PM 59
Séminaire de Théorie des Nombres
Paris 1983–84

UPPER BOUNDS FOR THE NUMBERS OF SOLUTIONS OF CERTAIN DIOPHANTINE EQUATIONS

J.H. EVERTSE

§ 1 - Introduction

In this lecture we shall consider, among other things, the diophantine equation

$$F(x,y) = m \quad \text{in} \quad x,y \in \mathbb{Z}, \tag{1}$$

where $F(x,y)$ in an irreducible binary form of degree $n \geq 3$ with coefficients in $\mathbb{Z}$ and m is a non-zero integer. In 1909, A. Thue [39] showed that this equation has only finitely many solutions. In fact, Thue showed that every solution (x,y) of (1) yields a good approximation x/y of one of the zeros of $F(x,1)$ and that there are only finitely many of such approximations. Unfortunately, Thue's method was ineffective. In 1967, A. Baker [2], [3] gave an effective proof of the finiteness of the number of solutions of (1), using lower bounds for linear forms in logarithms. Baker's method is totally different from Thue's and it is not very likely, that a modification of Thue's method can lead to general effective results on (1). Only in certain special cases, modifications of Thue's ideas can lead to effective finiteness results for the number of solutions of (1), cf. Thue [40], Baker [1], Choodnovsky [5]. Although Thue's method can not be made effective in general, it can be used in principle to give upper bounds for the *number* of solutions of (1). In this lecture we shall discuss certain interesting upper bounds which have been obtained by modifications and generalisations of Thue's ideas. Before doing this, we shall give a historical survey of results which have been derived concerning upper bounds for the number of solutions of (1).

Let $F(x,y)$ be an irreducible cubic form with coefficients in $\mathbb{Z}$.

Between 1920 and 1930, Delone [6] and Nagell [27] independently proved that the equation

$$F(x,y) = 1 \quad \text{in} \quad x,y \in \mathbb{Z} \tag{2}$$

has at most *five* solutions if F has negative discriminant. They used a method totally different from Thue's namely they studied units in the field $\mathbb{Q}(\alpha)$ where α is a zero of $F(x,1)$. In 1929, Siegel [32] showed that (2) has at most *eighteen* solutions if F has a positive discriminant which exceeds some (explicitly computable) absolute constant. Siegel proved this by modifying some of Thue's ideas. In fact, by refining Siegel's techniques one can show that for all irreducible cubic forms F with coefficients in $\mathbb{Z}$ and positive discriminant, (2) has at most *twelve* solutions (cf. Evertse [9]).

In 1933, K. Mahler [21] [22] generalised Thue's result in the following way. Let F be as in (1) and let $\{p_1,\ldots,p_t\}$ be a (possibly empty) set of distinct prime numbers. Then the number of solutions of the equation

$$|F(x,y)| = p_1^{k_1},\ldots,p_t^{k_t} \quad \text{in} \quad x,y,k,\ldots,k_t \in \mathbb{Z} \quad \text{with} \quad (x,y) = 1 \tag{3}$$

is finite and bounded above by c^{t+1}, where c is a constant depending on F only. Mahler proved this by generalising approximation techniques of Thue and Siegel to p-adic valuations. In 1950, C.J. Parry [28] generalised Mahler's result to equations of type (3) with variables in the ring of integers of some algebraic number field. It is worth while to mention, that in 1961, Lewis and Mahler [20] gave a more explicit bound for the number of solutions of (3), namely

$$c_1\, a^{c_2\sqrt{n}} + (c_3 n)^{t+1},$$

where c_1, c_2, c_3 are explicitly computable constants, n is the degree of F and a is the maximum of the absolute values of the coefficients of F. Very recently, J. Silverman [35], [36] proved that the number of solutions of (1) can be estimated from above by a constant depending only on the degree of F and the rank of $J_m(\mathbb{Q})$, where J_m is the Jacobian variety of the curve $F(x,y) = m$ $z^{\deg F}$, provided that m satisfies certain conditions.

