Updated: *February 12, 2012*

These are informal notes of my five courses on Diophantine Approximation and Diophantine Equations, given in November 29, 30 and December 5, 8, 12, 2011, for the "Special Years in Mathematics" Project at HRI Harish-Chandra Research Institute (HRI), Allahabad (India).
This text is available on the website
http://people.math.jussieu.fr/∼miw/articles/pdf/HRI2011.pdf

Diophantine approximation and Diophantine equations

Michel Waldschmidt

1 First course, November 29, 2011

The first course is devoted to the basic setup of Diophantine approximation: we start with rational approximation to a single real number. Firstly, positive results tell us that a real number x has "good" rational approximation p/q, where "good" is when one compares $|x - p/q|$ and q. We discuss Dirichlet's result in 1842 (see [**?**] Course N°2 §2.1) and the Markoff–Lagrange spectrum ([**?**] Course N°10).

Next we consider negative results for rational approximation, with Liouville's estimate for the approximation of a real algebraic number by rational numbers. We state explicit versions of Liouville's inequality (see [**?**] §3.5 and exercise 3.6; [**?**] Course N°3 §4.1 Lemma 24 and Proposition 26 and Course N°4 §4.1.2), involving the absolute logarithmic height ([**?**] §3.2).

2 Second course, November 30, 2011

The second course includes a short historical survey of the improvements of Liouville's inequality: in the lower bound

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$$

for α real algebraic number of degree $d \geq 3$, the exponent d of q in the denominator of the right hand side is replaced by κ with
• any $\kappa > (d/2) + 1$ by A. Thue (1909),
• $2\sqrt{d}$ by C.L. Siegel in 1921,
• $\sqrt{2d}$ by Dyson and Gel'fond in 1947,
• any $\kappa > 2$ by K.F. Roth in 1955.
See [**?**] Course N°4 §4.1.3.

Theorem 1 (A. Thue, C.L. Siegel, F. Dyson, K.F. Roth 1955)**.** *For any real algebraic number α, for any $\epsilon > 0$, the set of $p/q \in \mathbf{Q}$ with $|\alpha - p/q| < q^{-2-\epsilon}$ is finite.*

An equivalent statement is that, for any real algebraic number α and for any $\epsilon > 0$, there exists $q_0 > 0$ such that, for $p/q \in \mathbf{Q}$ with $q \geq q_0$, we have $|\alpha - p/q| > q^{-2-\epsilon}$.

We now explain that, if one restricts the denominators q of the rational approximations p/q by requesting that their prime factors belong to a given finite set, then the exponent 2 can be replaced by 1 (D. Ridout, 1957). See ([**?**] Course N°4 §4.1.3 Th. 47).

Let S be a finite set of primes. A rational number is called *an S–integer* if it can be written a/b where all prime factors of the denominator b belong to S. The set of S–integers is the subring of $\mathbf{Q}$ generated by the elements $1/p$ with $p \in S$. We denote it by $S^{-1}\mathbf{Z}$. The group of units of $S^{-1}\mathbf{Z}$ is a multiplicative subgroup $(S^{-1}\mathbf{Z})^\times$ of $\mathbf{Q}^\times$, its elements are the *S–units*. If $S = \{p_1, \ldots, p_s\}$, then

$$(S^{-1}\mathbf{Z})^\times = \left\{ p_1^{k_1} \cdots p_s^{k_s} \;\mid\; (k_1, \ldots, k_s) \in \mathbf{Z}^s \right\} \subset \mathbf{Q}^\times$$

and

$$S^{-1}\mathbf{Z} = \left\{ \frac{a}{b} \;\mid\; a \in \mathbf{Z},\ b \in (S^{-1}\mathbf{Z})^\times \right\} \subset \mathbf{Q}.$$

A corollary to Ridout's Theorem **??** below is the following:

> *Let S be a finite set of prime numbers. Let α be a real algebraic number. For any $\epsilon > 0$, the set of S–integers a/b such that $|\alpha - a/b| < b^{-1-\epsilon}$, is finite.*

Actually, the statement by Ridout is more general (see for instance [**?**] §2.1).

Theorem 2 (D. Ridout, 1957)**.** *Let α and β be two algebraic numbers with $(\alpha, \beta) \neq (0, 0)$. For $1 \leq i \leq s$, let α_i and β_i be two rational numbers with $(\alpha_i, \beta_i) \neq (0, 0)$. Let $\epsilon > 0$. Then the set of rational numbers p/q such that*

$$q|q\alpha - p\beta| \prod_{i=1}^{s} |q\alpha_i - p\beta_i|_{p_i} < \frac{1}{\max\{|p|, q\}^\epsilon}$$

is finite.

The previous corollary follows by taking $\beta = 1$, $\alpha_i = 0$ and $\beta_i = 1$ for $1 \leq i \leq s$: if q is a positive integer which is an S–unit, then

$$\prod_{i=1}^{s} |q|_{p_i} = \frac{1}{q}.$$

3 Third course, December 5, 2011

The third course is devoted to Schmidt's Subspace Theorem and one of its many applications to exponential Diophantine equations. We first state a special case of Schmidt's Subspace Theorem (1972) together with its p-adic extension by H.P. Schlickewei (1976).

