LINEAR FORMS IN LOGARITHMS

JAN-HENDRIK EVERTSE

April 2011

Literature:

T.N. Shorey, R. Tijdeman, Exponential Diophantine equations, Cambridge University Press, 1986; reprinted 2008.

1. Linear forms in logarithms and applications

We start with recalling some results from transcendence theory and then work towards lower bounds for linear forms in logarithms which are of crucial importance in effectively solving Diophantine equations.

We start with a transcendence result proved independently by the Russian Gel'fond and the German Schneider in 1934.

Theorem 1.1. (Gel'fond, Schneider, 1934) *Let α, β be algebraic numbers in $\mathbb{C}$, with $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$. Then α^β is transcendental.*

Here, $\alpha^\beta := e^{\beta \log \alpha}$, where $e^z = \sum_{n=0}^{\infty} z^n/n!$ and $\log \alpha = \log|\alpha| + i \arg(\alpha)$. The argument of α is determined only up to a multiple of 2π. Thus, $\log \alpha$ and hence α^β are multi-valued. The theorem holds for any choice of value of $\arg \alpha$.

Corollary 1.2. *Let β be an algebraic number in $\mathbb{C}$ with $i\beta \notin \mathbb{Q}$. Then $e^{\pi\beta}$ is transcendental.*

Proof. $e^{\pi\beta} = e^{\pi i \cdot (-i\beta)} = (-1)^{-i\beta}$. $\square$

Given a subring R of $\mathbb{C}$ (e.g., $\mathbb{Z}$, $\mathbb{Q}$, field of algebraic numbers), we say that complex numbers $\theta_1, \dots, \theta_m$ are called linearly independent over R if the equation $x_1\theta_1 + \cdots + x_m\theta_m = 0$ has no solution $(x_1, \dots, x_m) \in R^m \setminus \{\mathbf{0}\}$.

Corollary 1.3. *Let α, β be algebraic numbers from $\mathbb{C}$ different from $0, 1$ such that $\log \alpha$, $\log \beta$ are linearly independent over $\mathbb{Q}$. Then for all non-zero algebraic numbers γ, δ from $\mathbb{C}$ we have $\gamma \log \alpha + \delta \log \beta \neq 0$.*

Proof. Assume $\gamma \log \alpha + \delta \log \beta = 0$. Then $\log \alpha = -(\delta/\gamma) \log \beta$, hence $\alpha = \beta^{-\delta/\gamma}$. By Theorem 1.1 this is possible only if $a := \delta/\gamma \in \mathbb{Q}$. But then, $\log \alpha - a \log \beta = 0$, contrary to our assumption. $\square$

We now come to Baker's generalization to linear forms in an arbitrary number of logarithms of algebraic numbers.

Theorem 1.4. (A. Baker, 1966) *Let $\alpha_1, \dots, \alpha_m$ be algebraic numbers from $\mathbb{C}$ different from $0, 1$ such that $\log \alpha_1, \dots, \log \alpha_m$ are linearly independent over $\mathbb{Q}$. Then for every tuple $(\beta_0, \beta_1, \dots, \beta_m)$ of algebraic numbers from $\mathbb{C}$ different from $(0, 0, \dots, 0)$ we have*

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m \neq 0.$$

For applications to Diophantine problems, it is important that not only the above linear form is non-zero, but also that we have a strong enough lower bound for the absolute value of this linear form. We give a special case, where $\beta_0 = 0$ and $\beta_1, \dots, \beta_m$ are rational integers.

Theorem 1.5. (A. Baker, 1975) *Let $\alpha_1, \dots, \alpha_m$ be algebraic numbers from $\mathbb{C}$ different from $0, 1$. Further, let $b_1, \dots, b_m$ be rational integers such that*

$$b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m \neq 0.$$

Then

$$|b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m| \geqslant (eB)^{-C},$$

where $B := \max(|b_1|, \dots, |b_m|)$ and C is an effectively computable constant depending only on m and on $\alpha_1, \dots, \alpha_m$.

