Seventh course: september 24, 2007. [9]

2.2.3 Diophantine approximation and Diophantine Equations

There are deep connexions between diophantine approximation and Diophantine equations. In this section we show how continued fractions expansions are used for solving the equation:

$$x^2 - dy^2 = \pm 1 \tag{2.18}$$

(where the unknowns x, y are in $\mathbb{Z}$) which is named Pell's equation. Later we shall consider other examples.

There is a natural ordering among the solutions, by increasing x (or y, it amounts to the same). Since we are looking at positive solutions there is a smallest one, called the *fundamental solution*, say (x_1, y_1).

From $x_1^2 - dy_1^2 = \pm 1$ it readily follows that the sequence of pairs of integers (x_n, y_n) defined by

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$$

satisfies also $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$ hence

$$x_n^2 - dy_n^2 = \pm 1.$$

If the fundamental solution has $x_1^2 - dy_1^2 = 1$, then all x_n, y_n also have $x_n^2 - dy_n^2 = 1$, while if $x_1^2 - dy_1^2 = -1$, then for all n we have $x_n^2 - dy_n^2 = (-1)^n$. In the second case (x_2, y_2) is the fundamental solution of the equation $x_1^2 - dy_1^2 = 1$.

Let us check that all solutions of the Pell's equation are the (x_n, y_n) with $n \geq 0$ (with $n = 0$ giving the trivial solution $(1, 0)$). Consider the following subset of $\mathbb{R}^2$:

$$G = \bigl\{(\log|x + y\sqrt{d}|, \log|x - y\sqrt{d}|)\ ;\ (x, y) \in \mathbb{Z}^2,\ x^2 - dy^2 = \pm 1\bigr\}.$$

It is easily checked that G is an additive subgroup of $\mathbb{R}^2$. This is due to the fact that the equation $x^2 - dy^2 = \pm 1$ can be written $(x + \sqrt{d}y)(x - \sqrt{d}y) = \pm 1$, hence the solutions (x, y) form a multiplicative group with the law given by

$$(x + y\sqrt{d})(x' + y'\sqrt{d}) = xx' + dyy' + (xy' + x'y)\sqrt{d},$$

corresponding to the identity

$$(xx' + dyy')^2 - d(xy' + x'y)^2 = (x^2 - dy^2)(x'^2 - dy'^2).$$

Now G is *discrete* in $\mathbb{R}^2$: any compact subset of $\mathbb{R}^2$ contains only finitely many elements in G, because for each $C > 0$, if $(x, y) \in \mathbb{Z}^2$ satisfies $|x + y\sqrt{d}| \leq C$ and $|x - y\sqrt{d}| \leq C$, then $|x|$ and $|y|$ are bounded.

[9] Updated: October 12, 2007

Further G is contained in the one dimensional subspace $t_1 + t_2 = 0$ of $\mathbb{R}^2$. A discrete subgroup in a real vector space of dimension 1 has rank ≤ 1 (see § 2.2.7). It easily follows that any solution $(x, y) \in \mathbb{Z}^2$ with $x > 0$ and $y \geq 0$ of Pell's equation satisfies $x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ for some $n \geq 0$.

Hence the problems remains to find the fundamental solution (x_1, y_1). It turns out, as we shall see, that x_1 may be quite large without d being to large. But there is an efficient algorithm to solve the problem.

The connexion with Diophantine approximation arises from the following remark. If (x, y) is a solution, then $(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$, hence x/y is a good rational approximation of $\sqrt{d}$ and this approximation is sharper when x is larger. Hence a strategy for solving Pell's equation (2.18) is based on the continued fraction expansion of $\sqrt{d}$.

Let again d be a positive integer which is not a square. It is known that the continued fraction expansion

$$\sqrt{d} = [a_0;\ \overline{a_1,\ a_2,\ \ldots,\ a_k}]$$

of the square root of $d > 0$ has $a_0 = [\sqrt{d}]$ and $a_k = 2a_0$. Moreover

$$a_1,\ a_2,\ \ldots,\ a_{k-1}$$

is a *palindrome*: $a_i = a_{k-i}$ $(1 \leq i \leq k-1)$. The next proposition shows that the length k of the period is odd if and only if the Diophantine equation $x^2 - dy^2 = -1$ has a root in rational integers x, y.

