7. Mahler's Work on Diophantine Equations and Subsequent Developments

Jan-Hendrik Evertse, Kálmán Győry, and Cameron L. Stewart

The main body of Mahler's work on Diophantine equations consists of his 1933 papers [M17, M18, M19], in which he proved a generalisation of the Thue–Siegel Theorem on the approximation of algebraic numbers by rationals, involving P-adic absolute values, and applied this to get finiteness results for the number of solutions for what became later known as Thue–Mahler equations. He was also the first to give upper bounds for the number of solutions of such equations. In fact, Mahler's extension of the Thue–Siegel Theorem made it possible to extend various finiteness results for Diophantine equations over the integers to S-integers, for any arbitrary finite set of primes S. For instance Mahler himself [M21] extended Siegel's finiteness theorem on integral points on elliptic curves to S-integral points.

In this chapter, we discuss Mahler's work on Diophantine approximation and its applications to Diophantine equations, in particular Thue–Mahler equations, S-unit equations and S-integral points on elliptic curves, and go into later developments concerning the number of solutions to Thue–Mahler equations and effective finiteness results for Thue–Mahler equations. For the latter we need estimates for P-adic logarithmic forms, which may be viewed as an outgrowth of Mahler's work on the P-adic Gel'fond–Schneider theorem [M30]. We also go briefly into decomposable form equations, these are certain higher dimensional generalisations of Thue–Mahler equations.

1 Mahler's P-adic generalization of the Thue–Siegel Theorem

We adopt the convention that if p/q denotes a rational number then p, q are integers with $\gcd(p, q) = 1$ and $q > 0$. Thue [72] proved in 1909 that if ζ is any real algebraic number of degree n and $\beta > \frac{1}{2}n + 1$, then the inequality

$$\left|\zeta - \frac{p}{q}\right| \leq q^{-\beta}$$

has only finitely many solutions in rational numbers p/q. This was later generalised by Siegel [62] in 1921 to all β with

$$\beta > \beta_0 := \min_{s=1,\dots,n-1} \left(\frac{n}{s+1} + s \right). \tag{1}$$

This condition is satisfied for instance if $\beta \geq 2\sqrt{n}$. Siegel's result was further extended in the late 1940s to $\beta > \sqrt{2n}$ by Gel'fond [30] and Dyson [19], and finally by Roth [56] in 1955 to the weakest possible condition $\beta > 2$.

To state Mahler's generalisation of Siegel's theorem we introduce some notation. For a prime number P, we denote by $|\cdot|_P$ the standard P-adic absolute value on $\mathbb{Q}$ with $|P|_P = P^{-1}$. This has a unique extension to $\overline{\mathbb{Q}_P}$. To uniformise our notation, we write $|\cdot|_\infty$ for the ordinary absolute value, and $\mathbb{Q}_\infty$, $\overline{\mathbb{Q}_\infty}$ for $\mathbb{R}$ and $\mathbb{C}$, respectively. Further, we set $M_\mathbb{Q} := \{\infty\} \cup \{\text{primes}\}$. We use the notation $|p, q|$ for $\max(|p|, |q|)$.

Now Mahler's main theorem on Diophantine approximation [M17, Satz 1, p. 710] can be stated somewhat more efficiently as follows:

Theorem 1.1. *Let S be a finite subset of $M_\mathbb{Q}$, let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $n \geq 3$ having a zero $\zeta_P \in \mathbb{Q}_P$ for $P \in S$, and let $k \geq 1$ and $\beta > \beta_0$. Then the inequality*

$$\prod_{P \in S} \min\left(1, \left|\zeta_P - \frac{p}{q}\right|_P\right) \leq k \cdot |p, q|^{-\beta} \tag{2}$$

has only finitely many solutions in rational numbers p/q.

An important step in the proof is to reduce the single inequality (2) to a finite number of systems of inequalities each of which involves only one absolute value. To this end, Mahler used a combinatorial argument which was also an important tool in later work, e.g., quantitative versions of the P-adic Subspace Theorem.

Choose β_1 with

$$\beta_0 < \beta_1 < \min(n, \beta)$$

and define λ by $\beta = (1+\lambda)\beta_1$. We restrict ourselves to rational solutions p/q of (2) with

$$|p, q| \geq k^{1/\beta_1}. \tag{3}$$

For each such solution we have $k \cdot |p, q|^{-\beta} \leq (k \cdot |p, q|^{-\beta_1})^{1+\lambda} \leq 1$ since $k \geq 1$, and

$$\min\left(1, \left|\zeta_P - \frac{p}{q}\right|_P\right) = (k \cdot |p, q|^{-\beta_1})^{(1+\lambda)\gamma_P} \quad \text{for } P \in S,$$

where $\gamma_P \geq 0$ for $P \in S$ and $\sum_{P \in S} \gamma_P \geq 1$. Take

$$v := 1 + \left[\frac{t+1}{\lambda}\right] = 1 + \left[\frac{\beta_1}{\beta - \beta_1} \cdot (t+1)\right] \tag{4}$$

and let $g_P := [(1+\lambda)\gamma_P \cdot v]$ for $P \in S$. Then $\sum_{P\in S} g_P \geq v$, hence there are integers f_P with $0 \leq f_P \leq g_P$ for $P \in S$ and $\sum_{P\in S} f_P = v$. Taking $\Gamma_P := f_P/v$ for $P \in S$, we get $\Gamma_P \leq (1+\lambda)\gamma_P$ for $P \in S$ and thus,

$$\min\left(1, \left|\zeta_P - \frac{p}{q}\right|_P\right) \leq (k \cdot |p,q|^{-\beta_1})^{\Gamma_P} \quad \text{for } P \in S. \tag{5}$$

Notice that $(\Gamma_P : P \in S)$ belongs to the finite set $\mathcal{S}$ of rational tuples $(f_P/v : P \in S)$, where the f_P are non-negative integers with $\sum_{P\in S} f_P = v$. For later reference we record that for all $(\Gamma_P : P \in S) \in \mathcal{S}$ we have

$$\sum_{P\in S} \Gamma_P = 1, \quad \Gamma_P \geq 0 \text{ for } P \in S \tag{6}$$

and, by (4),

$$|\mathcal{S}| = \binom{v+t}{t} \leq 2^{v+t} \leq 2^{\frac{\beta}{\beta-\beta_1}\cdot(t+1)}, \tag{7}$$

where here and below, we denote by $|\mathcal{A}|$ the cardinality of a set $\mathcal{A}$. Thus, inequality (2) has been reduced to at most $|\mathcal{S}|$ systems (5), hence to prove Theorem 1.1, it suffices to prove that each of these systems (5) has only finitely many solutions $p/q \in \mathbb{Q}$. In fact, Mahler [M17, p. 709] proved the following more precise result.

Theorem 1.2. *Let $\beta_0 < \beta_1 < n$ and let Γ_P $(P \in S)$ be non-negative reals with $\sum_{P\in S} \Gamma_P = 1$. There are effectively computable numbers C_1, C_2, depending only on k, f and β_1, and thus independent of the set S and the reals Γ_P, such that if (5) has a solution $p_1/q_1 \in \mathbb{Q}$ with $|p_1,q_1| \geq C_1$ then for any other solution $p_2/q_2 \in \mathbb{Q}$ of (5) we have $|p_2,q_2| \leq |p_1,q_1|^{C_2}$.*

Sketch of proof. Mahler's proof is an adaptation of that of Siegel [62]. We give a very brief outline. Assume that Theorem 1.2 is false and take two rational solutions p_1/q_1, p_2/q_2 of (5) such that $|p_1,q_1| \geq C_1$ and $\lambda := \frac{\log|p_2,q_2|}{\log|p_1,q_1|} > C_2$. Let $r := [\lambda]+1$ and choose an integer s with $1 \leq s \leq n-1$ such that $\frac{n}{s+1}+s = \beta_0$. Let m be an integer with $m > r$ and $(m+1)(s+1) > nr$. Following Siegel, Mahler shows that there is a polynomial $R_m(X,Y)$ of degree at most m in X and degree at most s in Y, with integer coefficients of not too large size, such that $R_m(p_1/q_1, p_2/q_2) \neq 0$ and $\frac{\partial^i R_m}{\partial X^i}(\zeta,\zeta) = 0$ for $i = 0,\ldots,r-1$ and each root ζ of $f(X)$. Then

$$R_m(X,Y) = F_m(X,Y,\zeta)(X-\zeta)^r + G_m(X,Y,\zeta)(X-\zeta)$$

for each root ζ of $f(X)$, where $F_m(X,Y,Z)$, $G_m(X,Y,Z)$ are polynomials with integral coefficients. Now $A_m := q_1^m q_2^s R_m(p_1/q_1, p_2/q_2)$ is a non-zero integer, hence $\prod_{P\in S} |A_m|_P \geq 1$. On the other hand, using that p_1/q_1, p_2/q_2 are solutions of (5) and that $\beta > \beta_0$ one can deduce good upper bounds for $|A_m|_P$ for $P \in S$, and in fact show that there is m with $\prod_{P\in S} |A_m|_P < 1$. This leads to a contradiction. □

Mahler used Theorem 1.2 in [M18] to compute an upper bound for the number of solutions of (5) or (2). Another important tool is the following simple observation that solutions of (5) are far apart [M18, p. 40], nowadays called a *gap principle*.