From the historical remarks made above we infer that it is possible to give an upper bound for the number of solutions of (1) which depends only on the height of F, the degree of F and $\omega(m)$ (i.e. the number of primes dividing m). Moreover, in case that F is cubic and $m = 1$ we saw that it is possible to give a bound not depending on the coefficients of F. This leads to the conjecture that the number of solutions of (1) can be estimated from above by a constant not depending on the coefficients of F. In fact, we shall see that it is possible to give an upper bound depending only on $\omega(m)$ and the degree of F. We shall state the general result after having considered some special cases. It is not our intention to give proofs in full detail. We shall however indicate the main ideas behind the proofs whenever possible.

§ 2 - The equation $ax^n - by^n = c$.

The equation of the title has been studied by many mathematicians. In 1918, Thue [40] solved some of these equations. In 1937, Siegel [33] showed, by modifying some of Thue's techniques, that the equation

$$ax^n - by^n = c \quad \text{in} \quad x,y \in \mathbb{N}, \tag{4}$$

where a,b,c,n are non-zero integers with $n \geq 3$, has at most *one* solution if

$$|ab|^{1/2} \geq 188\, n\, |c|^4.$$

If for instance $c > 0$ and $b \geq 188\, n\, c^4$ then the equation

$$(b+c)x^n - by^n = c \quad \text{in} \quad x,y \in \mathbb{N}$$

has only one solution, namely $x = 1$, $y = 1$. For historical remarks about the method used by Siegel we refer to Siegel [34].

Using Siegel's method it is possible to give an upper bound for the number of solutions of (4) under more general conditions. We restrict ourselves to *primitive* solutions of (4), i.e. solutions (x,y) with $(x,y) = 1$. In fact we have

THEOREM 1. (4) has at most $2R(n,c) + 4$ primitive solutions, where $R(n,c)$ is the number of congruence classes $u \pmod c$ with $u^n \equiv 1 \pmod c$.

Using elementary number theory one can show that $R(n,c) \leq 2n^{\omega(c)}$. A complete proof of Theorem 1 can be found in Evertse [10] Chapter 2. Here we shall only indicate how we can derive a bound of the type $C_1 R(n,c)$, where C_1 (similar to $C_2, C_3, \ldots$) will denote an absolute constant.

For convenience we assume that $(a,c) = (b,c) = 1$ which is in fact no restriction. Then all primitive solutions (x,y) of (4) satisfy $(x,c) = (y,c) = 1$. We call two primitive solutions $(x_1,y_1), (x_2,y_2)$ of (4) *congruent* mod c if $x_1y_2 - x_2y_1 \equiv 0 \pmod{c}$, i.e. if $x_1/y_1 \equiv x_2/y_2 \pmod{c}$. The number of congruence classes mod c of primitive solutions of (4) is clearly at most equal to the number of congruence classes $u \pmod{c}$ satisfying $u^n \equiv b/a \pmod{c}$. But if the latter congruence equation has one solution then it has at most $R(n,c)$ solutions. Hence if suffices to show the following :

THEOREM 2. The number of primitive solutions of (4) in a fixed congruence class is at most C_1.

In fact it is possible to prove Theorem 2 with $C_1 = 6$ but to this end we need better estimates than those we use in this paper.

We shall now sketch the proof of Theorem 2. First of all, we introduce some notations. For positive integers x,y we define the height $w(x,y)$ by $w(x,y) := \mathrm{Max}\,(|ax^n|, |by^n|)$. Moreover, $\theta \in \mathbb{C}$ is a fixed n-th root of b/a such that $|\mathrm{Arg}\,\theta| \leq \pi/n$. Then we have for each other n-th root θ' of b/a that

$$|1 - \theta' \tfrac{y}{x}| \geq |1 - \theta \tfrac{y}{x}| \quad \text{for} \quad x,y \in \mathbb{N}. \tag{5}$$

Using this fact we can prove

LEMMA 1. If (x,y) is a solution of (4) then

$$\mathrm{Min}\,(1, |1-\theta\tfrac{y}{x}|) \leq \frac{2^n}{n} |c|\, W(x,y)^{-1}. \tag{6}$$

