20 mai 2015

18 - 29 mai 2015: Oujda (Maroc)
École de recherche CIMPA-Oujda
Théorie des Nombres et ses Applications.

Continued fractions

Michel Waldschmidt

We first consider generalized continued fractions of the form

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{\ddots}}},$$

which we denote by[1]

$$a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \frac{b_3|}{\ddots}\cdot$$

Next we restrict to the special case where $b_1 = b_2 = \cdots = 1$, which yields the simple continued fractions

$$a_0 + \frac{1\,|}{|a_1} + \frac{1\,|}{|a_2} + \cdots = [a_0, a_1, a_2, \dots].$$

We conclude by considering the so–called Fermat–Pell equation.

[1] Another notation for $a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \cdots + \frac{b_n|}{a_n}$ introduced by Th. Muir and used by Perron in [9] Chap. 1 is

$$K\begin{pmatrix} b_1, \dots, b_n \\ a_0, a_1, \dots, a_n \end{pmatrix}$$

1 Generalized continued fractions

To start with, $a_0, \dots, a_n, \dots$ and $b_1, \dots, b_n, \dots$ will be independent variables. Later, we shall specialize to positive integers (apart from a_0 which may be negative).

Consider the three rational fractions

$$a_0, \qquad a_0 + \frac{b_1}{a_1} \quad \text{and} \quad a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2}}.$$

We write them as

$$\frac{A_0}{B_0}, \qquad \frac{A_1}{B_1} \quad \text{and} \quad \frac{A_2}{B_2}$$

with

$$\begin{array}{lll} A_0 = a_0, & A_1 = a_0a_1 + b_1, & A_2 = a_0a_1a_2 + a_0b_2 + a_2b_1, \\ B_0 = 1, & B_1 = a_1, & B_2 = a_1a_2 + b_2. \end{array}$$

Observe that

$$A_2 = a_2A_1 + b_2A_0, \quad B_2 = a_2B_1 + b_2B_0.$$

Write these relations as

$$\begin{pmatrix} A_2 & A_1 \\ B_2 & B_1 \end{pmatrix} = \begin{pmatrix} A_1 & A_0 \\ B_1 & B_0 \end{pmatrix} \begin{pmatrix} a_2 & 1 \\ b_2 & 0 \end{pmatrix}.$$

Define inductively two sequences of polynomials with positive rational coefficients A_n and B_n for $n \geq 3$ by

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ b_n & 0 \end{pmatrix}. \tag{1}$$

This means

$$A_n = a_nA_{n-1} + b_nA_{n-2}, \qquad B_n = a_nB_{n-1} + b_nB_{n-2}.$$

This recurrence relation holds for $n \geq 2$. It will also hold for $n = 1$ if we set $A_{-1} = 1$ and $B_{-1} = 0$:

$$\begin{pmatrix} A_1 & A_0 \\ B_1 & B_0 \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ b_1 & 0 \end{pmatrix}$$

and it will hold also for $n = 0$ if we set $b_0 = 1$, $A_{-2} = 0$ and $B_{-2} = 1$:

$$\begin{pmatrix} A_0 & A_{-1} \\ B_0 & B_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ b_0 & 0 \end{pmatrix}.$$

Obviously, an equivalent definition is

$$(2) \qquad \begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ b_0 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ b_1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1} & 1 \\ b_{n-1} & 0 \end{pmatrix} \begin{pmatrix} a_n & 1 \\ b_n & 0 \end{pmatrix}.$$

These relations (2) hold for $n \geq -1$, with the empty product (for $n = -1$) being the identity matrix, as always.

Hence $A_n \in \mathbb{Z}[a_0, \ldots, a_n, b_1, \ldots, b_n]$ is a polynomial in $2n+1$ variables, while $B_n \in \mathbb{Z}[a_1 \ldots, a_n, b_2, \ldots, b_n]$ is a polynomial in $2n-1$ variables.

Exercise 1. *Check, for $n \geq -1$,*

$$B_n(a_1, \ldots, a_n, b_2, \ldots, b_n) = A_{n-1}(a_1, \ldots, a_n, b_2, \ldots, b_n).$$

Lemma 3. *For $n \geq 0$,*

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_n|}{|a_n} = \frac{A_n}{B_n}\cdot$$

Proof. By induction. We have checked the result for $n = 0$, $n = 1$ and $n = 2$. Assume the formula holds with $n-1$ where $n \geq 3$. We write

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|x}$$

with

$$x = a_{n-1} + \frac{b_n}{a_n}\cdot$$

We have, by induction hypothesis and by the definition (1),

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} = \frac{A_{n-1}}{B_{n-1}} = \frac{a_{n-1}A_{n-2} + b_{n-1}A_{n-3}}{a_{n-1}B_{n-2} + b_{n-1}B_{n-3}}\cdot$$

Since A_{n-2}, A_{n-3}, B_{n-2} and B_{n-3} do not depend on the variable a_{n-1}, we deduce

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|x} = \frac{xA_{n-2} + b_{n-1}A_{n-3}}{xB_{n-2} + b_{n-1}B_{n-3}}\cdot$$

The product of the numerator by a_n is

$$\begin{aligned}(a_na_{n-1}+b_n)A_{n-2}+a_nb_{n-1}A_{n-3} &= a_n(a_{n-1}A_{n-2}+b_{n-1}A_{n-3})+b_nA_{n-2}\\ &= a_nA_{n-1}+b_nA_{n-2}=A_n\end{aligned}$$

and similarly, the product of the denominator by a_n is

$$\begin{aligned}(a_na_{n-1}+b_n)B_{n-2}+a_nb_{n-1}B_{n-3} &= a_n(a_{n-1}B_{n-2}+b_{n-1}B_{n-3})+b_nB_{n-2}\\ &= a_nB_{n-1}+b_nB_{n-2}=B_n.\end{aligned}$$

$\square$

From (2), taking the determinant, we deduce, for $n \geq -1$,

(4) $$A_nB_{n-1}-A_{n-1}B_n=(-1)^{n+1}b_0\cdots b_n.$$

which can be written, for $n \geq 1$,

(5) $$\frac{A_n}{B_n}-\frac{A_{n-1}}{B_{n-1}}=\frac{(-1)^{n+1}b_0\cdots b_n}{B_{n-1}B_n}\cdot$$

Adding the telescoping sum, we get, for $n \geq 0$,

(6) $$\frac{A_n}{B_n}=A_0+\sum_{k=1}^{n}\frac{(-1)^{k+1}b_0\cdots b_k}{B_{k-1}B_k}\cdot$$

We now substitute for $a_0, a_1, \ldots$ and $b_1, b_2, \ldots$ rational integers, all of which are ≥ 1, apart from a_0 which may be ≤ 0. We denote by p_n (resp. q_n) the value of A_n (resp. B_n) for these special values. Hence p_n and q_n are rational integers, with $q_n > 0$ for $n \geq 0$. A consequence of Lemma 3 is

$$\frac{p_n}{q_n}=a_0+\frac{b_1|}{|a_1}+\cdots+\frac{b_n|}{|a_n}\quad\text{for}\quad n\geq 0.$$

We deduce from (1),

$$p_n=a_np_{n-1}+b_np_{n-2},\qquad q_n=a_nq_{n-1}+b_nq_{n-2}\quad\text{for}\quad n\geq 0,$$

and from (4),

$$p_nq_{n-1}-p_{n-1}q_n=(-1)^{n+1}b_0\cdots b_n\quad\text{for}\quad n\geq -1,$$

which can be written, for $n \geq 1$,

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n+1} b_0 \cdots b_n}{q_{n-1} q_n}. \tag{7}$$

Adding the telescoping sum (or using (6)), we get the alternating sum

$$\frac{p_n}{q_n} = a_0 + \sum_{k=1}^{n} \frac{(-1)^{k+1} b_0 \cdots b_k}{q_{k-1} q_k}. \tag{8}$$

Recall that for real numbers a, b, c, d, with b and d positive, we have

$$\frac{a}{b} < \frac{c}{d} \implies \frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}. \tag{9}$$

Since a_n and b_n are positive for $n \geq 0$, we deduce that for $n \geq 2$, the rational number

$$\frac{p_n}{q_n} = \frac{a_n p_{n-1} + b_n p_{n-2}}{a_n q_{n-1} + b_n q_{n-2}}$$

lies between p_{n-1}/q_{n-1} and p_{n-2}/q_{n-2}. Therefore we have

$$\frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \frac{p_{2n}}{q_{2n}} < \cdots < \frac{p_{2m+1}}{q_{2m+1}} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}. \tag{10}$$

From (7), we deduce, for $n \geq 3$, $q_{n-1} > q_{n-2}$, hence $q_n > (a_n + b_n) q_{n-2}$.

The previous discussion was valid without any restriction, now we assume $a_n \geq b_n$ for all sufficiently large n, say $n \geq n_0$. Then for $n > n_0$, using $q_n > 2 b_n q_{n-2}$, we get

$$\left| \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} \right| = \frac{b_0 \cdots b_n}{q_{n-1} q_n} < \frac{b_n \cdots b_0}{2^{n-n_0} b_n b_{n-1} \cdots b_{n_0+1} q_{n_0} q_{n_0-1}} = \frac{b_{n_0} \cdots b_0}{2^{n-n_0} q_{n_0} q_{n_0-1}}$$

and the right hand side tends to 0 as n tends to infinity. Hence the sequence $(p_n/q_n)_{n \geq 0}$ has a limit, which we denote by

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} + \cdots$$

From (8), it follows that x is also given by an alternating series

$$x = a_0 + \sum_{k=1}^{\infty} \frac{(-1)^{k+1} b_0 \cdots b_k}{q_{k-1} q_k}.$$

We now prove that x is irrational. Define, for $n \geq 0$,

$$x_n = a_n + \frac{b_{n+1}|}{|a_{n+1}} + \cdots$$

so that $x = x_0$ and, for all $n \geq 0$,

$$x_n = a_n + \frac{b_{n+1}}{x_{n+1}}, \qquad x_{n+1} = \frac{b_{n+1}}{x_n - a_n}$$

and $a_n < x_n < a_n + 1$. Hence for $n \geq 0$, x_n is rational if and only if x_{n+1} is rational, and therefore, if x is rational, then all x_n for $n \geq 0$ are also rational. Assume x is rational. Consider the rational numbers x_n with $n \geq n_0$ and select a value of n for which the denominator v of x_n is minimal, say $x_n = u/v$. From

$$x_{n+1} = \frac{b_{n+1}}{x_n - a_n} = \frac{b_{n+1}v}{u - a_n v} \quad \text{with} \quad 0 < u - a_n v < v,$$

it follows that x_{n+1} has a denominator strictly less than v, which is a contradiction. Hence x is irrational.

Conversely, given an irrational number x and a sequence $b_1, b_2, \ldots$ of positive integers, there is a unique integer a_0 and a unique sequence $a_1, \ldots, a_n, \ldots$ of positive integers satisfying $a_n \geq b_n$ for all $n \geq 1$, such that

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} + \cdots$$

Indeed, the unique solution is given inductively as follows: $a_0 = \lfloor x \rfloor$, $x_1 = b_1/\{x\}$, and once $a_0, \ldots, a_{n-1}$ and $x_1, \ldots, x_n$ are known, then a_n and x_{n+1} are given by

$$a_n = \lfloor x_n \rfloor, \quad x_{n+1} = b_{n+1}/\{x_n\},$$

so that for $n \geq 1$ we have $0 < x_n - a_n < 1$ and

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|x_n}.$$

Here is what we have proved.