LEMMA 1.3. *Let p_1/q_1, p_2/q_2 be two distinct rational solutions of (5), with $|p_2, q_2| \geq |p_1, q_1| > k^{1/\beta_1}$. Then*

$$|p_2, q_2| \geq \frac{1}{2k} \cdot |p_1, q_1|^{\beta_1 - 1}.$$

Proof. Write $s(\infty) = 1$ and $s(P) = 0$ if P is a prime. Let $S' := S \cup \{\infty\}$ and put $\Gamma_\infty := 0$ if $\infty \notin S$. Let $P \in S'$. Then if $\Gamma_P > 0$ we have $\left|\zeta_P - \frac{p_i}{q_i}\right|_P \leq (k \cdot |p_i, q_i|^{-\beta})^{\Gamma_P}$ for $i = 1, 2$ and so

$$\begin{aligned} |p_1 q_2 - p_2 q_1|_P &\leq (|p_1, q_1| \cdot |p_2, q_2|)^{s(P)} \left|\frac{p_1}{q_1} - \frac{p_2}{q_2}\right|_P \\ &\leq (2|p_1, q_1| \cdot |p_1, q_2|)^{s(P)} \max\left(\left|\frac{p_1}{q_1} - \zeta_P\right|_P, \left|\frac{p_2}{q_2} - \zeta_P\right|_P\right) \\ &\leq (2|p_1, q_1| \cdot |p_1, q_2|)^{s(P)} (k \cdot |p_1, q_1|^{-\beta_1})^{\Gamma_P} \end{aligned}$$

while if $\Gamma_P = 0$ we have the trivial estimate

$$|p_1 q_2 - p_2 q_1|_P \leq (2|p_1, q_1| \cdot |p_1, q_2|)^{s(P)}.$$

By taking the product over $P \in S'$, using $\prod_{P \in S'} |p_1 q_2 - p_2 q_1|_P \geq 1$, we obtain

$$1 \leq 2k \cdot |p_1, q_1|^{1-\beta_1} \cdot |p_2, q_2|,$$

which implies our lemma. □

Assume $n = \deg f \geq 3$. Combining Theorem 1.2 with Lemma 1.3, one easily deduces that the number of solutions of (5) is at most a quantity depending only on k, f and β_1. Invoking (7), we arrive at the following (see [M18, pp. 46–47, Hilfssatz 3]).

THEOREM 1.4. *The following statements hold:*

(i) System (5) has at most C_3 solutions in rationals p/q with $|p, q| > k^{1/\beta_1}$, where C_3 is effectively computable and depends only on k, f and β_1;

(ii) Inequality (2) has at most $C_3 \cdot 2^{\frac{\beta}{\beta - \beta_1} \cdot (t+1)}$ solutions in rationals p/q with $|p, q| > k^{1/\beta_1}$.

Theorems 1.1 and 1.4 have been generalised and refined in several respects. Already Siegel [62] considered approximation of algebraic numbers by elements from a given number field. In his PhD-work from 1939, published much later in a journal [52], Parry proved a common generalisation of the results of Siegel and

Mahler for inequalities over a given number field involving various Archimedean and non-Archimedean absolute values. Roth [56] and Ridout [55] extended the results of Siegel and Mahler from $\beta > \beta_0$ to $\beta > 2$. Lang [49] extended this further to number fields, thereby also improving Parry's result.

Also there has been much work on estimating the number of approximants. Davenport and Roth [18] were the first to give an upper bound for the number of solutions of $|\zeta - p/q| \le q^{-\beta}$ in rational numbers p/q, where ζ is a real algebraic number and β is any real > 2. Their bound was improved by Mignotte and then further by Bombieri and van der Poorten. We give the up to now best quantitative result for the number of solutions of a system (5), which can be deduced from a more general result of Bugeaud and Evertse [13, Prop. A.1] over number fields. The height $H(P)$ of a polynomial P with integer coefficients is the maximum of the absolute values of its coefficients.

Theorem 1.5. *Let $k \ge 1$, let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n \ge 3$, let S be a finite subset of $M_{\mathbb{Q}}$, for $P \in S$ let ζ_P be a zero of $f(X)$ in $\overline{\mathbb{Q}_P}$, let $\beta_1 > 2$, and let Γ_P ($P \in S$) be non-negative reals with $\sum_{P\in S} \Gamma_P = 1$. Put $\delta := 1 - 2/\beta_1$. Then the number of $p/q \in \mathbb{Q}$ with*

$$|p, q| \ge (4k)^{2/(\beta_1-2)} H(f),$$

$$\min\left(1, \left|\zeta_P - \tfrac{p}{q}\right|_P\right) \le (k \cdot |p, q|^{-\beta_1})^{\Gamma_P} \text{ for } P \in S$$

is at most $2^{30}\delta^{-3} \log 3n \cdot \log(\delta^{-1} \log 3n)$.

As said, Bugeaud and Evertse proved a generalisation of this result over number fields. There are further, higher dimensional generalisations, namely, quantitative versions of Schmidt's Subspace Theorem [60] and generalisations by Schlickewei [58], which allow the unknowns to be taken from a number field and which involve both Archimedean and non-Archimedean absolute values. Evertse and Schlickewei and lastly Evertse and Ferretti obtained various sharpenings of Schlickewei's result. We refer only to [25], which contains the sharpest result, as well as a historical overview of the subject.

2 Thue–Mahler equations and S-unit equations

Let $F(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in \mathbb{Z}[X, Y]$ be an irreducible (i.e., over $\mathbb{Q}$) binary form of degree $n \ge 3$. Thue [72] proved that for every positive integer m, the equation

$$F(p, q) = m \tag{8}$$

has only finitely many solutions in integers p, q.

Mahler considerably extended this result. Let $\beta > \beta_0$ where as before $\beta_0 = \min_{s=1,\dots,n-1}\left(\frac{n}{s+1} + s\right)$ and let $P_1, \dots, P_t$ be distinct prime numbers. Put $S := \{\infty, P_1, \dots, P_t\}$. Mahler considered the inequality

$$\prod_{P\in S} |F(p, q)|_P \le |p, q|^{n-\beta} \tag{9}$$

to be solved in integers p, q with $\gcd(p, q) = 1$. In [M17, Satz 2] he proved that this inequality has only finitely many solutions. In [M18, Satz 6] he gave an upper bound for the number of solutions of (9) which we state here in a simplified form.