PROOF. Let ρ be a primitive n-th root of unity. Then we have by (5),

$$\frac{|c|}{|ax^n|} = |1 - \frac{by^n}{ax^n}| = \prod_{i=0}^{n-1} |1-\rho^i \theta \tfrac{y}{x}| \geq |1-\theta\tfrac{y}{x}| \cdot \prod_{i=1}^{n-1} \tfrac{1}{2} \{|\rho^{-i} - \theta\tfrac{y}{x}| + |1-\theta\tfrac{y}{x}|\}$$

$$\geq |1-\theta\tfrac{y}{x}| 2^{1-n} \prod_{i=1}^{n-1} |\rho^{-i}-1| = \frac{n}{2^{n-1}} |1-\theta\tfrac{y}{x}|.$$

Hence

$$|1-\theta\frac{y}{x}| \le \frac{2^{n-1}}{n}\frac{|c|}{|ax^n|}. \tag{7}$$

Similarly we have

$$|1-\theta^{-1}\frac{x}{y}| \le \frac{2^{n-1}}{n}\frac{|c|}{|by^n|}. \tag{8}$$

If $|ax^n| \ge |by^n|$ then (6) follows from (7). Suppose $|by^n| \ge |ax^n|$. Then $|\theta y/x| \ge 1$. If $|\theta^{-1}x/y| \le \frac{1}{2}$ then $|1-\theta^{-1}x/y| \ge \frac{1}{2}$; if $|\theta^{-1}x/y| > \frac{1}{2}$ then $|1-\theta^{-1}x/y| = |\theta^{-1}x/y| \times |1-\theta y/x| \ge \frac{1}{2}|1-\theta y/x|$. Hence $|1-\theta^{-1}x/y| \ge \frac{1}{2}\mathrm{Min}(1,|1-\theta y/x|)$. Together with (8) this proves (6). □

LEMMA 2. Let β be a real with $2/n < \beta < 1$. Put

$$U = U(\beta) = \left(\frac{n^\beta}{2^{n\beta+1}}|c|^{1-\beta}\right)^{\frac{n}{n\beta-2}}.$$

(i) If $(x_1,y_1),(x_2,y_2)$ are two distinct, primitive solutions of (4) which are congruent mod c and which satisfy $w(x_2,y_2) \ge w(x_1,y_1)$ then

$$w(x_2,y_2) \ge U^{n\beta-2}w(x_1,y_1)^{n\beta-1}.$$

(ii) Let M_1,M_2 be constants with $U < M_1 < M_2$. Then the number of primitive solutions (x,y) of (4) in a fixed congruence class mod c with

$$M_1 \le w(x,y) \le M_2$$

is at most

$$1 + \frac{\log\{\log(UM_2)/\log(UM_1)\}}{\log(n\beta-1)}.$$

PROOF. (i) Put $w_i = w(x_i,y_i)$ for $i = 1,2$. Note that $|x_1y_2-x_2y_1| \le 2(w_1w_2)^{1/n}$ and

$$|x_1y_2 - x_2y_1| = |x_1x_2||\frac{y_1}{x_1} - \frac{y_2}{x_2}| \le 2(w_1w_2)^{1/n}\mathrm{Max}(|1-\theta\frac{y_1}{x_1}|,|1-\theta\frac{y_2}{x_2}|).$$

Since $\mathrm{Min}(a,\mathrm{Max}(b,c)) = \mathrm{Max}(\mathrm{Min}(a,c),\mathrm{Min}(b,c))$ for $a,b,c \in \mathbb{R}$ and since $2/n < \beta < 1$ we have by Lemma 1,

$$|c| \le |x_1y_2 - x_2y_1| \le 2(w_1w_2)^{1/n}\max\{\min(1,|1-\theta\frac{y_1}{x_1}|),\min(1,|1-\theta\frac{y_2}{x_2}|)\}^{\beta}$$

$$\le 2(w_1w_2)^{1/n}(\frac{2^n}{n})^{\beta}|c|^{\beta}w_1^{-\beta}.$$

This clearly proves (i).

