Chapter 9

The p-adic Subspace Theorem

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

9.1 Results

The p-adic Subspace Theorem deals with Diophantine inequalities in which several different absolute values occur (e.g., the ordinary absolute value and $|\cdot|_{p_1}, \dots, |\cdot|_{p_s}$ for distinct primes $p_1, \dots, p_s$). Recall that 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 $\mathbb{Q}$'.

We start with a generalization of Roth's Theorem.

Theorem 9.1. *Let $p_1, \dots, p_s$ be distinct prime numbers. Let α be an algebraic number in $\mathbb{R}$ and for $i = 1, \dots, s$, let α_{p_i} be a number in $\mathbb{Q}_p$ which is algebraic over $\mathbb{Q}$. Finally, let $\kappa > 2$. Then the inequality*

$$|\alpha - \xi| \cdot |\alpha_{p_1} - \xi|_{p_1} \cdots |\alpha_{p_s} - \xi|_{p_s} \leqslant H(\xi)^{-\kappa} \text{ in } \xi \in \mathbb{Q} \tag{9.1}$$

has only finitely many solutions.

Example. Consider

$$|\sqrt[3]{2} - \xi| \cdot |\sqrt[3]{3} - \xi|_2 \leqslant H(\xi)^{-\kappa} \text{ in } \xi \in \mathbb{Q}$$

where $\kappa > 2$. Here, $\sqrt[3]{3} = 3^{1/3} \in \mathbb{Q}_2$ is defined by Exercise 8.6.
Theorem 9.1 implies that there are only finitely many $\xi \in \mathbb{Q}$ such that ξ is very close to $\sqrt[3]{2}$ but 2-adically not too close to $\sqrt[3]{3}$ or conversely; and also if ξ is moderately close to $\sqrt[3]{2}$ and also 2-adically moderately close to $\sqrt[3]{3}$.

We now formulate the p-adic Subspace Theorem. This involves again absolute values $|\cdot|, |\cdot|_{p_1}, \dots, |\cdot|_{p_s}$ and for each of these absolute values, a system of n linearly independent linear forms in $X_1, \dots, X_n$.

Theorem 9.2. *Let $n \geqslant 2$, $\varepsilon > 0$, and let $p_1, \dots, p_s$ be distinct prime numbers. Further, let $L_{1\infty}, \dots, L_{n\infty}$ be linearly independent linear forms in $X_1, \dots, X_n$ with coefficients in $\mathbb{C}$ that are algebraic over $\mathbb{Q}$, and for $j = 1, \dots, s$, let $L_{1,p_j}, \dots, L_{n,p_j}$ be linearly independent linear forms in $X_1, \dots, X_n$ with coefficients in $\overline{\mathbb{Q}}_{p_j}$ that are algebraic over $\mathbb{Q}$. Consider the inequality*

$$|L_{1\infty}(\mathbf{x}) \cdots L_{n\infty}(\mathbf{x})| \cdot \prod_{j=1}^{s} |L_{1,p_j}(\mathbf{x}) \cdots L_{n,p_j}(\mathbf{x})|_{p_j} \leqslant \|\mathbf{x}\|^{-\varepsilon} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n \,. \tag{9.2}$$

Then there are a finite number of proper linear subspaces $T_1, \dots, T_t$ of $\mathbb{Q}^n$ such that all solutions of (9.2) lie in $T_1 \cup \cdots \cup T_t$.

Proof of Theorem 9.1. Let ξ be a solution of (9.1). Write $\xi = x/y$ with $x, y \in \mathbb{Z}$, $\gcd(x, y) = 1$. Multiply (9.1) with $A := \big(|y| \cdot |y|_{p_1} \cdots |y|_{p_s}\big)^2$. Notice that $|y|_{p_j} \leqslant 1$ for $j = 1, \dots, s$. Hence $A \leqslant y^2 \leqslant H(\xi)^2$. Let $\varepsilon = \kappa - 2$. Then (9.1) implies

$$|(x - \alpha y)y| \cdot \prod_{j=1}^{s} |(x - \alpha_{p_j} y)y|_{p_j} \leqslant \max(|x|, |y|)^{-\varepsilon}.$$

The solutions $(x, y) \in \mathbb{Z}^2$ of the latter lie in only finitely many proper one-dimensional linear subspaces of $\mathbb{Q}^2$, and each of these gives rise to a single fraction $\xi = x/y$. So (9.1) has only finitely many solutions. □

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

$$|2^u + 3^v - 5^w| \leqslant \max(|2^u|, |3^v|, |5^w|)^{1-\varepsilon} \tag{9.3}$$

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 the union of finitely many proper linear subspaces of $\mathbb{Q}^3$. Consider for the moment those solutions for which $\|\mathbf{x}\| = |x_3|$. Notice that

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

In combination with (9.3), this gives

$$|(x_1 + x_2 - x_3)x_1x_2| \cdot |x_1x_2x_3|_2 \cdot |x_1x_2x_3|_3 \cdot |x_1x_2x_3|_5 \leqslant |x_3|^{-1}\|\mathbf{x}\|^{1-\varepsilon} \leqslant \|\mathbf{x}\|^{-\varepsilon}.$$

The solutions of the latter inequality lie in the union of finitely many proper linear subspaces of $\mathbb{Q}^3$. So the solutions of (9.3) with $\|\mathbf{x}\| = |x_3|$ lie in finitely many proper linear subspaces of $\mathbb{Q}^3$. In a similar way one proves that the solutions with $\|\mathbf{x}\| = |x_1|$ or with $\|\mathbf{x}\| = |x_2|$ lie in finitely many proper linear subspaces of $\mathbb{Q}^3$.

