THE P-ADIC SUBSPACE THEOREM

JAN-HENDRIK EVERTSE

May 2011

Literature:
B. Edixhoven, J.-H. Evertse (eds.), Diophantine Approximation and Abelian Varieties, Introductory Lectures, Lecture Notes in Mathematics 1566, Springer Verlag 1993, Chap.IV

1. The p-adic Subspace Theorem

The p-adic Subspace Theorem deals with Diophantine inequalities in which several different absolute values occur, i.e., the ordinary absolute value, which we denote by $|\cdot|_\infty$ and p-adic absolute values $|\cdot|_{p_1}, \ldots, |\cdot|_{p_t}$ for certain distinct primes $p_1, \ldots, p_t$. The p-adic absolute value $|\cdot|_p$ has a unique continuation to $\overline{\mathbb{Q}}_p$ (the algebraic closure of $\mathbb{Q}_p$).

By 'algebraic' we always mean 'algebraic over $\mathbb{Q}$'.

A point $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ is called *primitive* if $\gcd(x_1, \ldots, x_n) = 1$.

Theorem 1.1. (Schlickewei, 1977) *Let $r \geqslant n \geqslant 2$, $C > 0$, $\delta > 0$ and $S := \{\infty, p_1, \ldots, p_t\}$ where $p_1, \ldots, p_t$ are distinct prime numbers. Further, let $L_{1\infty}, \ldots, L_{r,\infty}$ be linear forms in $X_1, \ldots, X_n$ with algebraic coefficients in $\mathbb{C}$ in general position, and for $j = 1, \ldots, t$, let $L_{1,p_j}, \ldots, L_{r,p_j}$ be linear forms in $X_1, \ldots, X_n$ with algebraic coefficients in $\overline{\mathbb{Q}}_{p_j}$ in general position. Consider the inequality*

$$\prod_{p \in S} |L_{1p}(\mathbf{x}) \cdots L_{rp}(\mathbf{x})|_p \leqslant C\|\mathbf{x}\|^{r-n-\delta} \quad \text{in primitive } \mathbf{x} \in \mathbb{Z}^n\,. \tag{1.1}$$

Then there are a finite number of proper linear subspaces $T_1, \ldots, T_s$ of $\mathbb{Q}^n$ such that all solutions of (1.1) lie in $T_1 \cup \cdots \cup T_s$.

Remarks. 1. In all our applications, for the prime numbers $p_1, \ldots, p_t$ the product of the linear forms $L_{1,p_j} \cdots L_{r,p_j}$ will be a polynomial with coefficients in $\mathbb{Q}$. This implies that if $\mathbf{x}$ is a solution of (1.1), then $\prod_{i=1}^r L_{i,p_j}(\mathbf{x}) \in \mathbb{Q}$, and

so we don't have to work with numbers in $\overline{\mathbb{Q}}_{p_j}$.

2. Similarly as for the Subspace Theorem discussed in the previous section, the proof of the p-adic Subspace Theorem is ineffective, i.e., it does not give a method to determine the subspaces.

Example. Let $\delta > 0$. We show that the inequality

$$|2^u + 3^v - 5^w| \leqslant \max(|2^u|, |3^v|, |5^w|)^{1-\delta} \tag{1.2}$$

has only finitely many solutions in non-negative integers u, v, w.

Write $x_1 = 2^u$, $x_2 = 3^v$, $x_3 = 5^w$, $\mathbf{x} = (x_1, x_2, x_3)$. We first show that the set of solutions $\mathbf{x}$ lies in a union of finitely many proper linear subspaces of $\mathbb{Q}^3$. Notice that

$$|x_1x_2x_3| \cdot |x_1x_2x_3|_2 \cdot |x_1x_2x_3|_3 \cdot |x_1x_2x_3|_5 = 2^u3^v5^w2^{-u}3^{-v}5^{-w} = 1$$

and $|x_1 + x_2 - x_3|_p \leqslant 1$ for $p = 2, 3, 5$. In combination with (1.2), this gives

$$|(x_1 + x_2 - x_3)x_1x_2x_3| \cdot \prod_{p=2,3,5} |(x_1 + x_2 - x_3)x_1x_2x_3|_p \leqslant \|\mathbf{x}\|^{1-\delta}.$$

The solutions of the latter inequality lie in a union of finitely many proper linear subspaces of $\mathbb{Q}^3$, since the linear forms $X_1, X_2, X_3, X_1 + X_2 - X_3$ are in general position. So the triples $(x_1, x_2, x_3) = (2^u, 3^v, 5^w)$ with (1.2) lie in finitely many proper linear subspaces of $\mathbb{Q}^3$.