It is possible to get rid of the logarithms. Then Theorem 1.5 leads to the following:

Corollary 1.6. *Let $\alpha_1, \dots, \alpha_m$ be algebraic numbers from $\mathbb{C}$ different from $0, 1$ and let $b_1, \dots, b_m$ be rational integers such that*

$$\alpha_1^{b_1} \cdots \alpha_m^{b_m} \neq 1.$$

Then

$$|\alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1| \geqslant (eB)^{-C'},$$

where again $B := \max(|b_1|, \dots, |b_m|)$ and where C' is an effectively computable constant depending only on m and on $\alpha_1, \dots, \alpha_m$.

Proof. For the logarithm of a complex number z we choose $\log z = \log|z| + i\arg z$ with $-\pi < \arg z \leqslant \pi$. With this choice of log we have $\log(1+w) = \sum_{n=1}^{\infty}(-1)^{n-1}w^n/n$ for $w \in \mathbb{C}$ with $|w| < 1$. Using this power series expansion, one easily shows that

$$|\log(1+w)| \leqslant 2|w| \text{ if } |w| \leqslant 1/2.$$

We apply this with $w := \alpha_1^{b_1}\cdots\alpha_m^{b_m} - 1$. If $|w| > 1/2$ we are done, so we suppose that $|w| \leqslant 1/2$. We have to estimate from below $|\log(1+w)|$.

Recall that the complex logarithm is additive only modulo $2\pi i$. That is,

$$\log(1+w) = b_1\log\alpha_1 + \cdots + b_m\log\alpha_m + 2k\pi i$$

for some $k \in \mathbb{Z}$. We can apply Theorem 1.5 since $2k\pi i = 2k\log(-1)$. Thus, we obtain

$$|\log(1+w)| \geqslant \big(e\max(B,|2k|)\big)^{-C_1}$$

where C_1 is an effectively computable constant depending only on m and $\alpha_1,\ldots,\alpha_m$. Since $|\log(1+w)| \leqslant 2|w| \leqslant 1$ we have

$$|2k\pi i| \leqslant 1 + \sum_{j=1}^{m}|\log\alpha_j|\cdot|b_j| \leqslant (1 + \sum_{j=1}^{m}\log|\alpha_j|)B.$$

Hence $|k| \leqslant C_2B$, say, and $|\log(1+w)| \geqslant (eC_2B)^{-C_1}$. This implies $|w| \geqslant \frac{1}{2}(eC_2B)^{-C_1} \geqslant (eB)^{-C'}$ for a suitable C', as required. □

For completeness, we give a completely explicit version of Corollary 1.6 in the case that $\alpha_1,\ldots,\alpha_m$ are integers. The *height* of a rational number $a = x/y$, with $x, y \in \mathbb{Z}$ coprime, is defined by $H(a) := \max(|x|,|y|)$.

Theorem 1.7. (Matveev, 2000) *Let $a_1,\ldots,a_m$ be non-zero rational numbers and let $b_1,\ldots,b_m$ be integers such that*

$$a_1^{b_1}\cdots a_m^{b_m} \neq 1.$$

Then $|a_1^{b_1}\cdots a_m^{b_m} - 1| \geqslant (eB)^{-C'}$, where

$$B = \max(|b_1|,\ldots,|b_m|),$$
$$C' = \tfrac{1}{2}e\cdot m^{4.5}30^{m+3}\prod_{j=1}^{m}\max\big(1,\log H(a_j)\big).$$

To illustrate the power of this result we give a quick application.

Corollary 1.8. *let a, b be integers with $a \geqslant 2, b \geqslant 2$. Then there is an effectively computable number $C_1 > 0$, depending only on a, b, such that for any two positive integers m, n,*

$$|a^m - b^n| \geqslant \frac{\max(a^m, b^n)}{(e\max(m,n))^{C_1}}.$$

Consequently, for any non-zero integer k, there exists an effectively computable number C_2, depending on a, b, k such that if m, n are positive integers with $a^m - b^n = k$, then $m, n \leqslant C_2$.

Proof. Let m, n be positive integers. Put $B := \max(m, n)$. Assume without loss of generality that $a^m \geqslant b^n$. By Corollary 1.6 or Theorem 1.7 we have

$$|1 - b^n a^{-m}| \geqslant (eB)^{-C_1},$$

where C_1 is an effectively computable number depending only on a, b. Multiplying with a^m gives our first assertion.