Proposition 2.19. *Let d be a positive which is not a square. Write*

$$\sqrt{d} = [a_0;\ \overline{a_1,\ a_2,\ \ldots,\ a_k}].$$

a) When k is even, the fundamental solution of the equation $x^2 - dy^2 = 1$ is given by

$$\frac{x_1}{y_1} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1}]$$

and there is no solution to the equation $x^2 - dy^2 = -1$.
b) When k is odd, the fundamental solution to $x^2 - dy^2 = -1$ is given by

$$\frac{x_1}{y_1} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1}]$$

and the fundamental solution to $x^2 - dy^2 = 1$ is given by

$$\frac{x_2}{y_2} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1},\ a_k,\ a_1,\ a_2,\ \ldots,\ a_{k-1}].$$

The solutions (x_n, y_n) are obtained by a similar formula: writing A for the block $a_1,\ a_2,\ \ldots,\ a_{k-1}$,

$$\frac{x_n}{y_n} = [a_0;\ A,\ a_k,\ A,\ a_k,\ \ldots,\ A,\ a_k,\ A]$$

where A occurs n times.

We consider numerical examples. The easiest Pell's equation is $x^2-2y^2=-1$ with $d=2$ and $\sqrt{2}=[1;\overline{2}]$. The fundamental solution is $(x_1,y_1)=(1,1)$. For the equation $x^2-2y^2=1$ the fundamental solution is $x=3$, $y=2$, corresponding to the expansion

$$[1;2]=1+\frac{1}{2}=\frac{3}{2}\cdot$$

Here is another example due to Brahmagupta in 628:

$$x^2-92y^2=1.$$

Brahmagupta did not use continued fractions but a method of his own (called "cyclic method" — Chakravala — see [2]), and he found the fundamental solution which is $x=1151$, $y=120$:

$$1151^2-92\cdot 120^2=1\,324\,801-1\,324\,800=1.$$

The continued fraction expansion of $\sqrt{92}=9,591663046625\dots$ is [10]

$$\sqrt{92}=[9;\overline{1,\ 1,\ 2,\ 4,\ 2,\ 1,\ 1,\ 18}]$$

and the fundamental solution arises from

$$[9;\ 1,\ 1,\ 2,\ 4,\ 2,\ 1,\ 1]=\frac{1151}{120}\cdot$$

The next example is due to Bhaskara II in his work *Bijaganita* (1150): the fundamental solution to $x^2-61y^2=1$ is

$$x=1\,766\,319\,049,\qquad y=226\,153\,980.$$

Here $\sqrt{61}=[7;\overline{1,\ 4,\ 3,\ 1,\ 2,\ 2,\ 1,\ 3,\ 4,\ 1,\ 14}]$ and

$$[7;1,4,3,1,2,2,1,3,4,1,14,1,4,3,1,2,2,1,3,5]=\frac{1\,766\,319\,049}{226\,153\,980}\cdot$$

The fundamental solution to $x^2-61y^2=-1$ is obtained as follows:

$$[7;1,4,3,1,2,2,1,3,5]=\frac{29\ 718}{3\ 805},$$

$$29\ 718^2=883\ 159\ 524,\quad 61\cdot 3805^2=883\ 159\ 525.$$

A further example due to Narayana (14th Century) is $x^2-103y^2=1$ with the fundamental solution $x=227\,528$, $y=22\,419$. Indeed

$$227\,528^2-103\cdot 22\,419^2=51\,768\,990\,784-51\,768\,990\,783=1.$$

[10]Easy to compute using http://wims.unice.fr/wims/

$$\sqrt{103} = [10; \overline{6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6,\ 20}]$$

and

$$[10; 6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6] = \frac{227\,528}{22\,419}.$$

Fermat also knew how to solve Pell's equation $x^2 - dy^2 = 1$: he found the fundamental solution for $d = 61$ (Bhaskara's equation) as well as for $d = 109$:

$$x = 158070671986249, \quad y = 15140424455100.$$

A Pell equation occurred already much earlier in the *Cattle problem* attributed to Archimedes. There are bulls and cows of different colors, the first part of the problem involves several unknowns and easy equations so solve:

$$B - \left(\frac{1}{2} + \frac{1}{3}\right) N = N - \left(\frac{1}{4} + \frac{1}{5}\right) X = X - \left(\frac{1}{6} + \frac{1}{7}\right) B = J.$$

Up to a factor, the solution is

$$B = 2226,\ N = 1602,\ X = 1580,\ J = 891.$$

The second part of the Cattle problem amounts to solving the Pell equation

$$x^2 - 4729494 y^2 = 1.$$

A partial solution was given in 1880 by A. Amthor. The fundamental solution has been given in 1998 by Ilan Vardi in a simple explicit formula

$$\left[\frac{25194541}{184119152} (109931986732829734979866232821433543901088049 + 50549485234315033074477819735540408986340\sqrt{4729494})^{4658}\right]$$

The size of the fundamental solution is $\simeq 10^{103275}$.

Pell-Fermat Diophantine equations occur in the construction of Riemannian varieties with negative curvature called *arithmetic varieties.* See [1].

We consider another connexion between Diophantine approximation and Diophantine equations which we shall expand in § 2.2.9. In 1909 A. Thue found a connection between Diophantine equation and refinements of Liouville's estimate. We restrict here on one specific example.