For x a nonzero rational number, write the decomposition of x into prime factors

$$x = \pm \prod_p p^{v_p(x)},$$

where p runs over the set of prime numbers and $v_p(x) \in \mathbf{Z}$ (with only finitely many $v_p(x)$ distinct from 0), and set

$$|x|_p = p^{-v_p(x)}.$$

The product formula is

$$|x| \prod_p |x|_p = 1$$

for all $x \in \mathbf{Q}^\times$ (see [**?**] §3.1.1 for the rational field case and §3.1.5 for algebraic number fields).

For $\mathbf{x} = (x_1, \dots, x_m) \in \mathbf{Z}^m$, define

$$|\mathbf{x}| = \max\{|x_1|, \dots, |x_m|\}.$$

Here is a simplified version of this fundamental result ([**?**] Course N°4 §4.1.3 Th. 49; see also Theorem 2.3 of [**?**]).

Theorem 3 (Schmidt's Subspace Theorem, simplified form)**.** *Let $m \geq 2$ be a positive integer, S a finite set of prime numbers. Let $L_1, \dots, L_m$ be m independent linear forms in m variables with algebraic coefficients. Further, for each $p \in S$ let $L_{1,p}, \dots, L_{m,p}$ be m independent linear forms in m variables with rational coefficients. Let $\epsilon > 0$. Then the set of $\mathbf{x} = (x_1, \dots, x_m) \in \mathbf{Z}^m$ such that*

$$|L_1(\mathbf{x}) \cdots L_m(\mathbf{x})| \prod_{p \in S} |L_{1,p}(\mathbf{x}) \cdots L_{m,p}(\mathbf{x})|_p \leq |\mathbf{x}|^{-\epsilon}$$

is contained in the union of finitely many proper subspaces of $\mathbf{Q}^m$.

Thue–Siegel–Roth's Theorem **??** follows from Theorem **??** by taking

$$S = \emptyset, \qquad m = 2, \quad L_1(x_1, x_2) = x_1, \quad L_2(x_1, x_2) = \alpha x_1 - x_2.$$

A $\mathbf{Q}$-vector subspace of $\mathbf{Q}^2$ which is not $\{0\}$ nor $\mathbf{Q}^2$ (that is, *a proper subspace*) is generated by an element $(q_0, p_0) \in \mathbf{Q}^2$. There is one such subspace with $q_0 = 0$, namely $\mathbf{Q} \times \{0\}$ generated by $(1, 0)$, the other ones have $q_0 \neq 0$. Mapping such a rational subspace to the rational number p_0/q_0 yields a 1 to 1 correspondence. Hence Theorem **??** says that there is only a finite set of exceptions p/q in Thue–Siegel–Roth's Theorem **??**.

Ridout's Theorem **??** is the special case $n = 1$ of Schmidt's Subspace Theorem **??**. Indeed, a subset E of $\mathbf{Z}^2$ is contained in a finite union of hyperplanes of $\mathbf{Q}^2$ if and only if the set of $y/x \in \mathbf{Q}$, where (x, y) ranges over the set of elements in E with $x \neq 0$, is finite. Hence Thue–Siegel–Roth's Theorem **??** is the special case ($n = 1$, $S = \emptyset$) of Theorem **??**.

We derive a further consequence, dealing with exponential Diophantine equations, of the special case of Schmidt's Subspace Theorem **??** where the linear forms $L_1, \dots, L_k$ also have rational coefficients. We start with an exercise.

Exercise 1. *Show that the only solutions of the equation $2^a + 3^b = 5^c$ in non-negative integers a, b and c are given by*

$$2 + 3 = 5, \quad 2^2 + 1 = 5, \quad 2^4 + 3^2 = 5^2.$$

The finiteness of the set of solutions of such an equation is a general fact: we deduce from Ridout's Theorem **??** the following statement:

Corollary 4. *Let $S = \{p_1, \dots, p_s\}$ be a finite set of prime numbers and let $n \geq 2$. Then the set of solutions of the equation $x_1 + x_2 = 1$ in S–units x_1, x_2 is finite.*

Proof. Let (x_1, x_2) be a solution of the equation $x_1 + x_2 = 1$ in S–units. Let y_0 be the least common denominator of x_1 and x_2. Set $y_1 = y_0 x_1$ and $y_2 = y_0 x_2$. Then y_0, y_1, y_2 are relatively prime integers, they are S–units, and $y_1 + y_2 = y_0$. Introduce the three linear forms in two variables Y_1, Y_2

$$\Lambda_1(Y_1, Y_2) = Y_1, \quad \Lambda_2(Y_1, Y_2) = Y_2, \quad \Lambda_0(Y_1, Y_2) = Y_1 + Y_2.$$

Notice that $\Lambda_i(y_1, y_2) = y_j$ for $j = 0, 1, 2$, and that any two linear forms among $\Lambda_0, \Lambda_1, \Lambda_2$ are linearly independent. Let $k \in \{0, 1, 2\}$ be an index such that $\max\{|y_0|, |y_1|, |y_2|\} = |y_k|$, and let ℓ, m be the two other indices, so that $\{0, 1, 2\} = \{k, \ell, m\}$.

Since y_0, y_1, y_2 are relatively prime rational integers, for $j = 1, \dots, s$, we have $\max\{|y_0|_{p_j}, |y_1|_{p_j}, |y_2|_{p_j}\} = 1$; let $k_j \in \{0, 1, 2\}$ be an index such that $|y_k|_{p_j} = 1$, and let ℓ_j, m_j be the two other indices, so that $\{0, 1, 2\} = \{k_j, \ell_j, m_j\}$.