Theorem 2.1. *The number of solutions of* (9) *is at most* C_4^{t+1}*, where* C_4 *is an effectively computable number that depends only on* F *and* β*, and so is independent of* $P_1, \dots, P_t$*.*

Sketch of proof. Without loss of generality we consider solutions with $q > 0$. Put $f(X) := F(X, 1)$. Then by an elementary argument Mahler [M17, pp. 716–722] shows that for every $P \in M_{\mathbb{Q}} = \{\infty\} \cup \{\text{primes}\}$ there is $c_{F,P}$ with $0 < c_{F,P} \le 1$ such that if p, q are any two coprime integers with $q > 0$, then

$$\begin{aligned} |F(p,q)|_P &\ge c_{F,\infty} M_{F,\infty} |p,q|^n && \text{if } P = \infty, \\ |F(p,q)|_P &\ge c_{F,P} M_{F,P} && \text{if } P \text{ is a prime,} \end{aligned}$$

where

$$M_{F,P} = \begin{cases} 1 \ \text{ if } f(X) \text{ has no zeros in } \mathbb{Q}_P, \\ \min\left(1, \left|\zeta_P - \frac{p}{q}\right|_P\right) \quad \text{otherwise,} \end{cases}$$

with ζ_P the zero of f in $\mathbb{Q}_P$ P-adically closest to p/q. Further, $c_{F,P} = 1$ for all but finitely many P. Hence $c_F := \prod_{P \in M_{\mathbb{Q}}} c_{F,P}$ is positive. Now let S' be the subset of $P \in S$ such that $f(X)$ has roots in $\mathbb{Q}_P$. Let (p, q) be a solution of (2) and for $P \in S'$, let ζ_P be as above. Then

$$|p,q|^{n-\beta} \ge c_F \cdot |p,q|^n \prod_{P \in S'} \min\left(1, \left|\zeta_P - \frac{p}{q}\right|_P\right),$$

that is, (p, q) satisfies (2) with $k = c_F^{-1}$ and S' in place of S for certain roots $\zeta_P \in \mathbb{Q}_P$ of $f(X)$. Now Theorem 2.1 follows from Theorem 1.4, taking into consideration that for every $P \in S'$ there are at most n possibilities for ζ_P. □

We state some immediate consequences. We keep the assumption that F is a binary form with integer coefficients that is irreducible over $\mathbb{Q}$. First note that if in (9) we take $\beta = n$, we get $\prod_{P \in S} |F(p, q)|_P = 1$ and thus,

$$|F(p,q)| = P_1^{z_1} \cdots P_t^{z_t} \tag{10}$$

where $z_1, \dots, z_t$ are non-negative integers. This equation is nowadays called the *Thue–Mahler* equation. Then from Theorem 2.1 we immediately deduce (cf. [M18, Folgerung 1, p. 52]):

Corollary 2.2. *Eq.* (10) *has at most* C_5^{t+1} *solutions in integers* $p, q, z_1, \dots, z_t$ *with* $\gcd(p, q) = 1$*, where* C_5 *is effectively computable and depends only on* F*.*

Another quick consequence gives an upper bound for the number of solutions of (13). Let $P_1, \dots, P_t$ denote the primes dividing m. Let (p, q) be a solution of (13) and let $(p', q') = (p/d, q/d)$ where $d = \gcd(p, q)$. Then $|F(p', q')|$ is composed of primes from $P_1, \dots, P_t$. Further, given (p', q') there is at most one positive integer d such that $(p, q) := (dp', dq')$ satisfies (13). Thus, we obtain the following quantitative version of Thue's Theorem:

Corollary 2.3. *Eq.* (13) *has at most* $C_5^{\omega(m)+1}$ *solutions in integers* p, q*, where* $\omega(m)$ *is the number of prime divisors of* m*.*

We give another result of Mahler, which for later purposes we have reformulated in more modern language. Let $S := \{P_1, \dots, P_t\}$ be a set of primes. An *S-unit* is a rational number of the shape $\pm P_1^{z_1} \cdots P_t^{z_t}$ with $z_1, \dots, z_t \in \mathbb{Z}$. Consider the so-called *S-unit equation*

$$x + y = 1 \quad \text{in } S\text{-units } x, y. \tag{11}$$

Given such a solution, we may write $x = A/C$, $y = B/C$ where A, B, C are integers with $\gcd(A, B, C) = 1$, all composed of primes from S. Subsequently, we can write $A = ap^5$, $B = bq^5$, with a, b from finite sets independent of A, B and p, q coprime integers. Thus, (11) becomes $|ap^5 + bq^5| = P_1^{z_1} \cdots P_t^{z_t}$ with $z_1, \dots, z_t$ non-negative integers. If $-a/b$ is not the fifth power of a rational number then the binary form $aX^5 + bY^5$ is irreducible, in which case we can directly apply Corollary 2.2. Otherwise, there is a factorisation $aX^5 + bY^5 = (a'X + b'Y)G(X, Y)$ where a', b' are integers and $G(X, Y)$ is an irreducible binary form of degree 4 with integral coefficients, and then (11) leads to an equation $|G(p, q)| = P_1^{z_1} \cdots P_t^{z_t}$ to which Corollary 2.2 can be applied. This leads to:

Corollary 2.4. *Equation* (11) *has only finitely many solutions.*

With Mahler's results one can compute an upper bound for the number of solutions of (11), but this does not lead to anything interesting.

In 1961, Lewis and Mahler [M147] obtained explicit versions of Corollaries 2.2 and 2.4. In this paper they proved that if $F(X, Y)$ is a not necessarily irreducible binary form with integer coefficients of degree $n \geq 3$ with non-zero discriminant and with $F(1, 0)F(0, 1) \neq 0$, then (10) has at most

$$(c_1 n H(F))^{\sqrt{n}} + (c_2 n)^{t+1} \tag{12}$$

solutions, where c_1, c_2 are absolute constants. By means of the argument described above, they derived an upper bound for the number of solutions of (11) depending on the primes in the set S, and they posed as an open problem to obtain an upper bound depending only on the cardinality of S. However, the condition $F(1, 0)F(0, 1) \neq 0$ is not necessary in the result of Lewis and Mahler. Indeed, there are integers $u, v \in \{0, \dots, n-1\}$ such that $F(1, u) \neq 0$ and $F(v, uv + 1) \neq 0$. Put $G(X, Y) := F(X + vY, uX + (uv + 1)Y)$. Then

$G(1,0)G(0,1) \neq 0$, and the number of solutions of (10) does not change if we replace F by G, since G is obtained from F by means of a transformation from $\mathrm{SL}_2(\mathbb{Z})$. So we can apply the result of Lewis and Mahler with $F(X,Y) = XY(X+Y)$ and deduce at once that (11) has at most c_3^{t+1} solutions, where c_3 is an absolute constant. Erdős, Stewart and Tijdeman showed in 1998 [20] that this estimate cannot be improved that much. Let ϵ be a positive real number. They proved that if t is sufficiently large in terms of ϵ then there exist a set of primes $S = \{P_1, \ldots, P_t\}$ such that (11) has at least $\exp((4-\epsilon)(t/\log t)^{1/2})$ solutions. In 2007, Konyagin and Soundararajan [48] improved the lower bound to $\exp(t^{2-\sqrt{2}-\epsilon})$.

After the result of Lewis and Mahler it remained as an open problem whether (12) can be replaced by a bound depending only on $n = \deg F$ and t, so independent of the height of F. In his PhD-thesis [21] Evertse established such a bound, though with a much worse dependence on n than (12). Independently of Evertse, Mahler [M215] took up again the study of the number of solutions of Thue equations (13). He proved that if $F(X,Y) \in \mathbb{Z}[X,Y]$ is an irreducible binary form of degree $n \geq 3$ and $|m| \geq (450n^4 H(F)^4)^{n/(n-2)}$, then the Thue equation

$$F(p,q) = m \tag{13}$$

has at most $64n^{\omega(m)+1}$ solutions $p, q \in \mathbb{Z}$ with $\gcd(p,m) = \gcd(q,m) = 1$. Some years later, Bombieri and Schmidt [10] proved, without any condition on m, that (13) has at most $c_0 n^{\omega(m)+1}$ solutions $p, q \in \mathbb{Z}$ with $\gcd(p,q) = 1$, where c_0 is an absolute constant. Let g be a divisor of m, coprime with the discriminant of F, with $g \geq |m|^{\frac{2.5}{n}}$. Stewart [66] showed in 1991 that (13) has at most $4200n^{\omega(g)+1}$ solutions in pairs of coprime integers (p,q). Erdős and Mahler [M47] were the first to estimate the number of solutions of (13) in terms of a divisor g of m. Bombieri improved Evertse's bound for the number of solutions of the Thue–Mahler equation (10) in terms of the degree n of F, and this was subsequently improved by Evertse by a different method. We mention only Evertse's result [24], which asserts that if $F(X,Y)$ is an irreducible binary form of degree $n \geq 3$, then (10) has at most

$$2 \times (10^5 n)^{t+1}$$

solutions. In fact, he proved a generalisation of this for Thue–Mahler equations over number fields. Evertse's result implies that (13) has at most $2 \times (10^5 n)^{\omega(m)+1}$ solutions $p, q \in \mathbb{Z}$, without the requirement $\gcd(p,q) = 1$.