Liouville's estimate for the rational Diophantine approximation of $\sqrt[3]{2}$ is

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{9q^3}$$

for sufficiently large q (use Lemma 1.13 with $P(X) = X^3 - 2$, $c = 3\sqrt[3]{2} < 9$). Thue was the first to achieve an improvement of the exponent 3. A explicit estimate was then obtained by A. Baker

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{10^6 q^{2.955}}$$

and refined by Chudnovskii, Easton, Rickert, Voutier and others, until 1997 when M. Bennett proved that *for any* $p/q \in \mathbb{Q}$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{1}{4\, q^{2,5}}\cdot$$

From his result, Thue deduced that *for any fixed* $k \in \mathbb{Z} \setminus \{0\}$, *there are only finitely many* $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ *satisfying the Diophantine equation* $x^3 - 2y^3 = k$. The result of Baker shows more precisely that if $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is a solution to $x^3 - 2y^3 = k$, then

$$|x| \leq 10^{137}|k|^{23}.$$

M. Bennett gave the sharper estimate: *for any* $(x, y) \in \mathbb{Z}^2$ *with* $x > 0$,

$$|x^3 - 2y^3| \geq \sqrt{x}.$$

The connexion between Diophantine approximation to $\sqrt[3]{2}$ and the Diophantine equation $x^3 - 2y^3 = k$ is explained in the next lemma.

Lemma 2.20. *Let* η *be a positive real number. The two following properties are equivalent.*
(i) There exists a constant $c_1 > 0$ *such that, for any* $p/q \in \mathbb{Q}$ *with* $q > 0$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{c_1}{q^\eta}\cdot$$

(ii) There exists a constant $c_2 > 0$ *such that, for any* $(x, y) \in \mathbb{Z}^2$ *with* $x > 0$,

$$|x^3 - 2y^3| \geq c_2 x^{3-\eta}.$$

Properties (i) and (ii) are true but uninteresting with $\eta \geq 3$. They are not true with $\eta < 2$. It is not expected that they are true with $\eta = 2$, but it is expected that they are true for any $\eta > 2$.

Proof. We assume $\eta < 3$, otherwise the result is trivial. Set $\alpha = \sqrt[3]{2}$.

Assume (i) and let $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ have $x > 0$. Set $k = x^3 - 2y^3$. Since 2 is not the cube of a rational number we have $k \neq 0$. If $y = 0$ assertion (ii) plainly holds. So assume $y \neq 0$.

Write

$$x^3 - 2y^3 = (x - \alpha y)(x^2 + \alpha xy + \alpha^2 y^2).$$

The polynomial $X^2 + \alpha X + \alpha^2$ has negative discriminant $-3\alpha^2$, hence has a positive minimum $c_0 = 3\alpha^2/4$. Hence the value at (x, y) of the quadratic form $X^2 + \alpha XY + \alpha^2 Y^2$ is bounded form below by $c_0 y^2$. From (i) we deduce

$$|k| = |y|^3 \left|\sqrt[3]{2} - \frac{x}{y}\right| (x^2 + \alpha xy + \alpha^2 y^2) \geq \frac{c_1 c_0 |y|^3}{|y|^\eta} = c_3 |y|^{3-\eta}.$$

This gives an upper bound for $|y|$:

$$|y| \leq c_4 |k|^{1/(3-\eta)}, \quad \text{hence} \quad |y^3| \leq c_4 |k|^{3/(3-\eta)}.$$

We want an upper bound for x: we use $x^3 = k + 2y^3$ and we bound $|k|$ by $|k|^{3/(3-\eta)}$ since $3/(3-\eta) > 1$. Hence

$$x^3 \leq c_5|k|^{3/(3-\eta)} \quad \text{and} \quad x^{3-\eta} \leq c_6|k|.$$

Conversely, assume (ii). Let p/q be a rational number. If p is not the nearest integer to $q\alpha$, then $|q\alpha - p| > 1/2$ and the estimate (i) is trivial. So we assume $|q\alpha - p| \leq 1/2$. We need only the weaker estimate $c_7 q < p < c_8 q$ with some positive constants c_7 and c_8, showing that we may replace p by q or q by p in our estimates, provided that we adjust the constants. From

$$p^3 - 2q^3 = (p - \alpha q)(p^2 + \alpha pq + \alpha^2 q^2),$$

using (ii), we deduce

$$c_2 p^{3-\eta} \leq c_{10} q^3 \left|\alpha - \frac{p}{q}\right|,$$

and (i) easily follows.

□

References

[1] N. Bergeron – *Sur la topologie de certains espaces provenant de constructions arithmétiques.*

[2] A. Weil – *Number theory. An approach through history. From Hammurapi to Legendre,* Birkhäuser Boston, Inc., Boston, Mass., (1984) 375 pp.