Consider the linear forms

$$L_1 = \Lambda_\ell, \quad L_2 = \Lambda_m, \qquad L_{1j} = \Lambda_{\ell_j}, \quad L_{2j} = \Lambda_{m_j} \quad (1 \leq j \leq s).$$

Notice that

$$L_1(y_1, y_2) L_2(y_1, y_2) = y_\ell y_m = \frac{y_0 y_1 y_2}{y_k} = \pm \frac{y_0 y_1 y_2}{\max\{|y_0|, |y_1|, |y_2|\}},$$

while

$$L_{1j}(y_1, y_2) L_{2j}(y_1, y_2) = y_{\ell_j} y_{m_j} = \frac{y_0 y_1 y_2}{y_k}$$

and

$$|L_{1j}(y_1, y_2) L_{2j}(y_1, y_2)|_{p_j} = |y_0 y_1 y_2|_{p_j}.$$

From the product formula, using the fact that $y_0y_1y_2$ is an S unit, one deduces

$$|y_0y_1y_2| \prod_{j=1}^{s} |y_0y_1y_2|_{p_j} = 1$$

Therefore

$$|L_1(y_1,y_2)L_2(y_1,y_2)| \prod_{j=1}^{s} |L_{1j}(y_1,y_2)L_{2j}(y_1,y_2)|_{p_j} = \frac{1}{\max\{|y_0|,|y_1|,|y_2|\}}.$$

From Ridout's Theorem **??** with $\epsilon = 1$, one deduces that the set of y_1/y_2 is finite, and Corollary **??** follows.

□

We come back to this S–unit equation $X + Y = 1$ in §**??**. In particular, we will see there that the result of Corollary **??** is effective: one can bound from above the (numerators and denominators of the) solutions x_1 and x_2.

We now consider the more general equation

$$X_1 + \cdots + X_k = 1, \tag{5}$$

where k is a fixed positive integer and the values $x_1, \ldots, x_k$ taken by the unknown $X_1, \ldots, X_k$ are S–units in $\mathbf{Q}$ for a fixed given finite set S of prime numbers. This equation has infinitely many solutions as soon as $k \geq 3$ and S is nonempty: for $p \in S$ and $a \in \mathbf{Z}$,

$$x_1 = p^a, \quad x_2 = -p^a, \quad x_3 = 1, \qquad p^a - p^a + 1 = 1.$$

In view of this example, we will say that a solution $(x_1, \ldots, x_k) \in ((S^{-1}\mathbf{Z})^\times)^k$ of equation (**??**) is *non degenerate* if no nontrivial subsum vanishes:

$$x_1 + \cdots + x_k = 1$$

and

$$\sum_{i \in I} x_i \neq 0 \quad \text{for any nonempty subset } I \text{ of } \{1, \ldots, k\}.$$

Without giving all details, we explain how to deduce, from Schmidt's Subspace Theorem **??**, the following statement.

Corollary 6. *Let S be a finite set of primes and k a positive integer. Then the set of nondegenerate solutions $(x_1, \ldots, x_k) \in ((S^{-1}\mathbf{Z})^\times)^k$ of equation (**??**) is finite.*

*Sketch of proof of Corollary **??** as a consequence of Theorem **??**.* The proof is by induction on k. A first remark is that the statement of Corollary **??** is equivalent to the next one (which only looks more general):

For any finite set S of primes, any positive integer k and any rational numbers $c_1, \dots, c_k$, the set of $(x_1, \dots, x_k) \in ((S^{-1}\mathbf{Z})^\times)^k$ satisfying

$$c_1 x_1 + \cdots + c_k x_k = 1$$

and

$$\sum_{i \in I} c_i x_i \neq 0 \quad \text{for any nonempty subset } I \text{ of } \{1, \dots, k\}$$

is finite.

This last statement is in fact a consequence of Corollary **??**: we deduce it by enlarging the set S of primes to a finite set $S' \supset S$, so that $c_1, \dots, c_k$ are S'–units.

In the same vein, by reducing to the same denominator, one can phrase Corollary **??** in an equivalent form by stating that the set of $(y_1, \dots, y_{k+1}) \in (\mathbf{Z} \cap (S^{-1}\mathbf{Z})^\times)^{k+1}$, satisfying

$$y_1 + \cdots + y_k = y_{k+1} \quad \text{and} \quad \gcd(y_1, \dots, y_{k+1}) = 1,$$

and

$$\sum_{i \in I} y_i \neq 0 \quad \text{when } I \text{ is a nonempty subset of } \{1, \dots, k\},$$

is finite.

Starting with a solution $\mathbf{y}$, using the assumption $\gcd(y_1, \dots, y_{k+1}) = 1$, we consider for each prime $p \in S$ an index $i_p \in \{1, \dots, k+1\}$ such that $|y_{i_p}|_p = 1$. We also consider an index i_0 such that $|y_{i_0}| = \max_{1 \le i \le k+1} |y_i|$. In other terms $|y_{i_0}| = |\mathbf{y}|$. The tuple $\big(i_0, (i_p)_{p \in S}\big)$ can take only finitely many possible values – we fix one of them.