Instead of (11) one may consider the weighted S-unit equation

$$ax + by = 1 \quad \text{in } S\text{-units } x, y, \tag{14}$$

where again $S = \{P_1, \ldots, P_t\}$ with $P_1, \ldots, P_t$ distinct primes, and where a, b are non-zero rationals. Evertse [22] obtained a uniform upper bound for the number of solutions, independent of a, b and the primes in S, i.e., 7^{2t+4}. Again, Evertse

proved a more general result over number fields. A substantial generalisation was obtained by Beukers and Schlickewei [8]. From their result it follows that if a and b are any two complex numbers and Γ is any multiplicative subgroup of $\mathbb{C}^*$ of finite rank r (i.e., r is the maximal number of multiplicatively independent elements that can be chosen from Γ), then the equation

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

has at most $2^{16(r+1)}$ solutions.

Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a binary form of degree $n \geq 3$ which is irreducible over $\mathbb{Q}$, $Z \geq 1$ a real, and $P_1, \ldots, P_t$ distinct primes. Put $S := \{\infty, P_1, \ldots, P_t\}$. Denote by $A_F(Z)$ the number of solutions of the inequality

$$|F(p, q)| \leq Z \quad \text{in } (p, q) \in \mathbb{Z}^2.$$

More generally, denote by $A_{F,S}(Z)$ the number of solutions of

$$\prod_{P \in S} |F(p, q)|_P \leq Z \quad \text{in } (p, q) \in \mathbb{Z}^2 \text{ with } \gcd(p, q, P_1 \cdots P_t) = 1. \tag{15}$$

For instance, taking $Z = 1$ we get the number of pairs (p, q) such that $|F(p, q)|$ is composed of primes from $\{P_1, \ldots, P_t\}$ and $\gcd(p, q, P_1, \ldots, P_t) = 1$.

By a minor modification of the proof of Theorem 2.1 one can show that $A_{F,S}(Z)$ is finite for every Z. Based on unpublished work of Siegel on $A_F(Z)$, Mahler [M19, pp. 93–94] derived an asymptotic formula for $A_{F,S}(Z)$. His result is as follows.

Theorem 2.5. *There is $\sigma_{F,S} > 0$ such that*

$$A_{F,S}(Z) = \sigma_{F,S} Z^{2/n} + O(Z^{1/n}) \text{ as } Z \to \infty \quad \text{if } t_0 = 0,$$
$$A_{F,S}(Z) = \sigma_{F,S} Z^{2/n} + O(Z^{1/(n-1)} (\log Z)^{t_0 - 1}) \text{ as } k \to \infty \quad \text{if } t_0 > 0,$$

where t_0 is the number of $P \in S$ such that $F(X, 1)$ has a zero in $\mathbb{Q}_P$, and where the implied constants depend on F and S.

We mention that with Mahler's proof the implied constants cannot be computed effectively.

In the special case $S = \{\infty\}$, i.e., if there are no primes, Theorem 2.5 asserts that there is $\sigma_F > 0$ such that $A_F(Z) = \sigma_F Z^{2/n} + O(Z^{1/(n-1)})$ if $F(X, 1)$ has a real root, and $A_F(Z) = \sigma_F Z^{2/n} + O(Z^{1/n})$ if $F(X, 1)$ has no real root. Here, σ_F is the area of the set of $(x, y) \in \mathbb{R}^2$ with $|F(x, y)| \leq 1$ and $\sigma_F Z^{2/n}$ is the area of $(x, y) \in \mathbb{R}^2$ with $|F(x, y)| \leq Z$.

For arbitrary S, Mahler expressed $\sigma_{F,S}$ as a product of local factors $\prod_{P \in S} \sigma_{F,P}$. Another formulation of $\sigma_{F,S}$ is as follows. Let $\mu^r = \mu^r_\infty$ be the Lebesgue measure on $\mathbb{R}^r$, normalised such that $\mu^r_\infty([0, 1]^r) = 1$, for a prime P let μ^r_P be the Haar measure on $\mathbb{Q}^r_P$ normalised such that $\mu^r_P(\mathbb{Z}^r_P) = 1$ and subsequently

let μ_S^r be the product measure on $\mathbb{A}_S^r := \prod_{P\in S} \mathbb{Q}_P^r$. Write elements of this product as $(\mathbf{x}_P)_{P\in S}$ where $\mathbf{x}_P \in \mathbb{Q}_P^r$ and for $\mathbf{x}_P = (x_1, \dots, x_r) \in \mathbb{Q}_P^r$, write $|\mathbf{x}_P|_P := \max_i |x_i|_P$. Define the sets

$$\mathcal{S}_{F,S}(Z) := \Big\{(\mathbf{x}_P)_{P\in S} \in \mathbb{A}_S^2 : \prod_{P\in S} |F(\mathbf{x}_P)|_P \le Z, \\ |\mathbf{x}_P|_P = 1 \text{ for } P \in S \setminus \{\infty\}\Big\}$$

and $\mathcal{S}_{F,S} := \mathcal{S}_{F,S}(1)$. Then $\sigma_{F,S} = \mu_S^2(\mathcal{S}_{F,S})$ and $\sigma_{F,S} Z^{2/n} = \mu_S^2(\mathcal{S}_{F,S}(Z))$ for $Z > 0$. If we identify $\mathbf{x} \in \mathbb{Z}^2$ with $(\mathbf{x})_{P\in S} \in \mathbb{A}_S^2$, then $A_{F,S}(Z)$ counts the number of lattice points in $\mathcal{S}_{F,S}(Z)$, and Theorem 2.5 states in a more precise form that this number is approximately the measure of $\mathcal{S}_{F,S}(Z)$.

Sketch of proof of Theorem 2.5. We give a very brief outline of Mahler's lengthy proof. Mahler divides the solutions (p, q) of (15) into *large* solutions, i.e., with $|p, q| \ge (4Z)^{1/(n-2)}$, *medium* solutions, i.e., with $Z^{1/(n-1)} \le |p, q| < (4Z)^{1/(n-2)}$, and *small* solutions, i.e., with $|p, q| < Z^{1/(n-1)}$. Mahler estimates the number of large numbers using the approximation techniques discussed in the previous section, and the number of medium solutions by means of an elementary argument based on congruences and continued fractions. As it turns out, both the numbers of large and medium solutions go into the error term. Then Mahler estimates the number of small solutions by combining congruence results for binary forms with elementary estimates for the difference between the number of lattice points in a bounded two-dimensional region and the area of that region. □

Since we know that for the number of solutions of the Thue–Mahler equation we have an upper bound independent of the coefficients of the involved binary form F, one may wonder whether $A_{F,S}(Z)$ can be estimated from above independently of the coefficients of F. More precisely, one may ask whether $\sigma_{F,S}$ and the implied constant of the error term can be estimated from above independently of F.

Some progress has been made on these problems. Bean [6] showed that if $F(X, Y) \in \mathbb{R}[X, Y]$ is a binary form of degree $n \ge 3$ with discriminant $D(F) \ne 0$, then $\sigma_F \le 16|D(F)|^{-1/n(n-1)}$. Thunder [73] proved that if $F(X, Y) \in \mathbb{Z}[X, Y]$ is a cubic binary form which is irreducible over $\mathbb{Q}$, then

$$|A_F(Z) - Z^{2/3}\sigma_F| < 9 + \frac{2000k^{1/3}}{|D(F)|^{1/2}} + 3156Z^{1/3}.$$

Later, Thunder proved some general results for inequalities involving decomposable forms. Specialised to binary forms, these results imply that if $F(X, Y) \in \mathbb{Z}[X, Y]$ is a binary form of degree n with non-zero discriminant, having no linear factor over $\mathbb{Q}$, then for all $Z \ge 1$ we have

$$A_F(Z) \le c_1(n)Z^{2/n} \quad \text{if } n \ge 3 \text{ [74]},$$
$$|A_F(Z) - \sigma_F Z^{2/n}| \le c_2(n)Z^{2/(n+1)} \quad \text{if } n \ge 3,\ n \text{ odd [75]},$$

where $c_1(n)$, $c_2(n)$ are effectively computable and depend on n only. An estimate with error term depending only on n and Z has not been deduced yet for even n.

