a_1, \ldots, a_{k-1}, \alpha_k] = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}.$$

Conjugating, we have that

$$\alpha' = \frac{\alpha'_k p_{k-1} + p_{k-2}}{\alpha'_k q_{k-1} + q_{k-2}}, \tag{5}$$

where $\alpha' = (P_0 - \sqrt{d})/Q_0$ and $\alpha'_k = (P_k - \sqrt{d})/Q_k$. From formula (5), we infer that

$$\alpha'_k = -\frac{q_{k-2}}{q_{k-1}} \left(\frac{\alpha' - C_{k-2}}{\alpha' - C_{k-1}} \right).$$

Since $C_k \to \alpha$ as $k \to \infty$, we get that $\alpha'_k < 0$ if k is sufficiently large. Since $\alpha_k > 0$, we get that $\alpha_k - \alpha'_k = 2\sqrt{d}/Q_k > 0$ for all large k. Since $Q_k Q_{k+1} = d - P_{k+1}^2$, we obtain that $P_{k+1}^2 < d$ for all large k. Thus, the set $\{P_k : k \geq 0\}$ is finite, and since $Q_k \mid d - P_k^2$, we have that the set $\{Q_k : k \geq 0\}$ is also finite. Since $a_i = \lfloor (P_i + \sqrt{d})/Q_i \rfloor$, we conclude that there exist $i < j$ such that $a_i = a_j$. Since the numbers $(a_k)_{k \geq 0}$ are defined recursively, we get that

$$\alpha = [a_0, \ldots, a_{i-1}, \overline{a_i, \ldots, a_{j-1}}].$$

Conversely, let $\alpha = [a_0, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+h-1}}]$ be a number whose continued fraction is periodic. Put $\beta = [\overline{a_{n+1}, \ldots, a_{n+h-1}}]$. Clearly,

$$\beta = [a_n, \ldots, a_{n+h-1}, \beta] = \frac{\beta p'_{h-1} + p'_{h-2}}{\beta q'_{h-1} + q'_{h-2}},$$

where p'_k/q'_k is the kth convergent of β. Thus,

$$q'_{h-1}\beta^2 + (q'_{h-2} - p'_{h-1})\beta - p'_{h-2} = 0, \tag{6}$$

showing that β is either quadratic or rational. Since

$$\alpha = [a_0, \ldots, a_{n-1}, \beta] = \frac{\beta p_{n-1} + p_{n-2}}{\beta q_{n-2} + q_{n-1}},$$

we deduce that α is also either quadratic or rational. Finally, let us note that α is not rational because its continued fraction is not finite. $\square$

Observe that the main ingredient of the previous proof was the fact that $\alpha'_k \in (-1,0)$ if k is large enough. Since $\alpha_{k+1} = 1/(\alpha_k - a_k)$, we get that if $\alpha'_k \in (-1,0)$, then $\alpha'_{k+1} = 1/(\alpha'_k - a_k) \in (-1,0)$ also.

Definition 1.5.3. *The quadratic number α is called reduced if $\alpha > 1$ and $\alpha' \in (-1,0)$.*

The next result is due to Galois.

Proposition 1.5.4. *A quadratic irrational $\alpha > 1$ is reduced if and only if its continued fraction is purely periodic.*

Proof. Suppose that the continued fraction of α is purely periodic of period h. Formula (6) tells us that α is a root of the polynomial

$$f(x) = q_{h-1}x^2 + (q_{h-2} - p_{h-1})x - p_{h-2}.$$

It is clear that $f(0) = -p_{h-2} < 0$ and $f(-1) = (q_{h-1} - q_{h-2}) + (p_{h-1} - p_{h-2}) > 0$, so that $f(x)$ has another root in $(-1,0)$. It is also clear that this root is α'.

Conversely, if $\alpha'_0 = \alpha' \in (-1,0)$, then by the remark before Definition 1.5.3, we have that $\alpha'_k \in (-1,0)$ for all $k \geq 0$. Suppose that the continued fraction of α is given by (6) and it is not purely periodic. In particular, $n > 1$ and $a_{n-1} \neq a_{n+h-1}$ (for if not, then the period would start earlier). However, $\alpha_n = \alpha_{n+h}$, which gives us

$$\alpha_{n-1} - \alpha_{n-1+h} = \left(a_{n-1} + \frac{1}{\alpha_n}\right) - \left(a_{n+h-1} + \frac{1}{\alpha_{n+h}}\right) = a_{n-1} - a_{n+h-1} \in \mathbb{Z}.$$

Conjugating, we get that $\alpha'_{n-1} - \alpha'_{n-1+h} \in \mathbb{Z}$, but this last number is in $(-1,1)$. We infer that $\alpha'_{n-1} = \alpha'_{n-1+h}$, so $\alpha_{n-1} = \alpha_{n-1+h}$. Then, $a_{n-1} = a_{n-1+h}$, which is the desired contradiction. □

Corollary 1.5.5. *If $\alpha = [\overline{a_0, \ldots, a_{h-1}}]$, then $-1/\alpha' = [\overline{a_{h-1}, \ldots, a_0}]$.*

Proof. We have

$$\alpha_0 = a_0 + \frac{1}{\alpha_1}, \quad \alpha_1 = a_1 + \frac{1}{\alpha_2}, \quad \ldots \quad \alpha_{h-1} = a_{h-1} + \frac{1}{\alpha_0}.$$

Conjugating, we get

$$\alpha'_0 = a_0 + \frac{1}{\alpha'_1}, \quad \alpha'_1 = a_1 + \frac{1}{\alpha'_2}, \quad \ldots \quad \alpha_{h-1} = a_{h-1} + \frac{1}{\alpha'_0}.$$

Solving the above equations in the opposite order, we get

$$-\frac{1}{\alpha'_0} = a_{h-1} - \alpha'_1, \quad -\frac{1}{\alpha'_1} = a_{h-2} - \alpha'_2, \quad \dots \quad -\frac{1}{\alpha'_1} = a_0 - \alpha'_0.$$

Since each one of the numbers $-1/\alpha'_k$ is > 1, by Proposition 1.5.4, we get that $-1/\alpha'_0 = [\overline{a_{h-1}, a_{h-2}, \dots, a_0}]$. □

The next result is due to Legendre.

Proposition 1.5.6. *Let $d > 1$ be a rational which is not a perfect square. Then*

$$\sqrt{d} = [a_0, \overline{a_1, \dots, a_1, 2a_0}].$$

Proof. It is clear that $a_0 = \lfloor \sqrt{d} \rfloor$. Furthermore, since $\alpha = \lfloor \sqrt{d} \rfloor + \sqrt{d} = a_0 + \sqrt{d}$ satisfies the conditions that $\alpha > 1$ and $\alpha' = a_0 - \sqrt{d} \in (-1, 0)$, we infer that α is reduced. Thus, the continued fraction of α is purely periodic. Let us write $\alpha = [\overline{2a_0, a_1, \dots, a_{h-1}}]$. Furthermore, $\alpha_1 = 1/(\sqrt{d} - a_0)$, therefore $-1/\alpha'_1 = a_0 + \sqrt{d} = \alpha$. Since $\alpha_1 = [\overline{a_1, \dots, a_h}]$, Corollary 1.5.5 implies that $-1/\alpha'_1 = [\overline{a_h, a_{h-1}, \dots, a_1}]$. Identifying the continued fractions of α and $-1/\alpha'_1$, we get

$$a_h = 2a_0, \quad a_{h-1} = a_1, \quad \dots \quad a_1 = a_{h-1},$$

which implies the desired conclusion. □

Example 1.5.7. *To find the continued fraction of $\sqrt{11/7}$, we write it as*

$$\sqrt{\frac{11}{7}} = \frac{0 + \sqrt{77}}{7}.$$

Thus, $Q_0 = 7,\ P_0 = 0,\ D = 77$ satisfy $Q_0 \mid D - P_0^2$. Proceeding as in (3)*, we get*

$$\sqrt{\frac{11}{7}} = [1, \overline{3, 1, 16, 1, 3, 2}],$$

where

k	0	1	2	3	4	5	6
P_k	0	7	5	8	8	5	7
Q_k	7	4	13	1	13	4	7.

Similarly, we have

$$\sqrt{\frac{29}{17}} = [1, \overline{3, 3, 1, 2, 1, 14, 14, 1, 2, 1, 3, 3, 2}].$$

1.6 Pell Equations

In this section, we present some applications of the theory of continued fractions to the Pell equations, which are equations in integers (x, y) of the form

$$x^2 - dy^2 = N, \tag{7}$$

where $d > 1$ is not a perfect square and $N \neq 0$. It is clear that we can assume that x and y positive.

If $N \geq 1$, we factor equation (7) en positive factors

$$(x - \sqrt{d}y)(x + \sqrt{d}y) = N,$$

to obtain

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

and therefore

$$0 < \frac{x}{y} - \sqrt{d} < \frac{N}{2y^2\sqrt{d}}. \tag{8}$$

If $N < 0$, we rewrite equation (7) as

$$y^2 - \frac{1}{d}x^2 = -\frac{N}{d},$$

to interchange the roles of x and y and obtain an equation in which the right hand side is positive. Proceeding as before, we get

$$\left(y - \frac{x}{\sqrt{d}}\right)^2 + \left(y - \frac{x}{\sqrt{d}}\right)\left(\frac{2x}{\sqrt{d}}\right) = -\frac{N}{d},$$

therefore

$$0 < \frac{y}{x} - \frac{1}{\sqrt{d}} < \frac{-N}{2x^2\sqrt{d}}. \tag{9}$$

In both cases, since $0 < |N| < \sqrt{d}$, we infer, by Proposition 1.4.1 (ii), that x/y is a convergent of $\sqrt{d}$ if $N > 0$, and that y/x is a convergent of $1/\sqrt{d} = [0, \sqrt{d}]$ if $N < 0$. However, this last condition is equivalent with the fact that x/y is a convergent of $\sqrt{d}$. Thus, we have just proved the following result.

Theorem 1.6.1. *If $0 < |N| < \sqrt{d}$, then all the solutions (x, y) in positive integers of the equation de (7) have the property that x/y is a convergent of $\sqrt{d}$.*

By Theorem 1.6.1, it seems of interest to study the amount $p_k^2 - dq_k^2$ for the convergents p_k/q_k of $\sqrt{d}$.

Proposition 1.6.2. *If $d > 1$ is an integer which is not a square and $\alpha = \alpha_0 = \sqrt{d}$, then*

$$p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q_k.$$

Proof. Observe that $P_0 = 0$, $Q_0 = 1$, $P_1 = \lfloor\sqrt{d}\rfloor$ and $Q_1 = d - P_0^2 = d - \lfloor\sqrt{d}\rfloor^2$. Thus, $p_0^2 - dq_0^2 = \lfloor\sqrt{d}\rfloor^2 - d = -Q_1$. Assume that $k \geq 2$. We write

$$\sqrt{d} = \alpha = [a_0, \ldots, a_{k-1}, \alpha_k] = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}.$$

Since $\alpha_k = (P_k + \sqrt{d})/Q_k$, we get that

$$\sqrt{d} = \frac{(P_k + \sqrt{d})p_{k-1} + Q_k p_{k-2}}{(P_k + \sqrt{d})q_{k-1} + Q_k q_{k-2}},$$

that is,

$$dq_{k-1} + \sqrt{d}(P_k q_{k-1} + Q_{k-1} q_{k-2}) = P_k p_{k-1} + Q_k p_{k-2} + p_{k-1}\sqrt{d}.$$

Identifying coefficients, we get that

$$\begin{aligned} dq_{k-1} &= P_k p_{k-1} + Q_k p_{k-2}, \\ p_{k-1} &= P_k q_{k-1} + Q_k q_{k-2}. \end{aligned}$$

Finally,

$$\begin{aligned} p_{k-1}^2 - dq_{k-1}^2 &= (P_k q_{k-1} + Q_k q_{k-2})p_{k-1} - (P_k p_{k-1} + Q_k p_{k-2})q_{k-1} \\ &= (p_{k-1}q_{k-2} - p_{k-2}q_{k-1})Q_k = (-1)^k Q_k. \end{aligned}$$

□

The following result classifies all the solutions of the Pell equation (7) when $N = \pm 1$.

Proposition 1.6.3. *Let h be the period of the continued fraction of $\sqrt{d}$. Then $Q_k = 1$ if and only if $h \mid k$.*

Proof. Since there are h terms, $\alpha_1 = \alpha_{h+1}$ and $\alpha_0, \alpha_1, \ldots, \alpha_{h-1}$ are distinct. Thus,

$$\alpha_h = 2a_0 + \frac{1}{\alpha_{h+1}} = 2a_0 + \frac{1}{\alpha_1} = 2a_0 + (\sqrt{d} - a_0) = \sqrt{d} + a_0.$$

But $\alpha_h = (P_h + \sqrt{d})/Q_h$. If $Q_h > 1$, then $P_h - a_0 Q_h = (Q_h - 1)\sqrt{d} \notin \mathbb{Q}$, which is impossible. Thus, $Q_h = 1$ and the same argument proves that $Q_k = 1$ for all multiples k of h.

Assume now that $Q_k = 1$. Then $\alpha_k = P_k + \sqrt{d}$. Since α_k is purely periodic, $\alpha_k' \in (-1, 0)$, therefore $P_k - \sqrt{d} \in (-1, 0)$. We conclude that $P_k = \lfloor \sqrt{d} \rfloor = a_0$. Thus, $\alpha_k = \alpha_h$ which implies that k is a multiple of h. □

Corollary 1.6.4. *The equation $x^2 - dy^2 = 1$ has infinitely many integer solutions (x, y). The equation $x^2 - dy^2 = -1$ has one integer solution (x, y) (and so, infinitely many) if and only if the period h of the continued fraction of $\sqrt{d}$ is odd.*

The next result describes all the solutions of the Pell equation (7) when $N = \pm 1$.

Theorem 1.6.5. *Let h be the period of the continued fraction of $\sqrt{d}$. Then all positive integer solutions (x, y) of the Pell equation (7) with $N = \pm 1$ are given by*

$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^\ell \qquad \text{for all integers } \ell \geq 1,$$

where $x_1 + y_1\sqrt{d} = p_{h-1} + q_{h-1}\sqrt{d}$.

Proof. The minimal solution (x_1, y_1) of the equation $x^2 - dy^2 = \pm 1$ is $x/y = p_{h-1}/q_{h-1}$ by Theorem 1.6.1 and Propositions 1.6.2 y 1.6.3. Given $\ell \geq 1$, we write

$$x_\ell + \sqrt{d} y_\ell = (x_1 + \sqrt{d} y_1)^\ell. \tag{10}$$

Conjugating, we get

$$x_\ell - \sqrt{d} y_\ell = (x_1 - \sqrt{d} y_1)^\ell. \tag{11}$$

Multiplying relations (10) and (11), we get

$$x_\ell^2 - d y_\ell^2 = (x_1^2 - d y_1^2)^\ell = \pm 1.$$

In fact, $x_\ell^2 - d y_\ell^2 = (-1)^\ell$ if h is odd and is 1 otherwise. To see that all the positive integer solutions of the Pell equation (7) with $N = \pm 1$ are obtained in this way, we proceed by contradiction. Suppose that

$$X^2 - dY^2 = \pm 1$$

holds with some positive integers $(X, Y) \neq (x_\ell, y_\ell)$ for all $\ell \geq 1$. Let ℓ be such that

$$(x_1 + \sqrt{d} y_1)^\ell < X + \sqrt{d} Y < (x_1 + \sqrt{d} y_1)^{\ell+1}. \tag{12}$$

Let

$$\begin{aligned} X_1 + \sqrt{d}Y_1 &:= (X + \sqrt{d}Y)(x_1 + \sqrt{d}y_1)^{-\ell} = (X + \sqrt{d}Y)(x_\ell + \sqrt{d}y_\ell)^{-1} \\ &= \pm(X + \sqrt{d}Y)(x_\ell - \sqrt{d}y_\ell) \\ &= \pm(Xx_\ell - dYy_\ell) \pm \sqrt{d}(x_\ell Y - Xy_\ell). \end{aligned}$$

Here, we put $(X_1, Y_1) = \pm(Xx_\ell - Yy_\ell, x_\ell Y - Xy_\ell)$. By inequality (12), we have that

$$1 < X_1 + \sqrt{d}Y_1 < x_1 + \sqrt{d}y_1.$$

Furthermore, conjugating and multiplying, we get that

$$X_1^2 - dY_1^2 = (X^2 - dY^2)(x_1^2 - dy_1^2)^\ell = \pm 1,$$

therefore $|X_1 - \sqrt{d}Y_1| \in (0, 1)$. We conclude that $X_1 - \sqrt{d}Y_1 < X_1 + \sqrt{d}Y_1$, which implies that $Y_1 > 0$. If $X_1 < 0$, then $X_1 - Y_1\sqrt{d} \leq -1 - \sqrt{d}$, which is impossible because this number is < 1 in absolute value. Thus, $X_1 > 0$. We have therefore obtained a positive integer solution (X_1, Y_1) of the Pell equation (7) with $N = \pm 1$ such that $X_1 + \sqrt{Y_1} < x_1 + \sqrt{d}y_1$, which is impossible. This completes the proof of the theorem. □

1.7 Problems

Problem 1.7.1. *Prove that if a and b are positive integers such that $(a^2 + b^2)/(ab + 1) = k \in \mathbb{Z}$, then k is a perfect square.*

Problem 1.7.2. *Let x and y be positive integers such that $xy \mid x^2 + y^2 + 1$. Prove that*

$$\frac{x^2 + y^2 + 1}{xy} = 3.$$

Problem 1.7.3. *Find infinitely many pairs of integers (a, b) with $1 < a < b$ such that $ab \mid a^2 + b^2 - 1$. What are the possible values of the quotient $(a^2 + b^2 - 1)/ab$?*

Problem 1.7.4. *Let n be a positive integer such that $2 + 2\sqrt{28n^2 + 1} = k$. Prove that k is a perfect square.*

Problem 1.7.5. *Let (x_ℓ, y_ℓ) be the ℓth solution of the Pell equation $x^2 - dy^2 = \pm 1$. For a positive integer m let $P(m)$ be the largest prime factor of m. Prove that if $P(x_\ell) \leq 5$, then $\ell = 1$.*

Problem 1.7.6. *Find all the integer solutions (n, x) of the equation*

$$(2^n - 1)(3^n - 1) = x^2.$$

Problem 1.7.7. *Find all the integer solutions (n, x) of the equation*

$$(2^n - 1)(6^n - 1) = x^2.$$

Problem 1.7.8. *Prove that there is no odd $n > 1$ and two divisors d_1 and d_2 of $(n^2 + 1)/2$ such that $d_1 + d_2 = n + 1$.*

Problem 1.7.9. *Let $d > 1$ be an integer which is not a perfect square and let (x_ℓ, y_ℓ) be the ℓth positive integer solution of the equation $x^2 - dy^2 = \pm 1$. Prove that there exist two polynomials $P_\ell(x),\ Q_\ell(x) \in \mathbb{Z}[x]$ of degrees ℓ and $\ell - 1$, respectively, such that $x_\ell = P_\ell(x_1)$ and $y_\ell/y_1 = Q_{\ell-1}(x_1)$.*

Problem 1.7.10. *Let $d > 1$ be an integer which is not a perfect square and let h be the period of the continued fraction of $\sqrt{d}$. Prove that $h = O(\sqrt{d} \log d)$.*

1.8 Notes

The minimal positive integer solution (x_1, y_1) of the Pell equation (7) with $N = \pm 1$ satisfies $x_1 + \sqrt{d}y_1 < e^{3\sqrt{d}\log d}$ (see Theorem 13.5 on page 329 en [37]). Some times it actually is large; for example,

$$1766319049^2 - 61 \cdot 226153980^2 = 1$$

is the smallest solution for $d = 61$. Problem 1.7.1 is Problem 6 from the 1988 IMO (see [55] for a solution using continued fractions). For the problems 1.7.3 and 1.7.4, see the first chapter of [80]. For Problem 1.7.5, see [44]. For Problems 1.7.6 and 1.7.7, see [78], [36], and [58]. Problem 1.7.8 is a result of Ayad and Luca [1]. The published paper contains a small oversight which was observed and corrected by Dujella. The two polynomials from Problem 1.7.9 are related to the Chebyshef polynomials $T_\ell(x) = \cos(\ell \arccos(x))$. For Problem 1.7.10, see [14], or Theorem 1 on page 50 in [68].