Proposition 1. *Given a rational integer a_0 and two sequences $a_0, a_1, \ldots$ and $b_1, b_2, \ldots$ of positive rational integers with $a_n \geq b_n$ for all sufficiently large n, the infinite continued fraction*

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} + \cdots$$

exists and is an irrational number.
Conversely, given an irrational number x and a sequence $b_1, b_2, \dots$ of positive integers, there is a unique $a_0 \in \mathbb{Z}$ and a unique sequence $a_1, \dots, a_n, \dots$ of positive integers satisfying $a_n \geq b_n$ for all $n \geq 1$ such that

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} + \cdots$$

These results are useful for proving the irrationality of π and e^r when r is a non–zero rational number, following the proof by Lambert. See for instance Chapter 7 (Lambert's Irrationality Proofs) of David Angell's course on Irrationality and Transcendence([2]) at the University of New South Wales:

`http://www.maths.unsw.edu.au/ angell/5535/`

The following example is related with Lambert's proof of the irrationality of π

$$\tanh z = \frac{z|}{|1} + \frac{z^2|}{|\,3} + \frac{z^2|}{|\,5} + \cdots + \frac{z^2\quad|}{|2n+1} + \cdots$$

Here, z is a complex number and the right hand side is a complex valued function. Here are other examples (see Sloane's Encyclopaedia of Integer Sequences([3]))

$$\frac{1}{\sqrt{e}-1} = 1 + \frac{2|}{|3} + \frac{4|}{|5} + \frac{6|}{|7} + \frac{8|}{|9} + \cdots = 1.541\,494\,082\dots \qquad \text{(A113011)}$$
$$\frac{1}{e-1} = \frac{1|}{|1} + \frac{2|}{|2} + \frac{3|}{|3} + \frac{4|}{|4} + \cdots = 0.581\,976\,706\dots \qquad \text{(A073333)}$$

Remark 1. *A variant of the algorithm of simple continued fractions is the following. Given two sequences $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ of elements in a field K and an element x in K, one defines a sequence (possibly finite) $(x_n)_{n\geq 1}$ of elements in K as follows. If $x = a_0$, the sequence is empty. Otherwise x_1 is defined by $x = a_0 + (b_1/x_1)$. Inductively, once $x_1, \dots, x_n$ are defined, there are two cases:*

- *If $x_n = a_n$, the algorithm stops.*
- *Otherwise, x_{n+1} is defined by*

$$x_{n+1} = \frac{b_{n+1}}{x_n - a_n}, \qquad \text{so that} \quad x_n = a_n + \frac{b_{n+1}}{x_{n+1}}\cdot$$

[2] I found this reference from the website of John Cosgrave `http://staff.spd.dcu.ie/johnbcos/transcendental_numbers.htm`.
[3] `http://www.research.att.com/~njas/sequences/`

If the algorithm does not stop, then for any $n \geq 1$, one has

$$x = a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|x_n}\cdot$$

In the special case where $a_0 = a_1 = \cdots = b_1 = b_2 = \cdots = 1$, the set of x such that the algorithm stops after finitely many steps is the set $(F_{n+1}/F_n)_{n\geq 1}$ of quotients of consecutive Fibonacci numbers. In this special case, the limit of

$$a_0 + \frac{b_1|}{|a_1} + \cdots + \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n}$$

is the Golden ratio, which is independent of x, of course!

2 Simple continued fractions

We restrict now the discussion of § 1 to the case where $b_1 = b_2 = \cdots = b_n = \cdots = 1$. We keep the notations A_n and B_n which are now polynomials in $\mathbb{Z}[a_0, a_1, \ldots, a_n]$ and $\mathbb{Z}[a_1, \ldots, a_n]$ respectively, and when we specialize to integers $a_0, a_1, \ldots, a_n \ldots$ with $a_n \geq 1$ for $n \geq 1$ we use the notations p_n and q_n for the values of A_n and B_n.

The recurrence relations (1) are now, for $n \geq 0$,

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}, \tag{11}$$

while (2) becomes, for $n \geq -1$,

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}. \tag{12}$$

From Lemma 3 one deduces, for $n \geq 0$,

$$[a_0, \ldots, a_n] = \frac{A_n}{B_n}\cdot$$

Taking the determinant in (12), we deduce the following special case of (4)

$$A_n B_{n-1} - A_{n-1} B_n = (-1)^{n+1}. \tag{13}$$

The specialization of these relations to integral values of $a_0, a_1, a_2 \ldots$ yields

$$(14) \qquad \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{for } n \geq 0,$$

(15)
$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{for } n \geq -1,$$

$$(16) \qquad [a_0, \ldots, a_n] = \frac{p_n}{q_n} \qquad \text{for } n \geq 0$$

and

$$(17) \qquad p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1} \qquad \text{for } n \geq -1.$$

From (17), it follows that for $n \geq 0$, the fraction p_n/q_n is in lowest terms: $\gcd(p_n, q_n) = 1$.

Transposing (15) yields, for $n \geq -1$,

$$\begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}$$

from which we deduce, for $n \geq 1$,

$$[a_n, \ldots, a_0] = \frac{p_n}{p_{n-1}} \quad \text{and} \quad [a_n, \ldots, a_1] = \frac{q_n}{q_{n-1}}$$

Lemma 18. *For $n \geq 0$,*

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n.$$

Proof. We multiply both sides of (14) on the left by the inverse of the matrix

$$\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \qquad \text{which is} \quad (-1)^n \begin{pmatrix} q_{n-2} & -p_{n-2} \\ -q_{n-1} & p_{n-1} \end{pmatrix}.$$

We get

$$(-1)^n \begin{pmatrix} p_n q_{n-2} - p_{n-2} q_n & p_{n-1} q_{n-2} - p_{n-2} q_{n-1} \\ -p_n q_{n-1} + p_{n-1} q_n & 0 \end{pmatrix} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$$

$\square$

2.1 Finite simple continued fraction of a rational number

Let u_0 and u_1 be two integers with u_1 positive. The first step in Euclid's algorithm to find the gcd of u_0 and u_1 consists in dividing u_0 by u_1:

$$u_0 = a_0 u_1 + u_2$$

with $a_0 \in \mathbb{Z}$ and $0 \leq u_2 < u_1$. This means

$$\frac{u_0}{u_1} = a_0 + \frac{u_2}{u_1},$$

which amonts to dividing the rational number $x_0 = u_0/u_1$ by 1 with quotient a_0 and remainder $u_2/u_1 < 1$. This algorithms continues with

$$u_m = a_m u_{m+1} + u_{m+2},$$

where a_m is the integral part of $x_m = u_m/u_{m+1}$ and $0 \leq u_{m+2} < u_{m+1}$, until some $u_{\ell+2}$ is 0, in which case the algorithms stops with

$$u_\ell = a_\ell u_{\ell+1}.$$

Since the gcd of u_m and u_{m+1} is the same as the gcd of u_{m+1} and u_{m+2}, it follows that the gcd of u_0 and u_1 is $u_{\ell+1}$. This is how one gets the regular continued fraction expansion $x_0 = [a_0, a_1, \ldots, a_\ell]$, where $\ell = 0$ in case x_0 is a rational integer, while $a_\ell \geq 2$ if x_0 is a rational number which is not an integer.

Proposition 2. *Any finite regular continued fraction*

$$[a_0, a_1, \ldots, a_n],$$

where $a_0, a_1, \ldots, a_n$ are rational numbers with $a_i \geq 2$ for $1 \leq i \leq n$ and $n \geq 0$, represents a rational number. Conversely, any rational number x has two representations as a continued fraction, the first one, given by Euclid's algorithm, is

$$x = [a_0, a_1, \ldots, a_n]$$

and the second one is

$$x = [a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1].$$

If $x \in \mathbb{Z}$, then $n = 0$ and the two simple continued fractions representations of x are $[x]$ and $[x-1, 1]$, while if x is not an integer, then $n \geq 1$ and $a_n \geq 2$.

We shall use later (in the proof of Lemma 26 in § 3.7) the fact that any rational number has one simple continued fraction expansion with an odd number of terms and one with an even number of terms.

2.2 Infinite simple continued fraction of an irrational number

Given a rational integer a_0 and an infinite sequence of positive integers $a_1, a_2, \ldots$, the continued fraction

$$[a_0, a_1, \ldots, a_n, \ldots]$$

represents an irrational number. Conversely, given an irrational number x, there is a unique representation of x as an infinite simple continued fraction

$$x = [a_0, a_1, \ldots, a_n, \ldots]$$

Definitions The numbers a_n are the *partial quotients*, the rational numbers

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$$

are the *convergents* (in French *réduites*), and the numbers

$$x_n = [a_n, a_{n+1}, \ldots]$$

are the *complete quotients.*

From these definitions we deduce, for $n \geq 0$,

$$x = [a_0, a_1, \ldots, a_n, x_{n+1}] = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}. \tag{19}$$

Lemma 20. *For $n \geq 0$,*

$$q_n x - p_n = \frac{(-1)^n}{x_{n+1}q_n + q_{n-1}}.$$

Proof. From (19) one deduces

$$x - \frac{p_n}{q_n} = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{(x_{n+1}q_n + q_{n-1})q_n} \cdot$$

□

Corollary 1. *For $n \geq 0$,*

$$\frac{1}{q_{n+1} + q_n} < |q_n x - p_n| < \frac{1}{q_{n+1}} \cdot$$

Proof. Since a_{n+1} is the integral part of x_{n+1}, we have

$$a_{n+1} < x_{n+1} < a_{n+1} + 1.$$

Using the recurrence relation $q_{n+1} = a_{n+1}q_n + q_{n-1}$, we deduce

$$q_{n+1} < x_{n+1}q_n + q_{n-1} < a_{n+1}q_n + q_{n-1} + q_n = q_{n+1} + q_n.$$

□

In particular, since $x_{n+1} > a_{n+1}$ and $q_{n-1} > 0$, one deduces from Lemma 20

$$\frac{1}{(a_{n+1} + 2)q_n^2} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{a_{n+1}q_n^2} \cdot \tag{21}$$

Therefore any convergent p/q of x satisfies $|x - p/q| < 1/q^2$. Moreover, if a_{n+1} is large, then the approximation p_n/q_n is sharp. Hence, large partial quotients yield good rational approximations by truncating the continued fraction expansion just before the given partial quotient.

3 Fermat–Pell's equation

Let D be a positive integer which is not the square of an integer. It follows that $\sqrt{D}$ is an irrational number. The Diophantine equation

$$x^2 - Dy^2 = \pm 1, \tag{22}$$

where the unknowns x and y are in $\mathbb{Z}$, is called *Pell's equation.*

An introduction to the subject has been given in the colloquium lecture on April 15. We refer to

`http://seminarios.impa.br/cgi-bin/SEMINAR_palestra.cgi?id=4752`

`http://www.math.jussieu.fr/∼ miw/articles/pdf/PellFermatEn2010.pdf`

and

`http://www.math.jussieu.fr/∼ miw/articles/pdf/PellFermatEn2010VI.pdf`

Here we supply complete proofs of the results introduced in that lecture.

3.1 Examples

The three first examples below are special cases of results initiated by O. Perron and related with real quadratic fields of Richaud-Degert type.

Example 1. Take $D = a^2b^2 + 2b$ where a and b are positive integers. A solution to

$$x^2 - (a^2b^2 + 2b)y^2 = 1$$

is $(x, y) = (a^2b + 1, a)$. As we shall see, this is related with the continued fraction expansion of $\sqrt{D}$ which is

$$\sqrt{a^2b^2 + 2b} = [ab, \overline{a, 2ab}]$$

since

$$t = \sqrt{a^2b^2 + 2b} \Longleftrightarrow t = ab + \cfrac{1}{a + \cfrac{1}{t + ab}}\cdot$$

This includes the examples $D = a^2 + 2$ (take $b = 1$) and $D = b^2 + 2b$ (take $a = 1$). For $a = 1$ and $b = c - 1$ his includes the example $D = c^2 - 1$.

Example 2. Take $D = a^2b^2 + b$ where a and b are positive integers. A solution to

$$x^2 - (a^2b^2 + b)y^2 = 1$$

is $(x, y) = (2a^2b + 1, 2a)$. The continued fraction expansion of $\sqrt{D}$ is

$$\sqrt{a^2b^2 + b} = [ab, \overline{2a, 2ab}]$$

since

$$t = \sqrt{a^2b^2 + b} \Longleftrightarrow t = ab + \cfrac{1}{2a + \cfrac{1}{t + ab}}\cdot$$

This includes the example $D = b^2 + b$ (take $a = 1$).