It is left as an exercise to prove that if T is a two-dimensional linear subspace of $\mathbb{Q}^3$ then T contains only finitely many solutions of (9.3). $\square$

Similarly as for the basic Subspace Theorem discussed in Chapter 7, there is a version with linear forms in general position.

Theorem 9.3. *Let $\varepsilon > 0$, and let $p_1, \dots, p_s$ be distinct prime numbers. Further, let $L_{1\infty}, \dots, L_{r\infty}$ ($r \geqslant n$) be linear forms in $X_1, \dots, X_n$ in general position with coefficients in $\mathbb{C}$ that are algebraic over $\mathbb{Q}$, and for $j = 1, \dots, s$, let $L_{1,p_j}, \dots, L_{r_j,p_j}$ ($r_j \geqslant n$) be linear forms in $X_1, \dots, X_n$ in general position with coefficients in $\overline{\mathbb{Q}}_{p_j}$ that are algebraic over $\mathbb{Q}$. Consider the inequality*

$$(9.4)\qquad |L_{1\infty}(\mathbf{x}) \cdots L_{r\infty}(\mathbf{x})| \cdot \prod_{j=1}^{s} |L_{1,p_j}(\mathbf{x}) \cdots L_{r_j,p_j}(\mathbf{x})|_{p_j} \leqslant \|\mathbf{x}\|^{r-n-\varepsilon}$$
$$\text{in } \mathbf{x} \in \mathbb{Z}^n \text{ with } \gcd(x_1, \dots, x_n) = 1.$$

Then there are a finite number of proper linear subspaces $T_1, \dots, T_t$ of $\mathbb{Q}^n$ such that all solutions of (9.4) lie in $T_1 \cup \cdots \cup T_t$.

Proof. We partition the solutions $\mathbf{x} \in \mathbb{Z}^n$ of (9.4) in classes depending on which n quantities among $|L_{1\infty}(\mathbf{x})|, \dots, |L_{r\infty}(\mathbf{x})|$ are the smallest, and likewise, for $j = 1, \dots, s$, which n quantities among $|L_{1,p_j}(\mathbf{x})|_{p_j}, \dots, |L_{r_j,p_j}(\mathbf{x})|_{p_j}$ are the smallest. It suffices to show that the solutions in a given class lie in finitely many proper linear subspaces of $\mathbb{Q}^n$.

Consider for instance the solutions $\mathbf{x} \in \mathbb{Z}^n$ such that $|L_{1\infty}(\mathbf{x})|, \dots, |L_{n\infty}(\mathbf{x})|$ are the smallest among $|L_{1\infty}(\mathbf{x})|, \dots, |L_{r\infty}(\mathbf{x})|$ and $|L_{1,p_j}(\mathbf{x})|_{p_j}, \dots, |L_{n,p_j}(\mathbf{x})|_{p_j}$ are the smallest among $|L_{1,p_j}(\mathbf{x})|_{p_j}, \dots, |L_{r_j,p_j}(\mathbf{x})|_{p_j}$ for $j = 1, \dots, s$.

Let $i \geqslant n+1$. According to Lemma 7.4, there is a constant C_i such that for the solutions under consideration,

$$\|\mathbf{x}\| \leqslant C_i |L_{i\infty}(\mathbf{x})|\,.$$

Let $j \in \{1, \dots, s\}$. Since we consider only solutions whose coordinates have gcd 1, for each solution $\mathbf{x} = (x_1, \dots, x_n)$ under consideration, there is an index k with $|x_k|_{p_j} = 1$. Since $L_{1,p_1}, \dots, L_{n-1,p_j}, L_{i,p_j}$ span the vector space of all linear forms in $\overline{\mathbb{Q}}_{p_j}$, we have

$$X_k = \alpha_1 L_{1,p_j} + \cdots + \alpha_{n-1} L_{n-1,p_j} + \alpha_n L_{i,p_j}$$

for certain constants $\alpha_1, \dots, \alpha_n$. So by the ultrametric inequality,

$$1 = |x_k|_{p_j} \leqslant \max_l |\alpha_l|_{p_j} |L_{l,p_j}(\mathbf{x})|_{p_j} \leqslant C_{i,p_j} |L_{i,p_j}(\mathbf{x})|_{p_j}$$

for some constant C_{i,p_j}. By combining these inequalities with (9.4), we obtain

$$|L_{1\infty}(\mathbf{x}) \cdots L_{n\infty}(\mathbf{x})| \cdot \prod_{j=1}^{s} |L_{1,p_j}(\mathbf{x}) \cdots L_{n,p_j}(\mathbf{x})|_{p_j} \leqslant C \|\mathbf{x}\|^{-\varepsilon}$$

for some constant $C > 0$. Now apply Theorem 9.2 to the latter. □

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

(9.5) $\qquad |F(x,y)| = p_1^{z_1} \cdots p_s^{z_s}$ in $x, y, z_1, \dots, z_s \in \mathbb{Z}$ with $\gcd(x,y) = 1$.