Chapter 2

Binary recurrent sequences

Definition 2.0.1. *Let $k \geq 1$ be an integer. A sequence $(u_n)_{n\geq 0} \subseteq \mathbb{C}$ is called linearly recurrent of order k if the recurrence*

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n \tag{1}$$

holds for all $n \geq 0$ with some fixed coefficients $a_1, \ldots, a_k \in \mathbb{C}$.

Let us suppose that $a_k \neq 0$ (for if not, the sequence $(u_n)_{n\geq 0}$ satisfies a linear recurrence of order smaller than k). If $a_1, \ldots, a_k \in \mathbb{Z}$ and $u_0, \ldots, u_{k-1} \in \mathbb{Z}$, then, by induction on n, we get that u_n is an integer for all $n \geq 0$. The polynomial

$$f(X) = X^k - a_1 X^{k-1} - \cdots - a_k \in \mathbb{C}[X]$$

is called the *characteristic polynomial* $(u_n)_{n\geq 0}$. Suppose that

$$f(X) = \prod_{i=1}^{s} (X - \alpha_i)^{\sigma_i},$$

where $\alpha_1, \ldots, \alpha_s$ are the distinct roots of $f(X)$ with multiplicities $\sigma_1, \ldots, \sigma_s$, respectively.

Proposition 2.0.2. *Suppose that $f(X) \in \mathbb{Z}[X]$ has distinct roots. Then there exist constants $c_1, \ldots, c_k \in \mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ such that the formula*

$$u_n = \sum_{i=1}^{k} c_i \alpha_i^n \qquad \text{holds for all } n \geq 0. \tag{2}$$

Proof. Let

$$u(z) = \sum_{n\geq 0} u_n z^n.$$

We observe that

$$\begin{aligned} u(z)(1 - a_1 z - \cdots - a_k z^k) &= u_0 + (u_1 - u_0 a_1)z + (u_2 - u_1 a_1 - u_2 a_0)z^2 \\ &+ \cdots + \sum_{m\geq k} (u_m - a_1 u_{m-1} - \cdots - a_k u_{m-k}) z^m \\ &:= P(z), \end{aligned}$$

where $P(z) = \sum_{m=0}^{k-1}(u_m - a_1 u_{m-1} - \cdots - a_m u_0)z^m \in \mathbb{C}[z]$. Thus,

$$\begin{aligned} u(z) &= \frac{P(z)}{1 - a_1 z - \cdots - a_k z^k} = \frac{P(z)}{z^k f(1/z)} = \frac{P(z)}{z^k \prod_{i=1}^k (1/z - \alpha_i)} \\ &= \frac{P(z)}{\prod_{i=1}^k (1 - z\alpha_i)} = \sum_{i=1}^k \frac{c_i}{1 - z\alpha_i} \end{aligned}$$

for some coefficients $c_i \in \mathbb{K}$. For the last step we have used the theory of the partial fractions together with the fact that the roots $\alpha_1, \ldots, \alpha_k$ are distinct and the degree of $P(z)$ is smaller than k. If

$$|z| < \rho := \min\{|\alpha_i|^{-1} : i = 1, \ldots, k\},$$

then we can write

$$\frac{1}{1 - z\alpha_i} = \sum_{n\geq 0} (z\alpha_i)^n = \sum_{n\geq 0} \alpha_i^n z^n \qquad \text{for all } n \geq 0.$$

Thus, for $|z| < \rho$ we get that

$$\sum_{n\geq 0} u_n z^n = u(z) = \sum_{i=1}^k c_i \sum_{n\geq 0} \alpha_i^n z^n = \sum_{n\geq 0} \left(\sum_{i=1}^k c_i \alpha_i^n \right) z^n.$$

Identifying coefficients, we get the relation (2). □

If $k = 2$, the sequence $(u_n)_{n\geq 0}$ is called *binary recurrent*. In this case, its characteristic polynomial is of the form

$$f(X) = X^2 - a_1 X - a_2 = (X - \alpha_1)(X - \alpha_2).$$

Suppose that $\alpha_1 \neq \alpha_2$. Proposition 2.0.2 tells us that

$$u_n = c_1 \alpha_1^n + c_2 \alpha_2^n \qquad \text{for all } n \geq 0. \tag{3}$$

Definition 2.0.3. *A binary recurrent sequence $(u_n)_{n\geq 0}$ whose general term is given by formula* (3) *is called nondegenerate if $c_1 c_2 \alpha_1 \alpha_2 \neq 0$ and α_1/α_2 is not a root of* 1.

2.1 Examples of binary recurrent sequences

2.1.1 The Fibonacci and Lucas sequences

The Fibonacci sequence $(F_n)_{n\geq 0}$ is given by $F_0 = 0,\ F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. Its characteristic equation is

$$f(X) = X^2 - X - 1 = (X - \alpha)(X - \beta),$$

where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. In order to find c_1 and c_2 starting with formula (3), we give to n the values 0 and 1 and obtain the system

$$c_1 + c_2 = F_0 = 0, \qquad c_1\alpha + d_1\beta = F_1 = 1.$$

Solving it, we get $c_1 = 1/\sqrt{5},\ c_2 = -1/\sqrt{5}$. Since $\sqrt{5} = (\alpha - \beta)$, we can write

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{for all } n \geq 0. \tag{4}$$

A sequence related to the Fibonacci sequence is the Lucas sequence $(L_n)_{n\geq 0}$ given by $L_0 = 2,\ L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$. It has the same characteristic equation as the Fibonacci sequence, therefore there exist two constants d_1 and d_2 such that

$$L_n = d_1\alpha^n + d_2\beta^n \qquad \text{for all } n \geq 0.$$

Giving to n the values 0 and 1, we get that

$$d_1 + d_2 = L_0 = 2, \qquad d_1\alpha + d_2\beta = L_1 = 1.$$

Solving the above system of linear equations, we see that $d_1 = d_2 = 1$, and so

$$L_n = \alpha^n + \beta^n \qquad \text{for all } n \geq 0. \tag{5}$$

Using the formulas (4) and (5), one can easily prove various formulas which involve F_n and L_n.

Example 2.1.1. *The formula*

$$L_n^2 - 5F_n^2 = 4(-1)^n$$

holds for all $n \geq 0$. In fact,

$$\begin{aligned} L_n^2 - 5F_n^2 &= (\alpha^n + \beta^n)^2 - 5\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^2 \\ &= (\alpha^n + \beta^n)^2 - (\alpha^n - \beta^n)^2 = 4(\alpha\beta)^n = 4(-1)^n, \end{aligned}$$

where we used the fact that $(\alpha - \beta)^2 = 5$.

2.1.2 Binary recurrences associated to Pell equations with $N = \pm 1$

Let $d > 1$ be an integer which is not a perfect square and let (x_1, y_1) be the minimal solution in positive integers of the equation

$$x^2 - dy^2 = \pm 1. \tag{6}$$

We put

$$\zeta = x_1 + \sqrt{d}y_1 \qquad \text{and} \qquad \eta = x_1 - \sqrt{d}y_1.$$

Theorem 1.6.5 tells us that all positive integer solutions (x, y) of the equation (6) are of the form $(x, y) = (x_\ell, y_\ell)$ for some positive integer ℓ, where

$$x_\ell + \sqrt{d}y_\ell = (x_1 + \sqrt{d}y_1)^\ell = \zeta^\ell.$$

Conjugating the above relation, we get

$$x_\ell - \sqrt{d}y_\ell = (x_1 - \sqrt{d}y_1)^\ell = \eta^\ell.$$

From here, we deduce that

$$x_\ell = \frac{\zeta^\ell + \eta^\ell}{2} \qquad \text{and} \qquad y_\ell = \frac{\zeta^\ell - \eta^\ell}{2\sqrt{d}} \qquad \text{for all } \ell \geq 1. \tag{7}$$

It turns out to be useful to put $(x_0, y_0) = (1, 0)$ so that formula (7) holds also with $\ell = 0$.

It is easy to see that $(x_\ell)_{\ell \geq 0}$ and $(y_\ell)_{\ell \geq 0}$ are binary recurrent sequences of characteristic equation

$$\begin{aligned} f(X) &= X^2 - a_1 X - a_2 = (X - \zeta)(X - \eta) \\ &= X^2 - (\zeta + \eta)X + \zeta\eta = X^2 - 2x_1 X \pm 1. \end{aligned}$$

2.1.3 Binary recurrences associated to Pell equations with $N \neq \pm 1$

Let $d > 1$ be an integer which is not a perfect square and let N be a nonzero integer. Let (u, v) be a positive integer solution of the equation

$$u^2 - dv^2 = N. \tag{8}$$

We saw in Chapter 1 that if $0 < |N| < \sqrt{d}$, then u/v is a convergent of $\sqrt{d}$. In this section, we shall see that for all fixed N all the positive integer solutions (u, v) (if any), belong to a finite set of binary recurrent sequences.

Theorem 2.1.2. *Let $d > 1$ be an integer which is not a perfect square and let $N \neq 0$. Then all the positive integer solutions (u, v) of the equation (8) belong to a finite set of binary recurrent sequences. These sequences have the same characteristic equation $X^2 - 2x_1X + 1$, where (x_1, y_1) is the minimal solution in positive integers of the equation $x^2 - dy^2 = 1$.*

Proof. Let us observe first that if there is a solution (u_0, v_0) of the equation (8), then there are infinitely many of them. In fact, let (x_1, y_1) be the minimal solution of $x^2 - dy^2 = 1$, and put $\zeta = x_1 + \sqrt{d}y_1,\ \eta = x_1 - \sqrt{d}y_1$. Putting

$$u_\ell + \sqrt{d}v_\ell = (u_0 + \sqrt{d}v_0)\zeta^\ell$$

and conjugating, we get

$$u_\ell - \sqrt{d}v_\ell = (u_0 - \sqrt{d}v_0)\eta^\ell.$$

Multiplying the two relations above we get

$$u_\ell^2 - dv_\ell^2 = (u_0^2 - dv_0^2)(\zeta\eta)^\ell = N,$$

from where we read that (u_ℓ, v_ℓ) is also a solution of the Pell equation (8). Observe that

$$u_\ell = \frac{c_1\zeta^\ell + c_2\eta^\ell}{2} \qquad \text{and} \qquad v_\ell = \frac{c_1\zeta^\ell - c_2\eta^\ell}{2\sqrt{d}},$$

where $c_1 = u_0 + \sqrt{d}v_0$ and $c_2 = u_0 - \sqrt{d}v_0$. The sequences $(u_\ell)_{\ell\geq 0}$ and $(v_\ell)_{\ell\geq 0}$ are both binary recurrent of characteristic equation

$$f(X) = (X - \zeta)(X - \eta) = X^2 - (\zeta + \eta)X + \zeta\eta = X^2 - 2x_1X + 1.$$

Finally, let us prove that all the positive integer solutions (u, v) of the equation (8) are obtained the way we described above from some "small" positive integer solution (u_0, v_0). Let (u, v) be a positive integer solution of the equation (8). If $u + \sqrt{d}v \leq |N|\zeta$, then there are only finitely many possibilities for the pair (u, v). Suppose now that $u + \sqrt{d}v > |N|\zeta$, and let $\ell \geq 1$ be the minimal positive integer ℓ such that $(u + \sqrt{d}v)\zeta^{-\ell} \leq N\zeta$. We write

$$\begin{aligned} u_0 + \sqrt{d}v_0 &= (u + \sqrt{d}v)\zeta^{-\ell} = (u + \sqrt{d}v)(x_\ell - \sqrt{d}y_\ell) \\ &= (ux_\ell - dvy_\ell) + \sqrt{d}(-uy_\ell + vx_\ell). \end{aligned}$$

Since u and v are positive, by the definition of ℓ, we have that $u_0 + v_0\sqrt{d} > |N|$, for if not then we would have $0 < u_0 + \sqrt{d}v_0 < |N|$, therefore

$$(u + \sqrt{d}v)\zeta^{-(\ell-1)} < (u_0 + \sqrt{d}v_0)\zeta < |N|\zeta,$$

contradicting the way we chose ℓ. Let us now prove that u_0 and v_0 are positive. It is clear that at least one of them is positive. Since $u_0^2 - dy_0^2 = N$, we have that $|u_0 - \sqrt{d}v_0| = |N|/(u_0 + \sqrt{d}v_0) < 1$. If u_0 and v_0 would have opposite signs, then $1 > |u_0 - \sqrt{d}v_0| = |u_0| + \sqrt{d}|v_0|$, which is not possible. The above argument shows therefore that for every positive integer solution (u, v) of the Pell equation (8) there is some nonnegative integer ℓ and some positive integer solution (u_0, v_0) of the equation (8) with $u_0 + \sqrt{d}v_0 < |N|\zeta$, such that

$$u + \sqrt{d}v = (u_0 + \sqrt{d}v_0)\zeta^\ell,$$

which, via the argument from the beginning of this section, confirms that (u, v) belongs to a finite union of binary recurrent sequences. □

2.2 Lucas sequences

2.2.1 Definition and examples

Definition 2.2.1. *A binary recurrent sequence $(u_n)_{n\geq 0}$ with $u_0 = 0, u_1 = 1$ and such that a_1 and a_2 are coprime is called a Lucas sequence.*

If α_1 and α_2 are the roots of the characteristic equation, then one can check easily that for a Lucas sequence $(u_n)_{n\geq 0}$ the formula (3) takes the form

$$u_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} \qquad \text{for all } n \geq 0. \tag{9}$$

Example 2.2.2. *The Fibonacci sequence $(F_n)_{n\geq 0}$ is a Lucas sequence.*

Example 2.2.3. *Let $(x_\ell, y_\ell)_{\ell\geq 0}$ be the ℓth solution of the Pell equation $x^2 - dy^2 = N$ with $N = \pm 1$. The formula (7) proves that*

$$\frac{y_\ell}{y_1} = \frac{\zeta^\ell - \eta^\ell}{2\sqrt{d}y_1} = \frac{\zeta^\ell - \eta^\ell}{\zeta - \eta},$$

therefore the sequence $(y_\ell/y_1)_{\ell\geq 0}$ is Lucas.

Given a Lucas sequence $(u_n)_{n\geq 0}$ whose general term is given by (9), it is convenient to introduce its companion sequence $(v_n)_{n\geq 0}$ given by $v_0 = 2$, $v_1 = a_1$, which is also binary recurrent of the same characteristic equation as $(u_n)_{n\geq 0}$. One checks easily that the formula (3) for its general term is

$$v_n = \alpha_1^n + \alpha_2^n \qquad \text{for all } n \geq 0.$$

For example, the companion sequence of the Fibonacci sequence is the Lucas $(L_n)_{n\geq 0}$. For the Lucas sequence $(y_\ell/y_1)_{\ell\geq 0}$ appearing in example (2.2.3), its companion sequence is $(2x_\ell)_{\ell\geq 0}$.

2.2.2 Prime factors of terms of Lucas sequences

Throughout this section, $(u_n)_{n\geq 0}$ is a Lucas sequence.

The first question that we analyze here is the following: *What can we say about the prime numbers p such that $p \mid u_n$ for some n?*

Recall that if a is an integer and p is an odd prime, then the *Legendre symbol* $(a|p)$ is defined as

(i) $(a|p) = 0$ if $p \mid a$;

(ii) $(a|p) = 1$ if $p \nmid a$ and there exists an integer x such that $x^2 \equiv a \pmod{p}$;

(iii) $(a|p) = -1$ otherwise.

It is also useful to set $\Delta = (\alpha_1 - \alpha_2)^2$.

We recall that an algebraic number is a complex number which is the root of a monic polynomial with integer coefficients. The integers are algebraic integers. So are sums and products of algebraic integers. The only rationals that are algebraic integers are the integers. If m is an integer and α is an algebraic integer, we say that m divides α if α/m is an algebraic integer.

The following theorem summarizes the most important divisibility properties of the Lucas sequences.

Theorem 2.2.4. *Let p be a prime number. We have the following properties:*

(i) If $p \mid a_2$, then $p \nmid u_n$ for all $n \geq 1$;

(ii) If $p \mid \Delta$, then $p \mid u_p$;

(iii) If $p \nmid \Delta a_2$ and $(\Delta|p) = 1$, then $p \mid u_{p-1}$;

(iv) If p is an odd prime not covered by (i)–(iii), then $p \mid u_{p+1}$.

Proof. (i) Suppose that $p \mid u_n$ for some $n > 0$. Let n be minimal with this property. It is clear that $n \geq 2$ because $u_1 = 1$. Since

$$u_n = a_1 u_{n-1} + a_2 u_{n-2}$$

and $p \mid a_2$, we get that $p \mid a_1 u_{n-1}$. Since $\gcd(a_1, a_2) = 1$ and $p \mid a_2$, we conclude that $p \nmid a_1$, so that $p \mid u_{n-1}$, contradicting the choice of n.

(ii) Assume first that $p = 2$. Since $p \mid \Delta = a_1^2 + 4a_2$, we get that a_1 is even. Thus, $u_2 = a_1 \equiv 0 \pmod{2}$.

Let us now suppose that $p > 2$. Let

$$\alpha_1 = \frac{a_1 + \sqrt{\Delta}}{2} \qquad \text{and} \qquad \alpha_2 = \frac{a_1 - \sqrt{\Delta}}{2}.$$

Then

$$\begin{aligned} \alpha_1^p - \alpha_2^p &= \left(\frac{a_1 + \sqrt{\Delta}}{2}\right)^p - \left(\frac{a_1 - \sqrt{\Delta}}{2}\right)^p \\ &= \frac{2\sqrt{\Delta}}{2^p}\left(\binom{p}{1} a_1^{p-1} + \binom{p}{3} a_1^{p-3}\Delta + \cdots + \Delta^{(p-1)/2}\right). \end{aligned}$$

Since $\sqrt{\Delta} = \alpha_1 - \alpha_2$, we get

$$2^{p-1} u_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} a_1^{p-(2k+1)} \Delta^k.$$

Since $p \mid \Delta$, the right hand side of the above expression is a multiple of p. Thus, $p \mid 2^{p-1}u_p$, and since p is odd, we infer that $p \mid u_p$.