Let T be one of these subspaces. There exist integers a_1, a_2, a_3, not all zero, such that $a_1x_1 + a_2x_2 + a_3x_3 = 0$ identically on T. So if some solution $(x_1, x_2, x_3) = (2^u, 3^v, 5^w)$ of (1.2) lies in T, then $a_12^u + a_23^v + a_35^w = 0$. As is known, equations of this type have only finitely many solutions u, v, w; hence (1.2) has only finitely many solutions in T. So (1.2) has altogether only finitely many solutions. □

Example. Roth's theorem states that given an irrational algebraic number $\alpha \in \mathbb{C}$ and $\delta > 0$, there are only finitely many pairs of integers x, y with $y > 0$ such that $|\alpha - x/y| \leqslant y^{-2-\delta}$. This can be improved if we impose some restrictions on x or y.

For instance, let p be a prime number and consider the inequality

$$\left|\alpha - \frac{x}{y}\right| \leqslant y^{-1-\delta} \tag{1.3}$$

in integers x, y such that $p \nmid x$ and $y = p^u$ for some positive integer u. We show that (1.3) has only finitely many solutions. Indeed, if (x, y) is such a solution of (1.3) then

$$|y(x - \alpha y)|_\infty |xy|_p \leqslant |x - \alpha y| \leqslant y^{-\delta} \leqslant C \max(|x|, |y|)^{-\delta}$$

for an appropriate constant C. By Theorem 1.1 with $r = 2$, the solutions (x, y) under consideration lie in finitely many one-dimensional subspaces of $\mathbb{Q}^2$. Since the conditions imposed on our solutions imply $\gcd(x, y) = 1$, $y > 0$, each one-dimensional subspace contains at most one solutions (x, y). Hence (1.3) has only finitely many solutions. □

2. Applications to Diophantine equations

Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a binary form of degree $n \geqslant 3$ and $p_1, \ldots, p_t$ distinct prime numbers. We consider the so-called *Thue-Mahler equation*

$$|F(x, y)| = p_1^{z_1} \cdots p_t^{z_t} \text{ in } x, y, z_1, \ldots, z_t \in \mathbb{Z} \text{ with } \gcd(x, y) = 1. \tag{2.1}$$

Notice that if we drop the condition $\gcd(x, y) = 1$ it is possible to construct infinitely many solutions from a given solution, simply by multiplying it with integers composed of primes from $p_1, \ldots, p_t$.

Theorem 2.1. (Mahler, 1933). *Assume that F is divisible by at least three linear forms which are pairwise linearly independent. Then Eq.* (2.1) *has only finitely many solutions.*

We use the following important fact.

Lemma 2.2. *Let $u \in \mathbb{Q}$, $S = \{\infty, p_1, \ldots, p_t\}$. Then $u = \pm p_1^{w_1} \cdots p_t^{w_t}$ for certain integers $w_1, \ldots, w_t$ if and only if $\prod_{p \in S} |u|_p = 1$.*

Proof. Trivial. □

The next lemma makes a reduction to the case that F is square-free.