Notice that if we drop the condition $\gcd(x,y) = 1$ it is possible to construct infinitely many solutions from a given solution. We prove the following.

Theorem 9.4. (Mahler, 1933). *Equation* (9.5) *has only finitely many solutions.*

We use the following important fact.

Lemma 9.5. *Let $u \in \mathbb{Q}$. Then $u = \pm p_1^{w_1} \cdots p_s^{w_s}$ for certain integers $w_1, \dots, w_s$ if and only if $|u| \cdot |u|_{p_1} \cdots |u|_{p_s} = 1$.*

Proof. Trivial. □

Proof of Theorem 9.4. If $F(1,0) \neq 0$ then the form F can be factored as $a_0(X - \alpha_1 Y) \cdots (X - \alpha_n Y)$ with $\alpha_1, \ldots, \alpha_n$ distinct, while if $F(1,0) = 0$, F can be factored as $a_0 Y(X - \alpha_1 Y) \cdots (X - \alpha_{n-1} Y)$ with $\alpha_1, \ldots, \alpha_{n-1}$ distinct. In both cases, F is a product of n linear forms in two variables in general position.

Take ε with $0 < \varepsilon < n - 2$. Then by Lemma 9.5 we have for any solution $(x, y, z_1, \ldots, z_s)$ of (9.5),

$$|F(x,y)| \cdot \prod_{j=1}^{s} |F(x,y)|_{p_j} = 1 \leqslant \max(|x|, |y|)^{n-2-\varepsilon}.$$

By Theorem 9.3, the set of solutions $(x, y) \in \mathbb{Z}^2$ of this inequality lies in the 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 (9.5) 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 9.4. There are effective lower bounds for the p-adic absolute value of linear forms in p-adic logarithms of algebraic numbers, similar to those mentioned in Chapter 5. Then one can prove Theorem 9.4, with an effective upper bound for $\max(|x|, |y|)$, by combining estimates for linear forms in 'ordinary logarithms' with estimates for linear forms in p_j-adic logarithms for $j = 1, \ldots, s$.

Recall that in Chapter 5, we considered the unit equation $ax + by = 1$ where the unknowns x, y are taken from the unit group O_K^* of the ring of integers O_K of an algebraic number field K. It was proved that this equation has only finitely many solutions. By Dirichlet's Unit Theorem, the group O_K^* is finitely generated, and we have

$$O_K^* \cong W \times \mathbb{Z}^r$$

where W is the group of roots of unity in K (which is finite), and where r is the unit rank. Recall that $r = r_1 + r_2 - 1$ where r_1 is the number of embeddings $K \to \mathbb{R}$ and r_2 the number of complex conjugate pairs of embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$, where $\overline{\sigma}$ is the composition of σ and complex conjugation.

We consider a much more general situation where x, y are taken from an arbitrary finitely generated multiplicative group in an arbitrary field of characteristic 0. For such a finitely generated group Γ we have $\Gamma \cong \Gamma_{\rm tors} \times \mathbb{Z}^r$ where $\Gamma_{\rm tors}$ is the (necessarily finite) torsion subgroup of Γ, consisting of roots of unity. Thus,

$$\Gamma = \{\zeta g_1^{m_1} \cdots g_r^{m_r} : m_1, \ldots, m_r \in \mathbb{Z}\} \tag{9.6}$$

for certain generators $g_1, \ldots, g_r$.

Theorem 9.6. (Lang, 1960). *Let K be any field of characteristic 0, let a, b be non-zero elements from K, and let Γ be a finitely generated subgroup of the multiplicative group K^* of K. Then the equation*

$$ax + by = 1 \quad \textit{in } x, y \in \Gamma \tag{9.7}$$

has only finitely many solutions.

Lang's proof is ineffective.

From Theorem 5.17, that we proved in Chapter 5, one can derive an effective proof of the above theorem in the special case that Γ is a subgroup of $\mathbb{Q}^*$ and that a, b are non-zero elements of $\mathbb{Q}^*$. We now give another, but ineffective proof of this result. Let $g_1, \ldots, g_r$ be a set of generators of Γ as in (9.6). Let $p_1, \ldots, p_s$ be primes such that the numerators and denominators of $a, b, g_1, \ldots, g_r$ are composed of primes from $p_1, \ldots, p_s$. Write $ax = u/w$, $by = v/w$, where u, v, w are integers, necessarily composed of primes from $p_1, \ldots, p_s$, with $\gcd(u, v, w) = 1$ and $u + v = w$. Now clearly, we have

$$|uv(u + v)| = p_1^{z_1} \cdots p_s^{z_s}, \ \gcd(u, v) = 1$$

for certain non-negative integers $z_1, \ldots, z_s$. This is a Thue-Mahler equation. Therefore there are only finitely many possibilities for the pair (u, v), hence for (u, v, w), hence for (x, y). □

Remark. In case that the group Γ is contained in an algebraic number field K, it is possible to give an effective proof of Theorem 9.6, see Theorem 5.18. If the degree of K and the number of generators of Γ are not too large, there is a practical algorithm to determine all solutions.