Now let m, n be positive integers with $a^m - b^n = k$. Put again $B := \max(m, n)$. Then since $a, b \geqslant 2$,

$$|k| \geqslant 2^B \cdot (eB)^{-C_1}.$$

This proves that B is bounded above by an effectively computable number depending on a, b, k. □

In 1844, Catalan conjectured that the equation in four unknowns,

$$x^m - y^n = 1 \text{ in } x, y, m, n \in \mathbb{Z} \text{ with } x, y, m, n \geqslant 2$$

has only one solution, namely $3^2 - 2^3 = 1$. In 1976, as one of the striking consequences of the results on linear forms in logarithms mentioned above, Tijdeman proved that there is an effectively computable constant C, such that for every solution (x, y, m, n) of Catalan's equation, one has $x^m, y^n \leqslant C$. The constant C can be computed but it is extremely large. Several people tried to prove Catalan's conjecture, on the one hand by reducing Tijdeman's constant C using sharper linear forms in logarithm estimates, on the other hand by showing that x^m, y^n have to be very large as long as $(x^m, y^n) \neq (3^2, 2^3)$, and finally using heavy computations. This didn't lead to success. In 2000 Mihailescu managed to prove Catalan's conjecture by an algebraic method which is completely independent of linear forms in logarithms.

We give another application. Consider the sequence $\{a_n\}$ with $a_n = 2^n$ for $n = 0, 1, 2, \ldots$. Note that $a_{n+1} - a_n = a_n$. Similarly, we may consider the increasing sequence $\{a_n\}$ of numbers which are all composed of primes from $\{2, 3\}$, i.e., $1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, \ldots$ and ask how the gap $a_{n+1} - a_n$ compares with a_n as $n \to \infty$. More generally, we may take a finite set of primes and ask this question about the sequence of consecutive integers composed of these primes.

Theorem 1.9. (Tijdeman, 1974) *Let $S = \{p_1, \ldots, p_t\}$ be a finite set of distinct primes, and let $a_1 < a_2 < a_3 < \cdots$ be the sequence of consecutive positive integers composed of primes from S. Then there are effectively computable positive numbers c_1, c_2, depending on $t, p_1, \ldots, p_t$, such that*

$$a_{n+1} - a_n \geqslant \frac{a_n}{c_1(\log a_n)^{c_2}} \quad \textit{for } n = 1, 2, \ldots.$$

Proof. We have $a_n = p_1^{k_1} \cdots p_t^{k_t}$, and $a_{n+1} = p_1^{l_1} \cdots p_t^{l_t}$ with non-negative integers k_i, l_i. By Corollary 1.6,

$$\left| \frac{a_{n+1}}{a_n} - 1 \right| = |p_1^{l_1 - k_1} \cdots p_t^{l_t - k_t} - 1| \geqslant (eB)^{-C},$$

where $B := \max(|l_1 - k_1|, \ldots, |l_t - k_t|)$. First note that

$$k_i \leqslant \frac{\log a_n}{\log p_i} \leqslant \frac{\log a_n}{\log 2} \quad \text{for } i = 1, \ldots, t.$$

Next, $a_{n+1} \leqslant a_n^2$. So

$$l_i \leqslant \frac{\log a_{n+1}}{\log p_i} \leqslant \frac{\log a_n^2}{\log 2} \quad \text{for } i = 1, \ldots, t.$$

Hence $B \leqslant 2 \log a_n / \log 2$. It follows that $a_{n+1} - a_n \geqslant a_n (2e \log a_n / \log 2)^{-C}$. $\square$

Most results in Diophantine approximation that have been proved for algebraic numbers in $\mathbb{C}$ have an analogue for p-adic numbers. We can define p-adic exponentiation, p-adic logarithms, etc., and this enables us to formulate analogues for Theorem 1.1– Theorem 1.7 in the p-adic setting. We give an analogue of Corollary 1.6 in the case that $\alpha_1, \ldots, \alpha_m$ are rational numbers. There is a more general version for algebraic $\alpha_1, \ldots, \alpha_m$ but this is more difficult to state.