Lemma 2.3. *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a binary form which is divisible by at least three distinct, pairwise distinct linear forms. Then $F(X, Y)$ is divisible in $\mathbb{Z}[X, Y]$ by a square-free binary form $G(X, Y)$ of degree $\geqslant 3$. The binary form G is a product of linear forms in general position.*

Proof. First assume that $F(X,Y)$ is not divisible by Y, i.e., $F(X,Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d$ with $a_0 \neq 0$. In $\mathbb{Z}[X]$ we can factor $f(X) := F(X,1)$ as $cf_1(X)^{k_1}\cdots f_s(X)^{k_s}$, where c is an integer, and $f_1,\ldots,f_s$ are distinct, irreducible polynomials in $\mathbb{Z}[X]$ and $k_1,\ldots,k_s$ are positive integers. Clearly, $f(X)$ is divisible in $\mathbb{Z}[X]$ by $g(X) := f_1(X)\cdots f_s(X)$, and $g(X) = b_0(X-\alpha_1)\cdots(X-\alpha_r)$, say, with $\alpha_1,\ldots,\alpha_r$ distinct and $r \geqslant 3$. Consequently, $F(X,Y) = Y^d f(X/Y)$ is divisible in $\mathbb{Z}[X,Y]$ by $G(X,Y) = Y^r g(X/Y) = b_0\prod_{i=1}^r(X-\alpha_iY)$ and G is square-free.

Second, suppose that $F(X,Y)$ is divisible by Y. Then for some $t > 0$ we have $a_0 = \cdots = a_{t-1} = 0$ and $a_t \neq 0$. Then $f(X) := F(X,1)$ is a polynomial of degree $d-t$. $f(X)$ must have at least two different roots, since $F(X,Y)$ is apart from Y, divisible by at least two other linear forms. Again, $f(X)$ is divisible in $\mathbb{Z}[X]$ by a polynomial $g(X)$ all whose roots are distinct, say, $g(X) = b_0(X-\alpha_1)\cdots(X-\alpha_{r-1})$ with $r \geqslant 3$. Now $F(X,Y) = Y^d f(X/Y)$ is divisible by $G(X,Y) = Y^r g(X/Y) = b_0Y\prod_{i=1}^{r-1}(X-\alpha_iY)$, and G is square-free.

Finally, we see that in both cases we can write $G(X,Y) = \prod_{i=1}^r L_i(X,Y)$, where the L_i are pairwise linearly independent linear forms, i.e., in general position. □

Proof of Theorem 2.1. Clearly, if (x,y) is a pair of integers with $\gcd(x,y) = 1$ satisfying (2.1) for certain integers $z_1,\ldots,z_t$, then also

$$|G(x,y)| = p_1^{w_1}\cdots p_t^{w_t} \tag{2.2}$$

for certain integers $w_1,\ldots,w_t$. So it suffices to prove that (2.2) has only finitely many solutions with $\gcd(x,y) = 1$. If $G(1,0) \neq 0$ then the form G can be factored as $a_0(X-\alpha_1Y)\cdots(X-\alpha_rY)$ with $\alpha_1,\ldots,\alpha_r$ distinct, while if $G(1,0) = 0$, G can be factored as $a_0Y(X-\alpha_1Y)\cdots(X-\alpha_{r-1}Y)$ with $\alpha_1,\ldots,\alpha_{r-1}$ distinct. In both cases, G is a product of r linear forms in two variables in general position.

Take δ with $0 < \delta < r-2$. Then by Lemma 2.2 we have for any solution $(x,y,w_1,\ldots,w_t)$ of (2.2),

$$\prod_{p\in S}|G(x,y)|_p = \prod_{p\in S}|L_1(x,y)\cdots L_r(x,y)|_p = 1 \leqslant \max(|x|,|y|)^{r-2-\delta}.$$

By Theorem 1.1, the set of solutions $(x,y) \in \mathbb{Z}^2$ of this inequality lies in a union of finitely many one-dimensional linear subspaces of $\mathbb{Q}^2$. Each such subspace

contains only two solutions with $\gcd(x, y) = 1$. This proves that (2.2) has only finitely many solutions. □

Remark. The above proof of the finiteness of the number of solutions of the Thue-Mahler equation is based on the p-adic Subspace Theorem and is therefore ineffective. There is however an alternative, effective proof of Theorem 2.1, based on lower bounds for linear forms in ordinary and p-adic logarithms.