Example. Let Γ be the multiplicative group generated by $2, 3, 5, 7, 11, 13$ and consider the equation

$$x + y = 1 \ \text{ in } x, y \in \Gamma \text{ with } x \leqslant y. \tag{9.8}$$

We give some solutions:

$$\Big(\frac{1}{2},\frac{1}{2}\Big),\ \Big(\frac{3}{7},\frac{4}{7}\Big),\ \Big(\frac{2}{13},\frac{11}{13}\Big),\ \Big(\frac{3993}{20800},\frac{16807}{20800}\Big)=\Big(\frac{3\cdot 11^3}{2^6\cdot 5^2\cdot 13},\frac{7^5}{2^6\cdot 5^2\cdot 13}\Big).$$

In his thesis of 1988, de Weger determined all 545 solutions of (9.8).

9.2 Further applications

Let K be a field of characteristic 0 and Γ a finitely generated subgroup of K^*. Further, let $n \geqslant 2$ and $\alpha_1,\dots,\alpha_n \in K^*$. We consider the equation

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 1 \text{ in } x_1,\dots,x_n \in \Gamma. \tag{9.9}$$

If $n \geqslant 3$ this equation may have infinitely many solutions. For instance, let $2 \leqslant m < n$ and suppose (9.9) has a solution $(x_1,\dots,x_n)$ 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 $(x_1,\dots,x_m,ux_{m+1},\dots,ux_n)$ is also a solution of (9.9). Assuming the group Γ is infinite, we obtain in this way infinitely many solutions of (9.9). More generally, we can construct infinitely many solutions from a given solution $(x_1,\dots,x_n)$ with a *vanishing subsum* $\sum_{i\in I}\alpha_i x_i = 0$ for some non-empty subset I of $\{1,\dots,n\}$.

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

Definition. A solution $(x_1,\dots,x_n)$ of (9.9) is called *non-degenerate* if

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

Theorem 9.7. (Van der Poorten, Schlickewei, Laurent, E., 1980's) *Equation* (9.9) *has only finitely many non-degenerate solutions.*

Roughly speaking, the proof consists of two steps. In the first step one makes a reduction from the general case that K is a field of characteristic 0 to the special case that K is an algebraic number field by using techniques from algebraic geometry.

To treat the case that Γ is contained in an algebraic number field one has to apply 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.

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

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

and prove Theorem 9.9 in this special case. It will be convenient to consider instead of (9.9) the homogeneous equation

$$\alpha_0 x_0 + \cdots + \alpha_n x_n = 0 \ \text{ in } x_0, \dots, x_n \in \Gamma, \tag{9.10}$$

where $\alpha_0, \dots, \alpha_n$ are non-zero rational numbers. Solutions $(x_0, \dots, x_n)$ of (9.10) will be called non-degenerate if $\sum_{i \in I} \alpha_i x_i \neq 0$ for each proper, non-empty subset I of $\{0, \dots, n\}$. We prove the following.

Theorem 9.8. *There is a finite set U such that $x_i/x_j \in U$ for each non-degenerate solution $(x_0, \dots, x_n)$ of (9.10) and each pair of indices $i, j \in \{0, \dots, n\}$.*

By taking $\alpha_0 = -1$ and considering solutions of (9.10) with $x_0 = 1$ we obtain Theorem 9.7 in the case $\Gamma \subset \mathbb{Q}^*$.

Let H be the linear subspace of $\mathbb{Q}^{n+1}$ given by $\alpha_0 x_0 + \cdots + \alpha_n x_n = 0$.

Lemma 9.9. *There are finitely many proper linear subspaces $T_1, \dots, T_t$ of H such that the set of solutions $(x_0, \dots, x_n)$ of (9.9) (non-degenerate or not) lies in $T_1 \cup \cdots \cup T_t$.*

Proof. We use the 'general position version' of the p-adic Subspace Theorem. We start with some preparations.

There are $g_1, \dots, g_r$ of $\mathbb{Q}^*$ such that every element of Γ can be expressed as $\pm g_1^{u_1} \cdots g_r^{u_r}$ with $u_1, \dots, u_r \in \mathbb{Z}$. Let $p_1, \dots, p_s$ be the prime numbers occurring in the numerators and denominators of $\alpha_1, \dots, \alpha_n, g_1, \dots, g_r$. Let φ be the bijective linear map from H to $\mathbb{Q}^n$ given by $(x_0, \dots, x_n) \mapsto (\alpha_1 x_1, \dots, \alpha_n x_n)$.

Take a solution $\mathbf{x} = (x_0, \dots, x_n)$ of (9.10). Let w be a positive rational number such that

$$y_i := w\alpha_i x_i \in \mathbb{Z} \text{ for } i = 1, \dots, n, \ \ \gcd(y_1, \dots, y_n) = 1$$

and put $\mathbf{y} = (y_1, \dots, y_n)$. Thus, $\mathbf{y} = \varphi(w\mathbf{x})$. Further, $y_1 + \cdots + y_n = -w\alpha_0 x_0$. Clearly, $y_1, \dots, y_n$ and $y_1 + \cdots + y_n$ are composed of primes from $p_1, \dots, p_s$. This implies that for any ε with $0 < \varepsilon < 1$,

$$|y_1 \cdots y_n(y_1 + \cdots + y_n)| \cdot \prod_{j=1}^{s} |y_1 \cdots y_n(y_1 + \cdots + y_n)|_{p_j} = 1 \leqslant \|\mathbf{y}\|^{(n+1)-n-\varepsilon}. \tag{9.11}$$