(iii) and (iv). We observe that

$$\alpha_1^p = \left(\frac{a_1 + \sqrt{\Delta}}{2}\right)^p = \frac{1}{2^p}\left(a_1^p + \sum_{k=1}^{p} \binom{p}{k} a_1^{p-k} \Delta^{k/2}\right).$$

Thus, $2^p \alpha_1^p \equiv a_1^p + \Delta^{(p-1)/2}\sqrt{\Delta} \pmod{p}$. Suppose that $(\Delta|p) = 1$. Then $\Delta^{(p-1)/2} \equiv 1 \pmod{p}$, and we get that $2^p \alpha_1^p \equiv 2\alpha_1 \pmod{p}$. Since p is odd and $2^p \equiv 2 \pmod{p}$, we also get that $\alpha_1^p \equiv \alpha_1 \pmod{p}$. Thus,

$$\alpha_1^p \equiv \alpha_1 \pmod{p} \qquad \text{and} \qquad \alpha_1^{p+1} \equiv \alpha_1^2 \pmod{p}.$$

The same congruences are obtained if we change α_1 to α_2. Subtracting these congruences we get

$$(\alpha_1 - \alpha_2)(u_p - 1) \equiv 0 \pmod{p} \qquad \text{and} \qquad (\alpha_1 - \alpha_2)(u_{p+1} - u_1) \equiv 0 \pmod{p}.$$

In particular, $p \mid \Delta(u_p - 1)$ and $p \mid \Delta(u_{p+1} - u_1)$. Since $p \nmid \Delta$, we get that $u_{p+1} \equiv u_1$ and $u_p \equiv 1 \pmod{p}$. Thus,

$$u_{p+1} \equiv a_1 u_p + a_2 u_{p-1}$$

and reducing this last relation modulo p we get at $u_1 \equiv a_1 + a_2 u_{p-1} \pmod{p}$. Since $u_1 = a_1$, we conclude that $p \mid a_2 u_{p-1}$, and since $p \nmid a_2$, we finally get that $p \mid u_{p-1}$, which is what we wanted.

In the case when $(\Delta|p) = -1$, we have that $2^p\alpha_1 \equiv a_1 - \sqrt{\Delta} \pmod{p} \equiv 2\alpha_2 \pmod{p}$. Thus,

$$\alpha_1^p \equiv \alpha_2 \pmod{p},$$

which leads us to $\alpha_1^{p+1} \equiv \alpha_1\alpha_2 \pmod{p} \equiv -a_2 \pmod{p}$. The same argument shows that $\alpha_2^{p+1} \equiv -a_2 \pmod{p}$, and subtracting these two relations we get $\alpha_1^{p+1} - \alpha_2^{p+1} \equiv 0 \pmod{p}$. Thus, $p \mid \Delta u_{p+1}$, and since $p \nmid \Delta$, we conclude that $p \mid u_{p+1}$. □

Example 2.2.5. *For the Fibonacci sequence $(F_n)_{n\geq 0}$ we have that $\Delta = (\alpha - \beta)^2 = 5$. If $p = 13$, then, since $(5|13) = (13|5) = (3|5) = -1$, we have that $13 \mid F_{14}$. In fact, $F_{14} = 377 = 13 \cdot 29$.*

Proposition 2.2.6. *For all positive integers m and n we have*

$$\gcd(u_m, u_n) = u_{\gcd(m,n)}.$$

Proof. If $m \mid n$, then writing $n = m\ell$, we have that

$$\frac{u_n}{u_m} = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1^m - \alpha_2^m} = \frac{(\alpha_1^m)^\ell - (\alpha_2^m)^\ell}{\alpha_1^m - \alpha_2^m} = (\alpha_1^m)^{\ell-1} + (\alpha_1^m)^{\ell-2}\alpha_2^m + \cdots + (\alpha_2^m)^{\ell-1}.$$

The left hand side of the above formula is rational and the right hand side is an algebraic integer because it is a polynomial with integer coefficients in α_1 and α_2 which are algebraic integers. Thus, this number is an integer. We conclude that if $m \mid n$, then $u_m \mid u_n$. On the other hand, given integers m and n with $d = \mathrm{mcd}(m, n)$, we infer that $u_d \mid u_m,\ u_d \mid u_n$, which implies that $u_d \mid \gcd(u_m, u_n)$.

Conversely, we first suppose that m and n are coprime. By induction on $\max\{m, n\}$ one proves that there exist two polynomials $P(x)$ and $Q(x)$ with integer coefficients such that

$$\frac{x^m - 1}{x - 1} P(x) + \frac{x^n - 1}{x - 1} Q(x) = 1.$$

Indeed, if $m = n = 1$, we can take $P(x) = 1$ and $Q(x) = 0$. If $m > n \geq 1$, we write $m = nq + r$ with $1 \leq r < n$, and use the identity

$$\frac{x^m - 1}{x - 1} - \frac{x^n - 1}{x - 1}\left(\frac{x^{nq} - 1}{x^n - 1}\right) x^r = \frac{x^r - 1}{x - 1}. \tag{10}$$

Thus, if $P_1(x),\ Q_1(x) \in \mathbb{Z}[x]$ are such that

$$\frac{x^n - 1}{x - 1} P_1(x) + \frac{x^r - 1}{x - 1} Q_1(x) = 1,$$

then

$$\begin{aligned} 1 &= \frac{x^n-1}{x-1}\,P_1(x) + \left(\frac{x^m-1}{x-1} - \frac{x^n-1}{x-1}\left(\frac{x^{nq}-1}{x^n-1}\right)x^r\right)Q_1(x) \\ &= \frac{x^m-1}{x-1}\,P(x) + \frac{x^n-1}{x-1}\,Q(x) \end{aligned}$$

holds with $P(x) := Q_1(x)$ and $Q(x) := P_1(x) - ((x^{nq}-1)/(x^n-1))\,x^r Q_1(x)$, which proves formula (10) for the pair (m,n). We now tale two arbitrary positive integers m and n, and write them as $m = dm_1$ and $n = dn_1$, with $d = \mathrm{mcd}(m,n)$. In that formula

$$\frac{x^{m_1}-1}{x-1}\,P(x) + \frac{x^{n_1}-1}{x-1}Q(x) = 1$$

that we have just proved, we replace x by x^d and get

$$\frac{x^m-1}{x-1}\,P(x^d) + \frac{x^n-1}{x-1}\,Q(x^d) = \frac{x^d-1}{x-1}.$$

Homogenizing the above relation, we get that

$$\frac{x^m-y^m}{x-y}R(x,y) + \frac{x^n-y^n}{x-y}S(x,y) = \left(\frac{x^d-y^d}{x-y}\right)y^{D-d},$$

where $R(x,y)$, $S(x,y) \in \mathbb{Z}[x,y]$ are the homogenizations of $P(x^d)$ and $Q(x^d)$, respectively, and D is the degree of the polynomial $(x^m-1)P(x^d)/(x-1)$. Let us recall that if

$$f(x) = c_0x^k + c_1x^{k-1} + \cdots + c_k \in \mathbb{C}[x],$$

then its homogenization is $f(x,y) = c_0x^k + c_1x^{k-1}y + \cdots + c_ky^k \in \mathbb{C}[x,y]$. Substituting $(x,y) := (\alpha_1,\alpha_2)$, we get

$$u_mR(\alpha_1,\alpha_2) + u_nS(\alpha_1,\alpha_2) = u_d\alpha_2^{D-d}.$$

Thus,

$$\frac{u_d\alpha_2^{D-d}}{\gcd(u_m,u_n)} = \frac{u_m}{\gcd(u_m,u_n)}\,R(\alpha_1,\alpha_2) + \frac{u_n}{\gcd(u_m,u_n)}\,S(\alpha_1,\alpha_2).$$

In the above expression, the right hand side is an algebraic integer. Thus, the left hand side is also an algebraic integer and therefore $\gcd(u_m,u_n) \mid u_d\alpha_2^{D-d}$. The same is true is we replace α_2 by α_1. Thus, $\gcd(u_m,u_n)^2$ divides $u_d^2(\alpha_1\alpha_2)^{D-d} = \pm u_d^2(a_2)^{D-d}$. Since no prime dividing a_2 can divide any term u_n of our sequence (by (i) of Theorem 2.2.4), we get that in fact $\gcd(u_m,u_n)^2$ divides u_d^2, so $\gcd(u_m,u_n)$ divides u_d, which completes the proof of this proposition. □

From Theorem 2.2.4 and Proposition 2.2.6, we have that if p is any prime which does not divide a_2, then there is a minimal positive integer f_p such that $p \mid u_{f_p}$. Furthermore, if n is any other integer such that $p \mid u_n$, then $f_p \mid n$. In particular, $f_p \mid p - (\Delta|p)$. The number f_p is called *the order of apparition* of p in the sequence $(u_n)_{n\geq 0}$.

Definition 2.2.7. *A prime divisor p of u_n is called primitive for u_n if $p \nmid \Delta$ and $f_p = n$. In other words, $p \mid u_n$, but $p \nmid \Delta \prod_{1\leq m<n} u_m$.*

Since $f_p \mid p \pm 1$, we get that any primitive prime divisor p of u_n, whenever it exists, satisfies the congruence

$$p \equiv \pm 1 \pmod{n}. \tag{11}$$

Example 2.2.8. *The first 20 terms of the Fibonacci sequence are*

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765.$$

Observe that $F_1 = F_2 = 1$, $F_5 = 5$ (and $5 = \Delta$), $F_6 = 2^3$ (and $2 \mid F_3$), $F_{12} = 144 = 2^4 3^2$ (and $2 \mid F_3$, $3 \mid F_4$), and all the other terms in the above list have primitive divisors.

2.3 The Primitive Divisor Theorem

The Primitive Divisor Theorem says that if $n \notin \{1, 2, 3, 4, 6\}$, then u_n has a primitive divisor except in finitely many instances all of which are known.

Theorem 2.3.1. *If $n \notin \{1, 2, 3, 4, 6\}$, then u_n has a primitive divisor except when $((\alpha_1, \alpha_2), n)$ is of the form*

$$\left(\pm((a_1 + \sqrt{\Delta})/2, (a_1 - \sqrt{\Delta})/2)), n\right),$$

where (a_1, a_2, n) is one of the following triples:

n	(a_1, Δ)
5	$(1, 5)$, $(1, -7)$, $(2, -40)$, $(1, -11)$, $(1, -15)$, $(12, -76)$, $(12, -1364)$
7	$(1, -7)$, $(1, -19)$
8	$(2, -24)$, $(1, -7)$
10	$(2, -8)$, $(5, -3)$
12	$(1, 5)$, $(1, -7)$, $(1, -11)$, $(2, -56)$, $(1, -15)$, $(1, -19)$
13	$(1, -7)$
18	$(1, -7)$
30	$(1, -7)$

The preceding theorem is due to Zsygmondy [85] and rediscovered, independently, by Birkhoff and Vandiver [6] more than 10 years later for the case in which the roots (α_1, α_2) are integers. Later, Carmichael [9] proved it for the case when the roots are real. Bilu, Hanrot and Voutier [5], building upon prior work of Schinzel [71] and Stewart [74], finished off the case when the roots are complex nonreal.

In what follows, we give the proof of Theorem 2.3.1 for the case in which the roots α_1 and α_2 are real. Since α_1/α_2 is not a root of 1, we can suppose that $|\alpha_1| > |\alpha_2|$. If necessary, we can replace (α_1, α_2) by $(-\alpha_1, -\alpha_2)$ (that is, replace $(u_n)_{n\geq 0}$ by the sequence of general term $(-1)^{n-1}u_n$, which changes the sign of some of its terms but does not affect the prime factors), and so suppose that $\alpha_1 > 0$. In particular, $\alpha_1 > |\alpha_2|$, and so $u_n > 0$ for all n.

We need two lemmas.

Lemma 2.3.2. *If $m \mid n$ and p is a prime such that $p \mid \gcd(u_m, u_n/u_m)$, then $p \mid n/m$.*

Proof. Since $p \mid u_m$, it follows that $\alpha_1^m \equiv \alpha_2^m \pmod{p}$. If we write $n = m\ell$, we then have

$$\frac{u_n}{u_m} = \frac{(\alpha_1^m)^\ell - (\alpha_2^m)^\ell}{\alpha_1^m - \alpha_2^m} = (\alpha_1^m)^{\ell-1} + \cdots + (\alpha_2^m)^{\ell-1}.$$

Since $\alpha_1^m \equiv \alpha_2^m \pmod{p}$, and $p \mid u_n/u_m$, it follows that $p \mid \ell\alpha_1^{m(\ell-1)}$ and $p \mid \ell\alpha_2^{m(\ell-1)}$. Thus, $p \mid \ell^2(\alpha_1\alpha_2)^{m(\ell-1)}$. Since $\alpha_1\alpha_2 = -a_2$, we get that $p \mid \ell a_2$. But $p \nmid a_2$ (see (i) of Theorem 2.2.4), therefore $p \mid \ell$. □

Lemma 2.3.3. *(i) If $p > 2$ is prime and $p \mid u_n$, then $p \| u_{np}/u_n$.*

(ii) If $p = 2$, $p \mid u_n$ and $p^t \mid u_{pn}/u_n$, then $t = 1$ if n is even, and $p^t \leq 3\alpha_1^2$, otherwise.

Proof. (i) Since $p \mid \alpha_1^n - \alpha_2^n$, we can write $\alpha_1^n = \alpha_2^n + p\lambda$ for some algebraic integer λ. Then

$$\begin{aligned}
\frac{u_{np}}{u_n} &= \frac{\alpha_1^{np} - \alpha_2^{np}}{\alpha_1^n - \alpha_2^n} = (\alpha_1^n)^{p-1} + (\alpha_1^n)^{p-2}\alpha_2^n + \cdots + (\alpha_2^n)^{p-1} \\
&= (\alpha_2^n + p\lambda)^{p-1} + (\alpha_2^n + p\lambda)^{p-2}\alpha_2^n + \cdots + (\alpha_2^n)^{p-1} \\
&= \big((\alpha_2^n)^{p-1} + (p-1)p(\alpha_2^n)^{p-2}\lambda\big) + \big((\alpha_2^n)^{p-1} + (p-2)p(\alpha_2^n)^{p-2}\lambda\big) \\
&+ \cdots + (\alpha_2^n)^{p-1} + p^2\gamma \\
&= p(\alpha_2^n)^{p-1} + p(\alpha_2^n)^{p-2}\lambda((p-1) + (p-2) + \cdots + 0) + p^2\gamma \\
&= p\alpha_2^{(p-1)n} + \frac{p^2(p-1)}{2}\alpha_2^{n(p-2)}\lambda + p^2\gamma,
\end{aligned}$$

where γ is an algebraic integer. Observe that, since p is odd,

$$\frac{u_{pn}}{pu_n} \equiv \alpha_2^{(p-1)n} \pmod{p}.$$

The same argument shows that we can replace α_2 by α_1 in the above congruence. Multiplying the above two congruences, we get that

$$\left(\frac{u_{pn}}{pu_n}\right)^2 \equiv \pm a_2^{(p-1)n} \pmod{p},$$

and since $p \nmid a_2$, we get that $p \| u_{pn}/u_n$.

(ii) If $p = 2$, then $u_{pn}/u_n = u_{2n}/u_n = v_n$. We shall use the formula

$$v_n^2 - \Delta u_n^2 = (\alpha_1^n + \alpha_2^n)^2 - (\alpha_1^n - \alpha_2^n)^2 = 4(\alpha_1\alpha_2)^n = \pm 4a_2^n. \tag{12}$$

Observe that a_2 is odd and $f_2 = 2$ if a_1 is even and $f_2 = 3$ otherwise. If $f_2 = 2$, then $\Delta = a_1^2 + 4a_2$ is a multiple of 4. Since u_n is even, formula (12) reduced modulo 8 gives $v_n^2 \equiv 4 \pmod 8$, showing that $2 \| v_n$, which is what we wanted.

Assume next that $f_2 = 3$. Then Δ is odd and formula (12) shows that u_m and v_m have the same parity for all m. Since $2 \mid u_n$, it follows that $n = 3m$ for some positive integer m. If m is even, then writing it as $m = 2m_1$, we get that $u_n = u_{3m} = u_{3m_1}v_{3m_1}$ is a multiple of 4. Reducing formula (12) modulo 8 we get, as in the previous case, that $v_n^2 \equiv 4 \pmod 8$, so $2 \| v_n$, which is what we wanted. Finally, if $n = 3m$ and m is odd, then

$$v_n = (\alpha_1^3 + \alpha_2^3)\left(\frac{\alpha_1^{3m} + \alpha_2^{3m}}{\alpha_1^3 + \alpha_2^3}\right).$$

Since $\alpha_1^3 \equiv \alpha_2^3 \pmod 2$, it is easy to see that

$$\begin{aligned}\frac{\alpha_1^{3m} + \alpha_2^{3m}}{\alpha_1^3 + \alpha_2^3} &\equiv \alpha_1^{3(m-1)} - \alpha_1^{3(m-2)}\alpha_2^3 + \cdots + \alpha_2^{3(m-1)} \pmod 2 \\ &\equiv m\alpha_1^{3(m-1)} \pmod 2 \equiv \alpha_1^{3(m-1)} \pmod 2.\end{aligned}$$

Since we can interchange the rôles of α_1 and α_2 in the above argument, the above expression is also congruent to $\alpha_2^{3(m-1)}$ módulo 2. Thus,

$$\left(\frac{\alpha_1^{3m} + \alpha_2^{3m}}{\alpha_1^3 + \alpha_2^3}\right)^2 \equiv (\alpha_1\alpha_2)^{3(m-1)} \pmod 2 \equiv 1 \pmod 2$$

because $\alpha_1\alpha_2 = a_2$ is odd. Hence, $2^t \mid \alpha_1^3 + \alpha_2^3$ y $a_1 = \alpha_1 + \alpha_2$ is odd, which leads to the conclusion that

$$2^t \leq \frac{\alpha_1^3 + \alpha_2^3}{\alpha_1 + \alpha_2} = \alpha_1^2 - \alpha_1\alpha_2 + \alpha_2^2 < 3\alpha_1^2.$$

□

The proof of Theorem 2.3.1. The idea is to write

$$\frac{x^n - 1}{x - 1} = \prod_{\substack{d|n \\ d>1}} \Phi_d(x),$$

where for $m \geq 1$ we write $\Phi_m(x) \in \mathbb{Z}[x]$ for the cyclotomic polynomial whose roots are the primitive roots of unity of order m. Homogenizing, we get

$$u_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} = \prod_{\substack{d|n \\ d>1}} \Phi_d(\alpha_1, \alpha_2).$$

We observe that the cyclotomic polynomial $\Phi_d(x)$ with $d > 1$ is reciprocal; that is, it satisfies the relation $\Phi_d(x) = x^{\phi(d)}\Phi_d(1/x)$. To see this, we first observe that if ζ is a primitive root of unity of order d, then ζ^{-1} is also. Next, the constant coefficient of $\Phi_d(x)$ is, by the Viete relations,

$$(-1)^{\phi(d)} \exp\left(\frac{2\pi i}{d} \sum_{\substack{1\leq k\leq d \\ \text{mcd}(k,d)=1}} k\right) = (-1)^{\phi(d)} e^{\frac{2\pi i d\phi(d)}{2d}}$$
$$= (-1)^{\phi(d)} e^{\pi i\phi(d)} = (-1)^{2\phi(d)} = 1.$$

Here we use the fact that if $d > 1$, then

$$\sum_{\substack{1\leq k<d \\ \gcd(k,d)=1}} k = \frac{d\phi(d)}{2},$$

which follows from the fact that if $1 \leq d < k$, then $\gcd(d, k) = 1$ if and ony if $\gcd(d - k, d) = 1$.