The case $b = 1$, $D = a^2 + 1$ is special: there is an integer solution to

$$x^2 - (a^2 + 1)y^2 = -1,$$

namely $(x, y) = (a, 1)$. The continued fraction expansion of $\sqrt{D}$ is

$$\sqrt{a^2 + 1} = [a, \overline{2a}]$$

since

$$t = \sqrt{a^2 + 1} \iff t = a + \frac{1}{t + a}\cdot$$

Example 3. Let a and b be two positive integers such that $b^2 + 1$ divides $2ab + 1$. For instance $b = 2$ and $a \equiv 1 \pmod 5$. Write $2ab + 1 = k(b^2 + 1)$ and take $D = a^2 + k$. The continued fraction expansion of $\sqrt{D}$ is

$$[a, \overline{b, b, 2a}]$$

since $t = \sqrt{D}$ satisfies

$$t = a + \cfrac{1}{b + \cfrac{1}{b + \cfrac{1}{a + t}}} = [a, b, b, a + z].$$

A solution to $x^2 - Dy^2 = -1$ is $x = ab^2 + a + b$, $y = b^2 + 1$.

In the case $a = 1$ and $b = 2$ (so $k = 1$), the continued fraction has period length 1 only:

$$\sqrt{5} = [1, \overline{2}].$$

Example 4. Integers which are *Polygonal numbers* in two ways are given by the solutions to quadratic equations.

Triangular numbers are numbers of the form

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \quad \text{for } n \geq 1;$$

their sequence starts with

1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, 136, 153, 171, ...

http://www.research.att.com/∼njas/sequences/A000217.

Square numbers are numbers of the form

$$1+3+5+\cdots+(2n+1)=n^2 \quad \text{for } n\geq 1;$$

their sequence starts with

$$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 144,\ 169,\ 196,\ 225,\ 256,\ 289,\ldots$$

http://www.research.att.com/∼njas/sequences/A000290.

Pentagonal numbers are numbers of the form

$$1+4+7+\cdots+(3n+1)=\frac{n(3n-1)}{2} \quad \text{for } n\geq 1;$$

their sequence starts with

$$1,\ 5,\ 12,\ 22,\ 35,\ 51,\ 70,\ 92,\ 117,\ 145,\ 176,\ 210,\ 247,\ 287,\ 330,\ 376,\ 425,\ldots$$

http://www.research.att.com/∼njas/sequences/A000326.

Hexagonal numbers are numbers of the form

$$1+5+9+\cdots+(4n+1)=n(2n-1) \quad \text{for } n\geq 1;$$

their sequence starts with

$$1,\ 6,\ 15,\ 28,\ 45,\ 66,\ 91,\ 120,\ 153,\ 190,\ 231,\ 276,\ 325,\ 378,\ 435,\ 496,\ 561,\ldots$$

http://www.research.att.com/∼njas/sequences/A000384.

For instance, numbers which are at the same time triangular and squares are the numbers y^2 where (x,y) is a solution to Fermat–Pell's equation with $D=8$. Their list starts with

$$0, 1, 36, 1225, 41616, 1413721, 48024900, 1631432881, 55420693056, \ldots$$

See http://www.research.att.com/∼njas/sequences/A001110.

Example 5. Integer rectangle triangles having sides of the right angle as consecutive integers a and $a+1$ have an hypothenuse c which satisfies $a^2+(a+1)^2=c^2$. The admissible values for the hypothenuse is the set of positive integer solutions y to Fermat–Pell's equation $x^2-2y^2=-1$. The list of these hypothenuses starts with

$$1, 5, 29, 169, 985, 5741, 33461, 195025, 1136689, 6625109, 38613965,$$

See http://www.research.att.com/∼njas/sequences/A001653.

3.2 Existence of integer solutions

Let D be a positive integer which is not a square. We show that Fermat–Pell's equation (22) has a non–trivial solution $(x, y) \in \mathbb{Z}\times\mathbb{Z}$, that is a solution $\neq (\pm 1, 0)$.

Proposition 3. *Given a positive integer D which is not a square, there exists $(x, y) \in \mathbb{Z}^2$ with $x > 0$ and $y > 0$ such that $x^2 - Dy^2 = 1$.*

Proof. The first step of the proof is to show that there exists a non–zero integer k such that the Diophantine equation $x^2 - Dy^2 = k$ has infinitely many solutions $(x, y) \in \mathbb{Z}\times\mathbb{Z}$. The main idea behind the proof, which will be made explicit in Lemmas 23, 24 and Corollary 2 below, is to relate the integer solutions of such a Diophantine equation with rational approximations x/y of $\sqrt{D}$.

Using the fact that $\sqrt{D}$ is irrational, we deduce that there are infinitely many $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ with $y > 0$ (and hence $x > 0$) satisfying

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

For such a (x, y), we have $0 < x < y\sqrt{D} + 1 < y(\sqrt{D} + 1)$, hence

$$0 < |x^2 - Dy^2| = |x - y\sqrt{D}| \cdot |x + y\sqrt{D}| < 2\sqrt{D} + 1.$$

Since there are only finitely integers $k \neq 0$ in the range

$$-(2\sqrt{D} + 1) < k < 2\sqrt{D} + 1,$$

one at least of them is of the form $x^2 - Dy^2$ for infinitely many (x, y).

The second step is to notice that, since the subset of $(x, y) \pmod{k}$ in $(\mathbb{Z}/k\mathbb{Z})^2$ is finite, there is an infinite subset $E \subset \mathbb{Z} \times \mathbb{Z}$ of these solutions to $x^2 - Dy^2 = k$ having the same $(x \pmod{k}, y \pmod{k})$.

Let (u_1, v_1) and (u_2, v_2) be two distinct elements in E. Define $(x, y) \in \mathbb{Q}^2$ by

$$x + y\sqrt{D} = \frac{u_1 + v_1\sqrt{D}}{u_2 + v_2\sqrt{D}}.$$

From $u_2^2 - Dv_2^2 = k$, one deduces

$$x + y\sqrt{D} = \frac{1}{k}(u_1 + v_1\sqrt{D})(u_2 - v_2\sqrt{D}),$$

hence

$$x = \frac{u_1u_2 - Dv_1v_2}{k}, \quad y = \frac{-u_1v_2 + u_2v_1}{k}.$$

From $u_1 \equiv u_2 \pmod k$, $v_1 \equiv v_2 \pmod k$ and

$$u_1^2 - Dv_1^2 = k, \quad u_2^2 - Dv_2^2 = k,$$

we deduce

$$u_1u_2 - Dv_1v_2 \equiv u_1^2 - Dv_1^2 \equiv 0 \pmod k$$

and

$$-u_1v_2 + u_2v_1 \equiv -u_1v_1 + u_1v_1 \equiv 0 \pmod k,$$

hence x and y are in $\mathbb{Z}$. Further,

$$\begin{aligned} x^2 - Dy^2 &= (x + y\sqrt{D})(x - y\sqrt{D}) \\ &= \frac{(u_1 + v_1\sqrt{D})(u_1 - v_1\sqrt{D})}{(u_2 + v_2\sqrt{D})(u_2 - v_2\sqrt{D})} \\ &= \frac{u_1^2 - Dv_1^2}{u_2^2 - Dv_2^2} = 1. \end{aligned}$$

It remains to check that $y \neq 0$. If $y = 0$ then $x = \pm 1$, $u_1v_2 = u_2v_1$, $u_1u_2 - Dv_1v_2 = \pm 1$, and

$$ku_1 = \pm u_1(u_1u_2 - Dv_1v_2) = \pm u_2(u_1^2 - Dv_1^2) = \pm ku_2,$$

which implies $(u_1, u_2) = (v_1, v_2)$, a contradiction.

Finally, if $x < 0$ (resp. $y < 0$) we replace x by $-x$ (resp. y by $-y$).

□

Once we have a non–trivial integer solution (x, y) to Fermat–Pell's equation, we have infinitely many of them, obtained by considering the powers of $x + y\sqrt{D}$.

3.3 All integer solutions

There is a natural order for the positive integer solutions to Fermat–Pell's equation: we can order them by increasing values of x, or increasing values of y, or increasing values of $x + y\sqrt{D}$ - it is easily checked that the order is the same.

It follows that there is a minimal positive integer solution[4] (x_1, y_1), which is called *the fundamental solution to Fermat–Pell's equation* $x^2 - Dy^2 = \pm 1$. In the same way, there is a fundamental solution to Fermat–Pell's equations $x^2 - Dy^2 = 1$. Furthermore, when the equation $x^2 - Dy^2 = -1$ has an integer solution, then there is also a fundamental solution.

Proposition 4. *Denote by (x_1, y_1) the fundamental solution to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$. Then the set of all positive integer solutions to this equation is the sequence $(x_n, y_n)_{n \geq 1}$, where x_n and y_n are given by*

$$x_n + y_n \sqrt{D} = (x_1 + y_1 \sqrt{D})^n, \quad (n \in \mathbb{Z}, \quad n \geq 1).$$

In other terms, x_n and y_n are defined by the recurrence formulae

$$x_{n+1} = x_n x_1 + D y_n y_1 \qquad \text{and} \qquad y_{n+1} = x_1 y_n + x_n y_1, \qquad (n \geq 1).$$

More explicitly:
• *If $x_1^2 - Dy_1^2 = 1$, then (x_1, y_1) is the fundamental solution to Fermat–Pell's equation $x^2 - Dy^2 = 1$, and there is no integer solution to Fermat–Pell's equation $x^2 - Dy^2 = -1$.*
• *If $x_1^2 - Dy_1^2 = -1$, then (x_1, y_1) is the fundamental solution to Fermat–Pell's equation $x^2 - Dy^2 = -1$, and the fundamental solution to Fermat–Pell's equation $x^2 - Dy^2 = 1$ is (x_2, y_2). The set of positive integer solutions to Fermat–Pell's equation $x^2 - Dy^2 = 1$ is $\{(x_n, y_n) \; ; \; n \geq 2 \;\; \text{even}\}$, while the set of positive integer solutions to Fermat–Pell's equation $x^2 - Dy^2 = -1$ is $\{(x_n, y_n) \; ; \; n \geq 1 \;\; \text{odd}\}$.*
The set of all solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$ is the set $(\pm x_n, y_n)_{n \in \mathbb{Z}}$, where x_n and y_n are given by the same formula

$$x_n + y_n \sqrt{D} = (x_1 + y_1 \sqrt{D})^n, \quad (n \in \mathbb{Z}).$$

The trivial solution $(1, 0)$ is (x_0, y_0), the solution $(-1, 0)$ is a torsion element of order 2 in the group of units of the ring $\mathbb{Z}[\sqrt{D}]$.

Proof. Let (x, y) be a positive integer solution to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$. Denote by $n \geq 0$ the largest integer such that

$$(x_1 + y_1 \sqrt{D})^n \leq x + y \sqrt{D}.$$

[4] We use the letter x_1, which should not be confused with the first complete quotient in the section § 2.2 on continued fractions

Hence $x+y\sqrt{D} < (x_1+y_1\sqrt{D})^{n+1}$. Define $(u,v) \in \mathbb{Z}\times\mathbb{Z}$ by

$$u+v\sqrt{D} = (x+y\sqrt{D})(x_1-y_1\sqrt{D})^n.$$

From

$$u^2-Dv^2 = \pm 1 \quad \text{and} \quad 1 \le u+v\sqrt{D} < x_1+y_1\sqrt{D},$$

we deduce $u=1$ and $v=0$, hence $x=x_n$, $y=y_n$.