The linear forms $y_1, \dots, y_n$, $y_1 + \cdots + y_n$ are in general position. So by the 'general position-version' of the p-adic Subspace Theorem, the set of solutions $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{Z}^n$ of (9.11) with $\gcd(y_1, \dots, y_n) = 1$ lies in a union $S_1 \cup \cdots \cup S_t$ of proper linear subspaces of $\mathbb{Q}^n$. Hence the corresponding solutions $\mathbf{x} = (x_0, \dots, x_n)$ of (9.10) lie in $T_1 \cup \cdots \cup T_t$, where $T_i := \varphi^{-1}(S_i)$ is a proper linear subspace of H, for $i = 1, \dots, t$. This proves the lemma. □

Lemma 9.10. *There is a finite set $U' \in \mathbb{Q}^*$ such that for every solution $(x_1, \dots, x_n)$ of* (9.10) *(non-degenerate or not) there are distinct $i, j \in \{0, \dots, n\}$ with $x_i/x_j \in U$.*

Proof. We proceed by induction on n. If $n = 1$ we have an equation $\alpha_0 x_0 + \alpha_1 x_1 = 0$ and the lemma is obvious.

Now let $n \geqslant 2$ and assume that the lemma is true for equations of type (9.10) in fewer than $n + 1$ unknowns. By the previous lemma, there are proper linear subspaces $T_1, \dots, T_t$ of H such that the solutions of (9.10) lie in $T_1 \cup \cdots \cup T_t$. Consider the solutions in $T \in \{T_1, \dots, T_t\}$. The points $\mathbf{x} = (x_0, \dots, x_n) \in T$ satisfy, apart from the defining equation $\alpha_0 x_0 + \cdots + \alpha_n x_n = 0$ for H, another equation that is linearly independent of it, say $\gamma_0 x_0 + \cdots + \gamma_n x_n = 0$. If for instance $\gamma_n \neq 0$ then by subtracting γ_n/α_n times the first equation from the second, we get another equation

$$\beta_0 x_0 + \cdots + \beta_{n-1} x_{n-1} = 0 \tag{9.12}$$

valid for all $\mathbf{x} \in T$, where at least one of $\beta_0, \dots, \beta_{n-1}$ is non-zero.

By the induction hypothesis, applied to (9.12) with the terms with $\beta_i = 0$ removed, there is a finite set U_T such that for every solution $(x_0, \dots, x_n)$ of (9.10) lying in T there are distinct indices $i, j \in \{0, \dots, n-1\}$ such that $x_i/x_j \in U_T$.

Now the lemma holds with $U' = U_{T_1} \cup \cdots \cup U_{T_t}$. □

Proof of Theorem 9.8. We proceed again by induction on n. For $n = 1$ Theorem 9.8 is trivial. Let $n \geqslant 2$ and suppose Theorem 9.8 is true for equations in fewer than $n + 1$ unknowns.

Suppose the set U' from the previous lemma is $\{\beta_1, \ldots, \beta_m\}$. Then the non-degenerate solutions $(x_1, \ldots, x_n)$ of (9.10) can be divided into finitely many sets S_{pqr} $(p, q = 0, \ldots, n,\ p \neq q,\ r = 1, \ldots, m)$, where S_{pqr} is the set of solutions with $x_p/x_q = \beta_r$.

Consider for instance the non-degenerate solutions in $S_{n,n-1,1}$, i.e., with $x_n = \beta_1 x_{n-1}$. These solutions satisfy

$$\alpha_0 x_0 + \cdots + (\alpha_{n-1} + \beta_1 \alpha_n) x_{n-1} = 0.$$

Each non-empty subsum of the left-hand side is non-zero, since $(x_0, \ldots, x_n)$ is non-degenerate. By the induction hypothesis, there is a finite set $U_{n,n-1,1}$ such that $x_i/x_j \in U_{n,n-1,1}$ for all solutions $(x_0, \ldots, x_n)$ of (9.10) in $S_{n,n-1,1}$ and all $i, j \in \{0, \ldots, n-1\}$. Using $x_n/x_{n-1} = \beta_1$ we can enlarge $U_{n,n-1,1}$ such that it contains all quotients x_i/x_j with $i = n$ or $j = n$ as well. We get a similar set U_{pqr} for each other triple of indices p, q, r. Now Theorem 9.8 is satisfied with U equal to the union of the sets U_{pqr} with $p, q = 0, \ldots, n$, $p \neq q$ and $r = 1, \ldots, m$. □

We now deal with linear recurrence sequences.

A sequence $U = \{u_h\}_{h=0}^{\infty}$ with terms in $\mathbb{C}$ is called a linear recurrence sequence if it is given by a linear recurrence

$$u_h = c_1 u_{h-1} + \cdots + c_k u_{h-k} \text{ for } h \geqslant k, \tag{9.13}$$

where $c_1, \ldots, c_k$ are constants in $\mathbb{C}$ and $c_k \neq 0$, and by initial values $u_0, \ldots, u_{k-1}$.

Given a linear recurrence sequence U, there are various linear recurrences which it may satisfy but there is a unique one with minimal length k (exercise). This k is called the *order* of the linear recurrence sequence U, and the polynomial

$$f_U(X) = X^k - c_1 X^{k-1} - \cdots - c_k$$

the *companion polynomial* of U.