Since $\Phi_d(x)$ is reciprocal, the number $\Phi_d(\alpha_1, \alpha_2)$ is a symmetric expression in α_1 and α_2 which is also an algebraic integer. By Galois theory, it is a rational number; hence, an integer.

We write

$$\Phi_n(\alpha_1, \alpha_2) = AB,$$

where A and B are positive integers such that all the prime factors p of A have $f_p < n$, and all the prime factors of B have $f_p = n$. If u_n has no primitive prime divisor, then $B = 1$. If p divides A, then $p \mid u_d$ for some $d < n$. Since $p \mid u_n$, we have that $p \mid \gcd(u_d, u_n) = u_{\gcd(d,n)}$. Thus, we can replace d by $\gcd(d, n)$ and therefore assume that $d \mid n$. Since $\Phi_d(x) \mid (x^n - 1)/(x^d - 1)$, we have that

$$\Phi_n(\alpha_1, \alpha_2) \mid \frac{u_n}{u_d}.$$

Thus, $p \mid \gcd(u_d, u_n/u_d)$, and by Lemma 2.3.2 we may assume that $p \mid n/d$. We can now replace d by n/p (which is a multiple of d), and thus suppose that $n = pd$. Then $\Phi_d(\alpha_1, \alpha_2) \mid u_{pd}/u_d$. By Lemma 2.3.3, we have that $p \| u_{pd}/u_p$ if p is odd, and when $p = 2$ we have that if $2^t \mid u_{pd}/u_d$, then $2^t < 3\alpha_1^2$. Furthermore, $t = 1$ unless $f_2 = 3$, $3 \mid n$ and $2 \| n$. Thus, we get that

$$A = 2^t \prod_{\substack{p \mid A \\ p > 2}} p,$$

where all the prime factors p of A are divisors of n. Since $2^t < 3\alpha_1^2$, we deduce immediately that $A < 1.5\alpha_1^2 n$. Thus, if $B = 1$ we get the inequality

$$\Phi_n(\alpha, \beta) < 1.5\alpha_1^2 n. \tag{13}$$

In the above inequality we may replace the amount $1.5\alpha_1^2$ by 1 unless $f_2 = 3$, $3 \mid n$ and $2 \| n$. On the other hand, it is clear that

$$\Phi_n(\alpha_1, \alpha_2) = \frac{\alpha_1^n - \alpha_2^n}{\prod_{p \mid n}(\alpha_1^{n/p} - \alpha_2^{n/p})} \frac{\prod_{pq \mid n}(\alpha_1^{n/pq} - \alpha_2^{n/pq})}{\prod_{pqr \mid n}(\alpha_1^{n/pqr} - \alpha_2^{n/pqr})} \cdots .$$

Next, $\alpha_1^d - \alpha_2^d < 2\alpha_1^d$ for all $d \geq 1$. It is easy to see that the inequality

$$\alpha_1^d - \alpha_2^d \geq \alpha_1^{d-1} \tag{14}$$

holds for all $d \geq 1$. The above inequality is clear if $\alpha_2 < 0$ and d is odd. If $\alpha_2 > 0$, we then have that

$$\alpha_1^d - \alpha_2^d = (\alpha_1 - \alpha_2)(\alpha_1^{d-1} + \cdots + \alpha_2^{d-1}) \geq \sqrt{\Delta}\alpha_1^{d-1} \geq \alpha_1^{d-1}.$$

Finally, when $\alpha_2 < 0$ and d is even, then

$$\begin{aligned} \alpha_1^d - \alpha_2^d &= \alpha_1^d - (-\alpha_2)^d \\ &= (\alpha_1 + \alpha_2)(\alpha_1^{d_1} + \alpha_1^{d-2}|\alpha_2| + \cdots + |\alpha_2|^{d-1}) \\ &\geq a_1 \alpha_1^{d-1} \geq \alpha_1^{d-1}, \end{aligned}$$

which again proves inequality (14). Thus, writing $k = \omega(n)$ for the number of distinct prime factors of n and $p_1 < \cdots < p_k$ for these primes, we have

$$\begin{aligned} \Phi_n(A,B) &> \frac{1}{2^{2^{k-1}}} \alpha_1^{n - \sum_{i=1}^k \frac{n}{p_i} + \sum_{1 \leq i < j \leq k} \frac{n}{p_i p_j} + \cdots + (-1)^{k-1} \frac{n}{p_1 \cdots p_k} - 2^{k-1}} \\ &= \frac{1}{2^{2^{k-1}}} \alpha_1^{\phi(n) - 2^{k-1}}. \end{aligned}$$

Combining the last inequality above with the inequality (13), we arrive at the inequality

$$1.5 \cdot 2^{2^{k-1}} \cdot n > \alpha_1^{\phi(n) - 2 - 2^{k-1}}. \tag{15}$$

Observe that $\alpha_1 = (a_1 + \sqrt{\Delta})/2$, $a_1 \geq 1$ and $\Delta \geq 1$. Thus, if $a_1 \geq 3$, then $\alpha_1 \geq 2$. If $a_1 = 2$, then $\Delta = a_1^2 + 4a_2 > 0$, showing that $\Delta \geq 8$, therefore $\alpha_1 \geq 1 + \sqrt{2}$. Finally, if $a_1 = 1$, then $\Delta = 1 + 4a_2 \geq 5$, showing that $\alpha_1 \geq (1 + \sqrt{5})/2$.

Observe next that since $p_i \geq i + 1$ holds for all $i = 1, 2, \ldots, k$, we have

$$\phi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) \geq n \prod_{i=1}^k \left(1 - \frac{1}{i+1}\right) = \frac{n}{k+1}.$$

We next show that the inequality $2^k \leq (8n/3)^{1/2}$ holds for all $n \geq 2$. This inequality is equivalent to $n \geq 6 \cdot 4^{k-2}$. If $k = 1$, the inequality holds. If $k \geq 2$, then it suffices to prove that $q_1 \cdots q_k \geq 6 \cdot 4^{k-2}$, where q_i is the ith prime number. This last inequality is equivalent to $q_3 \cdots q_k \geq 4^{k-2}$, which holds because $q_i \geq 5 > 4$ for all $i \geq 3$. Thus, $2^{k-1} \leq (2n/3)^{1/2}$ so that

$$k + 1 \leq \frac{\log(2n/3)}{2 \log 2} + 2 = \frac{\log(32n/3)}{2 \log 2}.$$

The inequality (15) tells us now that

$$\frac{1}{\log((1+\sqrt{5})/2)} \left(\log(1.5n) + \left(\frac{2n}{3}\right)^{1/2} \log 2 \right) > \frac{2n \log 2}{\log(32n/3)} - \left(\frac{2n}{3}\right)^{1/2} - 2,$$

which yields $n < 272$. For $n < 272$, we have that $k \leq 4$. Returning to inequality (15), we have that

$$\frac{\log(384n)}{\log((1+\sqrt{5})/2)} > \frac{n}{5} - 10,$$

leading to $n \leq 170$, which implies that $k \leq 3$. In turn, this last inequality leads to

$$\frac{\log(24n)}{\log((1+\sqrt{5})/2)} > \frac{n}{4} - 6,$$

which implies that $n \leq 90$.

If $\phi(n) - 2 - 2^{k-1} \geq 12$, we then get

$$2160 \geq 1.5 \cdot 2^{2^{3-1}} \cdot \geq 1.5 \cdot 2^{2^{k-1}} \cdot n > \alpha_1^{12},$$

which gives $\alpha_1 < 2160^{1/12} < 2$. The only pair (α_1, α_2) of this form is $(\alpha_1, \alpha_2) = ((1+\sqrt{5})/2, (1-\sqrt{5})/2)$ for which $u_n = F_n$ is the nth Fibonacci number.

Thus, after verifying that F_n has a primitive prime factor for all $n \leq 90$, except for $n \in \{1, 2, 3, 4, 6, 12\}$ it suffices to assume that $\phi(n) - 2^{k-1} \leq 11$, which happens only for a few values of $n \leq 60$. For each one of the values of $n \leq 42$ except for $n = 10,\ 12$, one proves that

$$\alpha_1 < (1.5 \cdot 2^{2^{k-1}} \cdot n)^{1/(\phi(n)-2-2^{k-1})}.$$

The maximal value of the expression on the right is < 31. Thus, $a_1 \in [1, 62],\ |a_2| < 961,\ n \leq 60$. A quick calculation finishes the proof.

Our argument fails for $n = 10$ and 12 because for these values of n we have $\phi(n) - 2 - 2^{k-1} = 0$. However, for none of these values can we have $f_2 = 3$, $3 \mid n$ and $2 \| n$, showing that for these two values of n the inequality $A \leq 1.5\alpha_1^2 n$ can be replaced by the stronger inequality $A \leq n$. Following the above arguments with this better inequality, we get

$$2^{2^{k-1}} n > \alpha_1^{\phi(n)-2^{k-1}} \tag{16}$$

instead of the bound (15). The new exponent is now $\phi(n) - 2^{k-1} = 2$ for both $n = 10,\ 12$, and so the above inequality (16) gives us a bound for α_1. We do not give further details.

2.4 Applications

Proposition 2.4.1. *The largest solution of the equation*

$$F_n = m_1!m_2!\cdots m_k!$$

with $2 \le m_1 \le m_2 \le \cdots \le m_k$ *is* $F_{12} = 3!\ 4! = 2!^2 3!^2$.

Proof. If $n > 12$, then, by Theorem 2.3.1, F_n has a primitive prime factor p. Since $p \equiv \pm 1 \pmod{n}$, we get that $m_k \ge p \ge n-1$. By the elementary inequality $m_k! \ge (m_k/e)^{m_k}$, we get that $m_k! \ge ((n-1)/e)^{n-1}$. Since $n > 12$, we have that $(n-1)/e > \alpha$, so $m_k! > \alpha^{n-1}$. We have obtained

$$F_n = m_1!\cdots m_k! \ge m_k! > \alpha^{n-1},$$

which is false because $F_n \le \alpha^{n-1}$ for all n. This last inequality can be proved by checking it for $n = 1,\ 2$ and by using induction for $n \ge 3$ via the recurrence

$$F_n = F_{n-1} + F_{n-2} \le \alpha^{n-2} + \alpha^{n-3} = \alpha^{n-1}.$$

□

In 1844, E. Catalan [11] conjectured that the only solution in positive integers of the equation

$$x^m - y^n = 1 \qquad m \ge 2,\ n \ge 2 \tag{17}$$

is $3^2 - 2^3 = 1$. This conjecture was proved by Mihăilescu [62] in 2002. It is clear that we may assume that m and n are primes, because if (x, y, m, n) is a solution and $p \mid m$ and $q \mid n$ are primes, then $(x^{m/p}, y^{n/q}, p, q)$ is also a solution. Furthermore, m and n are distinct, because if $m = n$, then

$$1 = x^m - y^m = (x-y)(x^{m-1} + \cdots + y^{m-1}) > x - y > 0,$$

which is impossible.

In what follows, we present a result of Lebesque of 1850 [42] concerning this equation using the language of primitive divisors of terms of Lucas sequences.

Proposition 2.4.2. *Equation* (17) *has no solution with* $n = 2$.

Proof. Assume that there is a solution of the equation

$$x^m = y^2 + 1.$$

It is clear that y is even, because if y were odd, then $y^2 + 1 \equiv 2 \pmod 4$ cannot be a perfect power. Factoring the right hand side in $\mathbb{Z}[i]$ we get $(y + i)(y - i) = x^m$. The two numbers $y + i$ and $y - i$ are coprime in $\mathbb{Z}[i]$. In fact, if q is some prime of $\mathbb{Z}[i]$ dividing both $y + i$ and $y - i$, then $q \mid (y + i) - (y - i) = 2i \mid 2$, and $q \mid x^m$ where x is odd (because y is even), which is a contradiction. Thus, since $y + i$ and $y - i$ are coprime and their product is x^m, we infer that there exists $\alpha_1 = a + bi \in \mathbb{Z}[i]$ such that $y + i = \zeta\alpha_1^m$, where ζ is a unit. Furthermore, $x = a^2 + b^2$. The only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$ of finite orders dividing 4, and since m is odd, we can replace α_1 by one of its associates (for example, by $\zeta^m\alpha_1$) and conclude that $\zeta\alpha_1^m = \zeta^{m^2}\alpha_1^m = (\zeta^m\alpha_1)^m$. Thus, we can take $\zeta = 1$ to infer that

$$y + i = \alpha_1^m.$$

Conjugating the above relation and eliminating y between the two equations, we get

$$2i = \alpha_1^m - \alpha_2^m, \qquad \text{where} \qquad \alpha_2 = \overline{\alpha_1}.$$

Since $\alpha_1 - \alpha_2 = 2bi$ divides $2i$, we get that $b = \pm 1$ and

$$\pm 1 = \frac{\alpha_1^m - \alpha_2^m}{\alpha_1 - \alpha_2}. \tag{18}$$

Interchanging α_1 and α_2, we may assume that $b = 1$. The right hand side of the above equation is the mth term of a Lucas sequence with $a_1 = \alpha_1 + \alpha_2 = 2a$ and $a_2 = -(\alpha_1\alpha_2) = -(a^2 + 1) = -x$, which is odd. Thus, a_1 are a_2 coprime. We need that α_1/α_2 is not a root of 1. If it were, since it is also in $\mathbb{Q}[i]$, then it would be ± 1 or $\pm i$. If $\alpha_1/\alpha_2 = \pm 1$, we get either that $a + i = a - i$, which is false, or that $a + i = -a + i$, leading to $a = 0$, so $x = 1$, which is also false. If $\alpha_1/\alpha_2 = \pm i$, we then get $a + i = ai + 1$, so either $a = 1$, or $a + i = -ai - 1$, so $a = -1$. In both cases, we get $x = 2$, contradicting the fact that x is odd. Thus, the right hand side of (18) is the mth term of a Lucas sequence, and clearly it has no primitive divisors. Now either $m \in \{2, 3, 4, 6\}$, or the triple (α_1, α_2, m) appears in the table from Theorem 2.3.1. A rapid inspection of the table shows that none of the pairs of roots (α_1, α_2) appearing in the table has components in $\mathbb{Q}[i]$, therefore it must be the case that $m = 3$. In this way, we get

$$\pm 1 = \frac{(a + i)^3 - (a - i)^3}{2i} = (a + i)^2 + (a + i)(a - i) + (a - i)^2 = 3a^2 - 1,$$

which gives us $3a^2 \in \{0, 2\}$, and none of these possibilities leads to a solution of the initial equation. □

Let $P(m)$ be the maximal prime factor of m.

Proposition 2.4.3. *The largest solution of* $P(x^2-1) \leq 29$ *is*

$$36171409^2 - 1 = 2^5 \cdot 3 \cdot 5 \cdot 7^3 \cdot 11 \cdot 13^3 \cdot 17 \cdot 23 \cdot 29^2.$$

Proof. We write $x^2 - 1 = dy^2$, where d is squarefree. The only primes that can divide d are $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$. Thus there are only 1023 possible values for d. For each one of such d, let $(x_1(d), y_1(d))$ be the minimal solution of the Pell equation $x^2 - dy^2 = 1$, and let $(x_\ell(d), y_\ell(d))$ be its ℓth solution. Let $u_\ell = y_\ell(d)/y_1(d)$, which, from what we have seen is a Lucas sequence. It follows, by Theorem 2.3.1, that if $\ell \geq 31$, then $y_\ell(d)$ has a prime factor $\geq \ell - 1 \geq 30$. Thus, for each of the 1023 values of d it suffices to generate the first 30 terms of the sequence $(x_\ell(d))_{\ell \geq 1}$ and observe that all the positive integers x such that $P(x^2 - 1) \leq 29$ are obtained in this way. A quick computation with Mathematica shows that out of all these $1023 \cdot 30 = 30690$ candidates, $x = 36171409$ is the largest solution to our problem. Other interesting examples are

$$\begin{aligned} 16537599^2 - 1 &= 2^{12} \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 17 \cdot 19 \cdot 23^2 \cdot 29; \\ 12901780^2 - 1 &= 3^2 \cdot 11 \cdot 19^4 \cdot 23^2 \cdot 29^3. \end{aligned}$$

□

2.5 Lehmer sequences

A version a bit more general than that of a Lucas sequence is a *Lehmer sequence*. Let a_1 and a_2 be coprime nonzero integers, and let α_1 and α_2 be the roots of the equation

$$x^2 - \sqrt{a_1}x - a_2 = 0.$$

Its discriminant is $\Delta = (\alpha_1 - \alpha_2)^2 = a_1 + 4a_2$. Suppose that α_1/α_2 is not a root of 1. The Lehmer sequence $(w_n)_{n \geq 0}$ is given by

$$w_n = \begin{cases} \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} & \text{si } n \equiv 1 \pmod 2; \\ \frac{\alpha_1^n - \alpha_2^n}{\alpha_1^2 - \alpha_2^2} & \text{si } n \equiv 0 \pmod 2. \end{cases}$$

The Lehmer sequence $(w_n)_{n \geq 0}$ shares the divisibility properties of the Lucas sequences. In particular, $w_m \mid w_n$ if and only if $m \mid n$. A primitive prime divisor p of w_n is a prime factor of w_n which does not divide $a_1 \Delta \prod_{1 \leq m < n} w_m$. Observe that $a_1\Delta = (\alpha_1^2 - \alpha_2^2)$. The analogue of Theorem 2.3.1 for the Lehmer sequences is the following.