$\square$

3.4 On the group of units of $\mathbb{Z}[\sqrt{D}]$

Let D be a positive integer which is not a square. The ring $\mathbb{Z}[\sqrt{D}]$ is the subring of $\mathbb{R}$ generated by $\sqrt{D}$. The map $\sigma : z = x+y\sqrt{D} \longmapsto x-y\sqrt{D}$ is the *Galois automorphism* of this ring. The *norm* $N : \mathbb{Z}[\sqrt{D}] \longrightarrow \mathbb{Z}$ is defined by $N(z) = z\sigma(z)$. Hence

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

The restriction of N to the group of unit $\mathbb{Z}[\sqrt{D}]^\times$ of the ring $\mathbb{Z}[\sqrt{D}]$ is a homomorphism from the multiplicative group $\mathbb{Z}[\sqrt{D}]^\times$ to the group of units $\mathbb{Z}^\times$ of $\mathbb{Z}$. Since $\mathbb{Z}^\times = \{\pm 1\}$, it follows that

$$\mathbb{Z}[\sqrt{D}]^\times = \{z \in \mathbb{Z}[\sqrt{D}]\ ;\ N(z) = \pm 1\},$$

hence $\mathbb{Z}[\sqrt{D}]^\times$ is nothing else than the set of $x+y\sqrt{D}$ when (x,y) runs over the set of integer solutions to Fermat–Pell's equation $x^2-Dy^2=\pm 1$.

Proposition 3 means that $\mathbb{Z}[\sqrt{D}]^\times$ is not reduced to the torsion subgroup ± 1, while Proposition 4 gives the more precise information that this group $\mathbb{Z}[\sqrt{D}]^\times$ is a (multiplicative) abelian group of rank 1: there exists a so–called *fundamental unit* $u \in \mathbb{Z}[\sqrt{D}]^\times$ such that

$$\mathbb{Z}[\sqrt{D}]^\times = \{\pm u^n\ ;\ n \in \mathbb{Z}\}.$$

The fundamental unit $u>1$ is $x_1+y_1\sqrt{D}$, where (x_1,y_1) is the fundamental solution to Fermat–Pell's equation $x^2-Dy^2=\pm 1$. Fermat–Pell's equation $x^2-Dy^2=\pm 1$ has integer solutions if and only if the fundamental unit has norm -1.

That the rank of $\mathbb{Z}[\sqrt{D}]^\times$ is at most 1 also follows from the fact that the image of the map

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{D}]^\times & \longrightarrow & \mathbb{R}^2 \\ z & \longmapsto & \bigl(\log|z|,\ \log|z'|\bigr) \end{array}$$

is discrete in $\mathbb{R}^2$ and contained in the line $t_1 + t_2 = 0$ of $\mathbb{R}^2$. This proof is not really different from the proof we gave of Proposition 4: the proof that the discrete subgroups of $\mathbb{R}$ have rank ≤ 1 relies on Euclid's division.

3.5 Connection with rational approximation

Lemma 23. *Let D be a positive integer which is not a square. Let x and y be positive rational integers. The following conditions are equivalent:*
(i) $x^2 - Dy^2 = 1$.
(ii) $0 < \dfrac{x}{y} - \sqrt{D} < \dfrac{1}{2y^2\sqrt{D}}\cdot$
(iii) $0 < \dfrac{x}{y} - \sqrt{D} < \dfrac{1}{y^2\sqrt{D}+1}\cdot$

Proof. We have $\dfrac{1}{2y^2\sqrt{D}} < \dfrac{1}{y^2\sqrt{D}+1}$, hence (ii) implies (iii).
(i) implies $x^2 > Dy^2$, hence $x > y\sqrt{D}$, and consequently

$$0 < \frac{x}{y} - \sqrt{D} = \frac{1}{y(x+y\sqrt{D})} < \frac{1}{2y^2\sqrt{D}}\cdot$$

(iii) implies

$$x < y\sqrt{D} + \frac{1}{y\sqrt{D}} < y\sqrt{D} + \frac{2}{y},$$

and

$$y(x+y\sqrt{D}) < 2y^2\sqrt{D} + 2,$$

hence

$$0 < x^2 - Dy^2 = y\left(\frac{x}{y} - \sqrt{D}\right)(x+y\sqrt{D}) < 2.$$

Since $x^2 - Dy^2$ is an integer, it is equal to 1. □

The next variant will also be useful.

Lemma 24. *Let D be a positive integer which is not a square. Let x and y be positive rational integers. The following conditions are equivalent:*
(i) $x^2 - Dy^2 = -1$.
(ii) $0 < \sqrt{D} - \dfrac{x}{y} < \dfrac{1}{2y^2\sqrt{D}-1}\cdot$
(iii) $0 < \sqrt{D} - \dfrac{x}{y} < \dfrac{1}{y^2\sqrt{D}}\cdot$

Proof. We have $\dfrac{1}{2y^2\sqrt{D}-1} < \dfrac{1}{y^2\sqrt{D}}$, hence (ii) implies (iii).
The condition (i) implies $y\sqrt{D} > x$. We use the trivial estimate

$$2\sqrt{D} > 1 + 1/y^2$$

and write

$$x^2 = Dy^2 - 1 > Dy^2 - 2\sqrt{D} + 1/y^2 = (y\sqrt{D} - 1/y)^2,$$

hence $xy > y^2\sqrt{D} - 1$. From (i) one deduces

$$\begin{aligned} 1 = Dy^2 - x^2 &= (y\sqrt{D} - x)(y\sqrt{D} + x) \\ &> \left(\sqrt{D} - \frac{x}{y}\right)(y^2\sqrt{D} + xy) \\ &> \left(\sqrt{D} - \frac{x}{y}\right)(2y^2\sqrt{D} - 1). \end{aligned}$$

(iii) implies $x < y\sqrt{D}$ and

$$y(y\sqrt{D} + x) < 2y^2\sqrt{D},$$

hence

$$0 < Dy^2 - x^2 = y\left(\sqrt{D} - \frac{x}{y}\right)(y\sqrt{D} + x) < 2.$$

Since $Dy^2 - x^2$ is an integer, it is 1. □

From these two lemmas one deduces:

Corollary 2. *Let D be a positive integer which is not a square. Let x and y be positive rational integers. The following conditions are equivalent:*
(i) $x^2 - Dy^2 = \pm 1$.
(ii) $\left|\sqrt{D} - \dfrac{x}{y}\right| < \dfrac{1}{2y^2\sqrt{D} - 1}$.
(iii) $\left|\sqrt{D} - \dfrac{x}{y}\right| < \dfrac{1}{y^2\sqrt{D} + 1}$.

Proof. If $y > 1$ or $D > 3$ we have $2y^2\sqrt{D} - 1 > y^2\sqrt{D} + 1$, which means that (ii) implies trivially (iii), and we may apply Lemmas 23 and 24.

If $D = 2$ and $y = 1$, then each of the conditions (i), (ii) and (iii) is satisfied if and only if $x = 1$. This follows from

$$2 - \sqrt{2} > \frac{1}{2\sqrt{2} - 1} > \frac{1}{\sqrt{2} + 1} > \sqrt{2} - 1.$$

If $D = 3$ and $y = 1$, then each of the conditions (i), (ii) and (iii) is satisfied if and only if $x = 2$. This follows from

$$3 - \sqrt{3} > \sqrt{3} - 1 > \frac{1}{2\sqrt{3} - 1} > \frac{1}{\sqrt{3} + 1} > 2 - \sqrt{3}.$$

□

It is instructive to compare with Liouville's inequality.

Lemma 25. *Let D be a positive integer which is not a square. Let x and y be positive rational integers. Then*

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

Proof. If $x/y < \sqrt{D}$, then $x \le y\sqrt{D}$ and from

$$1 \le Dy^2 - x^2 = (y\sqrt{D} + x)(y\sqrt{D} - x) \le 2y\sqrt{D}(y\sqrt{D} - x),$$

one deduces

$$\sqrt{D} - \frac{x}{y} > \frac{1}{2y^2\sqrt{D}}.$$

We claim that if $x/y > \sqrt{D}$, then

$$\frac{x}{y} - \sqrt{D} > \frac{1}{2y^2\sqrt{D} + 1}.$$

Indeed, this estimate is true if $x - y\sqrt{D} \ge 1/y$, so we may assume $x - y\sqrt{D} < 1/y$. Our claim then follows from

$$1 \le x^2 - Dy^2 = (x + y\sqrt{D})(x - y\sqrt{D}) \le (2y\sqrt{D} + 1/y)(x - y\sqrt{D}).$$

□

This shows that a rational approximation x/y to $\sqrt{D}$, which is only slightly weaker than the limit given by Liouville's inequality, will produce a solution to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$. The distance $|\sqrt{D} - x/y|$ cannot be smaller than $1/(2y^2\sqrt{D} + 1)$, but it can be as small as $1/(2y^2\sqrt{D} - 1)$, and for that it suffices that it is less than $1/(y^2\sqrt{D} + 1)$

3.6 The main lemma

The theory which follows is well–known (a classical reference is the book [9] by O. Perron), but the point of view which we develop here is slightly different from most classical texts on the subject. We follow [2, 3, 11]. An important role in our presentation of the subject is the following result (Lemma 4.1 in [10]).

Lemma 26. *Let $\epsilon = \pm 1$ and let a, b, c, d be rational integers satisfying*

$$ad - bc = \epsilon$$

and $d \geq 1$. Then there is a unique finite sequence of rational integers $a_0, \ldots, a_s$ with $s \geq 1$ and $a_1, \ldots, a_{s-1}$ positive, such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_s & 1 \\ 1 & 0 \end{pmatrix} \tag{27}$$

These integers are also characterized by

$$\frac{b}{d} = [a_0, a_1, \ldots, a_{s-1}], \quad \frac{c}{d} = [a_s, \ldots, a_1], \quad (-1)^{s+1} = \epsilon. \tag{28}$$

For instance, when $d = 1$, for b and c rational integers,

$$\begin{pmatrix} bc+1 & b \\ c & 1 \end{pmatrix} = \begin{pmatrix} b & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} bc-1 & b \\ c & 1 \end{pmatrix} = \begin{pmatrix} b-1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c-1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Proof. We start with unicity. If $a_0, \ldots, a_s$ satisfy the conclusion of Lemma 26, then by using (27), we find $b/d = [a_0, a_1, \ldots, a_{s-1}]$. Taking the transpose, we also find $c/d = [a_s, \ldots, a_1]$. Next, taking the determinant, we obtain $(-1)^{s+1} = \epsilon$. The last equality fixes the parity of s, and each of the rational numbers b/d, c/d has a unique continued fraction expansion whose length has a given parity (cf. Proposition 2). This proves the unicity of the factorisation when it exists.

For the existence, we consider the simple continued fraction expansion of c/d with length of parity given by the last condition in (28), say $c/d =$

$[a_s, \ldots, a_1]$. Let a_0 be a rational integer such that the distance between b/d and $[a_0, a_1, \ldots, a_{s-1}]$ is $\leq 1/2$. Define a', b', c', d' by

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_s & 1 \\ 1 & 0 \end{pmatrix}.$$

We have

$$d' > 0, \quad a'd' - b'c' = \epsilon, \quad \frac{c'}{d'} = [a_s, \ldots, a_1] = \frac{c}{d}$$

and

$$\frac{b'}{d'} = [a_0, a_1, \ldots, a_{s-1}], \quad \left| \frac{b'}{d'} - \frac{b}{d} \right| \leq \frac{1}{2}.$$

From $\gcd(c, d) = \gcd(c', d') = 1$, $c/d = c'/d'$ and $d > 0$, $d' > 0$ we deduce $c' = c$, $d' = d$. From the equality between the determinants we deduce $a' = a + kc$, $b' = b + kd$ for some $k \in \mathbb{Z}$, and from

$$\frac{b'}{d'} - \frac{b}{d} = k$$

we conclude $k = 0$, $(a', b', c', d') = (a, b, c, d)$. Hence (27) follows.