Theorem 9.11. *Let $U = \{u_h\}_{h=0}^{\infty}$ be a linear recurrence sequence in $\mathbb{C}$ with companion polynomial $f_U(X) = X^k - c_1 X^{k-1} - \cdots - c_k$. Write*

$$f_U(X) = (X - \theta_1)^{e_1} \cdots (X - \theta_m)^{e_m},$$

where $\theta_1, \dots, \theta_m$ are distinct complex numbers and $e_1, \dots, e_m$ positive integers. Then there are polynomials $g_1, \dots, g_m \in \mathbb{C}[X]$ of degrees at most $e_1 - 1, \dots, e_m - 1$, respectively, such that

$$u_h = g_1(h)\theta_1^h + \cdots + g_m(h)\theta_m^h \quad \text{for } h \geqslant 0. \tag{9.14}$$

Conversely, any sequence satisfying (9.14) *is a linear recurrence sequence.*

Proof. Consider the power series

$$y(z) = \sum_{h=0}^{\infty} \frac{u_h}{h!} z^h.$$

One proves easily by induction on h that there is a constant $C > 0$ such that $|u_h| \leqslant C^h$ for all $h \geqslant 0$. Hence $y(z)$ converges, and thus defines an analytic function, everywhere on $\mathbb{C}$. Using that the sequence U satisfies recurrence relation (9.13), it follows easily that y satisfies the linear differential equation

$$y^{(k)} = c_1 y^{(k-1)} + \cdots + c_{k-1} y' + c_k y\,.$$

By the theory of linear differential equations, the set of solutions of the latter equation is a complex vector space with basis $\{z^j e^{\theta_i z} : i = 1, \dots, m,\ j = 0, \dots, e_i - 1\}$. Hence there are $c_{ij} \in \mathbb{C}$ such that

$$\begin{aligned} y(z) &= \sum_{i=1}^{m} \sum_{j=0}^{e_i-1} c_{ij} z^j e^{\theta_i z} = \sum_{i=1}^{m} \sum_{j=0}^{e_i-1} c_{ij} \sum_{l=0}^{\infty} \theta_i^l \frac{z^{l+j}}{l!} \\ &= \sum_{h=0}^{\infty} \left(\sum_{i=1}^{m} \left\{ \sum_{j=0}^{e_i-1} c_{ij} h(h-1)\cdots(h-j+1)\theta_i^{-j} \right\} \theta_i^h \right) \frac{z^h}{h!}. \end{aligned}$$

This implies that $\{u_h\}_{h=0}^{\infty}$ satisfies (9.14). Conversely, if $\{u_h\}_{h=0}^{\infty}$ satisfies (9.14) then by reversing the above argument one shows that $y(z) = \sum_{h=0}^{\infty} (u_h/h!) z^h$ satisfies a linear differential equation with constant coefficients, and subsequently that $\{u_h\}_{h=0}^{\infty}$ is a linear recurrence sequence. □

Example. Let $U = \{u_h\}_{h=0}^{\infty}$ be given by

$$u_h = 10u_{h-1} - 31u_{h-2} + 30u_{h-3} \ (h \geqslant 3), \quad u_0 = 1, u_1 = 0, u_2 = -12.$$

The companion polynomial of U is given by

$$f_U(X) = X^3 - 10X^2 + 31X - 30 = (X-2)(X-3)(X-5).$$

By Theorem 9.11 there are constants c_1, c_2, c_3 such that $u_h = c_1 2^h + c_2 3^h + c_3 5^h$. Substituting $h = 0, 1, 2$ one obtains $c_1 = 1, c_2 = 0, c_2 = -12$ and

$$u_h = 2^h + 3^h - 5^h.$$

The *zero set* of a linear recurrence sequence $U = \{u_h\}_{h=0}^{\infty}$ is defined by

$$Z_U := \{h \in \mathbb{Z}_{\geqslant 0} : \, u_h = 0\}$$

and the zero multiplicity of U is $N_U := \#Z_U$. With the notation from Theorem 9.11, the set Z_U is the set of solutions of

$$g_1(h)\theta_1^h + \cdots + g_m(h)\theta_m^h = 0 \text{ in } h \in \mathbb{Z}_{\geqslant 0}. \tag{9.15}$$

This is called an *exponential-polynomial equation*.

A linear recurrence sequence $U = \{u_h\}_{h=0}^{\infty}$ is called *non-degenerate* if the zeros of its companion polynomial $\theta_1, \ldots, \theta_m$ are such that none of the quotients θ_i/θ_j $(1 \leqslant i < j \leqslant m)$ is a root of unity.

Theorem 9.12. (Skolem-Mahler-Lech, 1953) *Let U be a non-degenerate linear recurrence sequence. Then its zero set is finite.*
Stated equivalently, if $\theta_1, \ldots, \theta_m$ are non-zero complex numbers such that none of the quotients θ_i/θ_j $(1 \leqslant i, j \leqslant m,\, i \neq j)$ is a root of unity and if $g_1(X), \ldots, g_m(X)$ are polynomials in $\mathbb{C}[X]$, not all equal to 0*, then Eq.* (9.15) *has only finitely many solutions.*

There are two very different proofs.

In the first proof, which was the one given by Skolem, Mahler and Lech, one 'maps' the linear recurrence sequence to a sequence with terms in $\mathbb{Q}_p$ for a suitable prime p and then uses techniques from p-adic analysis.