Theorem 2.5.1. *If $n \notin \{1,2,3,4,5,6,8,10,12\}$, then w_n has a primitive divisor except when the triple $((\alpha_1,\alpha_2),n)$ is of the form*

$$\left(\pm((\sqrt{a_1}+\sqrt{\Delta})/2,(\sqrt{a_1}-\sqrt{\Delta})/2)),n\right),$$

where (a_1,a_2,n) is one of the triples:

n	(a_1,Δ)
7	$(1,-7)$, $(1,-19)$, $(3,-5)$, $(5,-7)$, $(13,-3)$, $(14,-22)$
9	$(5,-3)$, $(7,-1)$, $(7,-5)$
13	$(1,-7)$
14	$(3,-13)$, $(5,-3)$, $(7,-1)$, $(7,-5)$, $(19,-1)$, $(22,-14)$
15	$(7,-1)$, $(10,-2)$
18	$(1,-7)$, $(3,-5)$, $(5,-7)$
24	$(3,-5)$, $(5,-3)$
26	$(7,-1)$
30	$(1,-7)$, $(2,-10)$

2.6 Problems

Problem 2.6.1. *Formulate and prove an analogue of Proposition 2.0.2 for the case when the roots $\alpha_1,\ldots,\alpha_s$ de $f(X)$ are not necessarily simple.*

Problem 2.6.2. *Prove that $(1+\sqrt{5})/2=[\overline{1}]$, and that the kth convergent of $(1+\sqrt{5})/2$ is F_{k+1}/F_k.*

Problem 2.6.3. *Find the simple continued fraction of $(F_{10n+1}/F_{10n})^5$.*

Problem 2.6.4. *Let $n\geq 2$ be an integer. Prove that n does not divide 2^n-1.*

Problem 2.6.5. *Let $k\geq 2$ and $n_1,n_2,\ldots,n_k$ positive integers such that*

$$n_2 \mid 2^{n_1}-1,\quad n_3\mid 2^{n_2}-1,\quad \ldots\quad n_k\mid 2^{n_{k-1}}-1,\quad n_k\mid 2^{n_1}-1.$$

Prove that $n_1=\cdots=n_k=1$.

Problem 2.6.6. *Determine if there exists an integer n with precisely 2000 distinct prime factors such that $n\mid 2^n+1$.*

Problem 2.6.7. *Let m and n be positive integers such that $A=((m+3)^n+1)/(3m)$ is an integer. Prove that A is odd.*

Problem 2.6.8. *Prove that*

$$\sum_{k=0}^{n} \binom{2n+1}{2k+1} 2^{3k}$$

is not a multiple of 5 *for any* $n \geq 0$.

Problem 2.6.9. *Let* $p_1, \ldots, p_n$ *be distinct primes. Prove that* $2^{p_1 \cdots p_n} + 1$ *has at least* 4^n *divisors.*

Problem 2.6.10. *Let* b, m, n *be positive integers with* $b > 1$ *and* $m \neq n$ *such that* $b^m - 1$ *and* $b^n - 1$ *have the same prime factors. Prove that* $b + 1$ *is a power of* 2.

Problem 2.6.11. *(i) Suppose that* $2^n + 1$ *is prime. Prove that* n *is a power of* 2.

(ii) Suppose that $4^n + 2^n + 1$ *is prime. Prove that* n *is a power of* 3.

Problem 2.6.12. *Determine all positive integers* n *such that* $(2^n + 1)/n^2$ *is an integer.*

Problem 2.6.13. *Determine all pairs* (n, p) *of positive integers with* p *prime,* $n < 2p$, *and such that* $p^{n-1} + 1$ *is divisible by* n^{p-1}.

Problem 2.6.14. *Determine all triples* (a, m, n) *of positive integers such that* $a^m + 1$ *divides* $(a + 1)^n$.

Problem 2.6.15. *(i) Find all positive integers* n *such that* $3^n - 1$ *is divisible by* 2^n.

(ii) Find all positive integers n *such that* $9^n - 1$ *is divisible by* 7^n.

Problem 2.6.16. *Prove that the Diophantine equation* $(n-1)! + 1 = n^k$ *has no solutions with* $n > 5$.

Problem 2.6.17. *Prove that*

$$F_{2n-1}^2 + F_{2n+1}^2 + 1 = 3F_{2n-1}F_{2n+1}$$

holds for all $n \geq 1$.

Problem 2.6.18. *The sequence* $(a_n)_{n \geq 1}$ *is given by*

$$a_1 = 1, \quad a_2 = 12, \quad a_3 = 20, \quad a_{n+3} = 2a_{n+2} + 2a_{n+1} - a_n.$$

Prove that $1 + 4a_n a_{n+1}$ *is a perfect square for all* $n \geq 1$.

Problem 2.6.19. *Prove that every positive integer can be represented as a sum of Fibonacci numbers in such a way that there are no two consecutive ones.*

Problem 2.6.20. *Prove that the largest solution of the equation*

$$F_{n_1}F_{n_2}\cdots F_{n_k} = m_1!m_2!\cdots m_\ell!$$

with $1 \le n_1 < n_2 < \cdots < n_k$ *y* $2 \le m_1 \le m_2 \le \cdots \le m_\ell$ *is*

$$F_1F_2F_3F_4F_5F_6F_8F_{10}F_{12} = 11!.$$

Problem 2.6.21. *Redo Problem 1.7.5 using what you know about primitive divisors.*

Problem 2.6.22. *If* $p \ge 5$ *is prime, prove that the Diophantine equation*

$$x^2 + 2^a \cdot 3^b = y^p$$

has no solutions $x \ge 1,\ a \ge 0,\ b \ge 0$ *and* $\gcd(x, y) = 1$.

Problem 2.6.23. *Find all Fibonacci numbers of the form* $\dfrac{1}{n+1}\binom{2n}{n}$.

Problem 2.6.24. *Prove that the only solution of the equation*

$$\frac{x^n - 1}{x - 1} = y^2$$

with n *odd is* $(x, n, y) = (3, 5, 11)$.

Problem 2.6.25. *Let* $\phi(n)$ *be the Euler function* n. *Prove that if* $\phi(n)^2 \mid n^2 - 1$, *then* $n \in \{1, 2, 3\}$.

Problem 2.6.26. *Let* $\phi(n)$ *and* $\sigma(n)$ *be the Euler function and the sum of divisors of* n, *respectively.*

(i) Prove $P(\phi(n)\sigma(n))$ *tends to infinity with* n.

(ii) Prove that $P(\phi(n)\sigma(n)) \ge (1 + o(1)) \log\log n$ *as* $n \to \infty$.

Problem 2.6.27. *Find all positive integers* n *such that* $n! \mid \sigma(n!)$.

Problem 2.6.28. *Suppose that* $m > n \ge 0$ *and that* $2^m - 2^n$ *divides* $3^m - 3^n$. *Prove that* $2^m - 2^n$ *divides* $x^m - x^n$ *for all positive integers* x.

Problem 2.6.29. *Find all positive integers* n *such that* $\binom{2n}{n} \mid \sigma(\sigma(\binom{2n}{n}))$.

2.7 Notes

Problem 2.6.1 is well-known in the theory of linearly recurrent sequences (see [33], or [73] for example). For Problem 2.6.3, see [15]. Problems 2.6.4–2.6.19 are from the book [80]. Some of these problems have appeared in mathematical competitions at national levels in various countries, or in the International Mathematical Olympiad. While their solutions are considered, in general, a collection of isolated tricks, we leave it to the solver to note that most of these problems are pretty easy consequences of either Theorem 2.3.1, or of the arguments that appear in the lemmas that we used to prove this beautiful result. For Problem 2.6.22, see [49]. Problem 2.6.25 is a result of Křížek and Luca [39]. Problem 2.6.27 is due to Pomerance see [67]. For Problem 2.6.28, see [69]. For Problem 2.6.29, see [57].

Chapter 3

Lower bounds for linear forms in logarithms

3.1 Statements

In 1966, A. Baker [2] gave an effective lower bound on the absolute value of a nonzero linear form in logarithms of algebraic numbers; that is, for a nonzero expression of the form

$$\sum_{i=1}^{n} b_i \log \alpha_i,$$

where $\alpha_1, \ldots, \alpha_n$ are algebraic numbers and $b_1, \ldots, b_n$ are integers. His result marked the dawn of the era of effective resolution of the Diophantine equations of certain types, namely the ones that can be reduced to exponential ones; i.e., where the unknown variables are in the exponents. Many of the computer programs available today which are used to solve Diophantine equations (PARI, MAGMA, KASH, etc.) use some version of Baker's inequality. For our purpose, we shall give some of the Baker type inequalities available today which are easy to apply. We start with some preliminaries about algebraic numbers. Let α be an algebraic number of degree d. Let

$$f(x) = \sum_{i=0}^{d} a_i x^{d-i} \in \mathbb{Z}[x]$$

be the minimal polynomial of α with $a_0 > 0$ and $\gcd(a_0, \ldots, a_d) = 1$. We put $H(\alpha) := \max\{|a_i| : i = 0, \ldots, d\}$ and call it the *height* of α. Now write

$$f(X) = a_0 \prod_{i=1}^{d} (X - \alpha^{(i)}),$$

where $\alpha = \alpha^{(1)}$. The numbers $\alpha^{(i)}$ are called the *conjugates* of α. The *logarithmic height* of α is

$$h(\alpha) = \frac{1}{d} \left(\log |a_0| + \sum_{i=1}^{d} \log \max\{|\alpha^{(i)}|, 1\} \right).$$

Example 3.1.1. *If $\alpha = p/q$ is a rational number, where p and $q > 0$ are coprime integers, then $H(\alpha) = \max\{|p|, q\}$ and $h(\alpha) = \log \max\{|p|, q\}$.*

3.1.1 The complex case

The following result is due to Matveev [59]. Let $\mathbb{L}$ be a number field of degree D; that is, a finite extension of degree D of $\mathbb{Q}$. Let $\alpha_1, \ldots, \alpha_n$ be nonzero elements of $\mathbb{L}$ and let $b_1, \ldots, b_n$ be integers. Put

$$B = \max\{|b_1|, \ldots, |b_n|\},$$

and

$$\Lambda = \prod_{i=1}^{n} \alpha_i^{b_i} - 1.$$

Let $A_1, \ldots, A_n$ be positive integers such that

$$A_j \geq h'(\alpha_j) := \max\{Dh(\alpha_j), |\log \alpha_j|, 0.16\} \qquad \text{for all } j = 1, \ldots, n. \quad (1)$$

With these notations, Matveev proved the following theorem (see also Theorem 9.4 in [8]).

Theorem 3.1.2. *If $\Lambda \neq 0$, then*

$$\log |\Lambda| > -3 \cdot 30^{n+4} (n+1)^{5.5} D^2 (1 + \log D)(1 + \log nB) A_1 A_2 \cdots A_n. \quad (2)$$

If furthermore $\mathbb{L}$ is real, then

$$\log \Lambda > -1.4 \cdot 30^{n+3} n^{4.5} D^2 (1 + \log D)(1 + \log B) A_1 A_2 \cdots A_n. \quad (3)$$

3.1.2 The p-adic case

In this section, we shall present a p-adic version of a lower bound for linear forms in logarithms of algebraic numbers due to Kunrui Yu [82]. Let π be a prime ideal in $\mathcal{O}_{\mathbb{L}}$. Let e_π and f_π be its indices of *ramification* and *inertia*, respectively. It is known that if $p \in \mathbb{Z}$ is the unique prime number such that $\pi \mid p$, then

$$p^D = \prod_{i=1}^{k} \pi_i^{e_i},$$

where $\pi_1, \ldots, \pi_k$ are prime ideals of $\mathcal{O}_{\mathbb{K}}$. The prime π is one of the primes π_i, say π_1, and its e_π equals e_1. The number f_π is the dimension of π over its prime field $\mathbb{Z}/p\mathbb{Z}$, or, to say it differently, can be computed via the formula $\#\mathcal{O}_{\mathbb{L}}/\pi = p^{f_\pi}$. Observe that $e_\pi f_\pi \leq D$. For an algebraic number $\alpha \in \mathbb{L}$ we write $\mathrm{ord}_\pi(\alpha)$ for the exponent of π in the factorization of the fractional ideal $\alpha\mathcal{O}_{\mathbb{L}}$ generated by α inside $\mathbb{L}$. Let

$$H_j \geq \max\{h(\alpha_j), \log p\} \qquad \text{for all } j = 1, \ldots, n.$$

With the above definitions and notations, Yu proved the following result.

Theorem 3.1.3. *If $\Lambda \neq 0$, then*

$$\mathrm{ord}_\pi(\Lambda) \leq 19(20\sqrt{n+1}D)^{2(n+1)} e_\pi^{n-1} \frac{p^{f_\pi}}{(f_\pi \log p)^2} \log(e^5 nD) H_1 \cdots H_n \log B. \tag{4}$$

3.1.3 Linear forms in two logarithms

The modern French school of transcendence theory developed some lower bounds for linear forms in two logarithms of algebraic numbers which have a slightly worse dependence in the parameter $\log B$ than the Baker–Matveev–Yu bounds, but have the property that the multiplicative constants involved are much smaller. Consequently, in applications they yield better results. Let us now see two of their results.

Let α_1 and α_2 be algebraic numbers and put $\mathbb{L} = \mathbb{Q}[\alpha_1, \alpha_2]$. Next, let $D_1 = D$, if $\mathbb{L}$ is real, and $D_1 = D/2$, otherwise. Suppose that

$$A_j \geq \max\{D_1 h(\alpha_j), |\log \alpha_j|, 1\} \qquad \text{for both } j = 1,\ 2.$$

Let

$$\Gamma = b_2 \log \alpha_2 - b_1 \log \alpha_1, \tag{5}$$

and

$$b' = \frac{b_1}{A_2} + \frac{b_2}{A_1}.$$

With these notations, Laurent, Mignotte and Nesterenko [41] proved the following theorem.

Theorem 3.1.4. *(i) If α_1 and α_2 are multiplicatively independent, then*

$$\log|\Gamma| \geq -30.9\left(\max\{D_1 \log b', 21, D_1/2\}\right)^2 A_1 A_2 \tag{6}$$

(ii) If furthermore α_1 and α_2 are real and positive, then

$$\log|\Gamma| \geq -23.34\left(\max\{D_1 \log b' + 0.14D_1, 21, D_1/2\}\right)^2 A_1 A_2 \tag{7}$$

Suppose next that π is a prime ideal in $\mathcal{O}_{\mathbb{L}}$ which does not divide $\alpha_1\alpha_2$. Let $D_2 = D/f_\pi$ and let g be the minimal positive integer such that both $\alpha_1^g - 1$ and $\alpha_2^g - 1$ belong to π. Suppose further that

$$H_j \geq \max\{D_2 h(\alpha_j), \log p\} \qquad \text{holds for both } j = 1, 2.$$

We put, as before,

$$\Lambda = \alpha_1^{b_1}\alpha_2^{b_2} - 1,$$

and

$$b'' = \frac{b_1}{H_2} + \frac{b_2}{H_1}.$$

With these notations, Bugeaud and Laurent proved the following theorem.

Theorem 3.1.5. *Suppose that α_1 and α_2 are multiplicatively independent. Then,*

$$\mathrm{ord}_\pi(\Lambda) \leq \frac{24pgH_1H_2D_2^2}{(p-1)(\log p)^4}\left(\max\{\log b'' + \log\log p + 0.4, 10(\log p)/D_2, 10\}\right)^2.$$

3.2 Applications

In this section, we give three applications of the results mentioned in the previous section.

3.2.1 Rep-digit Fibonacci numbers

Recall that a *rep-digit* is a positive integer having only distinct digit when written in base 10. The concept can be generalized to every base $b > 1$ the resulting numbers being called *base b rep-digits*. In this section, we look at those Fibonacci numbers F_n which are rep-digits. Putting d for the repeated digit and assuming that F_n has m digits, the problem reduces to finding all the solutions of the Diophantine equation

$$F_n = \overline{dd\cdots d}_{(10)} = d\cdot 10^{m-1} + d\cdot 10^{m-2} + \cdots + d = d\frac{10^m - 1}{10 - 1} \quad d \in \{1, \ldots, 9\}. \tag{8}$$

The result is the following.

Proposition 3.2.1. *The largest solution of equation* (8) *is* $F_{10} = 55$.

Proof. Suppose that $n > 1000$. We start by proving something a bit weaker.

Obtaining some bound on n. With $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$, equation (8) can be rewritten as

$$\frac{\alpha^n - \beta^n}{\sqrt{5}} = d\frac{10^m - 1}{9}.$$

We rewrite the above equation by separating on the one side the *large terms* and in the other side the *small terms*. That is, we rewrite the equation under the form

$$|\alpha^n - (d\sqrt{5}/9)10^m| = |\beta^n - d\sqrt{5}/9| \leq \alpha^{-1000} + \sqrt{5} < 2.5. \tag{9}$$

We need some estimates for m in terms of n. By induction over n, it is easy to prove that

$$\alpha^{n-2} < F_n < \alpha^{n-1} \qquad \text{for all } n \geq 3.$$

Thus,

$$\alpha^{n-2} < F_n < 10^m \qquad \text{or} \qquad n < (\log 10/\log \alpha)m + 2,$$

and

$$10^{m-1} < F_n < \alpha^{n-1}.$$

On the other hand,

$$\begin{aligned} n &> (\log 10/\log \alpha)(m-1) + 1 = (\log 10/\log \alpha)m - (\log 10/\log \alpha - 1) \\ &> (\log 10/\log \alpha)m - 4. \end{aligned}$$

We then deduce that

$$n \in [c_1 m - 4, c_1 m + 2] \qquad \text{con } c_1 = \log 10/\log \alpha = 4.78497\ldots \tag{10}$$

Since $c_1 > 4$, we check easily that for $n > 1000$ we have $n = \max\{m, n\}$. We now rewrite inequality (9) as

$$\Lambda = |(d\sqrt{5}/9)\alpha^{-n}10^m - 1| < \frac{2.5}{\alpha^n} < \frac{1}{\alpha^{n-2}},$$

which leads to

$$\log \Lambda < -(n-2)\log \alpha. \tag{11}$$

We compare this upper bound with the lower bound on the quantity Λ given by Theorem 3.1.2. Observe first that Λ is not zero, for if it were, then $\sqrt{5}$ would be of the form form $q\alpha^n$ with some $q \in \mathbb{Q}$. In particular, since on the one hand its square is 5 and on the other hand it is of the form $q^2\alpha^{-2n}$, we get that $\alpha^{2n} \in \mathbb{Q}$, which is false for any $n > 0$. With the notations of that theorem, we take

$$\alpha_1 = d\sqrt{5}/9,\ \alpha_2 = \alpha,\ \alpha_3 = 10; \qquad b_1 = 1,\ b_2 = -n,\ b_3 = m.$$

Observe that $\mathbb{L} = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\sqrt{5}]$, so $D = 2$. The above comments show that $B = n$. We note also that the conjugates of α_1, α_2 and α_3 are

$$\alpha_1' = -d\sqrt{5}/9,\ \alpha_2' = \beta,\ \alpha_3' = 10.$$

Furthermore, α_2 and α_3 are algebraic integers, while the minimal polynomial of α_1 over $\mathbb{Q}$ is

$$(X - \alpha_1)(X - \alpha_1') = X^2 - 5d^2/81.$$

Thus, the minimal polynomial of α_1 over the integers is a divisor of $81X^2 - 5d^2$. Hence,

$$h(\alpha_1) < \frac{1}{2}\left(\log 81 + 2\log\sqrt{5}\right) = \frac{1}{2}\log(405) < 3.01.$$

Clearly,

$$h(\alpha_2) = \frac{1}{2}(\log\alpha + 1) < 0.75, \qquad h(\alpha_3) = \log 10 < 2.31.$$

Hence, we can take $A_1 = 6.02,\ A_2 = 1.5,\ A_3 = 4.62$ and than the inequalities (1) hold. Theorem 3.1.2 tells us that

$$\log \Lambda > -1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 4 \cdot (1 + \log 4) \cdot 6.02 \cdot 1.5 \cdot 4.62(1 + \log n).$$

Comparing this last inequality with (11), leads to

$$(n-2)\log\alpha < 1.4\cdot 30^6\cdot 3^{4.5}\cdot 4\cdot(1+\log 4)\cdot 6.02\cdot 1.5\cdot 4.62(1+\log n),$$

giving

$$n-2 < 1.2\cdot 10^{14}(1+\log n).$$

Mathematica tells us that $n < 4.5\cdot 10^{15}$.