We introduce the following $k+1$ linear forms Λ_j $(1 \le j \le k+1)$ in $Y_1, \dots, Y_k$:

$$\Lambda_j = Y_j \quad \text{for} \quad 1 \le j \le k \quad \text{and} \quad \Lambda_{k+1} = Y_1 + \cdots + Y_k.$$

Clearly, any k distinct linear forms among $\Lambda_1, \dots, \Lambda_{k+1}$ are linearly independent. We shall use Theorem **??** with the following linear forms in the variables $Y_1, \dots, Y_k$:

$$\{L_1, \dots, L_k\} = \{\Lambda_j \mid 1 \le j \le k+1,\ j \neq i_0\}$$

and, for any prime p in S,

$$\{L_{1p}, \dots, L_{kp}\} = \{\Lambda_j \mid 1 \le j \le k+1,\ j \neq i_p\}.$$

We write

$$\prod_{i=1}^{k} |L_i(\mathbf{y})| = \frac{1}{|\mathbf{y}|} \prod_{j=1}^{k+1} |\Lambda_j(\mathbf{y})|$$

and, for each prime $p \in S$,

$$\prod_{i=1}^{k} |L_{ip}(\mathbf{y})|_p = \prod_{j=1}^{k+1} |\Lambda_j(\mathbf{y})|_p.$$

For any prime p not in S and for $j = 1, \dots, k+1$, we have $|\Lambda_j(\mathbf{y})|_p = 1$. From the product formula

$$|\Lambda_j(\mathbf{y})| \prod_p |\Lambda_j(\mathbf{y})|_p = 1$$

for $1 \le j \le k+1$, we deduce the estimate

$$|L_1(\mathbf{y}) \cdots L_k(\mathbf{y})| \prod_{p \in S} |L_{1p}(\mathbf{y}) \cdots L_{kp}(\mathbf{y})|_p = \frac{1}{|\mathbf{y}|},$$

which shows that we can apply Theorem **??** with $\epsilon = 1$.

It follows that the solutions $(y_1, \dots, y_k)$ we are considering belong to a finite union of proper subspaces of $\mathbf{Z}^k$. We are reduced to consider a finite set of Diophantine equations of the form

$$c_1 Y_1 + \cdots + c_k Y_k = 0,$$

where $c_1, \dots, c_k$ are fixed elements of $\mathbf{Z}$, not all 0. We fix such an equation, we fix an index $j_1 \in \{1, \dots, k\}$ with $c_{j_1} \neq 0$ and we write

$$\sum_{\substack{1 \le i \le k \\ i \neq j_1}} \frac{-c_i}{c_{j_1}} \frac{y_i}{y_{j_1}} = 1.$$

We use the preliminary remark of this proof (we enlarge S if necessary so that c_i/c_{j_1} becomes an S–unit for $i = 1, \dots, k$). We also select one such subsum which is non degenerate. We deduce from the induction hypothesis that there is an index j_2, $(1 \le j_2 \le k,\ j_2 \neq j_1)$ such that the set of y_{j_2}/y_{j_1} is finite. We now write the initial equation in the form

$$\sum_{\substack{1 \le i \le k \\ i \neq j_1, i \neq j_2}} \frac{y_i}{y_{j_1}} - \frac{y_{k+1}}{y_{j_1}} = -1 - \frac{y_{j_2}}{y_{j_1}}.$$

The right hand side is a nonzero constant, since $y_{j_2} + y_{j_1} \neq 0$ (here we use the assumption on nonvanishing subsums for subsums of two terms only). Again, we enlarge S if necessary, so that $-1 - y_{j_2}/y_{j_1}$ becomes an S–unit. The left hand side is a sum of $k-1$ terms which are S–units. This sum is non degenerate (no nontrivial subsum vanishes): indeed it follows from the assumption on nonvanishing subsums (here we need the full assumption, not only for subsums of two terms) that no sum of the form

$$\sum_{i \in I} y_i \quad \text{nor} \quad \sum_{i \in I} y_i - y_{k+1} \quad \text{for} \quad \emptyset \neq I \subset \{1, \dots, k\} \setminus \{i_1,\ i_2\}$$

can vanish. We obtain the final conclusion by using the induction hypothesis once more.

□

The proof of Corollary **??** is noneffective: in general, there is no method (yet) to derive an upper bound for the size of the solutions. But upper bounds for the number of solutions are available. To give an upper bound for the number of subspaces in the conclusion of Theorem **??** has been an open problem from 1970 to 1980, which has been solve by W.M. Schmidt (see the references to the works of Evertse and Schlickewei on the quantitative versions of Schmidt's Subspace Theorem in [**?**]).

The general case of Schmidt's Subspace Theorem ([**?**], Theorem 2.5) involves a finite set of places of a number field K, containing the places at infinity, and instead of $|\mathbf{x}|^{-\epsilon}$ it involves $H(\mathbf{x})^{-\epsilon}$ where

$$H(\mathbf{x}) = \prod_{v \in M_K} \max_{1 \le i \le k} |x_i|_v,$$

where M_K is the set of places of K.

4 Fourth course, December 8, 2011

The fact that the irrationality exponent is $< d$ in Thue's Theorem (§**??**) has very important corollaries in the theory of Diophantine equations. We start with a special 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. Thue was the first to achieve an improvement of the exponent 3. An explicit estimate was then obtained by A. Baker, namely

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

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

$$\left| \sqrt[3]{2} - \frac{p}{q} \right| \ge \frac{1}{4\ q^{2.5}}.$$

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

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

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

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

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 7. *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 $p/q \in \mathbf{Q}$ with $q > 0$,*

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

(ii) *There exists a constant $c_2 > 0$ such that, for any $(x, y) \in \mathbf{Z}^2$ 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 true with $\eta = 3$ (for $\eta = 3$, (i) is Liouville's estimate while (ii) is trivial); they are true also for any $\eta > 2$ by Thue–Siegel–Roth's Theorem **??**. They are not true with $\eta < 2$. It is expected that they are not true with $\eta = 2$. The constants are explicit for $\eta \geq 2.5$ by Bennett's result, but not yet for η in the range $2 < \eta < 2.5$.

