20 mai 2015

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

Schmidt Subspace Theorem and S–unit equation

Michel Waldschmidt

We start with 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 [3] Course N°4 §4.1.3.

Théorème 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 $p/q \in \mathbb{Q}$ 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 $p/q \in \mathbb{Q}$ 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 ([3] 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 $\mathbb{Q}$ generated by the elements $1/p$ with $p \in S$. We denote it by $S^{-1}\mathbb{Z}$. The group of units of $S^{-1}\mathbb{Z}$ is a multiplicative subgroup $(S^{-1}\mathbb{Z})^\times$ of $\mathbb{Q}^\times$, its elements are the *S–units*. If $S = \{p_1, \ldots, p_s\}$, then

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

and

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

A corollary to Ridout's Theorem 2 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 [1] §2.1).

Théorème 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

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

We now state a special case of Schmidt's Subspace Theorem (1972) together with its p-adic extension by H.P. Schlickewei (1976). Next we introduce one of its many applications to exponential Diophantine equations.

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 $v_p(x) \in \mathbb{Z}$ (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 $x \in \mathbb{Q}^\times$ (see [2] §3.1.1 for the rational field case and §3.1.5 for algebraic number fields).

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

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

Here is a simplified version of this fundamental result ([3] Course N°4 §4.1.3 Th. 49; see also Theorem 2.3 of [1]).

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

Thue–Siegel–Roth's Theorem 1 follows from Theorem 3 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 $\mathbb{Q}$-vector subspace of $\mathbb{Q}^2$ which is not $\{0\}$ nor $\mathbb{Q}^2$ (that is, *a proper subspace*) is generated by an element $(q_0, p_0) \in \mathbb{Q}^2$. There is one such subspace with $q_0 = 0$, namely $\mathbb{Q} \times \{0\}$ 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 3 says that there is only a finite set of exceptions p/q in Thue–Siegel–Roth's Theorem 1.

Ridout's Theorem 2 is the special case $n = 1$ of Schmidt's Subspace Theorem 3. Indeed, a subset E of $\mathbb{Z}^2$ is contained in a finite union of hyperplanes

of $\mathbb{Q}^2$ if and only if the set of $y/x \in \mathbb{Q}$, where (x, y) ranges over the set of elements in E with $x \neq 0$, is finite. Hence Thue–Siegel–Roth's Theorem 1 is the special case ($n = 1$, $S = \emptyset$) of Theorem 3.

We derive a further consequence, dealing with exponential Diophantine equations, of the special case of Schmidt's Subspace Theorem 3 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 nonnegative 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 2 the following statement:

Corollary 1. *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 $|y_{k_j}|_{p_j} = 1$, 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

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

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 $y_0 y_1 y_2$ is an S unit, one deduces

$$|y_0 y_1 y_2| \prod_{j=1}^{s} |y_0 y_1 y_2|_{p_j} = 1$$

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 2 with $\epsilon = 1$, one deduces that the set of y_1/y_2 is finite, and Corollary 1 follows.

□

It turns out that the result of Corollary 1 is effective: one can bound from above the (numerators and denominators of the) solutions x_1 and x_2. The proof rests on transcendence methods and lower bounds for linear combinations of logarithms of algebraic numbers.

We now consider the more general equation

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

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 $\mathbb{Q}$ 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 $a \in \mathbb{Z}$,

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

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

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

and

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

Without giving all details, we explain how to deduce, from Schmidt's Subspace Theorem 3, the following statement.

Corollary 2. *Let S be a finite set of primes and k a positive integer. Then the set of nondegenerate solutions $(x_1,\dots,x_k) \in ((S^{-1}\mathbb{Z})^\times)^k$ of equation (1) is finite.*

Sketch of proof of Corollary 2 *as a consequence of Theorem* 3. The proof is by induction on k. A first remark is that the statement of Corollary 2 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 $(x_1,\dots,x_k) \in ((S^{-1}\mathbb{Z})^\times)^k$ satisfying*
>
> $$c_1x_1 + \cdots + c_kx_k = 1$$
>
> *and*
>
> $$\sum_{i\in I} c_ix_i \neq 0 \quad \textit{for any nonempty subset } I \textit{ of } \{1,\dots,k\}$$
>
> *is finite.*

This last statement is in fact a consequence of Corollary 2: 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 2 in an equivalent form by stating that the set of $(y_1,\dots,y_{k+1}) \in (\mathbb{Z}\cap(S^{-1}\mathbb{Z})^\times)^{k+1}$, 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 3 with the following linear forms in the variables $Y_1, \dots, Y_k$:

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

and, for any prime p in S,

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

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

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

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 $i = 1, \ldots, k$). We also select one such subsum which is non degenerate. We deduce from the induction hypothesis that there is an index j_2, $(1 \leq j_2 \leq k,\ j_2 \neq j_1)$ such that the set of y_{j_2}/y_{j_1} is finite. We now write the initial equation in the form

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

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

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

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

□

The proof of Corollary 2 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 3 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 [1]).

The general case of Schmidt's Subspace Theorem ([1], 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.

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. Waldschmidt, *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://people.math.jussieu.fr/∼miw/articles/pdf/3-540-66785-7.pdf

[3] ——, *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://people.math.jussieu.fr/∼miw/articles/pdf/IMPA2010.pdf

This text is available on the internet at the address
http://people.math.jussieu.fr/~miw/articles/pdf/SubspaceTheoremOujda2015.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
http://webusers.imj-prg.fr/~michel.waldschmidt/