Reducing the bound. Observe that in the equality

$$1-(d\sqrt{5}/9)\alpha^{-n}10^m = \frac{1}{\alpha^n}\left(\beta^n - \frac{d\sqrt{5}}{9}\right)$$

the right hand side is negative. Thus, writing

$$z = \log\alpha_1 - n\log\alpha_2 + m\log\alpha_3,$$

we get that

$$-\frac{2.5}{\alpha^n} < 1-e^z < 0.$$

In particular, $z > 0$. Furthermore, since $n > 1000$, the right hand side exceeds $-1/2$, therefore $e^z < 1.5$. We thus have that

$$0 < e^z - 1 < \frac{2.5e^z}{\alpha^n} < \frac{4}{\alpha^n}.$$

Since $e^z - 1 > z$, we get

$$0 < m\log\alpha_3 - n\log\alpha_2 + \log\alpha_1 < \frac{4}{\alpha^n},$$

which can be rewritten as

$$0 < m\left(\frac{\log\alpha_3}{\log\alpha_2}\right) - n + \left(\frac{\log\alpha_1}{\log\alpha_2}\right) < \frac{4}{\alpha^n\log\alpha_2} < \frac{9}{\alpha^n}.$$

Since

$$|1-(d\sqrt{5}10^m/\alpha^n)| < 1,$$

we have that

$$\frac{d\sqrt{5}10^m}{\alpha^n} < 2,$$

therefore

$$\alpha^n > \frac{d\sqrt{5}10^m}{2} > 10^m.$$

We have obtained

$$0 < m\left(\frac{\log \alpha_3}{\log \alpha_2}\right) - n + \left(\frac{\log \alpha_1}{\log \alpha_2}\right) < \frac{9}{10^m}. \tag{12}$$

Since $n < 4.5 \cdot 10^{15}$, inequality (10) shows that $m < 9.5 \cdot 10^{14}$. With

$$\gamma = \frac{\log \alpha_3}{\log \alpha_2}, \quad \mu = \frac{\log \alpha_1}{\log \alpha_2}, \quad A = 9, \quad B = 10,$$

we get

$$0 < m\gamma - n + \mu < \frac{A}{B^m},$$

where $m < M := 10^{15}$. The conditions to apply Lemma 1.4.4 are fulfilled. Observe that

$$\frac{p_{35}}{q_{35}} = C_{35} = \frac{970939497358931987}{202914354378543655} \qquad \text{for } \gamma$$

and $q_{35} > 202914354378543655 > 2 \cdot 10^{17} > 6M$. We compute

$$M\|q_{35}\gamma\| = 0.00216711\ldots < 0.01.$$

For each one of the values of $d \in \{1, \ldots, 9\}$, we compute $\|q_{35}\mu\|$. The minimal value of this expression is obtained when $d = 5$ and is

$$0.029\ldots > 0.02.$$

Thus, we can take $\varepsilon = 0.01 < 0.02 - 0.01 < \|q_{35}\mu\| - M\|q_{35}\gamma\|$. Since

$$\frac{\log(Aq_{35}/\varepsilon)}{\log B} = 21.2313\ldots,$$

Lemma 1.4.4 tells us that there is no solution in the range $m \in [22, 10^{15}]$. Thus, $m \leq 21$ and now inequality (10) tells us that $n \leq 102$. However, we have assumed that $n > 1000$. To finish, we use Mathematica to print the values of all the Fibonacci numbers modulo 10000 (that is, their last four digits) and convince ourselves that there are no Fibonacci numbers F_n which are rep-digits in the range $11 \leq n \leq 1000$.

Using linear forms in two p-adic logarithms

Given that the multiplicative constant that appears in Theorem 3.1.2 is very large, it is better to use the Theorems from Section 3.1.3 whenever

this is possible. In what follows, we illustrate this phenomenon with our problem. We rewrite our equation

$$\frac{\alpha^n - \varepsilon\alpha^{-n}}{\sqrt{5}} = \frac{d(10^m - 1)}{9}, \qquad \text{with } \varepsilon = (-1)^n \in \{\pm 1\},$$

as

$$\alpha^n + \frac{d\sqrt{5}}{9} - \varepsilon\alpha^{-n} = \frac{d2^m\sqrt{5}^{2m+1}}{9},$$

or, equivalently, as

$$\alpha^{-n}(\alpha^n - z_1)(\alpha^n - z_2) = \frac{d2^m\sqrt{5}^{2m+1}}{9}, \tag{13}$$

where

$$z_{1,2} = \frac{-d\sqrt{5} \pm \sqrt{5d^2 + 324\varepsilon}}{18}$$

are the solutions to the quadratic equation

$$z^2 + \frac{d\sqrt{5}}{9}z - \varepsilon = 0.$$

The left hand side of equation (13) is not zero, an observation which is necessary in order to apply the machinery of lower bounds for linear forms in logarithms of algebraic numbers. Assume first that $d \neq 9$. We then claim that z_1 and α are multiplicatively independent and that the same is true with z_2 instead of z_1. To see this, observe that if $\varepsilon = -1$, then $5d^2 + 324\varepsilon < 0$, while if $\varepsilon = 1$, then $5d^2 + 324\varepsilon$ is coprime to 5 and it is not a perfect square for any $d \in \{1, \ldots, 8\}$. Thus, $z_{1,2}$ are of the form $x_1\sqrt{5} \pm x_2\sqrt{e}$ with $x_1,\ x_2 \in \mathbb{Q}^*$ and some squarefree integer $e \neq 0,\ 1,\ 5$. Hence, no power of $z_{1,2}$ can be in $\mathbb{Q}[\sqrt{5}]$ which contains the powers of α. Let $\mathbb{L} = \mathbb{Q}[z_1, z_2]$. Then $\mathbb{Q}[\sqrt{5}] \subset \mathbb{L}$ and $D = 4$. Let π be a prime ideal in $\mathbb{L}$ dividing $\sqrt{5}$. Equation (13) gives us

$$2m + 1 \leq \mathrm{ord}_\pi(\alpha^n - z_1) + \mathrm{ord}_\pi(\alpha^n - z_2).$$

To bound the two orders from the right hand side above, we use Theorem 3.1.5. Observe that all the conjugates of $z_{1,2}$ are of the form

$$\frac{\pm d\sqrt{5} \pm \sqrt{5d^2 + 324\varepsilon}}{18}$$

and their absolute values are $\leq (8\sqrt{5}+\sqrt{5\cdot 64+324})/18 < 2.41$. Moreover, the minimal polynomial of $z_{1,2}$ over the integers divides

$$9^2\left(X^2-\frac{d\sqrt{5}}{9}X-\varepsilon\right)\left(X^2+\frac{d\sqrt{5}}{9}X-\varepsilon\right)=81(X^2-\varepsilon)^2-5d^2X^2\in\mathbb{Z}[X],$$

therefore

$$h(z_{1,2})<\frac{\log 81+4\cdot\log 2.41}{4}<2.$$

Observe next that 5 is a perfect square in $\mathbb{Q}[\sqrt{5}]\subseteq\mathbb{L}$. Furthermore, 5 splits into two distinct prime ideals in the quadratic field $\mathbb{Q}[\sqrt{5d^2+324\varepsilon}]\subset\mathbb{L}$ because

$$(5d^2+324\varepsilon|5)=(324\varepsilon|5)=(18^2|5)(\pm 1|5)=1.$$

Hence, we have that $e_\pi=2$ and $f_\pi=1$ giving $D_2=4$. From the preceding calculations, we know that $h(\alpha)<0.75$. Thus, taking $\alpha_1=\alpha,\ \alpha_2=z_{1,2}$, $b_1=n,\ b_2=1$, it follows that we can take

$$H_1=3>\max\{4h(\alpha),\log 5\},$$

and

$$H_2=8>\max\{4h(z_{1,2}),\log 5\}.$$

To find g, observe that

$$z_1^2\equiv-\frac{d\sqrt{5}}{9}z_1+\varepsilon\pmod{\pi}\equiv\varepsilon\pmod{\pi},$$

so that $z_1^4\equiv 1\pmod{\pi}$. The same happens when we replace z_1 by z_2. Finally,

$$(2\alpha)^4=(1+\sqrt{5})^4\equiv 1\pmod{\pi}$$

and since $2^4=16\equiv 1\pmod 5$, we have that $\alpha^4\equiv 1\pmod{\pi}$. Thus, we can take $g=4$. Clearly,

$$b''\leq\frac{n}{8}+\frac{1}{3}<\frac{n+3}{8}.$$

Since $n<4.8m+2$ (see inequality (10)), we have that

$$b''<0.6m+3.8.$$

Finally, let us see that π cannot divide both α^n-z_1 and α^n-z_2, since if it were, then it would divide their difference

$$z_1-z_2=\frac{\sqrt{5d^2+324\varepsilon}}{9},$$

which is an algebraic number whose norm is a rational number having both the numerator and the denominator coprime to 5. Thus, applying Theorem 3.1.5 for $\mathrm{ord}_\pi(\alpha^n - z_i)$ for one of the indices $i = 1$ or 2 and the fact that $\mathrm{ord}_\pi(\alpha^n - z_j) = 0$ for the other index j such that $\{i, j\} = \{1, 2\}$, and using also the fact that $2.5 \log 5 < 10$ gives us

$$2m + 1 < \frac{24 \cdot 5 \cdot 3 \cdot 8 \cdot 16}{4(\log 5)^4} \left(\max\left\{\log(0.6m + 3.8) + \log\log 5 + 0.4, 10\right\}\right)^2,$$

which implies that

$$2m + 1 < 1717 \left(\max\{\log(0.6m + 3.8) + 1, 10\}\right)^2.$$

If the maximum is 10, then $2m + 1 < 1717 \cdot 10^2$, so $m < 858500$. In the other case,

$$2m + 1 < 1717(\log(0.6m + 3.8) + 1)^2,$$

giving $m < 104808$. Thus, $m < 104808$, leading to $n < 501506$. This is much better that the bound we have obtained by applying Theorem 3.1.2. In order to finish, it suffices to use Mathematica to generate $F_n \pmod{10^7}$ for all $1 \leq n \leq 501506$ (that is, generate the last 6 digits of F_n) and verify that there are no solutions to our problem for $n > 10$. It is interesting to note that

$$\begin{aligned}
F_{142266} &\equiv 1888888 \pmod{10^7} \\
F_{238103} &\equiv 5777777 \pmod{10^7} \\
F_{242740} &\equiv 9555555 \pmod{10^7} \\
F_{252314} &\equiv 8777777 \pmod{10^7} \\
F_{490387} &\equiv 9333333 \pmod{10^7}
\end{aligned}$$

but the above positive integers n are the only ones in the interval $[1, 501506]$ such that the last five digits of F_n are all equal and nonzero.

Assume now that $d = 9$. We then get that $F_n = 10^m - 1$. Thus, $10^m = F_n + 1$. On the other hand, for all positive integers $k \geq 0$, the formulas

$$F_{4k} + 1 = F_{2k-1}L_{2k+1}, \qquad F_{4k+1} + 1 = F_{2k+1}L_{2k}, \tag{14}$$

$$F_{4k+2} + 1 = F_{2k+2}L_{2k}, \qquad F_{4k+3} + 1 = F_{2k+1}L_{2k+2} \tag{15}$$

hold. In particular, $10^m = F_{(n-\delta)/2}L_{(n+\delta)/2}$, where $\delta \in \{\pm 1, \pm 2\}$ and $n \equiv \delta \pmod 2$. However, if $n > 26$, then $(n - \delta)/2 > 12$, and by Theorem 2.3.1 $F_{(n-\delta)/2}$ has a primitive prime factor $p > 12$ that does not divide 10^m. Thus, our equation has no solutions with $d = 9$ and $n > 26$. A calculation by hand finishes the proof.

□

3.2.2 Pillai's equation

Given positive integers $a > b > 1$, Pillai [66] proved that here are only finitely many integers $c \neq 0$ admitting more than one representation of the form

$$c = a^x - b^y \qquad \text{in nonnegative integers } x,\ y.$$

In particular, the equation

$$a^x - b^y = a^{x_1} - b^{y_1} \qquad \text{with } (x, y) \neq (x_1, y_1) \tag{16}$$

has only finitely many nonnegative integer solutions. We shall call such solutions *nontrivial* reserving the word *trivial* for the ones for which $(x, y) = (x_1, y_1)$. Here we shall apply the technology of the lower bounds for linear forms in logarithms of algebraic numbers to find all the solutions when $(a, b) = (3, 2)$.

Proposition 3.2.2. *The only nontrivial solutions of the* (16) *equation with* $(a, b) = (3, 2)$ *are*

$$3^1 - 2^2 = 3^0 - 2^1, \quad 3^2 - 2^4 = 3^0 - 2^3, \quad 3^2 - 2^3 = 3^1 - 2^1,$$

$$3^3 - 2^5 = 3^1 - 2^3, \qquad 3^5 - 2^8 = 3^1 - 2^4.$$

Proof. We rewrite the equation as

$$3^x - 3^{x_1} = 2^y - 2^{y_1}, \tag{17}$$

from where, after relabeling the variables, we may assume that $x > x_1$. Consequently, $y > y_1$. Since

$$2 \cdot 3^{x-1} = 3^x - 3^{x-1} \leq 3^x - 3^{x_1} = 2^y - 2^{y_1} < 2^y, \tag{18}$$

we get that $x < y$. We put $B = y$. Now

$$3^{x_1} \mid 2^y - 2^{y_1} = 2^{y_1}(2^{y-y_1} - 1). \tag{19}$$

Lemma 2.3.3 (i) for the Lucas sequence of general term $u_n = 2^n - 1$ implies easily that $3^m \mid 2^n - 1$ if and only if $2 \cdot 3^{m-1} \mid n$. In particular, from the relation

$$x_1 \leq 1 + \frac{\log((y - y_1)/2)}{\log 3} \leq \frac{\log(3B/2)}{\log 3}, \tag{20}$$

we get to

$$3^{x_1} < \frac{3B}{2} < 2B.$$

Similarly,

$$2^{y_1} \mid 3^x - 3^{x_1} = 3^{x_1}(3^{x-x_1} - 1).$$

The argument from Lemma 2.3.3 (ii) proves that if $m \geq 3$, then $2^m \mid 3^n - 1$ if and only if $2^{m-2} \mid n$. Thus,

$$y_1 \leq 2 + \frac{\log(x - x_1)}{\log 2} < \frac{\log(4B)}{\log 2}, \tag{21}$$

therefore,

$$2^{y_1} \leq 4B.$$

We now regroup again in the original equation the *large parts* in one side, and the *small parts* in the other, obtaining

$$|3^x - 2^y| = |3^{x_1} - 2^{y_1}| < 2B,$$

which in turn gives us

$$|1 - 3^x 2^{-y}| < \frac{2B}{2^B}.$$

Put $\Gamma = x \log 3 - y \log 2$. If $\Gamma > 0$, the above inequality gives us

$$e^{\Gamma} - 1 < \frac{2B}{2^B},$$

and since $e^{\Gamma} - 1 > \Gamma$, we get

$$0 < \Gamma < \frac{2B}{2^B}. \tag{22}$$

If $\Gamma < 0$, then assuming that $B > 10$, we have that $2B/2^B < 1/2$, therefore, $|1 - e^{\Gamma}| < 1/2$, which implies that $e^{|\Gamma|} < 2$. In particular,

$$e^{|\Gamma|} - 1 < \frac{2Be^{|\Gamma|}}{2^B} < \frac{4B}{2^B},$$

which implies that

$$|\Gamma| < \frac{4B}{2^B}. \tag{23}$$

From the inequalities (22) and (23), we deduce that the inequality (23) holds independently of the sign of Γ. For a lower bound on the parameter $|\Gamma|$, we use Theorem 3.1.4. Observe that $\Gamma \neq 0$, because in the opposite case we would have that $3^x = 2^y$, which by unique factorization implies that $x = y = 0$; a contradiction. We take,

$$\alpha_1 = 2,\ \alpha_2 = 3; \qquad b_1 = y,\ b_2 = x; \qquad B = y.$$

Observe that $\mathbb{L} = \mathbb{Q}$, $D_1 = D = 1$, and we can take $A_1 = 1,\ A_2 = \log 3$,

$$b' = \frac{y}{\log 3} + x < B\left(\frac{1}{\log 3} + 1\right) < 2B.$$

Since 2 and 3 are multiplicatively independent, real and positive, Theorem 3.1.4 yields the estimate

$$\log|\Gamma| > -23.34\left(\max\{\log(2B) + 0.14, 21\}\right)^2 \cdot \log 3.$$

Comparing this last inequality with inequality (23), we get that

$$B\log 2 - \log(4B) < 23.34 \cdot \log 3 \cdot \left(\max\{\log(2B) + 0.14, 21\}\right)^2.$$

If the above maximum is 21, we then get that $B\log 2 - \log(4B) < 25.7 \cdot 21^2$, yielding $B < 17,000$. Otherwise, we have

$$B\log 2 - \log(4B) < 25.7(\log(2B) + 0.14)^2,$$

yielding $B < 2900$. Thus, $B < 17000$. Inequalities (20) and (21) imply that $x_1 \leq 9$ and $y_1 \leq 16$. Inequality (18) implies that

$$x - 1 < (y-1)\frac{\log 2}{\log 3} < B\frac{\log 2}{\log 3} < 11000.$$

We shall now reduce this bound. Suppose that $B \geq 30$. Then

$$3^x > 3^x - 3^{x_1} = 2^y - 2^{y_1} \geq 2^{B-1} \geq 2^{29},$$

and so $x \geq 19$. With Mathematica, we checked that the congruence

$$3^x - 3^{x_1} - 2^{y_1} \equiv 0 \pmod{2^{30}}$$

does not hold for any triple (x, x_1, y_1) with $11 \leq x \leq 1100,\ 0 \leq x_1 \leq 9,\ 0 \leq y_1 \leq 16$, showing that $B \leq 29$. Since $3^{x-1} < 2^{y-1} \leq 2^{28}$, we get that $x \leq 18$. Now only a few seconds with Mathematica are needed to compute all the solutions in the remaining range. □

3.2.3 Simultaneous Pell equations

In this section, we give one more application of the theory of lower bounds for linear forms in logarithms. The following result is due to Baker and Davenport [3] and historically it was the first example of the successful use of lower bounds for linear forms in logarithms of algebraic numbers which actually allowed for the effective computation of all common members of two binary recurrent sequences with real roots.