Proof. See [**?**] §1 and [**?**] Course N°4 §4.1.3.

□

The following link, between the rational approximation on the one hand and the finiteness of the set of solutions of some diophantine equations on the other hand, is Proposition 2.1 of [**?**].

Proposition 8. *Let $f \in \mathbf{Z}[X]$ be an irreducible polynomial of degree d and let $F(X, Y) = Y^d f(X/Y)$ be the associated homogeneous binary form of degree d. Then the following two assertions are equivalent:*
(i) For any integer $k \neq 0$, the set of $(x, y) \in \mathbf{Z}^2$ verifying

$$F(x, y) = k \tag{9}$$

is finite.
(ii) For any real number $\kappa > 0$ and for any root $\alpha \in \mathbf{C}$ of f, the set of rational numbers p/q verifying

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{\kappa}{q^d} \tag{10}$$

is finite.

Exercise 2. *Let α be an algebraic number of degree $d \geq 3$ and minimal polynomial $f \in \mathbf{Z}[X]$, let $F(X, Y) = Y^d f(X/Y) \in \mathbf{Z}[X, Y]$ be the associated homogeneous polynomial. Let $0 < \kappa \leq d$. The following conditions are equivalent:*
(i) *There exists $c_1 > 0$ such that, for any $p/q \in \mathbf{Q}$,*

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c_1}{q^\kappa}.$$

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

$$|F(x, y)| \geq c_2 \ x^{d-\kappa}.$$

So far, we considered the basic situation of rational numbers and points with rational integer coordinates on Thue curves. Here we consider the algebraic numbers while the number field K may vary. We denote by $\mathbf{Z}_K$ the ring of algebraic integers of K and by $\mathbf{Z}_K^\times$ the unit group of K. The proof of the next result appears in [**?**]. See also §3 of [**?**].

Proposition 11. *The following statements are equivalent:*

• (M) *For any number field K and for any nonzero element k in K, the Mordell equation*

$$Y^2 = X^3 + k$$

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

• (E) *For any number field K and for any polynomial f in $K[X]$ of degree 3 with three distinct complex roots, the elliptic equation*

$$Y^2 = f(X)$$

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

• (HE) *For any number field K and for any polynomial f in $K[X]$ with at least three simple complex roots, the hyperelliptic equation*

$$Y^2 = f(X)$$

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

• (SE) *For any number field K, for any integer $m \geq 3$ and for any polynomial f in $K[X]$ with at least two distinct complex roots whose orders of multiplicity are prime to m, the superelliptic equation*

$$Y^m = f(X)$$

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

• (T) *For any number field K, for any nonzero element k in K and for any elements $\alpha_1, \ldots, \alpha_n$ in K with $\mathrm{Card}\{\alpha_1, \ldots, \alpha_n\} \geq 3$, the Thue equation*

$$(X - \alpha_1 Y) \cdots (X - \alpha_n Y) = k$$

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

• (S) *For any number field K and for any elements a_1 and a_2 in K with $a_1 a_2 \neq 0$, the Siegel equation*

$$a_1 E_1 + a_2 E_2 = 1$$

has but a finite number of solutions $(\varepsilon_1, \varepsilon_2) \in \mathbf{Z}_K^\times \times \mathbf{Z}_K^\times$.

Each of these statements is a theorem: the first four ones are due to Siegel who proved that the sets of integral points respectively on a Mordell curve (M), on an elliptic curve (E), on a hyperelliptic curve (HE), on a superelliptic curve (SE), are finite. Statement (T) is due to Thue and (S) deals with the unit equation introduced by Siegel (see §**??**).

For each of the six equivalent statements in Proposition **??**, an upper bound is known for the size of the solutions; the proofs of the equivalences between them are elementary and effective: they allow one to deduce, from an explicit version of any of these statements, an explicit version of the other ones.

A further result which is equivalent to the six statements of Proposition **??** is Siegel's fundamental theorem on the finiteness of points on a curve of genus ≥ 1. See for instance [**?**].

5 Fifth course, December 12, 2011

We first state the special case $K = \mathbf{Q}$ of Proposition 5.1 in [**?**]. We will provide explanations on the meaning of (iv) just after the statement.

Proposition 12. *The following four assertions are equivalent:*

(i) *For any finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers, for any $k \in \mathbf{Q}^\times$ and for any binary homogeneous form $F(X,Y) \in \mathbf{Q}[X,Y]$ with the property that the polynomial $F(X,1) \in \mathbf{Q}[X]$ has at least three linear factors involving three distinct roots in $\mathbf{Q}$, the Thue-Mahler equation*

$$F(X,Y) = \pm k p_1^{Z_1} \cdots p_s^{Z_s}$$

has only finitely many solutions $(x, y, z_1, \ldots, z_s)$ in $\mathbf{Z}^{2+s}$ with $\gcd(xy, p_1 \cdots p_s) = 1$.

