Updated: *Juen 7, 2010*

Diophantine approximation, irrationality and transcendence

Michel Waldschmidt

Course N°7, *May 10, 2010*

These are informal notes of my course given in April – June 2010 at IMPA (*Instituto Nacional de Matematica Pura e Aplicada*), Rio de Janeiro, Brazil.

6.3.6 The main lemma

The theory which follows is well–known (a classical reference is the book [7] 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, 9]. An important role in our presentation of the subject is the following result (Lemma 4.1 in [8]).

Lemma 81. *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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_s & 1 \\ 1 & 0 \end{pmatrix} \tag{82}$$

These integers are also characterized by

$$\frac{b}{d} = [a_0, a_1, \ldots, a_{s-1}], \quad \frac{c}{d} = [a_s, \ldots, a_1], \quad (-1)^{s+1} = \epsilon. \tag{83}$$

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 $a_0, \dots, a_s$ satisfy the conclusion of Lemma 81, then by using (82), we find $b/d = [a_0, a_1, \dots, a_{s-1}]$. Taking the transpose, we also find $c/d = [a_s, \dots, a_1]$. 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 69). 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 (83), say $c/d = [a_s, \dots, a_1]$. Let a_0 be a rational integer such that the distance between b/d and $[a_0, a_1, \dots, a_{s-1}]$ 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

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

and

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

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 $k \in \mathbf{Z}$, and from

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

we conclude $k = 0$, $(a', b', c', d') = (a, b, c, d)$. Hence (82) follows.

□

Corollary 84. *Assume the hypotheses of Lemma 81 are satisfied.*
a) If $c > d$, then $a_s \geq 1$ and

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

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

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

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 84. 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). □

Another consequence of Lemma 81 is the following classical result (Satz 13 p. 47 of [7]).

Corollary 85. *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*

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

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 81, 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 84, 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 $y = x_{s+1}$. □

6.3.7 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

$$a_{n+s} = a_n \quad \text{for all } n \geq 1. \tag{86}$$

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

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

If s_0 is the smallest positive integer satisfying (86), then the set of s satisfying (86) is the set of positive multiples of s_0. In this case $(a_1, \ldots, a_{s_0})$ is called *the fundamental period* of the original sequence.

Theorem 87. *Let D be a positive integer which is not a square. Write the simple continued fraction of $\sqrt{D}$ as $[a_0, a_1, \ldots]$ with $a_0 = \lfloor\sqrt{D}\rfloor$.*
a) The sequence $(a_1, a_2, \ldots)$ is periodic.
b) Let (x, y) be a positive integer solution to Pell's equation $x^2 - Dy^2 = \pm 1$. Then there exists $s \geq 1$ such that $x/y = [a_0, \ldots, a_{s-1}]$ and

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

is a period of the sequence $(a_1, a_2, \ldots)$. Further, $a_{s-i} = a_i$ for $1 \leq i \leq s-1$ [9]*).*
c) Let $(a_1, a_2, \ldots, a_{s-1}, 2a_0)$ be a period of the sequence $(a_1, a_2, \ldots)$. Set $x/y = [a_0, \ldots, a_{s-1}]$. 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 $(a_1, a_2, \ldots, a_{s-1}, 2a_0)$ is a period of the sequence $(a_1, a_2, \ldots)$, then

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

Consider the fundamental period $(a_1, a_2, \ldots, a_{s_0-1}, a_{s_0})$ of the sequence $(a_1, a_2, \ldots)$. By part b) of Theorem 87 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 87, it follows that the fundamental solution (x_1, y_1) to Pell's equation $x^2 - Dy^2 = \pm 1$ is given by $x_1/y_1 = [a_0, \ldots, a_{s_0-1}]$,

[9] One says that the word $a_1, \ldots, a_{s-1}$ 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`.

and that $x_1^2 - Dy_1^2 = (-1)^{s_0}$. Therefore, if s_0 is even, then there is no solution to the Pell's equation $x^2 - Dy^2 = -1$. If s_0 is odd, then (x_1, y_1) is the fundamental solution to Pell's equation $x^2 - Dy^2 = -1$, while the fundamental solution (x_2, y_2) to 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 87 that the $(ns_0 - 1)$-th convergent

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

satisfies

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n. \tag{88}$$

We shall check this relation directly (Lemma 92).

Proof. Start with a positive solution (x, y) to Pell's equation $x^2 - Dy^2 = \pm 1$, which exists according to Proposition 75. Since $Dy \geq x$ and $x > y$, we may use lemma 81 and corollary 84 with

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

and write

$$\begin{pmatrix} Dy & x \\ x & y \end{pmatrix} = \begin{pmatrix} a_0' & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1' & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_s' & 1 \\ 1 & 0 \end{pmatrix} \tag{89}$$

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 (89) 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 Pell's equation $x^2 - Dy^2 = \pm 1$, then the continued fraction expansion of $\sqrt{D}$ is of the form

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{s-1}, 2a_0}] \tag{90}$$

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

$$x/y = [a_0, a_1, \ldots, a_{s-1}]. \tag{91}$$

Consider a convergent $p_n/q_n = [a_0, a_1, \ldots, a_n]$. If $a_{n+1} = 2a_0$, then (73) 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 79 that (p_n, q_n) is a solution to 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 79 implies that (p_m, q_m) is a solution to Pell's equation $p_m^2 - Dq_m^2 = \pm 1$. Finally, Theorem 87 implies that $m+1$ is a multiple of s_0, hence $n+1$ also.

□

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

Lemma 92. *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 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 Pell's equation $x^2 - Dy^2 = \pm 1$. We check this result directly.

Proof. From Lemma 81 and relation (89), 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

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{ns_0-1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_n & Dy_n - a_0x_n \\ y_n & x_n - a_0y_n \end{pmatrix}. \tag{93}$$

Notice that the determinant is $(-1)^{ns_0} = x_n^2 - Dy_n^2$. Formula (93) 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 (93) 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

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

Therefore

$$\begin{pmatrix} x_{n+1} & D y_{n+1} - a_0 x_{n+1} \\ y_{n+1} & x_{n+1} - a_0 y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n & D y_n - a_0 x_n \\ y_n & x_n - a_0 y_n \end{pmatrix} \begin{pmatrix} x_1 + a_0 y_1 & (D - a_0^2) y_1 \\ y_1 & x_1 - a_0 y_1 \end{pmatrix}.$$

The first column gives

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

which was to be proved.

$\square$

6.3.9 Records

For large D, 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[10].

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

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

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

6.3.10 A criterion for the existence of a solution to the negative Pell equation

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

Proposition 94 (R.A. Mollin, A. Srinivasan[11]). *Let d be a positive integer which is not a square. Let (x_0, y_0) be the fundamental solution to Pell's equation $x^2 - dy^2 = 1$. Then the equation $x^2 - dy^2 = -1$ has a solution if and only if $x_0 \equiv -1 \pmod{2d}$.*

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 $a^2 - db^2 = -1$. □

6.3.11 Arithmetic varieties

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

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

The map

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

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 $\mathbf{R}^\times$, for which

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

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

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 $\mathbf{Z}$ which respect the quadratic form $x^2 - Dy^2$ is the group

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

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

This is not a new proof of Proposition 75, but an interpretation and a generalization. Such results are valid for *arithmetic varieties*[12].

[12] 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`.

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] 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.

[5] 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.

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

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

[8] 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`.

[9] 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.