In the second proof, one 'maps' the linear recurrence sequence to a sequence with terms in an algebraic number field, and then applies the p-adic Subspace Theorem over number fields.

Here we prove Theorem 9.12 in the special case that the companion polynomial f_U of $U = \{u_h\}_{h=0}^{\infty}$ does not have multiple zeros, i.e., in Theorem 9.11 we have $e_1 = \cdots = e_m = 1$. Then the polynomials $g_i(h)$ in (9.14) have degree 0, so $u_h = \sum_{i=1}^m g_i \theta_i^h$ for $h \geqslant 0$ where the g_i are constants. That is, we have to show that the equation

$$g_1\theta_1^h + \cdots + g_m\theta_m^h = 0$$

has finitely many solutions in $h \in \mathbb{Z}_{\geqslant 0}$.

We proceed by induction on m. For $m = 1$ there are no solutions and we are done. Let $m \geqslant 2$ and suppose the theorem is true if we have fewer than m terms.

Let $a_i := -g_i/g_m$, $\beta_i := \theta_i/\theta_m$. Then the equation reduces to

$$a_1\beta_1^h + \cdots + a_{m-1}\beta_{m-1}^h = 1. \tag{9.16}$$

Further, none of the numbers β_i, nor any of the quotients β_i/β_j $(i \neq j)$ is a root of unity.

We apply Theorem 9.7 with the group Γ generated by $\beta_1, \ldots, \beta_{m-1}$. It follows that there are only finitely many integers h which satisfy (9.16) and for which none of the subsums of the left-hand side of (9.16) vanishes, i.e.,

$$\sum_{i \in I} a_i\beta_i^h \neq 0 \text{ for each non-empty subset } I \text{ of } \{1, \ldots, m\}.$$

But by the induction hypothesis, each equation $\sum_{i\in I} a_i\beta_i^h = 0$ has only finitely many solutions h. So altogether, (9.16) has only finitely many solutions h. □

Remark. Using a much refined version of the p-adic Subspace over number fields, Schmidt proved the following:

Theorem 9.13. (Schmidt, 2000) *Let U be a non-degenerate linear recurrence sequence with terms in $\mathbb{C}$ of order k. Then for its zero multipicity we have*

$$N_U \leqslant \exp\exp\exp 20k.$$

This has been improved by Amoroso and Viada (2011) to $N_U \leqslant \exp\exp 70k$.

Bavencoffe and Bézivin (Une Famille Remarquable de Suites Récurrentes Linéaires, Monatshefte für Mathematik 120 (1995), 189–203) found examples of non-degenerate linear recurrence sequences U of arbitrarily large order k, having $N_U \geqslant \frac{1}{2}k^2 - \frac{1}{2}k + 1$;

no linear recurrence sequences of order k with larger zero multiplicity are known. In fact, let

$$P_k(X) := \frac{X^{k+1} + (-2)^{k-1}X + (-2)^k}{X+2};$$

verify that $P_k(X) \in \mathbb{Z}[X]$. Let $U = \{u_n\}_{n=0}^{\infty}$ be the linear recurrence sequence with companion polynomial P_k and initial values $u_0 = \cdots = u_{k-2} = 0$, $u_{k-1} = 1$. Bavencoffe and Bézivin proved that U is non-degenerate, and moreover, that $u_n = 0$ for

$$n = l(k+1) + q \text{ with } l \geqslant 0,\ q \geqslant 0,\ l + q \leqslant k - 2,$$
$$n = j(2k+1) \text{ with } 1 \leqslant j \leqslant k - 1.$$

9.3 Exercises

Exercise 9.1. *Let p_1, p_2, p_3 be distinct prime numbers, A_1, A_2, A_3 non-zero integers, and $\varepsilon > 0$. Prove that the inequality*

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

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

Exercise 9.2. *let p be a prime number, α a real, irrational algebraic number and $\varepsilon > 0$.*

(a) Prove that the inequality

$$\left|\alpha - \frac{x}{p^u}\right| \leqslant \max(|x|, p^u)^{-1-\varepsilon}$$

has only finitely many solutions in integers x, u with $u > 0$.

(b) Prove that the inequality

$$\left|\alpha - \frac{x}{p^u - 1}\right| \leqslant \max(|x|, p^u)^{-1-\varepsilon}$$

has only finitely many solutions in integers x, u with $u > 0$.

Exercise 9.3. *Let $\varepsilon > 0$. Prove that the inequality*

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

has only finitely many solutions in non-negative integers n, u.
Hint. *Let $x = 3^n$, $y = u2^n$ and apply in an appropriate way the p-adic Subspace Theorem.*

Exercise 9.4. *Let $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ 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*

$$|f(\xi)| = p_1^{z_1} \cdots p_s^{z_s} \text{ in } \xi \in \mathbb{Q},\ z_1, \ldots, z_s \in \mathbb{Z}\,. \tag{9.17}$$

(a) Let $(\xi, z_1, \ldots, z_s)$ be a solution of (9.17). 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 (9.17) 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 (9.17) to a Thue-Mahler equation.*

Exercise 9.5. *Let p be a prime number, $\alpha \in \mathbb{Z}_p$, $\alpha \notin \mathbb{Q}$.*

(a) Prove that for every positive integer m there are integers x, y, not both 0, such that

$$|x - \alpha y|_p \leqslant p^{-2m}, \quad |x| \leqslant p^m,\ |y| \leqslant p^m.$$

Hint. *Choose a positive integer a such that $|\alpha - a|_p \leqslant p^{-2m}$ and show that if x, y is a solution then $x - ay = p^{2m}u$ for some $u \in \mathbb{Z}$.*

(b) Prove that the inequality

$$|x - \alpha y|_p \leqslant \max(|x|, |y|)^{-2}$$

has infinitely many solutions in $(x, y) \in \mathbb{Z}^2$.