$\square$

Corollary 3. *Assume the hypotheses of Lemma 26 are satisfied.*
a) If $c > d$, then $a_s \geq 1$ and

$$\frac{a}{c} = [a_0, a_1, \ldots, a_s].$$

b) If $b > d$, then $a_0 \geq 1$ and

$$\frac{a}{b} = [a_s, \ldots, a_1, a_0].$$

The following examples show that the hypotheses of the corollary are not superfluous:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} b-1 & b \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} b-1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} c-1 & 1 \\ c & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c-1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Proof of Corollary 3. Any rational number $u/v > 1$ has two continued fractions. One of them starts with 0 only if $u/v = 1$ and the continued fraction is $[0, 1]$. Hence the assumption $c > d$ implies $a_s > 0$. This proves part a), and part b) follows by transposition (or repeating the proof). $\square$

Another consequence of Lemma 26 is the following classical result (Satz 13 p. 47 of [9]).

Corollary 4. *Let a, b, c, d be rational integers with $ad - bc = \pm 1$ and $c > d > 0$. Let x and y be two irrational numbers satisfying $y > 1$ and*

$$x = \frac{ay + b}{cy + d}\cdot$$

Let $x = [a_0, a_1, \ldots]$ be the simple continued fraction expansion of x. Then there exists $s \geq 1$ such that

$$a = p_s, \quad b = p_{s-1}, \quad c = q_s, \quad r = q_{s-1}, \quad y = x_{s+1}.$$

Proof. Using lemma 26, we write

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a'_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a'_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a'_s & 1 \\ 1 & 0 \end{pmatrix}$$

with $a'_1, \ldots, a'_{s-1}$ positive and

$$\frac{b}{d} = [a'_0, a'_1, \ldots, a'_{s-1}], \quad \frac{c}{d} = [a'_s, \ldots, a'_1].$$

From $c > d$ and corollary 3, we deduce $a'_s > 0$ and

$$\frac{a}{c} = [a'_0, a'_1, \ldots, a'_s] = \frac{p'_s}{q'_s}, \quad x = \frac{p'_s y + p'_{s-1}}{q'_s y + q'_{s-1}} = [a'_0, a'_1, \ldots, a'_s, y].$$

Since $y > 1$, it follows that $a'_i = a_i$, $p'_i = q'_i$ for $0 \leq i \leq s$ and $y = x_{s+1}$.

$\square$

3.7 Simple Continued fraction of $\sqrt{D}$

An infinite sequence $(a_n)_{n\geq 1}$ is *periodic* if there exists a positive integer s such that

$$a_{n+s} = a_n \quad \text{for all } n \geq 1. \tag{29}$$

In this case, the finite sequence $(a_1, \dots, a_s)$ is called a *period* of the original sequence. For the sake of notation, we write

$$(a_1, a_2, \dots) = (\overline{a_1, \dots, a_s}).$$

If s_0 is the smallest positive integer satisfying (29), then the set of s satisfying (29) is the set of positive multiples of s_0. In this case $(a_1, \dots, a_{s_0})$ is called *the fundamental period* of the original sequence.

Théorème 1. *Let D be a positive integer which is not a square. Write the simple continued fraction of $\sqrt{D}$ as $[a_0, a_1, \dots]$ with $a_0 = \lfloor \sqrt{D} \rfloor$.*
a) The sequence $(a_1, a_2, \dots)$ is periodic.
b) Let (x, y) be a positive integer solution to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$. Then there exists $s \geq 1$ such that $x/y = [a_0, \dots, a_{s-1}]$ and

$$(a_1, a_2, \dots, a_{s-1}, 2a_0)$$

is a period of the sequence $(a_1, a_2, \dots)$. Further, $a_{s-i} = a_i$ for $1 \leq i \leq s-1$ [5]).
c) Let $(a_1, a_2, \dots, a_{s-1}, 2a_0)$ be a period of the sequence $(a_1, a_2, \dots)$. Set $x/y = [a_0, \dots, a_{s-1}]$. Then $x^2 - Dy^2 = (-1)^s$.
d) Let s_0 be the length of the fundamental period. Then for $i \geq 0$ not multiple of s_0, we have $a_i \leq a_0$.

If $(a_1, a_2, \dots, a_{s-1}, 2a_0)$ is a period of the sequence $(a_1, a_2, \dots)$, then

$$\sqrt{D} = [a_0, \overline{a_1, \dots, a_{s-1}, 2a_0}] = [a_0, a_1, \dots, a_{s-1}, a_0 + \sqrt{D}].$$

Consider the fundamental period $(a_1, a_2, \dots, a_{s_0-1}, a_{s_0})$ of the sequence $(a_1, a_2, \dots)$. By part b) of Theorem 1 we have $a_{s_0} = 2a_0$, and by part d), it follows that s_0 is the smallest index i such that $a_i > a_0$.

From b) and c) in Theorem 1, it follows that the fundamental solution (x_1, y_1) to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$ is given by $x_1/y_1 = [a_0, \dots, a_{s_0-1}]$, and that $x_1^2 - Dy_1^2 = (-1)^{s_0}$. Therefore, if s_0 is even, then there is no solution to the Fermat–Pell's equation $x^2 - Dy^2 = -1$. If s_0

[5] One says that the word $a_1, \dots, a_{s-1}$ is a *palindrome*. This result is proved in the first paper published by Evariste Galois at the age of 17:
Démonstration d'un théorème sur les fractions continues périodiques.
Annales de Mathématiques Pures et Appliquées, **19** (1828-1829), p. 294-301.
`http://archive.numdam.org/article/AMPA_1828-1829__19__294_0.pdf`.

is odd, then (x_1, y_1) is the fundamental solution to Fermat–Pell's equation $x^2 - Dy^2 = -1$, while the fundamental solution (x_2, y_2) to Fermat–Pell's equation $x^2 - Dy^2 = 1$ is given by $x_2/y_2 = [a_0, \dots, a_{2s-1}]$.

It follows also from Theorem 1 that the $(ns_0 - 1)$-th convergent

$$x_n/y_n = [a_0, \dots, a_{ns_0-1}]$$

satisfies

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n. \tag{30}$$

We shall check this relation directly (Lemma 34).

Proof. Start with a positive solution (x, y) to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$, which exists according to Proposition 3. Since $Dy \geq x$ and $x > y$, we may use lemma 26 and corollary 3 with

$$a = Dy, \quad b = c = x, \quad d = y$$

and write

$$\begin{pmatrix} Dy & x \\ x & y \end{pmatrix} = \begin{pmatrix} a'_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a'_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a'_s & 1 \\ 1 & 0 \end{pmatrix} \tag{31}$$

with positive integers $a'_0, \dots, a'_s$ and with $a'_0 = \lfloor\sqrt{D}\rfloor$. Then the continued fraction expansion of Dy/x is $[a'_0, \dots, a'_s]$ and the continued fraction expansion of x/y is $[a'_0, \dots, a'_{s-1}]$.

Since the matrix on the left hand side of (31) is symmetric, the word $a'_0, \dots, a'_s$ is a palindrome. In particular $a'_s = a'_0$.

Consider the periodic continued fraction

$$\delta = [a'_0, \overline{a'_1, \dots, a'_{s-1}, 2a'_0}].$$

This number δ satisfies

$$\delta = [a'_0, a'_1, \dots, a'_{s-1}, a'_0 + \delta].$$

Using the inverse of the matrix

$$\begin{pmatrix} a'_0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{which is} \quad \begin{pmatrix} 0 & 1 \\ 1 & -a'_0 \end{pmatrix},$$

we write

$$\begin{pmatrix} a_0' + \delta & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_0' & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \delta & 1 \end{pmatrix}$$

Hence the product of matrices associated with the continued fraction of δ

$$\begin{pmatrix} a_0' & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1' & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s-1}' & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0' + \delta & 1 \\ 1 & 0 \end{pmatrix}$$

is

$$\begin{pmatrix} Dy & x \\ x & y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \delta & 1 \end{pmatrix} = \begin{pmatrix} Dy + \delta x & x \\ x + \delta y & y \end{pmatrix}.$$

It follows that

$$\delta = \frac{Dy + \delta x}{x + \delta y},$$

hence $\delta^2 = D$. As a consequence, $a_i' = a_i$ for $0 \le i \le s-1$ while $a_s' = a_0$, $a_s = 2a_0$.

This proves that if (x, y) is a non–trivial solution to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$, then the continued fraction expansion of $\sqrt{D}$ is of the form

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{s-1}, 2a_0}] \tag{32}$$

with $a_1, \ldots, a_{s-1}$ a palindrome, and x/y is given by the convergent

$$x/y = [a_0, a_1, \ldots, a_{s-1}]. \tag{33}$$

Consider a convergent $p_n/q_n = [a_0, a_1, \ldots, a_n]$. If $a_{n+1} = 2a_0$, then (21) with $x = \sqrt{D}$ implies the upper bound

$$\left| \sqrt{D} - \frac{p_n}{q_n} \right| \le \frac{1}{2a_0 q_n^2},$$

and it follows from Corollary 2 that (p_n, q_n) is a solution to Fermat–Pell's equation $p_n^2 - Dq_n^2 = \pm 1$. This already shows that $a_i < 2a_0$ when $i + 1$ is not the length of a period. We refine this estimate to $a_i \le a_0$.

Assume $a_{n+1} \ge a_0 + 1$. Since the sequence $(a_m)_{m \ge 1}$ is periodic of period length s_0, for any m congruent to n modulo s_0, we have $a_{m+1} > a_0$. For these m we have

$$\left| \sqrt{D} - \frac{p_m}{q_m} \right| \le \frac{1}{(a_0 + 1) q_m^2}.$$

For sufficiently large m congruent to n modulo s we have

$$(a_0+1)q_m^2 > q_m^2\sqrt{D}+1.$$

Corollary 2 implies that (p_m, q_m) is a solution to Fermat–Pell's equation $p_m^2 - Dq_m^2 = \pm 1$. Finally, Theorem 1 implies that $m+1$ is a multiple of s_0, hence $n+1$ also.

$\square$

3.8 Connection between the two formulae for the n-th positive solution to Fermat–Pell's equation

Lemma 34. *Let D be a positive integer which is not a square. Consider the simple continued fraction expansion $\sqrt{D} = [a_0, \overline{a_1, \dots, a_{s_0-1}, 2a_0}]$ where s_0 is the length of the fundamental period. Then the fundamental solution (x_1, y_1) to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$ is given by the continued fraction expansion $x_1/y_1 = [a_0, a_1, \dots, a_{s_0-1}]$. Let $n \geq 1$ be a positive integer. Define (x_n, y_n) by $x_n/y_n = [a_0, a_1, \dots, a_{ns_0-1}]$. Then $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$.*

This result is a consequence of the two formulae we gave for the n-th solution (x_n, y_n) to Fermat–Pell's equation $x^2 - Dy^2 = \pm 1$. We check this result directly.

Proof. From Lemma 26 and relation (31), one deduces

$$\begin{pmatrix} Dy_n & x_n \\ x_n & y_n \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{ns_0-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Since

$$\begin{pmatrix} Dy_n & x_n \\ x_n & y_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -a_0 \end{pmatrix} = \begin{pmatrix} x_n & Dy_n - a_0x_n \\ y_n & x_n - a_0y_n \end{pmatrix},$$

we obtain

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{ns_0-1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_n & Dy_n - a_0x_n \\ y_n & x_n - a_0y_n \end{pmatrix}. \tag{35}$$

Notice that the determinant is $(-1)^{ns_0} = x_n^2 - Dy_n^2$. Formula (35) for $n+1$ and the periodicity of the sequence $(a_1, \dots, a_n, \dots)$ with $a_{s_0} = 2a_0$ give :

$$\begin{pmatrix} x_{n+1} & Dy_{n+1} - a_0x_{n+1} \\ y_{n+1} & x_{n+1} - a_0y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n & Dy_n - a_0x_n \\ y_n & x_n - a_0y_n \end{pmatrix} \begin{pmatrix} 2a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s_0-1} & 1 \\ 1 & 0 \end{pmatrix}.$$

Take first $n = 1$ in (35) and multiply on the left by

$$\begin{pmatrix} 2a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -a_0 \end{pmatrix} = \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix}.$$

Since

$$\begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 & Dy_1 - a_0x_1 \\ y_1 & x_1 - a_0y_1 \end{pmatrix} = \begin{pmatrix} x_1 + a_0y_1 & (D - a_0^2)y_1 \\ y_1 & x_1 - a_0y_1 \end{pmatrix}.$$

we deduce

$$\begin{pmatrix} 2a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s_0-1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_1 + a_0y_1 & (D - a_0^2)y_1 \\ y_1 & x_1 - a_0y_1 \end{pmatrix}.$$

Therefore

$$\begin{pmatrix} x_{n+1} & Dy_{n+1} - a_0x_{n+1} \\ y_{n+1} & x_{n+1} - a_0y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n & Dy_n - a_0x_n \\ y_n & x_n - a_0y_n \end{pmatrix} \begin{pmatrix} x_1 + a_0y_1 & (D - a_0^2)y_1 \\ y_1 & x_1 - a_0y_1 \end{pmatrix}.$$

The first column gives

$$x_{n+1} = x_nx_1 + Dy_ny_1 \qquad \text{and} \qquad y_{n+1} = x_1y_n + x_ny_1,$$

which was to be proved.