Theorem 1.10. (Yu, 1986) *Let p be a prime number, let $a_1, \ldots, a_m$ be non-zero rational numbers which are not divisible by p. Further, let $b_1, \ldots, b_m$ be* *integers such that*

$$a_1^{b_1} \cdots a_m^{b_m} \neq 1.$$

Put $B := \max(|b_1|, \ldots, |b_m|)$. *Then*

$$|a_1^{b_1} \cdots a_m^{b_m} - 1|_p \geqslant (eB)^{-C}$$

where C *is an effectively computable number depending on* p, m *and* $a_1, \ldots, a_m$.

For $m = 1$ there is a sharper result which can be proved by elementary means (Exercise 6a). But for $m \geqslant 2$ the proof is very difficult.

2. The effective Siegel-Mahler-Lang Theorem

Let K be an algebraic number field and let Γ be a finitely generated, multiplicative subgroup of K^*, i.e., there are $\gamma_1, \ldots, \gamma_t \in \Gamma$ such that every element of Γ can be expressed as

$$\zeta \gamma_1^{z_1} \cdots \gamma_t^{z_t}$$

where ζ is a root of unity in K, and $z_1, \ldots, z_t$ are integers. Further, let a, b be non-zero elements from K and consider the equation

$$ax + by = 1 \quad \text{in } x, y \in \Gamma. \tag{2.1}$$

In 1979, Győry gave an effective proof of the Siegel-Mahler-Lang Theorem.

Theorem 2.1. (Győry, 1979) *Equation* (2.1) *has only finitely many solutions, and its set of solutions can be determined effectively.*

The idea of the proof is to express a solution (x, y) of (2.1) as

$$x = \zeta_1 \gamma_1^{b_1} \cdots \gamma_t^{b_t}, \quad y = \zeta_2 \gamma_1^{b'_1} \cdots \gamma_t^{b'_t}$$

with $\zeta_1, \zeta_2 \in U_K$, $b_i, b'_i \in \mathbb{Z}$. By combining Corollary 1.6 and a generalization of Theorem 1.10 for algebraic numbers instead of the rational numbers $a_1, \ldots, a_m$ in the statement of that lemma, Győry shows that for every solution (x, y) of (2.1) one has $\max(|b_1|, \ldots, |b'_t|) \leqslant C$, where C is effectively computable in terms of $K, \gamma_1, \ldots, \gamma_t$. Then one can find all solutions of (2.1) by checking for each $\zeta_1, \zeta_2 \in U_K$ and $b_i, b'_i \leqslant C$ whether $ax + by = 1$ holds.

We prove two special cases of Theorem 2.1, namely the case that $a, b \in \mathbb{Q}$ and Γ is contained in $\mathbb{Q}^*$, and the case that a, b lie in an algebraic number field K and Γ is the group of units of the ring of integers of K.

As has been explained before, if $a, b \in \mathbb{Q}$ and Γ is contained in $\mathbb{Q}^*$, then Eq. (2.1) can be reduced to an S-unit equation. There are rational numbers $\gamma_1, \dots, \gamma_t$ such that all elements of Γ are of the shape $\pm\gamma_1^{z_1} \cdots \gamma_t^{z_t}$. Let $S = \{p_1, \dots, p_t\}$ be the prime numbers occurring in the prime factorizations of the numerators and denominators of $a, b, \gamma_1, \dots, \gamma_t$. Then $a, b, \gamma_1, \dots, \gamma_t$ lie in the multiplicative group of S-units

$$\mathbb{Z}_S^* = \{\pm p_1^{z_1} \cdots p_t^{z_t} : z_1, \dots, z_t \in \mathbb{Z}\}.$$

Hence if (x, y) is a solution to (2.1), the numbers ax, by are S-units. So instead of (2.1), we may as well consider

$$x + y = 1 \quad \text{in } x, y \in \mathbb{Z}_S^*. \tag{2.2}$$

Theorem 2.2. *Let $S = \{p_1, \dots, p_t\}$ be a finite set of primes. Then* (2.2) *has only finitely many solutions, and its set of solutions can be determined effectively.*