In his PhD-thesis [51], Liu generalised the work of Thunder on decomposable forms to the p-adic case. We mention some consequences for binary forms. Let $P_1, \dots, P_t$ be distinct primes, $S = \{\infty, P_1, \dots, P_t\}$ and $F(X,Y) \in \mathbb{Z}[X,Y]$ a binary form of degree n with non-zero discriminant and without linear factor over $\mathbb{Q}$. Then

$$\sigma_{F,S} \le c_1(n,S), \quad A_{F,S}(Z) \le c_2(n,S) Z^{2/n} \quad \text{if } n \ge 3,$$
$$|A_{F,S} - \sigma_{F,S} Z^{2/n}| \le c_3(n,S) Z^{2/(n+1)} (1+\log Z)^{2n(t+1)} \quad \text{if } n \ge 3,\ n \text{ odd},$$

where the $c_i(n,S)$ are effectively computable and depend only on n and S. The constants $c_i(n,S)$ that arise from Liu's proof depend on the sizes of the primes in S. Another open problem is, whether the $c_i(n,S)$ can be replaced by numbers depending only on n and the cardinality of S.

Let F be a binary form with integer coefficients, non-zero discriminant and degree n with $n \ge 3$. For any positive number Z let $\mathcal{R}_F(Z)$ denote the set of non-zero integers h with $|h| \le Z$ for which there exist integers p and p with $F(p,q) = h$. Denote the cardinality of a set $\mathcal{A}$ by $|\mathcal{A}|$ and put $R_F(Z) := |\mathcal{R}_F(Z)|$. In 1938, Erdős and Mahler [M47] proved that if F is irreducible over $\mathbb{Q}$ then there exist positive numbers c_1 and c_2, which depend on F, such that

$$R_F(Z) > c_1 Z^{\frac{2}{n}}$$

for $Z > c_2$. In 1967, Hooley [43] determined the asymptotic growth rate of $R_F(Z)$ when F is an irreducible binary cubic form with discriminant which is not a square. He proved that

$$R_F(Z) = \sigma_F Z^{\frac{2}{3}} + O\left(Z^{\frac{2}{3}} (\log\log Z)^{-\frac{1}{600}}\right). \tag{16}$$

In 2000, Hooley [46] obtained an asymptotic estimate for $R_F(Z)$ in the case when the discriminant is a perfect square. Hooley [45] also obtained such an estimate for quartic forms of the shape

$$F(X,Y) = aX^4 + 2bX^2Y^2 + cY^4$$

and for forms which are the product of linear factors over the rationals [47]. Several authors, including Bennett, Dummigan, and Wooley [7], Browning [11], Greaves [36], Heath-Brown [42], Hooley [44], Skinner and Wooley [65] and Wooley [76], obtained an asymptotic estimate for $R_F(Z)$ when F is a binomial form. Stewart and Xiao [70] have recently proved that if F is a binary form with integer coefficients, non-zero discriminant and degree n with $n \ge 3$ then there is a positive number C_F such that $R_F(Z)$ is asymptotic to $C_F Z^{\frac{2}{n}}$. In the case that the form F is irreducible over the rationals a key ingredient in the

proof is Theorem 2.5. When F is reducible one appeals to a special case of a result of Thunder [74].

Let k be an integer with $k \geq 2$. An integer is said to be k-free if it is not divisible by the k-th power of a prime number. For any positive number Z let $\mathcal{R}_{F,k}(Z)$ denote the set of k-free integers h with $|h| \leq Z$ for which there exist integers p and q such that $F(p,q) = h$ and put $R_{F,k}(Z) := |\mathcal{R}_{F,k}(Z)|$. Gouvêa and Mazur [34] in 1991 proved that if there is no prime P such that P^2 divides $F(a,b)$ for all pairs of integers (a,b), if all the irreducible factors of F over $\mathbb{Q}$ have degree at most 3 and if ϵ is a positive real number then there are positive numbers C_1 and C_2, which depend on ϵ and F, such that if Z exceeds C_1 then

$$R_{F,2}(Z) > C_2 Z^{\frac{2}{n}-\epsilon}. \tag{17}$$

This was subsequently extended by Stewart and Top in [69]. Let r be the largest degree of an irreducible factor of F over $\mathbb{Q}$. Let k be an integer with $k \geq 2$ and suppose that there is no prime P such that P^k divides $F(a,b)$ for all integer pairs (a,b). They showed, by utilising an argument of Greaves [35] and the result of Erdős and Mahler [M47], that if k is at least $(r-1)/2$ or $k = 2$ and $r = 6$ then there are positive numbers C_3 and C_4, which depend on k and F, such that if Z exceeds C_3 then

$$R_{F,k}(Z) > C_4 Z^{\frac{2}{n}}. \tag{18}$$

The estimates of Gouvêa and Mazur and of Stewart and Top were used to count the number of twists of an elliptic curve defined over the rationals for which the rank of the group of rational points on the curve is at least 2.

Let F be a binary form with integer coefficients, non-zero discriminant and degree d with d at least 3 and let r denote the largest degree of an irreducible factor of F over the rationals. Let k be an integer with $k \geq 2$ and suppose again that there is no prime P such that P^k divides $F(a,b)$ for all pairs of integers (a,b). Stewart and Xiao [71] proved that there is a positive number $C_{F,k}$ such that $R_{F,k}(Z)$ is asymptotic to $C_{F,k} Z^{\frac{2}{n}}$ provided that k exceeds $\frac{7r}{18}$ or (k,r) is $(2,6)$ or $(3,8)$. For a positive number Z we put

$$\mathcal{N}_{F,k}(Z) := \{(p,q) \in \mathbb{Z}^2 : F(p,q) \text{ is } k\text{-free and } 1 \leq |F(p,q)| \leq Z\}$$

and

$$N_{F,k}(Z) := |\mathcal{N}_{F,k}(Z)|.$$

For each positive integer m we put

$$\rho_F(m) := |\{(i,j) \in \{0, \cdots, m-1\}^2 : F(i,j) \equiv 0 \pmod{m}\}|$$

and

$$\lambda_{F,k} := \prod_P \left(1 - \frac{\rho_F(P^k)}{P^{2k}}\right),$$

where the product is taken over the primes P. A first step in the proof of the estimate for $R_{F,k}(Z)$ is to estimate $N_{F,k}(Z)$ provided that k exceeds $\frac{7r}{18}$ or (k,r) is $(2,6)$ or $(3,8)$. Stewart and Xiao [71] proved that under this assumption

$$N_{F,k}(Z) \sim \lambda_{F,k}\sigma_F Z^{\frac{2}{n}} \tag{19}$$

which extends Mahler's result [M19].

3 Cubic Thue equations with many solutions

Chowla [15] was the first to show that there are cubic Thue equations with many solutions. He proved in 1933 that there is a positive number c_0 such that if k is a non-zero integer then the number of solutions of $p^3 - kq^3 = m$ in integers p and q is at least $c_0 \log\log m$ for infinitely many positive integers m. This was refined by Mahler [M28] in 1935. Let $F(X,Y)$ be a cubic binary form with integer coefficients and non-zero discriminant. Let m be a non-zero integer and consider the equation

$$F(p,q) = m, \tag{20}$$

in integers p and q. Mahler proved that there is a positive number c_1, which depends on F, such that for infinitely many positive integers m equation (20) has at least

$$c_1(\log m)^{1/4} \tag{21}$$

solutions. In 1983, Silverman [64] proved that the exponent of $1/4$ in (21) can be improved to $1/3$. Silverman streamlined the approach of Mahler by introducing the theory of height functions on elliptic curves into the argument. Chowla, Mahler and Silverman obtained their results by viewing (20), when it has a rational point, as defining an elliptic curve E and then by constructing, from rational points on E, integers m' for which $F(p,q) = m'$ has many solutions in integers p and q. The solutions (p,q) constructed by this method have very large common factors. By showing that it is always possible to find a twist of E for which the rank of the group of rational points is at least 2 Stewart [67] was able to make a further improvement on Mahler's result. He showed that (21) holds with $1/4$ replaced by $1/2$. In addition Stewart [68], utilising some elliptic curves whose group of rational points has rank 12 discovered by Quer [54], showed that there are infinitely many cubic binary forms with integer coefficients, content 1 and non-zero discriminant which are inequivalent under the action of $GL(2,\mathbb{Z})$ and for which the estimate (21) applies with $1/4$ replaced by $6/7$.

4 S-integral points on elliptic curves

In his celebrated paper [63], Siegel proved that non-singular affine plane curves of genus at least 1 over $\mathbb{Q}$ have only finitely many points in $\mathbb{Z}^2$. In fact, he proved a more general result for curves defined over a number field. Mahler

[M21] proved a generalisation to S-integers in a special case, namely for curves of genus 1 over $\mathbb{Q}$. We state his result. In what follows, $S = \{P_1, \ldots, P_t\}$ is a finite set primes and $\mathbb{Z}_S$ is the corresponding ring of S-integers, i.e., the ring of rational numbers whose denominators do not contain any prime factor different from $P_1, \ldots, P_t$.