In the previous sections, we considered equations $\alpha x + \beta y = 1$ in $x, y \in \Gamma$, where Γ is a finitely generated multiplicative group lying in some algebraic number field. We now consider equations of this type in more than two unknowns. Thus, let K be an algebraic number field, and Γ a finitely generated subgroup of the multiplicative group K^* of K. Further, let $n \geqslant 2$ and $\alpha_1, \ldots, \alpha_n \in K^*$. We consider the equation

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 1 \text{ in } x_1, \ldots, x_n \in \Gamma. \tag{2.3}$$

If $n \geqslant 3$ this equation may have infinitely many solutions. For instance, let $2 \leqslant m < n$ and suppose (2.3) has a solution $(x_1, \ldots, x_n)$ with

$$\alpha_1 x_1 + \cdots + \alpha_m x_m = 1, \quad \alpha_{m+1} x_{m+1} + \cdots + \alpha_n x_n = 0\,.$$

Then for every $u \in \Gamma$, the tuple $(x_1, \ldots, x_m, ux_{m+1}, \ldots, ux_n)$ is also a solution of (2.3). Assuming the group Γ is infinite, we obtain in this way infinitely many solutions of (2.3). More generally, we can construct infinitely many solutions from a given solution $(x_1, \ldots, x_n)$ with a *vanishing subsum* $\sum_{i \in I} \alpha_i x_i = 0$ for some non-empty subset I of $\{1, \ldots, n\}$.

To make such easy constructions of infinite sets of solutions impossible, we consider only solutions without vanishing subsums.

Definition. A solution $(x_1, \ldots, x_n)$ of (2.3) is called *non-degenerate* if

$$\sum_{i \in I} \alpha_i x_i \neq 0 \text{ for each non-empty subset } I \text{ of } \{1, \ldots, n\}.$$

Theorem 2.4. (Van der Poorten, Schlickewei, E., 1980's) *Equation* (2.3) *has only finitely many non-degenerate solutions.*

The main tool in the proof is the 'p-adic Subspace Theorem over number fields,' which is a generalization of the p-adic Subspace Theorem which involves absolute values on an algebraic number field and in which the unknowns are algebraic integers of that number field. This Subspace Theorem is ineffective,

and so the proof of Theorem 2.4 is ineffective. In contrast to the two-unknown case, for equations (2.3) in $n \geqslant 3$ unknowns, no effective finiteness proof is known.

Since in these notes we have only the p-adic Subspace Theorem over $\mathbb{Q}$ at our disposal, we assume henceforth

$$\Gamma \subset \mathbb{Q}^*, \ \alpha_1, \ldots, \alpha_n \in \mathbb{Q}^*$$

and prove Theorem 2.4 in this special case.

Lemma 2.5. *There are finitely many proper linear subspaces $T_1, \ldots, T_t$ of $\mathbb{Q}^n$ such that the set of solutions $(x_1, \ldots, x_n)$ of (2.3) (non-degenerate or not) lies in $T_1 \cup \cdots \cup T_t$.*

Proof. There are $\gamma_1, \ldots, \gamma_r \in \mathbb{Q}^*$ such that every element of Γ can be expressed as $\pm\gamma_1^{u_1} \cdots \gamma_r^{u_r}$ with $u_1, \ldots, u_r \in \mathbb{Z}$. Let $p_1, \ldots, p_t$ be the prime numbers occurring in the numerators and denominators of $\gamma_1, \ldots, \gamma_r$ and of $\alpha_1, \ldots, \alpha_n$. Take a solution $(x_1, \ldots, x_n)$ of (2.3) and write

$$\alpha_i x_i = \frac{y_i}{w} \ (i = 1, \ldots, n)$$

where $y_1, \ldots, y_n, w$ are integers with $\gcd(y_1, \ldots, y_n, w) = 1$. Further write $\mathbf{y} = (y_1, \ldots, y_n)$. Clearly, $y_1 + \cdots + y_n = w$ and $y_1, \ldots, y_n, w$ are composed of primes from $p_1, \ldots, p_t$. This implies

$$|y_1 \cdots y_n(y_1 + \cdots + y_n)| \cdot \prod_{j=1}^{t} |y_1 \cdots y_n(y_1 + \cdots + y_n)|_{p_j} = 1 \leqslant \|\mathbf{y}\|^{(n+1)-n-\delta} \tag{2.4}$$