Proof. Let (x, y) be a solution of (2.2). We may write $x = u/w$, $y = v/w$ where u, v, w are integers with $\gcd(u, v, w) = 1$. Then

$$u + v = w. \tag{2.3}$$

The integers u, v, w are composed of primes from S, and moreover, no prime divides two numbers among u, v, w since u, v, w are coprime. After reordering the primes $p_1, \dots, p_t$, we may assume that

$$u = \pm p_1^{b_1} \cdots p_r^{b_r}, \quad v = \pm p_{r+1}^{b_{r+1}} \cdots p_s^{b_s}, \quad w = \pm p_{s+1}^{b_{s+1}} \cdots p_t^{b_t},$$

where $0 \leqslant r \leqslant s \leqslant t$ and the b_i are non-negative integers (empty products are equal to 1; for instance if $r = 0$ then $u = \pm 1$). We have to prove that $B := \max(b_1, \dots, b_t)$ is bounded above by an effectively computable number depending only on $p_1, \dots, p_t$. By symmetry, we may assume that $B = b_t$. Then using $-(u/v) - 1 = -(w/v)$ we obtain

$$0 < |\pm p_1^{b_1} \cdots p_r^{b_r} p_{r+1}^{-b_{r+1}} \cdots p_s^{-b_s} - 1|_{p_t} = |w/v|_{p_t} = p_t^{-b_t} = p_t^{-B}.$$

From Theorem 1.10 we obtain that $|\cdots|_{p_t} \geqslant (eB)^{-C}$, where C is effectively computable in terms of $p_1, \dots, p_t$. Hence

$$(eB)^{-C_2} \leqslant p_t^{-B}.$$

So indeed, B is bounded above by an effectively computable number depending on $p_1, \dots, p_t$. $\square$

Remark. In his PhD-thesis from 1988, de Weger gave a practical algorithm, based on strong linear forms in logarithms estimates and the LLL-basis reduction algorithm, to solve equations of the type (2.2). As a consequence, he showed that the $x+y=z$ has precisely 545 solutions in positive integers x, y, z with $x \leqslant y$, all of the shape $2^{b_1}3^{b_2}5^{b_3}7^{b_4}11^{b_5}13^{b_6}$ with $b_i \in \mathbb{Z}$.

Theorem 2.3. *Let $a, b \in K^*$. Then the equation*

$$ax + by = 1 \quad \text{in } x, y \in \mathcal{O}_K^* \tag{2.4}$$

has only finitely many solutions and its set of solutions can be determined effectively.

Corollary 2.4. *Let $F(X,Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d$ be a binary form in $\mathbb{Z}[X,Y]$ such that $F(X,1)$ has at least three distinct roots in $\mathbb{C}$, and let m be a non-zero integer. Then the equation*

$$F(x,y) = m \quad \text{in } x, y \in \mathbb{Z}$$

has only finitely many solutions, and its set of solutions can be determined effectively.

Corollary 2.5. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial without multiple zeros and n an integer $\geqslant 2$. Assume that f has at least two zeros in $\mathbb{C}$ if $n \geqslant 3$ and at least three zeros in $\mathbb{C}$ if $n = 2$. Then the equation*

$$y^n = f(x) \quad \text{in } x, y \in \mathbb{Z}$$

has only finitely many solutions, and its set of solutions can be determined effectively.

In Frits' lecture notes on the Siegel-Mahler Theorem it was explained how the equations in Corollaries 2.4 and 2.5 can be reduced to (2.4).

In the proof of Theorem 2.3 we need some facts on units. Suppose the number field K has degree d. Then K has precisely d distinct embeddings in $\mathbb{C}$, which can be divided into real embeddings (of which the image lies in $\mathbb{R}$) and complex embeddings (with image in $\mathbb{C}$ but not in $\mathbb{R}$). Further, the complex embeddings occur in complex conjugate pairs $\sigma, \overline{\sigma}$, where $\overline{\sigma}(x) := \overline{\sigma(x)}$ for $x \in K$. Suppose that K has precisely r_1 real embeddings, and precisely r_2 pairs of complex conjugate embeddings, where $r_1 + 2r_2 = d$. We renumber the embeddings such that $\sigma_1, \ldots, \sigma_{r_1}$ are the real embeddings of K, and $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$ for $i = 1, \ldots, r_2$.