(ii) *For any finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers, the Thue-Mahler equation*

$$XY(X-Y) = \pm k p_1^{Z_1} \cdots p_s^{Z_s}$$

has but a finite number of solutions $(x, y, z_1, \ldots, z_s)$ in $\mathbf{Z}^{2+s}$ with $\gcd(xy, p_1 \cdots p_s) = 1$.

(iii) *For any finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers, the S–unit equation*

$$E_1 + E_2 = 1$$

has but a finite number of solutions $(\varepsilon_1, \varepsilon_2)$ in $(S^{-1}\mathbf{Z})^\times \times (S^{-1}\mathbf{Z})^\times$.

(iv) *For any finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers, every set of S–integral points of $\mathbf{P}^1(\mathbf{Q})$ minus three points is finite.*

We now explain the statement (iv). The projective line on the rational number field $\mathbf{P}^1(\mathbf{Q})$ can be described in several ways, one of them is to say that it is the set of equivalence classes of pairs (a, b) where a and b are two rational numbers, not both zero, with (a, b) being equivalent to (a', b') if there exists $c \in \mathbf{Q}^\times$ with

$$a' = ac, \quad b' = bc.$$

The class of (a, b) is denoted $(a : b)$. Each class has a unique representative (a, b) where a and b are in $\mathbf{Z}$ and are relatively prime. There are bijective maps

between $\mathbf{P}^1(\mathbf{Q})$ and the disjoint union of $\mathbf{Q}$ with one element, which we denote by ∞. One of these bijective maps is

$$(0:1) \mapsto \infty \text{ and } (a:b) \mapsto b/a \text{ for } a \neq 0.$$

If one removes from $\mathbf{P}^1(\mathbf{Q})$ the point $(0:1)$, then this mapping induces a bijective map $\mathbf{P}^1(\mathbf{Q}) \setminus \{(0:1)\} \mapsto \mathbf{Q}$. The inverse image of an element in $S^{-1}\mathbf{Z}$ will be called *an S–integral point on* $\mathbf{P}^1(\mathbf{Q}) \setminus \{(0:1)\}$. Hence, the point $(a:b)$ with $a, b \in \mathbf{Z}$ and $\gcd(a,b) = 1$ is an S–integral point on $\mathbf{P}^1(\mathbf{Q}) \setminus \{(0:1)\}$ if and only if a is an S–unit. As a consequence, a point of $\mathbf{P}^1(\mathbf{Q})$ with projective coordinates $(a:b)$ where $a, b \in \mathbf{Z}$ and $\gcd(a,b) = 1$ is an S–integral point on $\mathbf{P}^1(\mathbf{Q}) \setminus \{(0:1)\}$ is and only if, for any prime number p not in S, the image of $(a:b)$ in $\mathbf{P}^1(\mathbf{F}_p)$ (under the map $\mathbf{P}^1(\mathbf{Q}) \to \mathbf{P}^1(\mathbf{F}_p)$ induced by the reduction $\mathbf{Z} \to \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ modulo p) is not the point $(0:1)$.

Similarly, if one removes from $\mathbf{P}^1(\mathbf{Q})$ the point $(1:0)$, then the mapping given by

$$(1:0) \mapsto \infty \text{ and } (a:b) \mapsto a/b \text{ for } b \neq 0$$

induces a bijective map $\mathbf{P}^1(\mathbf{Q}) \setminus \{(1:0)\} \mapsto \mathbf{Q}$. The inverse image of an element in $S^{-1}\mathbf{Z}$ will be called *an S–integral point on* $\mathbf{P}^1(\mathbf{Q}) \setminus \{(1:0)\}$. Hence, the point $(a:b)$ with $a, b \in \mathbf{Z}$ and $\gcd(a,b) = 1$ is an S–integral point on $\mathbf{P}^1(\mathbf{Q}) \setminus \{(1:0)\}$ if and only if b is an S–unit. Therefore an S–integral point on $\mathbf{P}^1(\mathbf{Q}) \setminus \{(0:1),\ (1:0)\}$ is a projective point with coordinates $(a:b)$ with $a, b \in \mathbf{Z}$ and $\gcd(a,b) = 1$ where a and b are S–units.

Now we remove from $\mathbf{P}^1(\mathbf{Q})$ the point $(1:1)$. Then the mapping given by

$$(1:1) \mapsto \infty \text{ and } (a:b) \mapsto (2a-b)/(a-b) \text{ for } a - b \neq 0$$

is a bijective map $\mathbf{P}^1(\mathbf{Q}) \setminus \{(1:1)\} \mapsto \mathbf{Q}$. One could replace the numerator $2a - b$ by $\lambda a + \mu b$ provided that $(\lambda, \mu) \in \mathbf{Z} \times \mathbf{Z}$ satisfies $\lambda + \mu = \pm 1$. Hence a point $(a:b)$ with $a, b \in \mathbf{Z}$ and $\gcd(a,b) = 1$ of $\mathbf{P}^1(\mathbf{Q}) \setminus \{(1:1)\}$ will be called *an S–integral point on* $\mathbf{P}^1(\mathbf{Q}) \setminus \{(1:1)\}$ *if $a - b$ is an S–unit.* Notice that the condition for $(a:b)$ to be an S–integral point on $\mathbf{P}^1(\mathbf{Q}) \setminus \{(1:1)\}$ is that its reduction in $\mathbf{P}^1(\mathbf{F}_p)$ is not the point $(1:1)$ for all prime numbers p not in S.