$\square$

3.9 Records

For large D, Fermat–Pell's equation may obviously have small integer solutions. Examples are

For $D = m^2 - 1$ with $m \geq 2$ the numbers $x = m$, $y = 1$ satisfy $x^2 - Dy^2 = 1$,

for $D = m^2 + 1$ with $m \geq 1$ the numbers $x = m$, $y = 1$ satisfy $x^2 - Dy^2 = -1$,

for $D = m^2 \pm m$ with $m \geq 2$ the numbers $x = 2m \pm 1$ satisfy $y = 2$, $x^2 - Dy^2 = 1$,

for $D = t^2m^2 + 2m$ with $m \geq 1$ and $t \geq 1$ the numbers $x = t^2m + 1$, $y = t$ satisfy $x^2 - Dy^2 = 1$.

On the other hand, relatively small values of D may lead to large fundamental solutions. Tables are available on the internet[6].

For D a positive integer which is not a square, denote by $S(D)$ the base 10 logarithm of x_1, when (x_1, y_1) is the fundamental solution to $x^2 - Dy^2 = 1$. The integral part of $S(D)$ is the number of digits of the fundamental solution x_1. For instance, when $D = 61$, the fundamental solution (x_1, y_1) is

$$x_1 = 1\,766\,319\,049, \quad y_1 = 226\,153\,980$$

and $S(61) = \log_{10} x_1 = 9.247\,069\ldots$

An integer D is a *record holder* for S if $S(D') < S(D)$ for all $D' < D$.

Here are the record holders up to 1021:

D	2	5	10	13	29	46	53	61	109
$S(D)$	0.477	0.954	1.278	2.812	3.991	4.386	4.821	9.247	14.198

D	181	277	397	409	421	541	661	1021
$S(D)$	18.392	20.201	20.923	22.398	33.588	36.569	37.215	47.298

Some further records with number of digits successive powers of 10:

D	3061	169789	12765349	1021948981	85489307341
$S(D)$	104.051	1001.282	10191.729	100681.340	1003270.151

3.10 A criterion for the existence of a solution to the negative Fermat–Pell equation

Here is a recent result on the existence of a solution to Fermat–Pell's equation $x^2 - Dy^2 = -1$

Proposition 5 (R.A. Mollin, A. Srinivasan[7]). *Let d be a positive integer which is not a square. Let (x_0, y_0) be the fundamental solution to Fermat–Pell's equation $x^2 - dy^2 = 1$. Then the equation $x^2 - dy^2 = -1$ has a solution if and only if $x_0 \equiv -1 \pmod{2d}$.*

[6]For instance:
Tomás Oliveira e Silva: Record-Holder Solutions of Fermat–Pell's Equation
`http://www.ieeta.pt/~tos/pell.html`.

[7]Pell equation: non-principal Lagrange criteria and central norms; Canadian Math. Bull., to appear

Proof. If $a^2 - db^2 = -1$ is the fundamental solution to $x^2 - dy^2 = -1$, then $x_0 + y_0\sqrt{d} = (a + b\sqrt{d})^2$, hence

$$x_0 = a^2 + db^2 = 2db^2 - 1 \equiv -1 \pmod{2d}.$$

Conversely, if $x_0 = 2dk - 1$, then $x_0^2 = 4d^2k^2 - 4dk + 1 = dy_0^2 + 1$, hence $4dk^2 - 4k = y_0^2$. Therefore y_0 is even, $y_0 = 2z$, and $k(dk-1) = z^2$. Since k and $dk - 1$ are relatively prime, both are squares, $k = b^2$ and $dk - 1 = a^2$, which gives $a^2 - db^2 = -1$. □

3.11 Arithmetic varieties

Let D be a positive integer which is not a square. Define $\mathcal{G} = \{(x, y) \in \mathbb{R}^2 \; ; \; x^2 - Dy^2 = 1\}$.

The map

$$\begin{array}{ccc} \mathcal{G} & \longrightarrow & \mathbb{R}^\times \\ (x, y) & \longmapsto & t = x + y\sqrt{D} \end{array}$$

is bijective: the inverse of that map is obtained by writing $u = 1/t$, $2x = t+u$, $2y\sqrt{D} = t - u$, so that $t = x + y\sqrt{D}$ and $u = x - y\sqrt{D}$. By transfer of structure, this endows $\mathcal{G}$ with a multiplicative group structure, which is isomorphic to $\mathbb{R}^\times$, for which

$$\begin{array}{ccc} \mathcal{G} & \longrightarrow & \mathrm{GL}_2(\mathbb{R}) \\ (x, y) & \longmapsto & \begin{pmatrix} x & Dy \\ y & x \end{pmatrix}. \end{array}$$

is an injective group homomorphism. Let $G(\mathbb{R})$ be its image, which is therefore isomorphic to $\mathbb{R}^\times$.

A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ respects the quadratic form $x^2 - Dy^2$ if and only if

$$(ax + by)^2 - D(cx + dy)^2 = x^2 - Dy^2,$$

which can be written

$$a^2 - Dc^2 = 1, \quad b^2 - Dd^2 = D, \quad ab = cdD.$$

Hence the group of matrices of determinant 1 with coefficients in $\mathbb{Z}$ which respect the quadratic form $x^2 - Dy^2$ is the group

$$G(\mathbb{Z}) = \left\{ \begin{pmatrix} a & Dc \\ c & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \right\}.$$

According to the work of Siegel, Harish–Chandra, Borel and Godement, the quotient of $G(\mathbb{R})$ by $G(\mathbb{Z})$ is compact. Hence $G(\mathbb{Z})$ is infinite (of rank 1 over $\mathbb{Z}$), which means that there are infinitely many solutions to the equation $a^2 - Dc^2 = 1$.

This is not a new proof of Proposition 3, but an interpretation and a generalization. Such results are valid for *arithmetic varieties*[8].

Addition to Lemma 26.
In [5], § 4, there is a variant of the matrix formula (14) for the simple continued fraction of a real number.

Given integers $a_0, a_1, \dots$ with $a_i > 0$ for $i \geq 1$ and writing, for $n \geq 0$, as usual, $p_n/q_n = [a_0, a_1, \dots, a_n]$, one checks, by induction on n, the two formulae

$$\left.\begin{array}{lll}\begin{pmatrix}1 & a_0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ a_1 & 1\end{pmatrix}\cdots\begin{pmatrix}1 & a_n\\ 0 & 1\end{pmatrix} & = \begin{pmatrix}p_{n-1} & p_n\\ q_{n-1} & q_n\end{pmatrix} & \text{if } n \text{ is even}\\ \begin{pmatrix}1 & a_0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ a_1 & 1\end{pmatrix}\cdots\begin{pmatrix}1 & 0\\ a_n & 1\end{pmatrix} & = \begin{pmatrix}p_n & p_{n-1}\\ q_n & q_{n-1}\end{pmatrix} & \text{if } n \text{ is odd}\end{array}\right\} \tag{36}$$

Define two matrices U (up) and L (low) in $\mathrm{GL}_2(\mathbb{R})$ of determinant $+1$ by

$$U = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad \text{and} \quad L = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}.$$

For p and q in $\mathbb{Z}$, we have

$$U^p = \begin{pmatrix}1 & p\\ 0 & 1\end{pmatrix} \quad \text{and} \quad L^q = \begin{pmatrix}1 & 0\\ q & 1\end{pmatrix},$$

so that these formulae (36) are

$$U^{a_0} L^{a_1} \cdots U^{a_n} = \begin{pmatrix}p_{n-1} & p_n\\ q_{n-1} & q_n\end{pmatrix} \quad \text{if } n \text{ is even}$$

and

$$U^{a_0} L^{a_1} \cdots L^{a_n} = \begin{pmatrix}p_n & p_{n-1}\\ q_n & q_{n-1}\end{pmatrix} \quad \text{if } n \text{ is odd.}$$

[8]See for instance Nicolas Bergeron, "Sur la forme de certains espaces provenant de constructions arithmétiques", Images des Mathématiques, (2004).
`http://people.math.jussieu.fr/~bergeron/Recherche_files/Images.pdf`.

The connexion with Euclid's algorithm is

$$U^{-p}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-pc & b-pd \\ c & d \end{pmatrix} \quad \text{and} \quad L^{-q}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c-qa & d-qb \end{pmatrix}.$$

The corresponding variant of Lemma 26 is also given in [5], § 4: *If a, b, c, d are rational integers satisfying $b > a > 0$, $d > c \ge 0$ and $ad - bc = 1$, then there exist rational integers $a_0, \dots, a_n$ with n even and $a_1, \dots, a_n$ positive, such that*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ a_1 & 1 \end{pmatrix}\cdots\begin{pmatrix} 1 & a_n \\ 0 & 1 \end{pmatrix}$$

These integers are uniquely determined by $b/d = [a_0, \dots, a_n]$ with n even.

3.12 Periodic continued fractions

An infinite sequence $(a_n)_{n\ge 0}$ is said to be *ultimately periodic* if there exists $n_0 \ge 0$ and $s \ge 1$ such that

$$a_{n+s} = a_n \quad \text{for all } n \ge n_0. \tag{37}$$

The set of s satisfying this property (3.12) is the set of positive multiples of an integer s_0, and $(a_{n_0}, a_{n_0+1}, \dots, a_{n_0+s_0-1})$ is called *the fundamental period.*

A continued fraction with a sequence of partial quotients satisfying (37) will be written

$$[a_0, a_1, \dots, a_{n_0-1}, \overline{a_{n_0}, \dots, a_{n_0+s-1}}].$$

Example. For D a positive integer which is not a square, setting $a_0 = \lfloor\sqrt{D}\rfloor$, we have by Theorem 1

$$a_0 + \sqrt{D} = [\overline{2a_0, a_1, \dots, a_{s-1}}] \quad \text{and} \quad \frac{1}{\sqrt{D} - a_0} = [\overline{a_1, \dots, a_{s-1}, 2a_0}].$$

Lemma 38 (Euler 1737)**.** *If an infinite continued fraction*

$$x = [a_0, a_1, \dots, a_n, \dots]$$

is ultimately periodic, then x is a quadratic irrational number.

Proof. Since the continued fraction of x is infinite, x is irrational. Assume first that the continued fraction is periodic, namely that (37) holds with $n_0 = 0$:

$$x = [\overline{a_0, \dots, a_{s-1}}].$$

This can be written

$$x = [a_0, \ldots, a_{s-1}, x].$$

Hence

$$x = \frac{p_{s-1}x + p_{s-2}}{q_{s-1}x + q_{s-2}}\cdot$$

It follows that

$$q_{s-1}X^2 + (q_{s-2} - p_{s-1})X - p_{s-2}$$

is a non–zero quadratic polynomial with integer coefficients having x as a root. Since x is irrational, this polynomial is irreducible and x is quadratic.