The following fact is well known.

Lemma 2.6. *Let ε be a unit of $\mathcal{O}_K$. Then*

$$N_{K/\mathbb{Q}}(\varepsilon) = \prod_{i=1}^{d} \sigma_i(\varepsilon) = \pm 1.$$

Proof. Exercise. □

To study the units of $\mathcal{O}_K$, it is useful to consider the absolute values of their conjugates. Clearly, for $\varepsilon \in \mathcal{O}_K^*$ we have

$$\begin{aligned} &|\sigma_{r_1+r_2+i}(\varepsilon)| = |\sigma_{r_1+i}(\varepsilon)| \quad \text{for } i = 1 \dots r_2, \\ &\prod_{i=1}^{r_1} |\sigma_i(\varepsilon)| \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(\varepsilon)|^2 = 1, \end{aligned}$$

so $|\sigma_i(\varepsilon)|$ $(i = 1, \dots, r_1 + r_2 - 1)$ determine $|\sigma_i(\varepsilon)|$ $(i = r_1 + r_2, \dots, d)$.

The following lemma is a more precise version of Dirichlet's Unit Theorem.

Lemma 2.7. *Let $r := r_1 + r_2 - 1$ and define the map*

$$L : \mathcal{O}_K^* \to \mathbb{R}^r : \varepsilon \mapsto (\log|\sigma_1(\varepsilon), \dots, \log|\sigma_r(\varepsilon)|).$$

Then L is a group homomorphism. The kernel of L is the group U_K of roots of unity of K and the image of L is a lattice of rank r in $\mathbb{R}^r$.

Choose units $\varepsilon_1, \dots, \varepsilon_r$ such that $L(\varepsilon_1), \dots, L(\varepsilon_r)$ form a basis of the lattice $L(\mathcal{O}_K^*)$. Then every $\varepsilon \in \mathcal{O}_K^*$ can be expressed uniquely as

$$\zeta \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r} \text{ with } \zeta \in U_K,\ b_1, \dots, b_r \in \mathbb{Z}. \tag{2.5}$$

Further, the matrix

$$M := \begin{pmatrix} \log|\sigma_1(\varepsilon_1)| & \cdots & \log|\sigma_1(\varepsilon_r)| \\ \vdots & & \vdots \\ \log|\sigma_r(\varepsilon_1)| & \cdots & \log|\sigma_r(\varepsilon_r)| \end{pmatrix} \tag{2.6}$$

is invertible.

We deduce a consequence.

Lemma 2.8. *There is a constant $C > 0$ with the following property. If ε is any unit of $\mathcal{O}_K$, and $b_1, \dots, b_r$ are the corresponding integers defined by* (2.4)*,* *then*

$$\max(|b_1|,\ldots,|b_r|) \leqslant C \cdot \max_{1\leqslant i\leqslant d} \log|\sigma_i(\varepsilon)|.$$

Proof. Let $\mathbf{b} := (b_1,\ldots,b_r)^T$ (column vector). Then $L(\varepsilon) = M\mathbf{b}$, hence $\mathbf{b} = M^{-1}L(\varepsilon)$. Writing $M^{-1} = (a_{ij})$, we obtain

$$b_i = \sum_{j=1}^{r} a_{ij}\sigma_j(\varepsilon) \quad (i = 1,\ldots,r).$$

Applying the triangle inequality, we get

$$\max_{1\leqslant i\leqslant r} |b_i| \leqslant \left(\max_{1\leqslant i\leqslant r} \sum_{j=1}^{r} |a_{ij}|\right) \cdot \max_{1\leqslant j\leqslant r} |\sigma_j(\varepsilon)|.$$

□

Proof of Theorem 2.3. Let (x, y) be a solution of (2.3). There are $\zeta_1, \zeta_2 \in U_K$, as well as integers $a_1,\ldots,a_r$, $b_1,\ldots,b_r$, such that

$$x = \zeta_1\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}, \quad y = \zeta_2\varepsilon_1^{b_1}\cdots\varepsilon_r^{b_r}.$$

Thus

$$a\zeta_1\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r} + b\zeta_2\varepsilon_1^{b_1}\cdots\varepsilon_r^{b_r} = 1.$$

We assume without loss of generality that $B := \max(|a_1|,\ldots,|b_r|) = |b_r|$. We estimate from above and below,

$$\Lambda_i := |\sigma_i(a)\sigma(\zeta_1)\sigma_i(\varepsilon_1)^{a_1}\cdots\sigma_i(\varepsilon_r)^{a_r} - 1| = |\sigma_i(b)\sigma_i(y)|$$

for a suitable choice of i.