where $0 < \delta < 1$. The linear forms $y_1, \ldots, y_n, \ y_1 + \cdots + y_n$ are in general position. So by the p-adic Subspace Theorem, the set of solutions $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}^n$ of (2.4) lies in a union of at most finitely many proper linear subspaces of $\mathbb{Q}^n$. If for instance $\mathbf{y}$ lies in a subspace with equation $a_1 y_1 + \cdots + a_n y_n = 0$ then $(x_1, \ldots, x_n)$ lies in $a_1\alpha_1 x_1 + \cdots + a_n\alpha_n x_n = 0$. This proves the lemma. □

Proof of Theorem 2.4. We proceed by induction on n, starting with $n = 1$. For $n = 1$ we have an equation $\alpha_1 x_1 = 1$ which has at most one solution. Let $n \geqslant 2$ and suppose Theorem 2.4 is true for equations in fewer than n variables. According to Lemma 2.5, the solutions of (2.3) lie in finitely many proper linear subspaces of $\mathbb{Q}^n$. So we have to prove that each of these subspaces contains only finitely many non-degenerate solutions of (2.3).

Let T be one of these subspaces. Then there are $a_1, \dots, a_n \in \mathbb{Q}$, not all zero, such that $a_1x_1 + \cdots + a_nx_n = 0$ holds identically on T. Assuming for instance that $a_n \neq 0$, we can express x_n as a linear equation of the other variables. By substituting this into (2.3), we see that all solutions in T of (2.3) satisfy also an equation

$$b_1x_1 + \cdots + b_{n-1}x_{n-1} = 1.$$

We can not directly apply the induction hypothesis to this equation, since there may be vanishing subsums. But for each solution $\mathbf{x}$ of (2.3) in T, we can take a *minimal* subset I of $\{1, \dots, n-1\}$ such that

$$\sum_{i \in I} b_i x_i = 1. \tag{2.5}$$

This means that $\mathbf{x}$ does not satisfy a relation as (2.5) for any set smaller than I, and thus, that (2.5) has no vanishing subsums. We call such solutions associated with I. We clearly have to show that for any set I, Eq. (2.3) has only finitely many non-degenerate solutions which belong to T and are associated with I.

Assume for convenience that $I = \{1, \dots, m\}$, where $m < n$. So if $(x_1, \dots, x_n)$ is a solution of (2.3) associated with I, then $(x_1, \dots, x_m)$ is a non-degenerate solution of $b_1x_1 + \cdots + b_mx_m = 1$. By the induction hypothesis, there is a finite set S, such that for all solutions of (2.3) associated with I we have $(x_1, \dots, x_m) \in S$. Take a tuple $(x_1, \dots, x_m) \in S$, and consider the set of non-degenerate solutions of (2.3) with these prescribed values for $x_1, \dots, x_m$. For these solutions we have that $c := 1 - \sum_{i=1}^{m} \alpha_i x_i \neq 0$,

$$c^{-1}(\alpha_{m+1}x_{m+1} + \cdots + \alpha_n x_n) = 1,$$

and moreover, no proper subsum of the left-hand side vanishes. Again by the induction hypothesis, for any given $(x_1, \dots, x_m)$, there are only finitely many possibilities for the tuple $(x_{m+1}, \dots, x_n)$. It follows that altogether, (2.3) has only finitely many non-degenerate solutions in the subspace T associated with I. Since we had only finitely many possibilities for T and I, this completes our induction step. □

3. Exercises

Exercise 1. Let p_1, p_2, p_3 be distinct prime numbers, A_1, A_2, A_3 non-zero integers, and $\delta > 0$. Prove that the inequality

$$|A_1 p_1^{u_1} + A_2 p_2^{u_2} + A_3 p_3^{u_3}| \leqslant \max(p_1^{u_1}, p_2^{u_2}, p_3^{u_3})^{1-\delta}$$

has only finitely many solutions in non-negative integers u_1, u_2, u_3.