Finally, the S–integral points on $\mathbf{P}^1(\mathbf{Q}) \setminus \{(0:1),\ (1:0),\ (1:1)\}$ are the points of projective coordinates $(a:b)$ where $a, b \in \mathbf{Z}$, $\gcd(a,b) = 1$ and the three integers a, b, $a - b$ are S–units.

Before stating an extension of Proposition **??** to number fields, we give variants of the formulations of conditions (i), (ii) and (iii).

Consider the Diophantine equation

$$F(X,Y) = \pm k p_1^{Z_1} \cdots p_s^{Z_s}$$

in (i) where the unknowns $(X, Y, Z_1, \ldots, Z_s)$ now take their values in $(S^{-1}\mathbf{Z})^2 \times \mathbf{Z}^s$. Write the right hand side as $k\varepsilon$ with $\varepsilon \in (S^{-1}\mathbf{Z})^\times$. Two solutions (x, y, ε) and (x, y, ε) in $(S^{-1}\mathbf{Z})^2 \times (S^{-1}\mathbf{Z})^\times$ of the Thue–Mahler equation $F(X,Y) = kE$ are called *equivalent* if there exists $\eta \in (S^{-1}\mathbf{Z})^\times$ such that

$$x' = \eta x, \quad y' = \eta y, \quad \varepsilon' = \eta^m \varepsilon,$$

where m is the degree of F. Notice that a solution has always $(x, y) \neq 0$, and that there is only one class of solutions with $x = 0$ (hence $y \neq 0$) and one class with $y = 0$ (hence $x \neq 0$). Therefore (i) means that the Diophantine equation

$$F(X, Y) = kE$$

has but a finite number of classes of solutions $(x, y, \varepsilon) \in (S^{-1}\mathbf{Z})^2 \times (S^{-1}\mathbf{Z})^\times$.

For the same reason, assertion (ii) can be stated in an equivalent way as follows: *for any finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers, the Thue-Mahler equation $XY(X - Y) = E$ has but a finite number of classes of solutions $(x, y, \varepsilon) \in (S^{-1}\mathbf{Z})^2 \times (S^{-1}\mathbf{Z})^\times$.*

Another equivalent statement to (iii) is to say that the set of solutions in $(S^{-1}\mathbf{Z})^3$ of the homogeneous S–unit equation

$$E_1 + E_2 = E_0$$

is the union of finitely many classes, where two solutions $(\epsilon_0, \epsilon_1, \epsilon_2)$ and $(\epsilon'_0, \epsilon'_1, \epsilon'_2)$ are in the same class if they are proportional:

$$\frac{\epsilon_0}{\epsilon'_0} = \frac{\epsilon_1}{\epsilon'_1} = \frac{\epsilon_2}{\epsilon'_2}.$$

The next result is Proposition 5.1 of [**?**], which extends Proposition **??** to number fields. We now introduce the definitions of the ring of S–integers and the group of S–units of a number field K, when S is a finite set of places of K including the archimedean places. The ring O_S of S-integers of K is defined by

$$O_S \ = \ \{x \in K \ \mid \ |x|_v \leq 1 \ \text{ for each } \ v \notin S\} = \bigcap_{v \notin S} \mathcal{O}_v.$$

The group $O_S^\times$ of S-units of K is the group of units of O_S, namely

$$O_S^\times \ = \ \{x \in K \ \mid \ |x|_v = 1 \ \text{ for each } \ v \notin S\} = \bigcap_{v \notin S} \mathcal{O}_v^\times.$$

Thanks to the last formulas, when we will deal with S-integers α (resp. S-units ε), then α (resp. ε) belongs to the local rings $\mathcal{O}_v$ (resp. to the unit groups of the local rings $\mathcal{O}_v$) at all places v outside S.

We will consider an algebraic number field K and a finite set S of places of K containing all the archimedean places. Moreover F will denote a binary homogeneous form with coefficients in K. We will consider the Thue–Mahler equations $F(X, Y) = E$ where the two unknowns X, Y take respectively values x, y in a given set of S–integers of K while the unknown E takes its values ε in the set of S–units of K. If (x, y, ε) is a solution and if m denotes the degree of F, then, for all $\eta \in O_S^\times$, the triple $(\eta x, \eta y, \eta^m \varepsilon)$ is also a solution. Two solutions (x, y, ε) and (x', y', ε') in $O_S^2 \times O_S^\times$ of the equation $F(X, Y) = E$ are said to be *equivalent modulo $O_S^\times$* if the points of $\mathbf{P}^1(K)$ with projective coordinates $(x : y)$ and $(x' : y')$ are the same.

If the two solutions (x, y, ε) and (x', y', ε') are equivalent, there exists $\eta \in K^\times$ such that $x' = \eta x$ and $y' = \eta y$. Since (x, y, ε) and (x', y', ε') are solutions of the equation $F(X, Y) = E$, we also have $\varepsilon' = \eta^m \varepsilon$ where m is the degree of the binary homogeneous form $F(X, Y)$. Since ε and ε' are S–units, η^m is also an S–unit, hence $\eta \in O_S^\times$. In other terms, two solutions (x, y, ε) and (x', y', ε') are equivalent if there exists $\eta \in O_S^\times$ such that

$$x' = \eta x, \quad y' = \eta y, \quad \varepsilon' = \eta^m \varepsilon.$$

Proposition 13. *Let K be an algebraic number field.*
(1) *The following four assertions are equivalent:*

(i) For any finite set S of places of K containing all the archimedean places, for every $k \in K^\times$ and for any binary homogeneous form $F(X, Y)$ with the property that the polynomial $F(X, 1) \in K[X]$ has at least three linear factors involving three distinct roots in K, the Thue-Mahler equation

$$F(X, Y) = kE$$

has but a finite number of classes of solutions $(x, y, \varepsilon) \in O_S^2 \times O_S^\times$.