Proposition 3.2.3. *The only positive integer d such that $d+1$, $3d+1$ and $8d+1$ are all three perfect squares is $d = 120$.*

Proof. We write

$$d + 1 = x^2, \qquad 3d + 1 = y^2, \qquad 8d + 1 = z^2,$$

and eliminate d among the above equations getting

$$3x^2 - y^2 = 2 \qquad \text{and} \qquad 8x^2 - z^2 = 7.$$

The above system is called *a system of simultaneous Pell equations* since it consists a two Pell equations with a component in common, which in this case is x. We start by finding all the solutions (x, y) of the first Pell equation. If we put $\zeta = u + v\sqrt{3}$ for the smallest positive integer solution of the Pell equation

$$u^2 - 3v^2 = 1,$$

then $(u, v) = (2, 1)$. The proof of Theorem 2.1.2 shows that every positive integer solution (x, y) of the equation $y^2 - 3x^2 = -2$ is of the form $y + \sqrt{3}x = (y_1 + x_1\sqrt{3})\zeta^\ell$ with some integer $\ell \geq 0$, where $x_1,\ y_1$ are positive integers with

$$y_1 + x_1\sqrt{3} \leq 2\zeta = 2(2 + \sqrt{3}) < 7.5.$$

Thus, $y_1 \leq 7$ and $x_1 \leq 4$. The only solutions in this range are

$$1^2 - 3 \cdot 1^2 = -2 \qquad \text{and} \qquad 5^2 - 3 \cdot 3^2 = -2.$$

But observe that $5 + 3\sqrt{3} = (1 + \sqrt{3})\zeta$, so that the second solution is in fact obtained from the first one. Thus,

$$y + x\sqrt{3} = (1 + \sqrt{3})\zeta^n \qquad \text{for some } n \geq 0.$$

Writing $\eta = 1 - \sqrt{3}$ and conjugating the above relation we get

$$y - x\sqrt{3} = (1 - \sqrt{3})\eta^n.$$

Eliminating y between the last two equations we get

$$x = \frac{1}{2\sqrt{3}} \left((1 + \sqrt{3})\zeta^n - (1 - \sqrt{3})\eta^n) \right) = \gamma\zeta^n + \delta\eta^n, \tag{24}$$

with

$$(\gamma, \delta) = \left(\frac{1 + \sqrt{3}}{2\sqrt{3}}, -\frac{1 - \sqrt{3}}{2\sqrt{3}} \right).$$

Observe that x belongs to a binary recurrent sequence $(u_n)_{n\geq 0}$ of roots $\zeta,\ \eta$, whose characteristic equation is

$$X^2-(\zeta+\eta)X+\zeta\eta = X^2-4X+1.$$

That is to say,

$$u_{n+2}=4u_{n+1}-u_n \qquad \text{for all } n\geq 0. \tag{25}$$

Moreover, $u_0=1$ and $u_1=3$. We use the same argument for the second equation. Here we have

$$z^2-8x^2=-7.$$

Putting $\zeta_1=u_1+v_1\sqrt{8}$ for the minimal solution of the equation $u^2-8v^2=1$, we have that $(u_1,v_1)=(3,1)$. Thus, $z+x\sqrt{8}=(z_1+x_1\sqrt{8})\zeta_1^{\ell}$ for some $\ell\geq 0$, where $x_1,\ z_1$ are positive integers such that

$$0<z_1+x_1\sqrt{8}<7(3+\sqrt{8})<41.$$

Thus, $z_1\leq 40$ and $x_1\leq 14$. The only solutions in this interval are

$$1^2-8\cdot 1^2=-7,\quad 5^2-8\cdot 2^2=-7,\quad 11^2-8\cdot 4^2=-7,\quad 31^2-8\cdot 11^2=-7.$$

Since

$$11+4\sqrt{8}=(1+\sqrt{8})\zeta_1 \qquad \text{and} \qquad 31+11\sqrt{8}=(5+2\sqrt{8})(3+\sqrt{8}),$$

we get that it suffices to assume that $(z_1,x_1)\in\{(1,1),(5,2)\}$. We now write

$$z+x\sqrt{8}=(z_1+x_1\sqrt{8})\zeta_1^m \qquad \text{for some } m\geq 0,$$

put $\eta_1=3-\sqrt{8}$, conjugate and then eliminate z in order to get

$$x=\frac{1}{2\sqrt{8}}\left((z_1+x_1\sqrt{8})\zeta_1^m-(z_1-x_1\sqrt{8})\eta_1^m\right)=\gamma_1\zeta^m+\delta_1\eta_1^m,$$

where

$$(\gamma_1,\delta_1)=\left(\frac{1+\sqrt{8}}{2\sqrt{8}},\ -\frac{1-\sqrt{8}}{2\sqrt{8}}\right)\quad \text{or}\quad \left(\frac{5+2\sqrt{8}}{2\sqrt{8}},-\frac{5-2\sqrt{8}}{2\sqrt{8}}\right).$$

Thus, x belongs to the sequence $(v_m)_{m\geq 0}$ whose recurrence relation is

$$v_{m+2}=6v_{m+1}-v_m \qquad \text{for all } m\geq 0,\quad \text{where } (v_0,v_1)=(1,4),\ (2,11).$$

Thus, it suffices to find the pairs of nonnegative integers (n,m) such that $u_n=v_m$. We follow the previous program which consists in putting in the

same side of the equation the *large parts* and in the other side of the equation the *small parts*. Since $\eta,\ \eta_1 \in (0,1)$, we get that

$$|\gamma\zeta^n - \gamma_1\zeta_1^m| = |\delta\eta^n - \delta_1\eta_1^m| \le \max\{|\delta|, |\delta_1|\} < \frac{1}{4}. \tag{26}$$

Suppose that $n \ge 20$. Then, since $\gamma = 0.788675\ldots > 1/4$, $\zeta^2 > \zeta + 1$ and $\gamma > \zeta^{-1}$, we have that

$$\gamma\zeta^n - \frac{1}{4} > \gamma(\zeta^n - 1) > \gamma\zeta^{n-1} > \zeta^{n-2},$$

and

$$\gamma\zeta^n + \frac{1}{4} < \gamma(\zeta^n + 1) < \gamma\zeta^{n+1} < \zeta^{n+1}.$$

Thus,

$$\gamma_1\zeta_1^m \in [\gamma\zeta^n - 1/4, \gamma\zeta^n + 1/4] \subset [\zeta^{n-2}, \zeta^{n+1}].$$

Since

$$\gamma_1 = \frac{1+\sqrt{8}}{2\sqrt{8}} \in [\zeta_1^{-1}, 1] \quad \text{or} \quad \gamma_1 = \frac{5+2\sqrt{8}}{2\sqrt{8}} \in [1, \zeta_1],$$

we get that

$$\zeta_1^{m-1} < \zeta^{n+2} \qquad \text{and} \qquad \zeta_1^{m+1} > \zeta^{n-2}. \tag{27}$$

Putting $c_1 = \log\zeta/\log\zeta_1 = 0.747160\ldots$, we have that

$$m < c_1(n+2) + 1 < c_1 n + 3, \quad \text{and} \quad m > c_1(n-2) - 1 = c_1 n - 3,$$

yielding

$$m \in [c_1 n - 3, c_1 n + 3]. \tag{28}$$

Since $c_1 n + 3 < n$ for $n \ge 12$, we deduce that $B = n = \max\{m, n\}$. Returning to inequality (26), we have

$$|1 - (\gamma_1\gamma^{-1})\zeta^{-n}\zeta_1^m| < \frac{1}{4\gamma\zeta^n} < \frac{1}{3\zeta^n}. \tag{29}$$

We now find a lower bound on the absolute value of the amount

$$\Lambda := (\gamma_1\gamma^{-1})\zeta^{-n}\zeta_1^m - 1$$

which appears in the left hand side of the above inequality (29) using Theorem 3.1.2. Observe that $\Lambda \neq 0$, since if it were zero, then we would get that $\gamma_1\zeta_1^n = \gamma\zeta^m$. However, the left hand side of the above relation is in $\mathbb{Q}[\sqrt{3}]\backslash\mathbb{Q}$,

while the right hand side is in $\mathbb{Q}[\sqrt{2}]\backslash\mathbb{Q}$, which leads to a contradiction since $\mathbb{Q}[\sqrt{3}] \cap \mathbb{Q}[\sqrt{2}] = \mathbb{Q}$. We write

$$\alpha_1 = \gamma_1\gamma^{-1},\ \alpha_2 = \zeta,\ \alpha_3 = \zeta_1; \qquad b_1 = 1,\ b_2 = -n,\ b_3 = m.$$

It is clear that $\mathbb{L} = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ has $D = 4$. Since ζ and ζ_1 have as conjugates η and η_1, respectively, both in $(0, 1)$, and are algebraic integers (that is, $a_0 = 1$ holds for both numbers ζ and ζ_1), we can take

$$A_2 = 2.7 > 4h(\alpha_2) = 2\log(2+\sqrt{3}), \qquad A_3 = 3.6 > 4h(\alpha_3) = 2\log(3+\sqrt{8}).$$

For α_1, suppose first that

$$\alpha_1 = \frac{\sqrt{8}(1+\sqrt{3})}{\sqrt{3}(1+\sqrt{8})}.$$

Its minimal polynomial over the integers is

$$441X^4 - 2016X^3 + 2880X^2 - 1536X + 256 \in \mathbb{Z}[X], \tag{30}$$

so that $a_0 = 441$. In fact, with $z = \alpha_1$, we have

$$z = \frac{\sqrt{8}(1+\sqrt{3})}{\sqrt{3}(1+\sqrt{8})},$$

which can be rewritten as

$$\sqrt{3}z + \sqrt{24}z = \sqrt{8} + \sqrt{24},$$

or

$$\sqrt{3}z - \sqrt{8} = \sqrt{24}(1-z).$$

Taking squares we get

$$3z^2 - 2\sqrt{24}z + 8 = 24(z-1)^2 = 24z^2 - 48z + 24,$$

therefore

$$21z^2 - 48z + 16 = -2\sqrt{24}z.$$

Taking squares again we get

$$(21z^2 - 48z + 16)^2 - 96z^2 = 0,$$

and the polynomial appearing in the left hand side above is precisely the polynomial that appears in equation (30). By Galois theory, the only automorphisms of $\mathbb{L}$ over $\mathbb{Q}$ are those maps σ such that $\sigma(\sqrt{3}) = \varepsilon_1\sqrt{3}$ and

$\sigma(\sqrt{2}) = \varepsilon_2\sqrt{2}$ with $\varepsilon_{1,2} \in \{\pm 1\}$ and leaving the rationals fixed. Thus, taking the conjugates of α_1 are

$$\varepsilon_1\varepsilon_2\frac{\sqrt{8}(1+\varepsilon_1\sqrt{3})}{\sqrt{3}(1+\varepsilon_2\sqrt{8})} \qquad \text{with } \varepsilon_{1,2} \in \{\pm 1\}.$$

From the four numbers above, two of them are < 1.17 and respectively < 2.45 in absolute values, and the absolute values of the other two are < 1. Consequently, we can take

$$A_1 = 7.2 > 4h(\alpha_1) > \log 441 + \log(2.45) + \log(1.17).$$

If

$$\alpha_1 = \frac{\sqrt{8}(1+\sqrt{3})}{\sqrt{3}(5+2\sqrt{8})},$$

we apply a similar procedure. Its minimal polynomial is

$$441X^4 - 4032X^3 + 7488X^2 - 3072X + 256 \in \mathbb{Z}[X].$$

Thus, $a_0 = 441$. Its conjugates are

$$\varepsilon_1\varepsilon_2\frac{\sqrt{8}(1+\varepsilon_1\sqrt{3})}{\sqrt{3}(5+2\varepsilon_2\sqrt{8})} \qquad \text{with } \varepsilon_{1,2} \in \{\pm 1\}.$$

Two of these four numbers are < 6.8 and < 1.9, respectively, in absolute values. The absolute values of the other two are < 1. Thus, we can take

$$A_1 = 8.7 > 4h(\alpha_1) = \log 441 + \log 6.8 + \log 1.9.$$

Since $\mathbb{L}$ is real, Theorem 3.1.2 implies that

$$\log\Lambda > -1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 4^2(1+\log 4)(1+\log n) \cdot 8.7 \cdot 2.7 \cdot 3.6,$$

which yields

$$\log\Lambda > -4.7 \cdot 10^{14}(1+\log n). \tag{31}$$

Comparing the above inequality with inequality (29), we get

$$n\log\zeta < 4.7 \cdot 10^{14}(1+\log n),$$

which yields $n < 1.4 \cdot 10^{16}$. We now have to reduce the above upper bound on n. We put

$$\Gamma := \log\alpha_1 - n\log\alpha_2 + m\log\alpha_3.$$

The right hand side of the above inequality (29) is less than $1/2$ in absolute value so, by the argument used in the proof of the Propositions 3.2.1 and 3.2.2, we deduce that

$$|\Gamma| < \frac{2}{3\zeta^n} < \frac{1}{\zeta^n}. \tag{32}$$

Suppose first that $\Gamma > 0$ (observe that $\Gamma \neq 0$ since $\Lambda \neq 0$). Then

$$0 < m\left(\frac{\log \alpha_3}{\log \alpha_2}\right) - n + \left(\frac{\log \alpha_1}{\log \alpha_2}\right) < \frac{1}{(\log \alpha_2)\zeta^n}.$$

Observe that by the inequalities (27), we have that $\zeta^n > \zeta_1^m \zeta_1^{-1} \zeta^{-2}$, therefore

$$0 < m\left(\frac{\log \alpha_3}{\log \alpha_2}\right) - n + \left(\frac{\log \alpha_1}{\log \alpha_2}\right) < \frac{\zeta^2 \zeta_1}{(\log \alpha_2)\zeta_1^m} < \frac{62}{\zeta_1^m}.$$

Moreover, $m \leq c_1 n + 3 < 1.1 \cdot 10^{16}$. We take $M = 1.1 \cdot 10^{16}$,

$$\gamma = \frac{\log \alpha_3}{\log \alpha_2}, \qquad \mu = \frac{\log \alpha_1}{\log \alpha_2}, \qquad A = 62, \qquad B = \zeta_1.$$

The number

$$\frac{p_{39}}{q_{39}} = C_{39} = \frac{54267087055577066273}{40543232684464392886}$$

is the 39 convergent of γ. We compute ε. The calculation reveals that $\|q_{39}\mu\| \geq 0.0966$, while $M\|q_{39}\alpha\| < 0.0002$. Thus, we can take $\varepsilon = 0.09 < \|q_{39}\mu\| - M\|q_{39}\alpha\|$, and now Lemma 1.4.4 tells us that there is no solution with

$$\frac{\log(Aq_{39}/\varepsilon)}{\log B} \leq m \leq M.$$

The left hand side above is $29.3201\ldots$. Thus, $m \leq 29$. If $\Gamma < 0$ we proceed in a similar way. Namely, in this case the inequality can be rewritten as

$$0 < n\left(\frac{\log \alpha_2}{\log \alpha_3}\right) - m + \frac{\log \alpha_1}{\log \alpha_3} < \frac{2}{3(\log \alpha_3)\zeta^n} < \frac{1}{\zeta^n}.$$

We put

$$\alpha = \frac{\log \alpha_2}{\log \alpha_3}, \quad \mu = \frac{\log \alpha_1}{\log \alpha_3}, \quad A = 1, \quad B = \zeta, \quad M = 1.4 \cdot 10^{16}.$$

We take again q to be the denominator of the 39th convergent of α, we have that $M\|q\alpha\| < 0.0002$, while $\|q\mu\| \geq 0.3033\cdots$. Thus, we can take $\varepsilon = 0.3$. With these numbers,

$$\frac{\log(Aq/\varepsilon)}{\log B} = 34.8477\ldots,$$

therefore $n \leq 34$. The above calculations prove that either $n \leq 34$ (and so that, $m < n \leq 34$) or $m \leq 29$ (in which case we have that $n \leq 42$ by inequality (28)). We now generate the first 33 terms of the sequence $(v_m)_{m\geq 1}$ and compare it with the first 42 terms of the sequence $(u_n)_{n\geq 1}$. For example,

$$\begin{aligned} u_n &= 3,\ 11,\ 41,\ 153,\ 571,\ 2131,\ 7953,\ 29681,\ \ldots, \\ &\quad 829268454325354994627611, \end{aligned}$$

while

$$\begin{aligned} v_m &= 1,\ 4,\ 23,\ 134,\ 781,\ 4552,\ \ldots, \\ &\quad 1240625283605594929207248 4, \end{aligned}$$

or

$$\begin{aligned} v_m &= 2,\ 11,\ 64,\ 373,\ 2174,\ 12671,\ 73852,\ \ldots, \\ &\quad 345341896157850611049261 23. \end{aligned}$$

The largest element in the intersection of the above u and v is $x = 11$, for which $1 + d = 11^2 = 121$, and so $d = 120$. □

3.3 Problems

Problem 3.3.1. *Let $\mathcal{P} = \{p_1, \cdots, p_k\}$ be a finite set of primes and put $\mathcal{S} = \{\pm p_1^{\alpha_1} \cdots p_k^{\alpha_k} : \alpha_i \in \mathbb{Z}, i = 1, \ldots, k\}$ for the set of all rational numbers which when written in reduced form have both the numerator and denominator divisible only by primes in $\mathcal{P}$. Prove, using the theorems from the Sections 3.1.1 and 3.1.2, that the equation*

$$x + y = 1 \qquad x,\ y \in \mathcal{S}$$

has only finitely many solutions (x, y) which, in practice (namely, given $\mathcal{P}$) can be computed explicitly.

Problem 3.3.2. *Prove that given integers $a > b > 1$ the Pillai equation* (16) *has only finitely many nontrivial solutions.*

Problem 3.3.3. *Compute all the solutions of the equation*

$$2^x + 3^y = 5^z$$

in nonnegative integers $x,\ y,\ z$.

Problem 3.3.4. *Compute all solutions of the equation*

$$5^u 7^v - 5^w = 7^x + 1$$

in nonnegative integers $u,\ v,\ w,\ x$.

Problem 3.3.5. *Prove that if* $k \geq 2$ *and* $d > 0$ *are integers such that* $(k-1)d+1,\ (k+1)d+1$ *and* $4kd+1$ *are all three perfect squares, then* $d = 16k^3 - 4k$.

Problem 3.3.6. *Prove that if* $k \geq 2$ *and* $d > 0$ *are integers such that* $F_{2(k-1)}d+1,\ F_{2k}d+1$ *and* $F_{2(k+1)}d+1$ *are all three perfect squares, then* $d = 4F_{2k-1}F_{2k}F_{2k+1}$.

Problem 3.3.7. *Let* p_k *be the* k*-th prime number. Find all the solutions of the Diophantine equation*

$$n! + 1 = p_k^a p_{k+1}^b \qquad \text{with } p_{k-1} \leq n < p_k$$

in integer unknowns $n \geq 1,\ k \geq 2,\ a \geq 0,\ b \geq 0$.