Theorem 4.1. *Let $f \in \mathbb{Q}[X, Y]$ be such that $f(x, y) = 0$ defines a non-singular affine algebraic curve of genus 1. Then there are only finitely many $x, y \in \mathbb{Z}_S$ with $f(x, y) = 0$.*

In his proof, Mahler closely follows Siegel and uses his own Theorem 1.1 instead of Siegel's approximation theorem.

Sketch of proof. Mahler proves in fact an essentially equivalent result, invariant under birational transformations over $\mathbb{Q}$, which in more modern form may be stated as follows:

let E be a non-singular projective curve of genus 1 over $\mathbb{Q}$ and $g \in \mathbb{Q}(E)$ a non-constant rational function on E over $\mathbb{Q}$; then the set of $\mathbf{p} \in E(\mathbb{Q})$ with $g(\mathbf{p}) \in \mathbb{Z}_S$ is finite.

Assume on the contrary that this set is infinite. After a birational transformation over $\mathbb{Q}$ we may assume that E is an elliptic curve with Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$ and point O at infinity. Fix an integer n which is later chosen to be sufficiently large. By the weak Mordell–Weil theorem, the quotient group $E(\mathbb{Q})/nE(\mathbb{Q})$ is finite. Hence there is $\mathbf{p}_0 \in E(\mathbb{Q})$ such that the set A_n of $\mathbf{p} \in E(\mathbb{Q})$ with $g(\mathbf{p}_0 + n\mathbf{p}) \in \mathbb{Z}_S$ is infinite. Suppose that g has degree r and let h be the maximum of the orders of its poles. Then $g_n : \mathbf{p} \mapsto g(\mathbf{p}_0 + n\mathbf{p})$ is a rational function on E defined over $\mathbb{Q}$ of degree $n^2 r$, whose poles still have order at most h. Let $\varphi : (x, y) \mapsto \frac{ax+b}{cx+d}$ with $a, b, c, d \in \mathbb{Q}$ with $ad - bc \neq 0$ be such that $\varphi(\mathbf{q}) \neq \infty$ for every pole $\mathbf{q}$ of g on E. By a straightforward generalisation of Siegel's arguments, Mahler shows that there are $P \in S' := S \cup \{\infty\}$, a pole $\mathbf{q} \in E(\overline{\mathbb{Q}_P})$ of g_n and infinitely many $\mathbf{p} \in A_n$ such that

$$|\varphi(\mathbf{q}) - \varphi(\mathbf{p})|_P \leq H(\varphi(\mathbf{p}))^{-n^2 r/6|S'|h},$$

where $H(p/q) := \max(|p|, |q|)$ for $p, q \in \mathbb{Z}$ with $q > 0$ and $\gcd(p, q) = 1$. The number $\varphi(\mathbf{q})$ is algebraic of degree at most $n^2 r$ since $\mathbf{q}$ is a pole of g_n and g_n has degree at most $n^2 r$. If we choose n large enough so that $n^2 r/6|S'|h > 2\sqrt{n^2 r} = 2n\sqrt{r}$, we obtain a contradiction with Theorem 1.1. □

Siegel treated the case of curves of genus larger than 1 by embedding such a curve in its Jacobian, applying the Mordell–Weil theorem to this Jacobian, and using a simultaneous Diophantine approximation argument. After Roth's approximation theorem and height theory became available, Siegel's method of proof could be greatly simplified. Lang [49] worked this out and obtained a version of Siegel's theorem for curves of arbitrary genus $g \geq 1$ over a number field K, implying that for every finite set of places S of K, such a curve has only

finitely S-integral points. For curves over K of genus > 1 this was of course superseded by Faltings [29], who proved that such curves have only finitely many K-rational points. The booklet [77] contains a translation into English by Fuchs of Siegel's paper [63], and a paper by Fuchs and Zannier giving an overview of several methods of proof of Siegel's theorem, including one by Corvaja and Zannier, which uses Schmidt's Subspace Theorem instead of the Mordell–Weil theorem.

5 Effective finiteness results for Thue equations, Thue–Mahler equations and unit equations

Consider again the Thue equation

$$F(p,q) = m \quad \text{in integers } p,q \tag{22}$$

and the Thue–Mahler equation

$$|F(p,q)| = P_1^{z_1} \cdots P_t^{z_t} \quad \text{in integers } p,q,z_1,\ldots,z_t \text{ with } \gcd(p,q) = 1, \tag{23}$$

where $F(X,Y)$ is an irreducible binary form of degree ≥ 3 with coefficients in $\mathbb{Z}$, m a non-zero integer and $P_1,\ldots,P_t$ a set of $t \geq 0$ distinct primes. The proofs of the finiteness theorems of Thue [72] and Mahler [M17, M18] concerning equations (22) and (23), respectively, were ineffective, i.e. did not provide any algorithm for determining the solutions of these equations.

The first effective proof for Thue theorem was given by Baker [4] and subsequently, for Mahler's theorem, by Coates [16, 17]. They obtained explicit upper bounds for $|p,q|$, the maximum of the absolute values of the solutions p,q.

Baker's proof is based on his effective lower bounds for linear forms in the logarithms of algebraic numbers. Gel'fond [31] and Schneider [61] proved independently of each other that if α and β are algebraic numbers such that $\alpha \neq 0,1$ and β is not rational, then α^β is transcendental. An equivalent formulation of this theorem is that if α_1,α_2 are non-zero algebraic numbers such that $\log\alpha_1$ and $\log\alpha_2$ are linearly independent over $\mathbb{Q}$, then they are linearly independent over $\overline{\mathbb{Q}}$. Further, Gel'fond [33] gave a non-trivial effective lower bound for $|\beta_1\log\alpha_1 + \beta_2\log\alpha_2|$, where β_1,β_2 denote algebraic numbers, not both 0, and α_1,α_2 denote algebraic numbers different from 0 and 1 such that $\log\alpha_2/\log\alpha_2$ is not rational. Baker [1, 2, 3] generalised the Gel'fond–Schneider theorem to arbitrary many logarithms and provided non-trivial effective lower bounds for $|\beta_1\log\alpha_1 + \cdots + \beta_k\log\alpha_k|$, where $\alpha_1,\ldots,\alpha_k$ are non-zero algebraic numbers such that $\log\alpha_1,\ldots,\log\alpha_k$ are linearly independent over $\mathbb{Q}$ and $\beta_1,\ldots,\beta_k$ are algebraic numbers, not all zero.

Baker's effective estimates for logarithmic forms led to significant applications in Diophantine equations and other parts of number theory. Baker [4] showed that $|p,q| \leq C$ for every solution p,q of (22), with an explicitly given C depending only on m and the degree and height of F.

Mahler [M30] proved a P-adic analogue of the Gel'fond–Schneider theorem. Gel'fond [33] gave an effective estimate for linear forms in two P-adic logarithms which was generalised by Coates [16] to arbitrarily many P-adic logarithms. Using his estimate, Coates [17] proved that $|p, q| \leq C'$ for every solution $p, q, z_1, \ldots, z_t$ of (23), with an explicit bound C' depending only on t, the maximum of the primes $P_1, \ldots, P_t$ and the degree and height of F.

Baker's and Coates' bounds for linear forms in logarithms and for the solutions of (22) and (23) were later improved by many people; for references see e.g. Baker and Wüstholz [5] and Bugeaud [12]. The best known bounds for (22) and (23), proved over number fields, are due to Bugeaud and Győry [14] and Győry and Yu [41]. In [14] it is proved that all solutions p, q of (22) satisfy

$$|p, q| < \exp\{c(n)H^{2n-2}(\log H)^{2n-1} \log M\},$$

where $c(n) = 3^{3(n+9)}n^{18(n+1)}$, and $M, H(\geq 3)$ are upper bounds for $|m|$ and for the maximum absolute value of the coefficients of F, respectively. A similar upper bound is given in [14] for the solutions of (23), but that bound depends also on t and the maximum of $P_1, \ldots, P_t$. In terms of $c(n)$ and H better bounds are obtained in [41] which depend, however, on some parameters of the splitting field of F. We note that the exponential dependence is a consequence of the exponential character of the bounds for linear forms in logarithms.

Effective generalisations to equations over finitely generated domains can be found in Bérczes, Evertse and Győry [9].