In fact, let $|\sigma_i(y)|$ be the smallest, and $|\sigma_j(y)|$ the largest among $|\sigma_1(y)|,\ldots,|\sigma_d(y)|$. Then by Lemma 2.6,

$$|\sigma_i(y)|^{d-1}|\sigma_j(y)| \leqslant 1$$

and subsequently by Lemma 2.8,

$$|\sigma_i(y)| \leqslant |\sigma_j(y)|^{-1/(d-1)} \leqslant e^{-B/C(d-1)}.$$

This leads to

$$\Lambda_i \leqslant |\sigma_i(\beta)|e^{-B/C(d-1)}.$$

By Corollary 1.6 we have $|\Lambda_i| \geqslant (eB)^{-C'}$ for some effectively computable number C' depending on a, $\varepsilon_1,\ldots,\varepsilon_r$ and the finitely many roots of unity of K. We infer

$$(eB)^{-C'} \leqslant |\sigma_i(a)|e^{-B/C(d-1)}$$

and this leads to an effectively computable upper bound for B. □

Remark. There are practical algorithms to solve equations of the type (2.4) which work well as long as the degree of the field K, and the fundamental units of the ring of integers of K, are not too large. These algorithms are again based on linear forms in logarithms estimates and the LLL-algorithm. For instance, in 2000 Wildanger determined all solutions of the equation $x+y=1$ in $x, y \in \mathcal{O}_K^*$, with $K = \mathbb{Q}(\cos(2\pi/19))$. The number field K has degree 9 and all its embeddings are real. Thus, the unit group $\mathcal{O}_K^*$ has rank 8.

3. Exercises

Exercise 1. Let $p_1, \ldots, p_s, p_{s+1}, \ldots, p_t$ be distinct prime numbers. Let A be the set of positive integers composed of primes from $p_1, \ldots, p_s$, and B the set of positive integers composed of primes from $p_{s+1}, \ldots, p_t$.

(a) Prove that there exist positive numbers c_1, c_2, effectively computable in terms of $p_1, \ldots, p_t$ such that

$$|x-y| \geqslant \frac{\max(x,y)}{c_1\big(\log\max(x,y)\big)^{c_2}} \quad \text{for all } x \in A,\ y \in B.$$

(b) Given a non-zero integer a, denote by $P(a)$ the largest prime number dividing a, with $P(\pm 1) := 1$. Prove that

$$\lim_{x\in A,\, y\in B,\, \max(|x|,|y|)\to\infty} P(x-y) = \infty.$$

Exercise 2. Let $f(X) = X^2 - AX - B$ be a polynomial with coefficients $A, B \in \mathbb{Z}$. Let α, β be the two zeros of f in $\mathbb{C}$. Assume that f is irreducible, and that α/β is not a root of unity. Let the sequence $U = \{u_n\}_{n=0}^{\infty}$ in $\mathbb{Z}$ be given by

$$u_n = Au_{n-1} + Bu_{n-2} \quad (n \geqslant 0)$$

and initial values $u_0, u_1 \in \mathbb{Z}$, not both 0.

(a) Prove that $M := \max(|\alpha|, |\beta|) > 1$.
(b) Prove that there are non-zero algebraic numbers γ_1, γ_2 such that $u_n = \gamma_1\alpha^n + \gamma_2\beta^n$ for $n \geqslant 0$.
(c) Prove that there is an effectively computable number C such that $u_n \neq 0$ for $n \geqslant C$.

(d) Prove that there are effectively computable positive numbers c_1, c_2 such that $|u_n| \geqslant M^n / c_1 n^{c_2}$ for $n \geqslant C$.