In the general case where (37) holds with $n_0 > 0$, we write

$$x = [a_0, a_1, \ldots, a_{n_0-1}, \overline{a_{n_0}, \ldots, a_{n_0+s-1}}] = [a_0, a_1, \ldots, a_{n_0-1}, y],$$

where $y = [\overline{a_{n_0}, \ldots, a_{n_0+s-1}}]$ is a periodic continued fraction, hence is quadratic. But

$$x = \frac{p_{n_0-1}y + p_{n_0-2}}{q_{n_0-1}y + q_{n_0-2}},$$

hence $x \in \mathbb{Q}(y)$ is also quadratic irrational.

□

Lemma 39 (Lagrange, 1770)**.** *If x is a quadratic irrational number, then its continued fraction*

$$x = [a_0, a_1, \ldots, a_n, \ldots]$$

is ultimately periodic.

Proof. For $n \geq 0$, define $d_n = q_n x - p_n$. According to Corollary 1, we have $|d_n| < 1/q_{n+1}$.

Let $AX^2 + BX + C$ with $A > 0$ be an irreducible quadratic polynomial having x as a root. For each $n \geq 2$, we deduce from (19) that the convergent x_n is a root of a quadratic polynomial $A_nX^2 + B_nX + C_n$, with

$$\begin{aligned}
A_n &= Ap_{n-1}^2 + Bp_{n-1}q_{n-1} + Cq_{n-1}^2,\\
B_n &= 2Ap_{n-1}p_{n-2} + B(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2Cq_{n-1}q_{n-2},\\
C_n &= A_{n-1}.
\end{aligned}$$

Using $Ax^2 + Bx + C = 0$, we deduce

$$\begin{aligned}
A_n &= (2Ax + B)d_{n-1}q_{n-1} + Ad_{n-1}^2,\\
B_n &= (2Ax + B)(d_{n-1}q_{n-2} + d_{n-2}q_{n-1}) + 2Ad_{n-1}d_{n-2}.
\end{aligned}$$

There are similar formulae expressing A, B, C as homogeneous linear combinations of A_n, B_n, C_n, and since $(A,B,C) \neq (0,0,0)$, it follows that $(A_n,B_n,C_n) \neq (0,0,0)$. Since x_n is irrational, one deduces $A_n \neq 0$.

From the inequalities

$$q_{n-1}|d_{n-2}| < 1, \quad q_{n-2}|d_{n-1}| < 1, \quad q_{n-1} < q_n, \quad |d_{n-1}d_{n-2}| < 1,$$

one deduces

$$\max\{|A_n|,\ |B_n|/2, |C_n|\} < A + |2Ax + B|.$$

This shows that $|A_n|$, $|B_n|$ and $|C_n|$ are bounded independently of n. Therefore there exists $n_0 \geq 0$ and $s > 0$ such that $x_{n_0} = x_{n_0+s}$. From this we deduce that the continued fraction of x_{n_0} is purely periodic, hence the continued fraction of x is ultimately periodic. $\square$

A *reduced quadratic irrational number* is an irrational number $x > 1$ which is a root of a degree 2 polynomial ax^2+bx+c with rational integer coefficients, such that the other root x' of this polynomial, which is the *Galois conjugate of* x, satisfies $-1 < x' < 0$. If x is reduced, then so is $-1/x'$.

Lemma 40. *A continued fraction*

$$x = [a_0, a_1, \ldots, a_n \ldots]$$

is purely periodic if and only if x is a reduced quadratic irrational number. In this case, if $x = [\overline{a_0, a_1, \ldots, a_{s-1}}]$ and if x' is the Galois conjugate of x, then

$$-1/x' = [\overline{a_{s-1}, \ldots, a_1, a_0}]$$

Proof. Assume first that the continued fraction of x is purely periodic:

$$x = [\overline{a_0, a_1, \ldots, a_{s-1}}].$$

From $a_s = a_0$ we deduce $a_0 > 0$, hence $x > 1$. From $x = [a_0, a_1, \ldots, a_{s-1}, x]$ and the unicity of the continued fraction expansion, we deduce

$$x = \frac{p_{s-1}x + p_{s-2}}{q_{s-1}x + q_{s-2}} \quad \text{and} \quad x = x_s.$$

Therefore x is a root of the quadratic polynomial

$$P_s(X) = q_{s-1}X^2 + (q_{s-2} - p_{s-1})X - p_{s-2}.$$

This polynomial P_s has a positive root, namely $x > 1$, and a negative root x', with the product $xx' = -p_{s-2}/q_{s-1}$. We transpose the relation

$$\begin{pmatrix} p_{s-1} & p_{s-2} \\ q_{s-1} & q_{s-2} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s-1} & 1 \\ 1 & 0 \end{pmatrix}$$

and obtain

$$\begin{pmatrix} p_{s-1} & q_{s-1} \\ p_{s-2} & q_{s-2} \end{pmatrix} = \begin{pmatrix} a_{s-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Define

$$y = [\overline{a_{s-1}, \ldots, a_1, a_0}],$$

so that $y > 1$,

$$y = [a_{s-1}, \ldots, a_1, a_0, y] = \frac{p_{s-1}y + q_{s-1}}{p_{s-2}y + q_{s-2}}$$

and y is the positive root of the polynomial

$$Q_s(X) = p_{s-2}X^2 + (q_{s-2} - p_{s-1})X - q_{s-1}.$$

The polynomials P_s and Q_s are related by $Q_s(X) = -X^2 P_s(-1/X)$. Hence $y = -1/x'$.

For the converse, assume $x > 1$ and $-1 < x' < 0$. Let $(x_n)_{n\geq 1}$ be the sequence of complete quotients of x. For $n \geq 1$, define x'_n as the Galois conjugate of x_n. One deduces by induction that $x'_n = a_n + 1/x'_{n+1}$, that $-1 < x'_n < 0$ (hence x_n is reduced), and that a_n is the integral part of $-1/x'_{n+1}$.

If the continued fraction expansion of x were not purely periodic, we would have

$$x = [a_0, \ldots, a_{h-1}, \overline{a_h, \ldots, a_{h+s-1}}]$$

with $a_{h-1} \neq a_{h+s-1}$. By periodicity we have $x_h = [a_h, \ldots, a_{h+s-1}, x_h]$, hence $x_h = x_{h+s}$, $x'_h = x'_{h+s}$. From $x'_h = x'_{h+s}$, taking integral parts, we deduce $a_{h-1} = a_{h+s-1}$, a contradiction. □

Corollary 5. *If $r > 1$ is a rational number which is not a square, then the continued fraction expansion of $\sqrt{r}$ is of the form*

$$\sqrt{r} = [a_0, \overline{a_1, \ldots, a_{s-1}, 2a_0}]$$

with $a_1,\dots,a_{s-1}$ a palindrome and $a_0=[\sqrt{r}]$.
Conversely, if the continued fraction expansion of an irrational number $t>1$ is of the form
$$t=[a_0,\overline{a_1,\dots,a_{s-1},2a_0}]$$
with $a_1,\dots,a_{s-1}$ a palindrome, then t^2 is a rational number.

Proof. If $t^2=r$ is rational >1, then for and $a_0=[\sqrt{t}]$ the number $x=t+a_0$ is reduced. Since $t'+t=0$, we have
$$-\frac{1}{x'}=\frac{1}{x-2a_0}\cdot$$
Hence
$$x=[\overline{2a_0,a_1,\dots,a_{s-1}}],\quad -\frac{1}{x'}=[\overline{a_{s-1},\dots,a_1,2a_0}]$$
and $a_1,\dots,a_{s-1}$ a palindrome.

Conversely, if $t=[a_0,\overline{a_1,\dots,a_{s-1},2a_0}]$ with $a_1,\dots,a_{s-1}$ a palindrome, then $x=t+a_0$ is periodic, hence reduced, and its Galois conjugate x' satisfies
$$-\frac{1}{x'}=[\overline{a_1,\dots,a_{s-1},2a_0}]=\frac{1}{x-2a_0},$$
which means $t+t'=0$, hence $t^2\in\mathbb{Q}$. □

Lemma 41 (Serret, 1878)**.** *Let x and y be two irrational numbers with continued fractions*
$$x=[a_0,a_1,\dots,a_n\dots]\quad \textit{and}\quad y=[b_0,b_1,\dots,b_m\dots]$$
respectively. Then the two following properties are equivalent.
(i) *There exists a matrix $\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ with rational integer coefficients and determinant ±1 such that*
$$y=\frac{ax+b}{cx+d}\cdot$$
(ii) *There exists $n_0\ge 0$ and $m_0\ge 0$ such that $a_{n_0+k}=b_{m_0+k}$ for all $k\ge 0$.*

Condition (i) means that *x and y are equivalent modulo the action of* $\mathrm{GL}_2(\mathbb{Z})$ *by homographies.*

Condition (ii) means that there exists integers n_0, m_0 and a real number $t>1$ such that
$$x=[a_0,a_1,\dots,a_{n_0-1},t]\quad\text{and}\quad y=[b_0,b_1,\dots,b_{m_0-1},t].$$

Example.

(42) If $x = [a_0, a_1, x_2]$, then $$-x = \begin{cases} [-a_0-1, 1, a_1-1, x_2] & \text{if } a_1 \geq 2, \\ [-a_0-1, 1+x_2] & \text{if } a_1 = 1. \end{cases}$$

Proof. We already know by (19) that if x_n is a complete quotient of x, then x and x_n are equivalent modulo $\mathrm{GL}_2(\mathbb{Z})$. Condition (ii) means that there is a partial quotient of x and a partial quotient of y which are equal. By transitivity of the $\mathrm{GL}_2(\mathbb{Z})$ equivalence, (ii) implies (i).

Conversely, assume (i):
$$y = \frac{ax+b}{cx+d}\cdot$$
Let n be a sufficiently large number. From
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} u_n & u_{n-1} \\ v_n & v_{n-1} \end{pmatrix}$$
with
$$u_n = ap_n + bq_n, \quad u_{n-1} = ap_{n-1} + bq_{n-1},$$
$$v_n = cp_n + dq_n, \quad v_{n-1} = cp_{n-1} + dq_{n-1},$$
we deduce
$$y = \frac{u_n x_{n+1} + u_{n-1}}{v_n x_{n+1} + v_{n-1}}\cdot$$
We have $v_n = (cx+d)q_n + c\delta_n$ with $\delta_n = p_n - q_n x$. We have $q_n \to \infty$, $q_n \geq q_{n-1} + 1$ and $\delta_n \to 0$ as $n \to \infty$. Hence, for sufficiently large n, we have $v_n > v_{n-1} > 0$. From part 1 of Corollary 3, we deduce
$$\begin{pmatrix} u_n & u_{n-1} \\ v_n & v_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_s & 1 \\ 1 & 0 \end{pmatrix}$$
with $a_0, \ldots, a_s$ in $\mathbb{Z}$ and $a_1, \ldots, a_s$ positive. Hence
$$y = [a_0, a_1, \ldots, a_s, x_{n+1}].$$
□

A computational proof of (i) ⇒ (ii). Another proof is given by Bombieri [2] (Theorem A.1 p. 209). He uses the fact that $\mathrm{GL}_2(\mathbb{Z})$ is generated by the two matrices
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The associated fractional linear transformations are K and J defined by

$$K(x) = x + 1 \quad \text{and} \quad J(x) = 1/x.$$

We have $J^2 = 1$ and

$$K([a_0, t]) = [a_0 + 1, t], \quad K^{-1}([a_0, t]) = [a_0 - 1, t].$$

Also $J([a_0, t]) = [0, a_0, t])$ if $a_0 > 0$ and $J([0, t]) = [t])$. According to (42), the continued fractions of x and $-x$ differ only by the first terms. This completes the proof. [9]

□

4 Diophantine approximation and simple continued fractions

Lemma 43 (Lagrange, 1770)**.** *The sequence* $(|q_n x - p_n|)_{n \geq 0}$ *is strictly decreasing: for* $n \geq 1$ *we have*

$$|q_n x - p_n| < |q_{n-1} x - p_{n-1}|.$$

Proof. We use Lemma 20 twice: on the one hand

$$|q_n x - p_n| = \frac{1}{x_{n+1} q_n + q_{n-1}} < \frac{1}{q_n + q_{n-1}}$$

because $x_{n+1} > 1$, on the other hand

$$|q_{n-1} x - p_{n-1}| = \frac{1}{x_n q_{n-1} + q_{n-2}} > \frac{1}{(a_n + 1) q_{n-1} + q_{n-2}} = \frac{1}{q_n + q_{n-1}}$$

because $x_n < a_n + 1$. □

Corollary 6. *The sequence* $(|x - p_n/q_n|)_{n \geq 0}$ *is strictly decreasing: for* $n \geq 1$ *we have*

$$\left| x - \frac{p_n}{q_n} \right| < \left| x - \frac{p_{n-1}}{q_{n-1}} \right|.$$

[9]Bombieri in [2] gives formulae for $J([a_0, t])$ when $a_0 \leq -1$. He distinguishes eight cases, namely four cases when $a_0 = -1$ ($a_1 > 2$, $a_1 = 2$, $a_1 = 1$ and $a_3 > 1$, $a_1 = a_3 = 1$), two cases when $a_0 = -2$ ($a_1 > 1$, $a_1 = 1$) and two cases when $a_0 \leq -3$ ($a_1 > 1$, $a_1 = 1$). Here, (42) enables us to simplify his proof by reducing to the case $a_0 \geq 0$.