Mahler's finiteness result [M17] concerning equation (23) implies that the greatest prime factor $P(F(p, q))$ of $F(p, q)$ at integral points (p, q) tend to infinity as $|p, q| \to \infty$. Coates [17] deduced from his effective theorem mentioned above the first general effective lower bound for $P(F(p, q))$ by showing that

$$P(F(p, q)) \gg (\log_2 |p, q|)^{1/4}. \tag{24}$$

Here and below $\log_i$ denotes the ith iterate of the logarithmic function with $\log_1 = \log$. The lower estimate (24) was improved by several authors; the best known estimate, due to Győry and Yu [41], is

$$P(F(p, q)) \gg \log_2 |p, q| \cdot \frac{\log_3 |p, q|}{\log_4 |p, q|}. \tag{25}$$

In (24) and (25) the constants implied by $\gg$ are effective and depend only on the degree and height of F. We note that (25) was established in a more general form, over number fields.

From Coates' explicit upper bound for the solutions of equation (23) one can easily deduce an explicit upper bound for the solutions of the S-unit equation (11) and its weighted version (14) over $\mathbb{Q}$. The first explicit bounds for the solutions of S-unit equations over number fields were obtained by Győry [37, 39]. These bounds were later improved by several people and led to many applications;

see e.g. Evertse and Győry [28] and the references given there. The best known bounds over number fields are due to Győry and Yu [41]. For effective generalisations to unit equations over finitely generated domains, see Evertse and Győry [27].

6 Higher dimensional generalisations of Thue equations, Thue–Mahler equations and unit equations

Let again $S = \{P_1, \dots, P_t\}$ be a set of $t \geq 0$ primes, and denote by $\mathbb{Z}_S$ the ring of S-integers in $\mathbb{Q}$, i.e. those rational numbers whose denominators do not contain any prime factor different from $P_1, \dots, P_t$. We consider decomposable form equations of the form

$$F(q_1, \dots, q_n) = m \quad \text{in} \quad q_1, \dots, q_n \in \mathbb{Z}_S, \tag{26}$$

where $m \in \mathbb{Z}_S \setminus \{0\}$ and $F \in \mathbb{Z}[X_1, \dots, X_n]$ is a decomposable form, i.e. a homogeneous polynomial which factorises into linear factors over $\overline{\mathbb{Q}}$.

Decomposable form equations are of basic importance in Diophantine number theory. For $n = 2$, equation (26) can be written in the form (23) and if F is irreducible and of degree ≥ 3, Mahler's result applies. Conversely, equation (23) can be easily reduced to finitely many equations of the shape (26). For $n \geq 2$, further important classes of decomposable form equations are norm form equations, discriminant form equations and index form equations. For norm form equations over $\mathbb{Q}$ Schmidt [59] (case $t = 0$), Schlickewei [57] (case $t \geq 0$), and over number fields Laurent [50] obtained finiteness results for equation (26), thereby considerably generalising Mahler's finiteness theorem on equation (23). For discriminant form equations and index form equations Győry [38, 40] provided finiteness criteria. The proofs in [59], [57] and [50] are ineffective because they depend of Schmidt's Subspace Theorem and its p-adic generalisation, while the proofs in [38], [40] are based on Baker's effective theory of logarithmic forms, hence are effective.

Evertse and Győry [26] gave a general finiteness criterion for equation (26). Let $\mathcal{L}$ be a maximal set of pairwise linearly independent linear factors of F over $\overline{\mathbb{Q}}$. A non-zero subspace V of the $\mathbb{Q}$-vector space $\mathbb{Q}^n$ is said to be *$\mathcal{L}$-non-degenerate* or *$\mathcal{L}$-degenerate* according as $\mathcal{L}$ does or does not contain a subset of at least three linear forms which are linearly dependent on V, but pairwise linearly independent on V. In particular, V is $\mathcal{L}$-degenerate if V has dimension 1. We call V *$\mathcal{L}$-admissible* if no form in $\mathcal{L}$ is identically zero on V. Evertse and Győry [26] proved that the following two statements are equivalent:

(i) Every $\mathcal{L}$-admissible subspace of $\mathbb{Q}^n$ of dimension ≥ 2 is $\mathcal{L}$-non degenerate.

(ii) For any finite set S of primes and any non-zero $m \in \mathbb{Z}_S$, equation (26) has only finitely many solutions.

This was proved in a more general form, over finitely generated domains over $\mathbb{Z}$.

The proof of the above finiteness criterion depends on the following finiteness result on multivariate unit equations of the form

$$a_1u_1 + \cdots + a_nu_n = 1 \quad \text{in} \quad u_1, \ldots, u_n \in \Gamma, \tag{27}$$

where $a_1, \ldots, a_n$ are non-zero elements of a number field K and Γ is a finitely generated subgroup of K^*. This equation is a generalisation of (14). A solution $u_1, \ldots, u_n$ of (27) is called *degenerate* if there is a vanishing subsum on the left hand side of (27). In this case (27) has infinitely many solutions if Γ is infinite. As a considerable generalisation of Mahler's finiteness theorem on S-unit equations (14), van der Poorten and Schlickewei [53] and independently Evertse [23] proved that equation (27) has only finitely many non-degenerate solutions. As is pointed out in Evertse and Győry [26], this theorem and the implication $(i) \Rightarrow (ii)$ concerning equation (26) are equivalent statements. For further related results, including bounds for the number of solutions, applications and references, see Evertse and Győry [28].

References

[M17] K. Mahler, *Zur Approximation algebraischer Zahlen, I: Über den größten Primteiler binärer Formen*, Math. Ann. 107 (1933), 691–730.

[M18] K. Mahler, *Zur Approximation algebraischer Zahlen, II: Über die Anzahl der Darstellungen ganzer Zahlen durch Binärformen*, Math. Ann. 108 (1933), 37–55.

[M19] K. Mahler, *Zur Approximation algebraischer Zahlen, III*, Acta Math. 62 (1934), 91–166.

[M21] K. Mahler, *Über rationalen Punkte auf Kurven vom Geschlecht Eins*, J. Reine Angew. Math. (Crelle) 170 (1934), 168–178.

[M28] K. Mahler, *On the lattice points on curves of genus 1*, Proc. London Math. Soc. (2) 39 (1935), 431–466 and 40 (1935), 558.

[M30] K. Mahler, *Über transzendente P-adische Zahlen*, Compositio Math. 2 (1935), 259–275.

[M47] P. Erdős and K. Mahler, *On the number of integers which can be represented by a binary form*, J. London Math. Soc. 13 (1938), 134–139.

[M147] D. J. Lewis and K. Mahler, *On the representation of integers by binary forms*, Acta Arithm. 6 (1961), 333–363.

[M215] K. Mahler, *On Thue's theorem*, Math. Scand. 55 (1984), 188–200.

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika 13 (1966), 204–216.

[2] A. Baker, *Linear forms in the logarithms of algebraic numbers, II*, Mathematika 14 (1967), 102–107.

[3] A. Baker, *Linear forms in the logarithms of algebraic numbers, IV*, Mathematika 15 (1968), 204–216.

[4] A. Baker, *Contributions to the theory of Diophantine equations*, Philos. Trans. Roy. Soc. London, Ser A 263 (1968), 173–208.

[5] A. Baker and G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, Cambridge University Press, 2007.

[6] M. A. Bean, *An isoperimetric inequality for the area of plane regions defined by binary forms*, Compos. Math. 92 (1994), 115–131.

[7] M. A. Bennett, N. P. Dummigan, and T. D. Wooley, *The representation of integers by binary additive forms*, Compositio Mathematica 111 (1998), 15–33.

[8] F. Beukers and H. P. Schlickewei, *The equation $x + y = 1$ in finitely generated groups*, Acta Arith. 78 (1996), 189–199.

[9] A. Bérczes, J.-H. Evertse, and K. Győry, *Effective results for Diophantine equations over finitely generated domains*, Acta Arith. 163 (2014), 71–100.

[10] E. Bombieri and W. M. Schmidt, *On Thue's equation*, Invent. Math. 88 (1987), 69–81.

[11] T. D. Browning, *Equal sums of two kth powers*, J. Number Theory 96 (2002), 293–318.

[12] Y. Bugeaud, *Linear Forms in Logarithms and Applications*, European Math. Soc. 2018.

[13] Y. Bugeaud and J.-H. Evertse, *On two notions of complexity of algebraic numbers*, Acta Arith. 133 (2008), 221–250 (volume dedicated to Wolfgang Schmidt on the occasion of his 75th birthday).