Exercise 2. Let $\delta > 0$. Prove that the inequality

$$\left| \left(\frac{3}{2}\right)^n - u \right| \leqslant e^{-\delta n}$$

has only finitely many solutions in non-negative integers n, u.
Hint. Let $x_1 = 3^n$, $x_2 = u2^n$ and apply in an appropriate way Theorem 1.1.

Exercise 3. Let $f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ be a square-free polynomial, i.e., without multiple zeros, and let $p_1, \ldots, p_s$ be distinct prime numbers. We consider the equation

$$|f(\xi)| = p_1^{z_1} \cdots p_s^{z_s} \text{ in } \xi \in \mathbb{Q},\ z_1, \ldots, z_s \in \mathbb{Z}\,. \tag{3.1}$$

(a) Let $(\xi, z_1, \ldots, z_s)$ be a solution of (3.1). Prove that $|\xi|_p \leqslant 1$ for every prime p with $p \notin \{p_1, \ldots, p_s\}$, $p \nmid a_0$.
(b) Let $n \geqslant 2$. Prove that (3.1) has only finitely many solutions. What if $n = 1$?
Hint. Write $\xi = x/y$ with $x, y \in \mathbb{Z}$, $\gcd(x, y) = 1$ and reduce (3.1) to a Thue-Mahler equation.

Exercise 4. Let $S = \{p_1, \ldots, p_t\}$ be a finite set of prime numbers, and denote by U_S the set of integers of the shape $\pm p_1^{z_1} \cdots p_t^{z_t}$, where $z_1, \ldots, z_t$ are non-negative integers. Let α be an irrational algebraic number in $\mathbb{C}$ and $\delta > 0$.

(a) Prove that the inequality

$$\left| \alpha - \frac{x}{y} \right| \leqslant |y|^{-1-\delta}$$

has only finitely many solutions with $x \in \mathbb{Z}$, $y \in S$, $\gcd(x, y) = 1$.
(b) Prove that the inequality

$$\left| \alpha - \frac{x}{y} \right| \leqslant |y|^{-\delta}$$

has only finitely many solutions with $x \in S$, $y \in S$, $\gcd(x, y) = 1$.

Exercise 5. Let p be a prime number. Prove that the inequality

$$\left|\alpha - \frac{x}{y}\right| \leqslant \max(|x|, |y|)^{-1-\delta}$$

has only finitely many solutions in integers x, y such that y is of the shape $p^u - 1$ with u a positive integer.

Exercise 6. Let $\mathcal{S}_0, \ldots, \mathcal{S}_n$ be pairwise disjoint, finite sets of prime numbers, and $a_0, \ldots, a_n$ non-zero integers.

(a) Prove that the equation

$$a_0x_0 + \cdots + a_nx_n = 0 \text{ in } x_0 \in U_{\mathcal{S}_0}, \ldots, x_n \in U_{\mathcal{S}_n}$$

has only finitely many solutions.

(b) Prove that for every $\delta > 0$, the inequality

$$|a_0x_0 + \cdots + a_nx_n| \leqslant \max(|x_0|, \ldots, |x_n|)^{1-\delta} \text{ in } x_0 \in U_{\mathcal{S}_0}, \ldots, x_n \in U_{\mathcal{S}_n}$$

has only finitely many solutions.

Exercise 7. Prove that there are at most finitely many positive integers N such that N has at most 10 ones in its binary expansion, and at most 5 non-zero digits in its ternary expansion.

Exercise 8. Using Theorem 2.4, prove the following special case of the Skolem-Mahler-Lech theorem. Let $c_1, \ldots, c_t$ be non-zero algebraic numbers, and let $\alpha_1, \ldots, \alpha_t$ be non-zero algebraic numbers such that none of the quotients α_i/α_j $(1 \leqslant i < j \leqslant t)$ is a root of unity. Then the equation

$$c_1\alpha_1^n + \cdots + c_t\alpha_t^n = 0$$

has only finitely many solutions in integers n.

Remark. There is an alternative proof of the general Skolem-Mahler-Lech theorem based on the p-adic Subspace Theorem.