Problem 3.3.8. *(i) Prove that if* $F_n = x^p$ *with* $n \geq 3,\ x \geq 2,\ k \geq 2$ *integers, then* k *is bounded (that is, there are no perfect powers of exponent arbitrarily large in the Fibonacci sequence).*

(ii) Prove that the conclusion of (i) holds also when we replace F_n *by the* n*th term of a nondegenerate binary recurrent sequence (see Definition 2.0.3) whose roots are real.*

Problem 3.3.9. *Using Theorem 3.1.2, prove that there are only finitely many triples* (α, β, n) *with* $n \notin \{1,2,3,4,6\}$ *and coprime integers* $\alpha+\beta = r$ *and* $\alpha\beta = s$ *and such that furthermore* α/β *is not a root of* 1*, such that the* n*-th term of the Lucas sequence of roots* α *and* β *does not admit a primitive divisor. This statement if a weak version of Theorem 2.3.1 whose proof in Chapter 2 was given only under the hypothesis that* α *and* β *are real.*

Problem 3.3.10. *Recall that a palindrome in base* $b \geq 2$ *is a positive integer such that the sequence of its base* b *reads the same from left to right as from right to left. Prove that* $99 = \overline{1100011}_{(2)}$ *is the largest positive integer of the form* $10^n \pm 1$ *which furthermore is a binary palindrome.*

Problem 3.3.11. *Prove that* $F_{10} = 55$ *is the largest Fibonacci number which in base* 10 *is the concatenation of other two Fibonacci numbers (i.e., is the largest solution of the equation* $F_n = \overline{F_\kappa F_\ell}_{(10)}$*).*

Problem 3.3.12. *Let $(u_n)_{n\geq 0}$ be the ternary recurrent sequence such that $u_0 = u_1 = 0,\ u_2 = 1$ and $u_{n+3} = u_{n+1} + u_n$. Find all solutions of the equation $u_n = F_m$ in nonnegative integers n and m.*

Problem 3.3.13. *Let $(u_n)_{n\geq 1}$ and $(v_m)_{m\geq 1}$ be linearly recurrent sequences such that*

$$u_n = c_1\alpha_1^n + \sum_{i=2}^{s} c_i\alpha_i^n; \qquad v_m = d_1\beta_1^m + \sum_{j=2}^{t} d_j\beta_j^m,$$

where $c_1d_1 \neq 0$, $|\alpha_1| > \max\{|\alpha_i| : i = 2, \ldots, s\}$ and $|\beta_1| > \max\{|\beta_j| : j = 2, \ldots, t\}$. Suppose furthermore that α_1 and β_1 are multiplicatively independent; that is, the only solution to the equation

$$\alpha_1^x\beta_1^y = 1$$

in integers x and y is $x = y = 0$. Prove that the Diophantine equation $u_n = v_m$ has only finitely many, effectively computable, positive integer solutions (m, n).

Problem 3.3.14. *Let $P(m)$ be the largest prime factor of m. Prove that*

$$P(2^p - 1) \gg p \log p.$$

Problem 3.3.15. *Let $(u_n)_{n\geq 0}$ be a nondegenerate binary recurrent sequence. Prove that $P(|u_n|) \gg n^{1/(d+1)}$, where $d = [\mathbb{K} : \mathbb{Q}]$ and $\mathbb{K} = \mathbb{Q}[\alpha]$ is the splitting field of the characteristic equation of the sequence $(u_n)_{n\geq 1}$.*

Problem 3.3.16. *Prove that there are only finitely many positive integer solutions (p, a, k) with $p \geq 3$ prime such that*

$$a^{p-1} + (p-1)! = p^k.$$

Can you compute them all?

Problem 3.3.17. *(i) Prove that if $k \geq 1$ is fixed, then there are only finitely many positive integer solutions of the equation*

$$F_n = m_1! + m_2! + \cdots + m_k! \qquad \text{with } 1 \leq m_1 \leq \cdots \leq m_k.$$

(ii) Prove that when $k = 2$ the largest solution of the equation appearing at (i) is $F_{12} = 3! + 4!$.

Problem 3.3.18. *(i) Prove that*

$$P(2^n + 3^n + 5^n) \to \infty \qquad as \qquad n \to \infty.$$

(ii) Deduce that there are only finitely many n such that $P(2^n+3^n+5^n) < 23$. Can you find them all? For example,

$$2^1 + 3^1 + 5^1 = 2 \cdot 5;$$

$$2^2 + 3^2 + 5^2 = 2 \cdot 19;$$

$$2^3 + 3^3 + 5^3 = 2^5 \cdot 5;$$

$$2^4 + 3^4 + 5^4 = 2 \cdot 19^2;$$

$$2^5 + 3^5 + 5^5 = 2^3 \cdot 5^2 \cdot 17.$$

Are there other values of n?

3.4 Notes

An elementary proof of Proposition 3.2.1 appears in [45]. The conclusion of Problem 3.3.1 is known as the theorem of the finiteness of the number of solutions of an equation in two $\mathcal{S}$-units. See the first two chapters of the book [73]. Problems 3.3.2, 3.3.3 and 3.3.4 are similar to Proposition 3.2.2. See [63] for a problem which is slightly more general, and [7] for an elementary treatment of Problems 3.3.3 and 3.3.4. The results of Problems 3.3.5 and 3.3.6 are due to Dujella [23] and [24]. Observe that these problems generalize the result of Proposition 3.2.3. A set $\{a_1, \ldots, a_m\}$ of positive integers such that $a_i a_j + 1$ is a perfect square is called a *Diophantine m-tuple*. It is conjectured that $m \leq 4$. Dujella [25], proved that $m \leq 5$ and that there can be at most finitely many Diophantine quintuples which are, in practice, effectively computable, but the available upper bounds are too large to allow one to enumerate all the possibilities. All the solutions to the equation appearing in Problem 3.3.7 were computed by Luca in [48]. The largest one is $5! + 1 = 11^2$. Concerning Problem 3.3.8, it is known that the largest perfect power in the Fibonacci sequence is $F_{12} = 144$ (see [8]). The result of (ii) was obtained independently by Pethő [65] and by Shorey and Stewart [72]. For Problem 3.3.9, see Stewart's paper [74], or the more modern paper [5]. Problem 3.3.10 is due to Luca and Togbé [56]. Problem 3.3.11 is a result of Banks and Luca [4]. For Problem 3.3.12, see De Weger's paper [19]. The result of Problem 3.3.14 was obtained idependently by

Erdős and Shorey in [31] and Stewart in [76]. The result of Problem 3.3.15 is due to Stewart [75]. Computing all triples (a, p, k) of Problem 3.3.16 was a problem proposed by Erdős and Graham in [29] and solved by Yu and Liu in [83]. The only solutions are $(a, p, k) = (1, 3, 1), (1, 5, 2), (5, 3, 3)$. The result of Problem 3.3.17 is due to Grossman and Luca [35].

Bibliography

[1] M. Ayad and F. Luca, "Two divisors of $(n^2+1)/2$ summing up to $n+1$", *J. Theorie Nombres Bordeaux* **19** (2007), 561–566.

[2] A. Baker, "Linear forms in logarithms of algebraic numbers. I, II, III", *Mathematika* **13** (1966); 204–216, ibid. **14** (1967), 102–107; ibid. **14** (1967), 220–228.

[3] A. Baker and H. Davenport, "The equations $3x^2-2=y^2$ and $8x^2-7=z^2$", *Quart. J. Math. Oxford Ser. (2)* **20** (1969), 129–137.

[4] W. D. Banks and F. Luca, "Concatenations with binary recurrent sequences", *J. Integer Seq.* **8** (2005), Article 05.1.3, 19pg.

[5] Yu. Bilu, G. Hanrot and P. M. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte", *J. Reine Angew. Math.* **539** (2001), 75–122.

[6] G. D. Birkhoff and H. S. Vandiver, "On the integral divisors of $a^n \pm b^n$", *Ann. Math. (2)* **5** (1904), 173–180.

[7] J. L. Brenner y L. L. Foster, "Exponential Diophantine equations", *Pacific J. Math.* **101** (1982), 263–301.

[8] Y. Bugeaud, M. Mignotte and S. Siksek, "Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers", *Ann. of Math. (2)* **163** (2006), 969–1018.

[9] R. D. Carmichael,"On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$", *Ann. Math. (2)* **15** (1913), 30–70.

[10] R. D. Carmichael, *The Theory of Numbers and Diophantine Analysis*, New York, Dover, 1952.

[11] E. Catalan, "Note extraite d'une lettre adressée à l'editeur", *J. Reine Angew. Math.* **27** (1844), 192.

[12] J. H. E. Cohn, "Square Fibonacci numbers, etc.", *Fibonacci Quart.* **2** (1964), 109–113.

[13] J. H. E. Cohn, "Lucas and Fibonacci numbers and some Diophantine equations", *Proc. Glasgow Math. Assoc.* **7** (1965), 24–28.

[14] J. H. E. Cohn, "The length of the period of the simple continued fraction of $d^{1/2}$", *Pacific J. Math.* **71** (1977), 21–32.

[15] H. Cohn and B. M. M. de Weger, "Solution to **10457**", *Amer. Math. Monthly* **104** (1997), 875.

[16] B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI Tract, **65** Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[17] B. M. M. de Weger, "A curious property of the eleventh Fibonacci number", *Rocky Mountain J. Math.* **25** (1995), 977–994.

[18] B. M. M. de Weger, "A binomial Diophantine equation", *Quart. J. Math. Oxford Ser. (2)* **47** (1996), 221–231.

[19] B. M. M. de Weger, "Padua and Pisa are exponentially far apart", *Publ. Mat.* **41** (1997), 631–651.

[20] M. Mignotte and B. M. M. de Weger, "On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$", *Glasgow Math. J.* **38** (1996), 77–85.

[21] B. M. M. de Weger and A. Pintér, "$210 = 14 \times 15 = 5 \times 6 \times 7 = \binom{21}{2} = \binom{10}{4}$", *Publ. Math. Debrecen* **51** (1997), 175–189.

[22] B. M. M. de Weger and N. Tzanakis, "On the practical solution of the Thue equation", *J. Number Theory* **31** (1989), 99–132.

[23] A. Dujella, "The problem of the extension of a parametric family of Diophantine triples", *Publ. Math. Debrecen* **51** (1997), 311–322.

[24] A. Dujella, "A proof of the Hoggatt-Bergum conjecture", *Proc. Amer. Math. Soc.* **127** (1999), 1999–2005.

[25] A. Dujella, "There are only finitely many Diophantine quintuples", *J. Reine Angew. Math.* **566** (2004), 183–214.

[26] A. Dujella and B. Jadrijević, "A family of quartic Thue inequalities", *Acta Arith.* **111** (2004), 61–76.

[27] A. Dujella and A. Pethő, "A generalization of a theorem of Baker and Davenport", *Quart. J. Math. Oxford Ser. (2)* **49** (1998), 291–306.

[28] T. Erdélyi, "On the equation $a(a+d)(a+2d)(a+3d) = x^2$", *Amer. Math. Monthly* **107** (2000), 166–169.

[29] P. Erdős and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématique **28** Université de Genève, *L'Enseignement Mathématique*, Geneva, 1980. 128 pp.

[30] P. Erdős and J. L. Selfridge, "The product of consecutive integers is never a power", *Illinois J. Math.* **19** (1975), 292–301.

[31] P. Erdős and T. N. Shorey, "On the greatest prime factor of $2^p - 1$ for a prime p and other expressions", *Acta Arith.* **30** (1976), 257–265.

[32] J. Esmonde y M. R. Murty, *Problems in Algebraic Number Theory*, Springer-Verlag, New York, 1999.

[33] G. Everest, A. van der Poorten, Alf, I. Shparlinski and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs, **104** American Mathematical Society, Providence, RI, 2003.

[34] I. Gaál, I. Járási and F. Luca, "A remark on prime divisors of lengths of sides of Heron triangles", *Experiment. Math.* **12** (2003), 303–310.

[35] G. Grossman and F. Luca, "Sums of factorials in binary recurrence sequences", *J. Number Theory* **93** (2002), 87–107.

[36] L. Hajdu and L. Szalay, "On the Diophantine equations $(2^n - 1)(6^n - 1) = x^2$ and $(a^n - 1)(a^{kn} - 1) = x^2$", *Period. Math. Hungar.* **40** (2000), 141–145.

[37] L. K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin-New York, 1982.

[38] J. F. Koksma, "On continued fraction", *Simon Stevin* **29** (1951/52), 96–102.

[39] M. Křížek and F. Luca, "On the solutions of the congruence $n^2 \equiv 1 \pmod{\phi^2(n)}$", *Proc. Amer. Math. Soc.* **129** (2001), 2191–2196.

[40] S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley, Reading, 1966.

[41] M. Laurent, M. Mignotte and Yu. Nesterenko,"Formes linéaires en deux logarithmes et déterminants d'interpolation", *J. Number Theory* **55** (1995), 285–321.

[42] V. A. Lebesgue, "Sur l'impossibilité en nombres entiers de l'quation $x^m = y^2 + 1$", *Nouv. Ann. Math.* **9** (1850), 178–181.

[43] H. London and R. Finkelstein, "On Fibonacci and Lucas numbers which are perfect powers", *Fibonacci Quart.* **5** (1969), 476–481.

[44] F. Luca, "A note on the Pell equation", *Indian J. Math.* **39** (1997), 99–105.

[45] F. Luca, "Fibonacci and Lucas numbers with only one distinct digit", *Portugal. Math.* **57** (2000), 243–254.

[46] F. Luca, "Perfect cuboids and perfect square triangles", *Math. Mag.* **73** (2000), 400–401.

[47] F. Luca, "Fermat numbers in the Pascal triangle", *Divulg. Mat.* **9** (2001), 189–194.

[48] F. Luca, "On a conjecture of Erdős and Stewart", *Math. Comp.* **70** (2001), 893–896.

[49] F. Luca, "On the equation $x^2 + 2^a 3^b = y^n$", *Int. J. Math. Math. Sci.* **29** (2002), 239–244.

[50] F. Luca, "Consecutive binomial coefficients in Pythagorean triples and squares in the Fibonacci sequence", *Fibonacci Quart.* **40** (2002), 76–78.

[51] F. Luca, "On the equation $\sum_{i=1}^{n} (i!)^k = x^2$", *Per. Math. Hungarica* **44** (2002), 217–222.

[52] F. Luca, "Fermat primes and Heron triangles with prime power sides", *Amer. Math. Monthly* **110** (2003), 46–49.

[53] F. Luca, "Fibonacci numbers with the Lehmer property", *Bull. Pol. Acad. Sci. Math.* **55** (2007), 7–15.

[54] F. Luca, "On the largest prime factor of sides of a Heron triangle", *Elem. Math.*, to appear.

[55] F. Luca, C. F. Osgood and P. G. Walsh, "Diophantine approximations and a problem from the 1988 IMO", *Rocky Mountain J. Math.* **36** (2006), 637–648.

[56] F. Luca and A. Togbé, "When is $10^n \pm 1$ a binary palindrome?", *C.R. Acad. Sci. Paris* **346** (2008), 487–489.

[57] F. Luca and J. L. Varona, "Multiperfect numbers on lines of the Pascal triangle", *J. Number Theory*, to appear.

[58] F. Luca and P. G. Walsh, "The product of like-indexed terms in binary recurrences", *J. Number Theory* **96** (2002), 152–173.

[59] E. M. Matveev, "An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II", *Izv. Ross. Akad. Nauk Ser. Mat.* **64** (2000), 125–180; English translation in *Izv. Math.* **64** (2000), 1217–1269.

[60] M. Mignotte and A. Pethő, "On the system of Diophantine equations $x^2 - 6y^2 = -5$ and $x = 2z^2 - 1$", *Math. Scand.* **76** (1995), 50–60.

[61] M. Mignotte and A. Pethő, "On the Diophantine equation $x^p - x = y^q - y$", *Publ. Mat.* **43** (1999), 207–216.

[62] P. Mihăilescu, "Primary cyclotomic units and a proof of Catalan's conjecture", *J. Reine Angew. Math.* **572** (2004), 167–195.

[63] D. Z. Mo and R. Tijdeman, "Exponential Diophantine equations with four terms", *Indag. Math. (N.S.)* **3** (1992), 47–57.

[64] T. Nagell, "The diophantine equation $x^2+7 = 2^n$", *Ark. Math.* **4** (1960), 185–187.

[65] A. Pethő, "Perfect powers in second order linear recurrences", *J. Number Theory* **15** (1982), 5–13.

[66] S. S. Pillai, "On $a^x - b^y = c$", *J. Indian Math. Soc. (N.S.)* **2** (1936), 119–122.

[67] C. Pomerance and U. Everling, "Solution to **10331**", *Amer. Math. Monthly* **103** (1996), 701–702.

[68] A. M. Rockett and P. Szüsz, *Continued fractions*, World Scientific, Singapore, 1992.

[69] H. Ruderman and C. Pomerance, "Solution to **E2468**", *Amer. Math. Monthly* **84** (1977), 59–60.

[70] C. Runge, "Uber ganzzahlige Losungen von Gleichungen zwischen zwei Veranderlichen", *J. Reine Angew. Math.* **100** (1887), 425–435.

[71] A. Schinzel, "Primitive divisors of the expression $A^n - B^n$ in algebraic number fields", *J. reine angew. Math.* **268/269** (1974), 27–33.

[72] T. N. Shorey and C. L. Stewart, "On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences", *Math. Scand.* **52** (1983), 24–36.

[73] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Mathematics, **87** Cambridge University Press, Cambridge, 1986.

[74] C. L. Stewart, "Primitive divisors of Lucas and Lehmer numbers", en *Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976)*, 79–92. Academic Press, London, 1977.

[75] C. L. Stewart, "On divisors of terms of linear recurrence sequences", *J. Reine Angew. Math.* **333** (1982), 12–31.

[76] C. L. Stewart, "On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. III", *J. London Math. Soc. (2)* **28** (1983), 211–217.

[77] S. R. Stroeker and B. M. M. de Weger, "On a quartic Diophantine equation", *Proc. Edinburgh Math. Soc. (2)* **39** (1996), 97–114.

[78] L. Szalay, "On the Diophantine equation $(2^n - 1)(3^n - 1) = x^2$", *Publ. Math. Debrecen* **57** (2000), 1–9.

[79] A. Thue, "Ueber Annäherungswerte algebraischer Zahlen", *J. reine angew. Math.* **135** (1909), 284–305.

[80] P. Vandendriessche and H. J. Lee, *Problems in Elementary Number Theory*, http://www.mathlinks.ro/.

[81] R. T. Worley, "Estimating $|\alpha - p/q|$", *J. Austral. Math. Soc.* **31** (1981), 202–206.

[82] K. Yu: "p-adic logarithmic forms and group varieties II", *Acta Arith.* **89** (1999), 337–378.

[83] K. Yu and D. Liu, "A complete resolution of a problem of Erdős and Graham", en *Symposium on Diophantine Problems (Boulder, CO, 1994)*, *Rocky Mountain J. Math.* **26** (1996), 1235–1244.

[84] R. Zimmert, "Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung", *Invent. Math.* **62** (1981), 367–380.

[85] K. Zsigmondy, "Zur Theorie der Potenzreste", *Monatsh. Math.* **3** (1892), 265–284.