[14] Y. Bugeaud and K. Győry, *Bounds for the solutions of Thue–Mahler equations and norm form equations*, Acta Arith. 74 (1996), 273–292.

[15] S. D. Chowla, *Contributions to the analytic theory of numbers (II)*, J. Indian Math. Soc. 20 (1933) 121–128.

[16] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), 279–305.

[17] J. Coates, *An effective p-adic analogue of a theorem of Thue II, The greatest prime factor of a binary form*, Acta Arith. 16 (1970), 392–412.

[18] H. Davenport and K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 160–167.

[19] F. J. Dyson, *The approximation of algebraic numbers by rationals*, Acta Math. 79 (1947), 225–240.

[20] P. Erdős, C. L. Stewart, and R. Tijdeman, *Some diophantine equations with many solutions*, Compositio Math. 66 (1988), 37–56.

[21] J.-H. Evertse, *Upper bounds for the numbers of solutions of Diophantine equations*, PhD-thesis, Leiden, 1983, also published as MC-tract 168, Centrum voor Wiskunde en Informatica, Amsterdam, 1983.

[22] J.-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. 75 (1984), 561–584.

[23] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compos. Math. 53 (1984), 225–244.

[24] J.-H. Evertse, *The number of solutions of the Thue-Mahler equation*, J. Reine Angew. Math. 482 (1997), 121–149.

[25] J.-H. Evertse and R. G. Ferretti, *A further improvement of the Quantitative Subspace Theorem*, Ann. Math. 177 (2013), 513–590.

[26] J.-H. Evertse and K. Győry, *Finiteness criteria for decomposable form equations*, Acta Arith. 50 (1988), 357–379.

[27] J.-H. Evertse and K. Győry, *Effective results for unit equations over finitely generated domains*, Math. Proc. Camb. Phil. Soc. 154 (2013), 351–380.

[28] J.-H. Evertse and K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge University Press, 2015.

[29] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366; *Erratum*, ibidum 75 (1984), 381.

[30] A. O. Gel'fond, *Transcendental and algebraic numbers*, Dover, New York, 1960.

[31] A. O. Gel'fond, *Sur le septième problème de Hilbert*, Izv. Akad. Nauk SSSR 7 (1934), 623–630.

[32] A. O. Gel'fond, *On approximating transcendental numbers by algebraic numbers*, Dokl. Akad. Nauk SSSR 2 (1935), 177–182.

[33] A. O. Gel'fond, *Sur la divisibilité de la différence des puissances de deux nombres premiers par une puissance d'un idéal premier*, Mat. Sbornik 7 (1940), 7–26.

[34] F. Q. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, Journal of the American Mathematical Society, (1) 4 (1991), 793–805.

[35] G. Greaves, *Power-free values of binary forms*, Quart. J. Math, (2) 43 (1992), 45–65.

[36] G. Greaves, *Representation of a number by the sum of two fourth powers*, Mat. Zametki 55 (1994), 47–58.

[37] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné II*, Publ. Math. Debrecen 21 (1974), 125–144.

[38] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné III*, Publ. Math. Debrecen 23 (1976), 141–165.

[39] K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. 54 (1979), 583–600.

[40] K. Győry, *On S-integral solutions of norm form, discriminant form and index form equations*, Studia Sci. Math. Hungar. 16 (1981), 149–161.

[41] K. Győry and K. Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith. 123 (2006), 9–41.

[42] D. R. Heath-Brown, *The density of rational points on cubic surfaces*, Acta Arith. 79 (1997), 17–30.

[43] C. Hooley, *On binary cubic forms*, J. Reine Angew. Math. 226 (1967), 30–87.

[44] C. Hooley, *On another sieve method and the numbers that are a sum of two h^{th} powers*, Proc. London Math. Soc. 43 (1981), 73–109.

[45] C. Hooley, *On binary quartic forms*, J. Reine Angew. Math. 366 (1986), 32–52.

[46] C. Hooley, *On binary cubic forms: II*, J. Reine Angew. Math. 521 (2000), 185–240.

[47] C. Hooley, *On totally reducible binary forms: II*, Hardy-Ramanujan Journal 25 (2002), 22–49.

[48] S. Konyagin and K. Soundararajan, *Two S-unit equations with many solutions*, J. Number Theory 124 (2007), 193–199.

[49] S. Lang, *Integral points on curves*, Inst. Hautes Études Sci. Publ. Math. 6 (1960), 27–43.

[50] M. Laurent, *Équations diophantines exponentielles*, Invent. Math. 78 (1984), 299–327.

[51] J. Liu, *On p-adic Decomposable Form Inequalities*, PhD-thesis, Leiden, 2015.

[52] C. J. Parry, *The $\mathfrak{p}$-adic generalisation of the Thue-Siegel theorem*, Acta Math. 83 (1950), 1–100.

[53] A. J. van der Poorten and H. P. Schlickewei, *The growth condition for recurrence sequences*, Macquarie Univ. Math. Rep. 82–0041 (1982).

[54] J. Quer, *Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12*, C.R. Acad. Sci. Paris 305 (1987) 215–218.

[55] D. Ridout, *Rational approximations to algebraic numbers*, Mathematika 4 (1957), 125–131.

[56] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 1–20; corrigendum, 168.

[57] H. P. Schlickewei, *On norm form equations*, J. Number Theory 9 (1977), 370–380.

[58] H. P. Schlickewei, *The quantitative subspace theorem for number fields*, Compos. Math. 82 (1992), 245–273.

[59] W. M. Schmidt, *Linearformen mit algebraischen Koefficienten II*, Math. Ann. 191 (1971), 1–20.

[60] W. M. Schmidt, *The subspace theorem in Diophantine approximations*, Compos. Math. 69 (1989), 121–173.

[61] T. Schneider, *Transzendenzuntersuchungen periodischer Funktionen; I Transzendenz von Potenzen; II Transzendenzeigenschaften elliptischer Funktionen*, J. Reine Angew. Math. 172 (1934), 65–74.

[62] C. L. Siegel, *Approximation algebraischer Zahlen*, Math. Zeitschr. 10 (1921), 173–213.

[63] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuß. Akad. Wissensch. Phys.-math. Klasse = Ges. Abh. Bd. I, Springer Verlag 1966, 209–266.

[64] J. H. Silverman, *Integer points on curves of genus 1*, J. London Math. Soc. 28 (1983) 1–7.

[65] C. Skinner and T. D. Wooley, *Sums of two k-th powers*, J. Reine Angew. Math. 462 (1995), 57–68.

[66] C. L. Stewart, *On the number of solutions to polynomial congruences and Thue equations*, J. Amer. Math. Soc. (4) 4 (1991), 793–835.

[67] C. L. Stewart, *Cubic Thue equations with many solutions*, Int. Math. Res. Not. IMRN (2008), no. 13, Art. ID rnn040, 11 pp.

[68] C. L. Stewart, *Integer points on cubic Thue equations*, C. R. Math. Acad. Sci. Paris, Ser. I 347 (2009), 715–718.

[69] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. (4) 8 (1995), 943–972.

[70] C. L. Stewart and S. Y. Xiao, *On the representation of integers by binary forms*, Math. Ann. 375 (2019), no. 1-2, 133–163.

[71] C. L. Stewart and S. Y. Xiao, *On the representation of k-free integers by binary forms*, arXiv:1612.00487.

[72] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135 (1909), 284–305.

[73] J. L. Thunder, *On cubic Thue inequalities and a result of Mahler*, Acta Arith. 83 (1998), 31–44.

[74] J. L. Thunder, *Decomposable form inequalities*, Ann. Math. 153 (2001), 767–804.

[75] J. L. Thunder, *Asymptotic estimates for the number of integer solutions to decomposable form inequalities*, Compos. Math. 141 (2005), 271–292.

[76] T. D. Wooley, *Sums of two cubes*, Int. Math. Res. Notices 4 (1995), 181–185.

[77] U. Zannier (ed.), *On Some Applications of Diophantine Approximations*, Edizioni Della Normale, Pisa, 2014.

Jan-Hendrik Evertse
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
The Netherlands
evertse@math.leidenuniv.nl

Kálmán Győry
Institute of Mathematics
University of Debrecen
P.O. Box 400
H-4002 Debrecen
Hungary
gyory@science.unideb.hu

Cameron L. Stewart
Dept. of Pure Mathematics
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
cstewart@uwaterloo.ca