Proof. For $n \geq 1$, since $q_{n-1} < q_n$, we have

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{q_n} |q_n x - p_n| < \frac{1}{q_n} |q_{n-1} x - p_{n-1}| = \frac{q_{n-1}}{q_n} \left| x - \frac{p_{n-1}}{q_{n-1}} \right| < \left| x - \frac{p_{n-1}}{q_{n-1}} \right|.$$

□

Here is the *law of best approximation* of the simple continued fraction.

Lemma 44. *Let $n \geq 0$ and $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ with $q > 0$ satisfy*

$$|qx - p| < |q_n x - p_n|.$$

Then $q \geq q_{n+1}$.

Proof. The system of two linear equations in two unknowns u, v

$$\begin{cases} p_n u + p_{n+1} v & = p \\ q_n u + q_{n+1} v & = q \end{cases} \tag{45}$$

has determinant ± 1, hence there is a solution $(u, v) \in \mathbb{Z} \times \mathbb{Z}$.

Since $p/q \neq p_n/q_n$, we have $v \neq 0$.

If $u = 0$, then $v = q/q_{n+1} > 0$, hence $v \geq 1$ and $q \geq q_{n+1}$.

We now assume $uv \neq 0$.

Since q, q_n and q_{n+1} are > 0, it is not possible for u and v to be both negative. In case u and v are positive, the desired result follows from the second relation of (45). Hence one may suppose u and v of opposite signs. Since $q_n x - p_n$ and $q_{n+1} x - p_{n+1}$ also have opposite signs, the numbers $u(q_n x - p_n)$ and $v(q_{n+1} x - p_{n+1})$ have same sign, and therefore

$$|q_n x - p_n| = |u(q_n x - p_n)| + |v(q_{n+1} x - p_{n+1})| = |qx - p| < |q_n x - p_n|,$$

which is a contradiction.

□

A consequence of Lemma 44 is that the sequence of p_n/q_n produces the best rational approximations to x in the following sense: any rational number p/q with denominator $q < q_n$ has $|qx - p| > |q_n x - p_n|$. This is sometimes referred to as *best rational approximations of type* 0.

Corollary 7. *The sequence $(q_n)_{n\geq 0}$ of denominators of the convergents of a real irrational number x is the increasing sequence of positive integers for which*

$$\|q_n x\| < \|qx\| \quad \textit{for} \quad 1 \leq q < q_n.$$

As a consequence,

$$\|q_n x\| = \min_{1\leq q\leq q_n} \|qx\|.$$

The theory of continued fractions is developed starting from Corollary 7 as a definition of the sequence $(q_n)_{n\geq 0}$ in Cassels's book [4].

Corollary 8. *Let $n \geq 0$ and $p/q \in \mathbb{Q}$ with $q > 0$ satisfy*

$$\left| x - \frac{p}{q} \right| < \left| x - \frac{p_n}{q_n} \right|.$$

Then $q > q_n$.

Proof. For $q \leq q_n$ we have

$$\left| x - \frac{p}{q} \right| = \frac{1}{q}|qx - p| > \frac{1}{q}|q_n x - p_n| \frac{q_n}{q} \left| x - \frac{p_n}{q_n} \right| \geq \left| x - \frac{p_n}{q_n} \right|.$$

□

Corollary 8 shows that the denominators q_n of the convergents are also among the *best rational approximations of type* 1 in the sense that

$$\left| x - \frac{p}{q} \right| > \left| x - \frac{p_n}{q_n} \right| \quad \text{for} \quad 1 \leq q < q_n,$$

but they do not produce the full list of them: to get the complete set, one needs to consider also some of the rational fractions of the form

$$\frac{p_{n-1} + ap_n}{q_{n-1} + aq_n}$$

with $0 \leq a \leq a_{n+1}$ (*semi–convergents*) – see for instance [9], Chap. II, § 16.

Lemma 46 (Vahlen, 1895)**.** *Among two consecutive convergents p_n/q_n and p_{n+1}/q_{n+1}, one at least satisfies $|x - p/q| < 1/2q^2$.*

Proof. Since $x - p_n/q_n$ and $x - p_{n-1}/q_{n-1}$ have opposite signs,

$$\left|x - \frac{p_n}{q_n}\right| + \left|x - \frac{p_{n-1}}{q_{n-1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_n q_{n-1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2}\cdot$$

The last inequality is $ab < (a^2+b^2)/2$ for $a \neq b$ with $a = 1/q_n$ and $b = 1/q_{n-1}$. Therefore,

$$\text{either} \quad \left|x - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{or} \quad \left|x - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2}\cdot$$

□

Lemma 47 (É. Borel, 1903)**.** *Among three consecutive convergents p_{n-1}/q_{n-1}, p_n/q_n and p_{n+1}/q_{n+1}, one at least satisfies $|x - p/q| < 1/\sqrt{5}q^2$.*

As a matter of fact, the constant $\sqrt{5}$ cannot be replaced by a larger one. This is true for any number with a continued fraction expansion having all but finitely many partial quotients equal to 1 (which means the Golden number Φ and all rational numbers which are equivalent to Φ modulo $\mathrm{GL}_2(\mathbb{Z})$).

Proof. Recall Lemma 20: for $n \geq 0$,

$$q_n x - p_n = \frac{(-1)^n}{x_{n+1}q_n + q_{n-1}}\cdot$$

Therefore $|q_n x - p_n| < 1/\sqrt{5}q_n$ if and only if $|x_{n+1}q_n + q_{n-1}| > \sqrt{5}q_n$. Define $r_n = q_{n-1}/q_n$. Then this condition is equivalent to $|x_{n+1} + r_n| > \sqrt{5}$.

Recall the inductive definition of the convergents:

$$x_{n+1} = a_{n+1} + \frac{1}{x_{n+2}}\cdot$$

Also, using the definitions of r_n, r_{n+1}, and the inductive relation $q_{n+1} = a_{n+1}q_n + q_{n-1}$, we can write

$$\frac{1}{r_{n+1}} = a_{n+1} + r_n.$$

Eliminate a_{n+1}:

$$\frac{1}{x_{n+2}} + \frac{1}{r_{n+1}} = x_{n+1} + r_n.$$

Assume now

$$|x_{n+1}+r_n|\le\sqrt{5}\quad\text{and}\quad |x_{n+2}+r_{n+1}|\le\sqrt{5}.$$

We deduce

$$\frac{1}{\sqrt{5}-r_{n+1}}+\frac{1}{r_{n+1}}\le\frac{1}{x_{n+2}}+\frac{1}{r_{n+1}}=x_{n+1}+r_n\le\sqrt{5},$$

which yields

$$r_{n+1}^2-\sqrt{5}r_{n+1}+1\le 0.$$

The roots of the polynomial $X^2-\sqrt{5}X+1$ are $\Phi=(1+\sqrt{5})/2$ and $\Phi^{-1}=(\sqrt{5}-1)/2$. Hence $r_{n+1}>\Phi^{-1}$ (the strict inequality is a consequence of the irrationality of the Golden ratio). .

This estimate follows from the hypotheses $|q_nx-p_n|<1/\sqrt{5}q_n$ and $|q_{n+1}x-p_{n+1}|<1/\sqrt{5}q_{n+1}$. If we also had $|q_{n+2}x-p_{n+2}|<1/\sqrt{5}q_{n+2}$, we would deduce in the same way $r_{n+2}>\Phi^{-1}$. This would give

$$1=(a_{n+2}+r_{n+1})r_{n+2}>(1+\Phi^{-1})\Phi^{-1}=1,$$

which is impossible.

□

Lemma 48 (Legendre, 1798)**.** *If $p/q\in\mathbb{Q}$ satisfies $|x-p/q|\le 1/2q^2$, then p/q is a convergent of x.*

Proof. Let r and s in $\mathbb{Z}$ satisfy $1\le s<q$. From

$$1\le|qr-ps|=|s(qx-p)-q(sx-r)|\le s|qx-p|+q|sx-r|\le\frac{s}{2q}+q|sx-r|$$

one deduces

$$q|sx-r|\ge 1-\frac{s}{2q}>\frac{1}{2}\ge q|qx-p|.$$

Hence $|sx-r|>|qx-p|$ and therefore Lemma 44 implies that p/q is a convergent of x.

□

References

[1] E. J. Barbeau, *Pell's equation*, Problem Books in Mathematics, Springer-Verlag, New York, 2003.

[2] E. Bombieri, *Continued fractions and the Markoff tree*, Expo. Math., 25 (2007), pp. 187–213.

[3] E. Bombieri and A. J. van der Poorten, *Continued fractions of algebraic numbers*, in Computational algebra and number theory (Sydney, 1992), vol. 325 of Math. Appl., Kluwer Acad. Publ., Dordrecht, 1995, pp. 137–152.

[4] J. W. S. Cassels, *An introduction to Diophantine approximation*, Hafner Publishing Co., New York, 1972. Facsimile reprint of the 1957 edition, Cambridge Tracts in Mathematics and Mathematical Physics, No. 45.

[5] P. Flajolet, B. Vallée, I. Vardi, *Continued fractions from Euclid to the present day*, 44p.
http://www.lix.polytechnique.fr/Labo/Ilan.Vardi/continued_fractions.ps

[6] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, sixth ed., 2008. Revised by D. R. Heath-Brown and J. H. Silverman.

[7] M. J. Jacobson, Jr. and H. C. Williams, *Solving the Pell equation*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, Springer, New York, 2009.

[8] H. W. Lenstra, Jr., *Solving the Pell equation*, Notices Amer. Math. Soc., 49 (2002), pp. 182–192.

[9] O. Perron, *Die Lehre von den Kettenbrüchen. Dritte, verbesserte und erweiterte Aufl. Bd. II. Analytisch-funktionentheoretische Kettenbrüche*, B. G. Teubner Verlagsgesellschaft, Stuttgart, 1957.

[10] D. Roy, *On the continued fraction expansion of a class of numbers*, in Diophantine approximation, vol. 16 of Dev. Math., SpringerWien-NewYork, Vienna, 2008, pp. 347–361.
`http://arxiv.org/abs/math/0409233`.

[11] A. J. van der Poorten, *An introduction to continued fractions*, in Diophantine analysis (Kensington, 1985), vol. 109 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1986, pp. 99–138.

The pdf file of this talk can be downloaded at URL
`http://www.imj-prg.fr/~michel.waldschmidt/`