(c) Suppose that α is algebraic and let $\varepsilon > 0$. Prove that the inequality

$$|x - \alpha y|_p \leqslant \max(|x|, |y|)^{-2-\varepsilon}$$

has only finitely many solutions in $(x, y) \in \mathbb{Z}^2$.

Exercise 9.6. *For a finite set of primes $\mathcal{S} = \{p_1, \ldots, p_s\}$, denote by $U_{\mathcal{S}}$ the set of integers of the shape $\pm p_1^{u_1} \cdots p_s^{u_s} : u_1, \ldots, u_s \in \mathbb{Z}_{\geqslant 0}$.*
Let $\mathcal{S}_0, \ldots, \mathcal{S}_n$ be pairwise disjoint sets of prime numbers, and $a_0, \ldots, a_n$ non-zero integers. Prove that the equation

$$a_0 x_0 + \cdots + a_n x_n = 0 \text{ in } x_0 \in U_{\mathcal{S}_0}, \ldots, x_n \in U_{\mathcal{S}_n}$$

has only finitely many solutions.

Exercise 9.7. *Let $U = \{u_h\}_{h=0}^{\infty}$ be a linear recurrence sequence with terms in $\mathbb{C}$.*

(c) Prove that the following two assertions are equivalent:
(i) $u_h = c_1 u_{h-1} + \cdots + c_k u_{h-k}$ for all $h \geqslant k$;
(ii) $\sum_{h=0}^{\infty} u_h X^h = g(X)/h(X)$, where $h(X) = 1 - c_1 X - \cdots - c_k X^k$ and $g(X)$ is a polynomial of degree at most $k-1$.

(b) Let I_U be the set of all polynomials $d_0 X^m + \cdots + d_m \in \mathbb{C}[X]$ ($m \geqslant 0$, $d_0, \ldots, d_m \in \mathbb{C}$) such that $d_0 u_h + d_1 u_{h-1} + \cdots + d_m u_{h-m} = 0$ for all $h \geqslant m$. Prove that I_U is an ideal of the ring $\mathbb{C}[X]$, generated by the companion polynomial of U.

(c) Give a necessary and sufficient condition, in terms of the companion polynomial of U, such that U is periodic (i.e., there is $m > 0$ such that $u_{h+m} = u_h$ for all $h \geqslant 0$.

(d) Give an example of a non-periodic linear recurrence sequence $U = \{u_h\}_{h=0}^{\infty}$ such that $Z_U = \{h \in \mathbb{Z}_{\geqslant 0} : u_h = 0\}$ is infinite.

Exercise 9.8. *An arithmetic progression is a sequence $a, a+d, a+2d, \ldots$ where a, d are integers with $d > 0$.*
Let $U = \{u_h\}_{h=0}^{\infty}$ be a linear recurrence sequence with terms in $\mathbb{C}$. We do not assume that U is non-degenerate. Assuming the Skolem-Mahler-Lech Theorem, prove that either Z_U is finite, or Z_U is the union of a finite set and a finite number of arithmetic progressions.
Hint. *Assume that U is degenerate and let $\theta_1, \ldots, \theta_m$ be the roots of the companion polynomial of U. Let N be a positive integer such that all roots of unity among the quotients θ_i/θ_j have order dividing N. Consider the sequences $\{u_{hN+i}\}_{h=0}^{\infty}$ ($i = 0, \ldots, N-1$).*

Exercise 9.9. *A linear recurrence sequence* $U = \{u_h\}_{h=0}^{\infty}$ *is called strongly non-degenerate if for the zeros* $\theta_1, \dots, \theta_m$ *of the companion polynomial of* U*, neither any of the numbers* θ_i $(i = 1, \dots, m)$*, nor any of the quotients* θ_i/θ_j $(1 \leqslant i, j \leqslant m\, i \neq j)$ *is a root of unity.*

(a) *Let* U *be a strongly non-degenerate linear recurrence sequence with terms in* $\mathbb{C}$*. Prove that for every* $a \in \mathbb{C}$*, the set* $Z_U(a) := \{h \in \mathbb{Z}_{\geqslant 0} : u_h = a\}$ *is finite.*

(b) *Let* $U = \{u_h\}_{h=0}^{\infty}$ *be a linear recurrence sequence with companion polynomial* $f(X) = (X - \theta_1)(X - \theta_2)$ *where none of* $\theta_1, \theta_2, \theta_1/\theta_2$ *is a root of unity. Prove that the set*

$$T_U := \{(h, l) \in \mathbb{Z}^2 : u_h = u_l,\, 0 < h < l\}$$

is finite.
Hint. *Use Theorem 9.7.*

Remark. One can show that T_U is finite for every strongly non-degenerate linear recurrence sequence U.