Exercise 3. Let A, B, C be integers such that $C \neq 0$ and

$$X^3 - AX^2 - BX - C = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3),$$

where $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$, and none of the quotients α_i/α_j $(1 \leqslant i < j \leqslant 3)$ is a root of unity. Consider the linear recurrence sequence $U = \{u_n\}_{n=0}^{\infty}$, given by

$$u_n = Au_{n-1} + Bu_{n-2} + Cu_{n-3} \quad (n \geqslant 3)$$

and initial values $u_0, u_1, u_2 \in \mathbb{Z}$, not all zero.

(a) Prove that there exist algebraic numbers $\gamma_1, \gamma_2, \gamma_3$ such that

$$u_n = \gamma_1 \alpha_1^n + \gamma_2 \alpha_2^n + \gamma_3 \alpha_3^n \quad \text{for } n \geqslant 0.$$

(b) Prove that $|\alpha_1| = |\alpha_2| = |\alpha_3|$ cannot hold.

(c) Prove that there exists an effectively computable number C, depending on A, B, C, such that if n is a non-negative integer with $u_n = 0$ then $n < C$.

Exercise 4. In 1995, Laurent, Mignotte and Nesterenko proved the following explicit estimate for linear forms in two logarithms. Let a_1, a_2 be two positive rational numbers $\neq 1$. Further, let b_1, b_2 be non-zero integers. Suppose that $\Lambda := b_1 \log a_1 - b_2 \log a_2 \neq 0$. Then

$$\log|\Lambda| \geqslant$$
$$-22\left(\max\left\{\log\left(\frac{|b_1|}{\log H(a_2)} + \frac{|b_2|}{\log H(a_1)}\right) + 0.06\,,\, 21\right\}\right)^2 \log H(a_1) \log H(a_2)\,.$$

Using this estimate, compute an upper bound C, such that for all positive integers m, n with $97^m - 89^n = 8$ we have $m, n \leqslant C$.

Hint. Use $|\log(1+z)| \leqslant 2|z|$ if $|z| \leqslant \frac{1}{2}$.

Exercise 5. In this exercise you are asked to apply the estimate of Laurent, Mignotte and Nesterenko to more advanced equations.

(a) Prove that the equation

$$x^n - 2y^n = 1 \quad \text{in unknowns } x, y \text{ with } x \geqslant 2, y \geqslant 2$$

has no solutions if $n > 10000$.

Hint. Applying Laurent-Mignotte-Nesterenko to an appropriate linear form in two logarithms you will get a lower estimate depending on n and x, y. But you can derive also an upper estimate which depends on n, x, y. Comparing the two estimates leads to an upper bound for n independent of x, y.

(b) Let a, b, c be positive integers. Prove that there is a number C, effectively computable in terms of a, b, c, such that the equation

$$ax^n - by^n = c$$

has no solutions if $n > C$. In the case $a = b$ you may give an elementary proof, without using the result of Laurent-Mignotte-Nesterenko.

(c) Let k be a fixed integer $\geqslant 2$. Prove that the equation

$$y^z = \binom{x}{k} \quad \text{in integers } x, y, z \text{ with } x > 0,\ y \geqslant 2,\ z \geqslant 3$$

has only finitely many solutions.

Exercise 6. In this exercise, you are asked to prove a very simple case of Theorem 1.10 and to apply this to certain Diophantine equations.

(a) Let a be an integer, and p a prime, such that $|a|_p \leqslant p^{-1}$ if $p > 2$ and $|a|_2 \leqslant 2^{-2}$ if $p = 2$. Prove that for any positive integer b we have

$$|(1+a)^b - 1|_p = |ab|_p \geqslant 1/ab.$$

Hint. You may either prove that $|\binom{b}{k}a^k|_p < |ab|_p$ for $k \geqslant 2$ or write $b = up^t$ where u is an integer not divisible by p and t a non-negative integer, and use induction on t.

(b) Let p be a prime $\geqslant 5$. Using (a), prove that the equation $p^x - 2^y = 1$ has no solutions in integers $x \geqslant 2$, $y \geqslant 2$. Prove also that the equation $2^x - p^y = 1$ has no solutions in integers $x \geq 2$, $y \geqslant 2$.