(ii) For any finite set S of places of K containing all the archimedean places, the Thue-Mahler equation

$$XY(X - Y) = E$$

has but a finite number of classes of solutions $(x, y, \varepsilon) \in O_S^2 \times O_S^\times$.

(iii) For any finite set S of places of K containing all the archimedean places, the S–unit equation

$$E_1 + E_2 = 1$$

has but a finite number of solutions $(\varepsilon_1, \varepsilon_2)$ in $O_S^\times \times O_S^\times$.

(iv) For any finite set S of places of K containing all the archimedean places, every set of S–integral points of $\mathbf{P}^1(K)$ minus three points is finite.

(2) *Moreover, each of these assertions is a consequence of the following one:*

(v) For any finite set S of places of K containing all the archimedean places, every set A of S–integral points on an open variety, obtained by removing from $\mathbf{P}^2(K)$ four hyperplanes, is contained in a finite union of projective hyperplanes of $\mathbf{P}^2(K)$.

The last statement is Proposition 6.1 of [**?**].

Proposition 14. *Let K be a number field. The following two assertions are equivalent.*

(i) Let $n \geq 1$ be an integer and let S a finite set of places of K including the archimedean places. Then the equation

$$E_0 + \cdots + E_n = 0$$

has only finitely many classes modulo $O_S^\times$ of solutions $(\varepsilon_0, \ldots, \varepsilon_n) \in (O_S^\times)^{n+1}$ for which no proper subsum $\sum_{i \in I} \varepsilon_i$ vanishes, with I being a subset of $\{0, \ldots, n\}$, with at least two elements and at most n.

(*ii*) *Let $n \geq 1$ be an integer and let S a finite set of places of K including the archimedean places. Then for any set of $n+2$ distinct hyperplanes $H_0, \ldots, H_{n+1}$ in $\mathbf{P}^n(K)$, the set of S–integral points of $\mathbf{P}^n(K) \setminus (H_0 \cup \cdots \cup H_{n+1})$ is contained in a finite union of hyperplanes of $\mathbf{P}^n(K)$.*

One may remark that the case $n = 1$ of assertion (*i*) in Proposition **??** is nothing else than assertion (*iii*) of Proposition **??**, and that the case $n = 1$ (resp. $n = 2$) of assertion (*ii*) of Proposition **??** is nothing else than assertion (*iv*) (resp. (*v*)) of Proposition **??**.

One of the earliest statements on Siegel Generalized S–unit equation goes back to the work of M. Laurent in 1984 (see [**?**] §4). Assertion (*i*) of Proposition **??** on the generalized unit equation has been proved independently by J.H. Evertse on the one hand, by H.P. Schlickewei and A.J. van der Poorten (1982) on the other hand. A special (but significant) case had been obtained earlier by E. Dubois and G. Rhin.

References

[1] Y. F. Bilu, *The many faces of the Subspace Theorem [after Adamczewski, Bugeaud, Corvaja, Zannier...]*, Astérisque, (2008), pp. Exp. No. 967, vii, 1–38. Séminaire Bourbaki. Vol. 2006/2007.
`http://www.math.u-bordeaux1.fr/~yuri/publ/preprs/subspace.pdf`

[2] M. Hindry and J.H. Silverman – *Diophantine geometry. An introduction.* Graduate Texts in Mathematics, **201**. Springer-Verlag, New York, 2000.

[3] C. Levesque and M. Waldschmidt – *Approximation of an algebraic number by products of rational numbers and units,* to appear.
`http://www.math.jussieu.fr/~miw/articles/pdf/CLMW-AANPRNU2011.pdf`

[4] M. Waldschmidt, *Diophantine equations and transcendental methods* (written by Noriko Hirata). In Transcendental numbers and related topics, RIMS Kôkyûroku, Kyoto, **599** (1986), n°8, 82-94. Notes by N. Hirata.
`http://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/599.html`

[5] ——, *Diophantine approximation on linear algebraic groups*, vol. 326 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 2000. Transcendence properties of the exponential function in several variables.
`http://www.math.jussieu.fr/~miw/articles/pdf/3-540-66785-7.pdf`

[6] ——, *Introduction to Diophantine approximation and transcendental number theory* ; notes of the course given at IMPA - Instituto Nacional de Matematica Pura e Aplicada, Rio de Janeiro, April 12 - June 29, 2010 (205 pages).
`http://www.math.jussieu.fr/~miw/articles/pdf/IMPA2010.pdf`

Michel WALDSCHMIDT
Université P. et M. Curie (Paris VI)
Institut Mathématique de Jussieu
Théorie des Nombres, Case 247
4, Place Jussieu
75252 Paris CEDEX 05, France
miw@math.jussieu.fr
http://www.math.jussieu.fr/∼miw/

This text is available on the internet at the address
http://www.math.jussieu.fr/∼miw/articles/pdf/HRI2011.pdf