(ii) Let $(x_1,y_1), (x_2,y_2),\dots,(x_k,y_k)$ be distinct primitive solutions of (4), belonging to the same congruence class mod c, such that $M_1 \le w(x_1,y_1) \le \dots \le w(x_k,y_k) \le M_2$. Then by (i),

$$Uw(x_{i+1},y_{i+1}) \ge (Uw(x_i,y_i))^{n\beta-1} \quad \text{for} \quad i=1,\dots,k-1,$$

hence

$$UM_2 \ge Uw(x_k,y_k) \ge (Uw(x_1,y_1))^{(n\beta-1)^{k-1}} \ge (UM_1)^{(n\beta-1)^{k-1}}.$$

This clearly implies (ii). □

We shall now apply an approximation method to (6) or more generally to the inequality

$$\text{(9)} \qquad \text{Min}\,(1,|1-\theta\frac{y}{x}|) \le Aw(x,y)^{-B} \quad \text{in} \quad x,y \in \mathbb{N},$$

where, as before, n is an integer with $n \ge 3$ and where A,B are positive constants with $A \ge 1$, $\frac{1}{2}+\frac{1}{n} < B \le 1$. Since the method we are going to apply is essentially Thue's we have to restrict ourselves to the case $B > n^{-1}(\frac{n}{2}+1)$.

LEMMA 3. There exist explicitly computable, absolute constants $C_2 \ge 1$, $C_3 \ge 1$ with the following property. If (x_1,y_1), (x_2,y_2) are two solutions of (9) with

$$\text{(10)} \qquad w(x_2,y_2) \ge w(x_1,y_1) \ge (C_2^nA^5)^{(B-\frac{1}{2}-\frac{1}{n})^{-1}},$$

then

$$\text{(11)} \qquad w(x_1,y_1) \le w(x_2,y_2) \le A^2(C_3^nw(x_1,y_1)^4)^{(B-\frac{1}{2}-\frac{1}{n})^{-1}}.$$

PROOF. We shall not give the complete proof of Lemma 3, but indicate the main steps in it. We assume that for every pair of integers $r \ge 1$, $n \ge 3$

there are polynomials $G_r(X)$, $H_r(X)$, $T_r(X) \in \mathbb{Z}[X]$, with coefficients depending on r, n, such that

(11) $\deg G_r = r$, $\deg H_r = r$, $\deg T_r = r(n-2)$;

(12) $G_r(X^n) - XH_r(X^n) = (1-X)^{2r+1}T_r(X)$;

(13) $G_r(Z)H_{r+1}(Z) \neq G_{r+1}(Z)H_r(Z)$ for $Z \in \mathbb{C} \setminus \{1\}$;

(14) G_r, H_r, T_r have positive coefficients which do not exceed C_4^{nr}.

For a proof of this we refer to Evertse [10], Chapter 1.

Let (x_1,y_1), (x_2,y_2) be two solutions of (9) with $w_2 > w_1 \geq A^{1/B}$, where $w_i = w(x_i,y_i)$ for $i = 1,2$. Put $Z = by_1^n/ax_1^n$ and

(15) $$U_r = x_1x_2(ax_1^n)^r \left\{\frac{y_2}{x_2} G_r(Z) - \frac{y_1}{x_1} H_r(Z)\right\}.$$

Note that $U_r \in \mathbb{Z}$. Hence if $U_r \neq 0$ then we have by (11), (12), (14), Lemma 1 and the fact that $|1-\theta y_i/x_i| \leq 1$ for $i = 1,2$,

$$1 \leq |U_r| = |ax_1^n|^{r+1/n}|ax_2^n|^{1/n}|\theta^{-1}||a|^{-2/n}|(\theta\frac{y_2}{x_2}-1)G_r(Z)+(1-\theta\frac{y_1}{x_1})^{2r+1}T_r(\theta\frac{y_1}{x_1})|$$

$$\leq w_1^{r+1/n}\, w_2^{1/n}(2\,C_4)^{nr}\,(Aw_2^{-B} + A^{2r+1}\, w_1^{-B(2r+1)})$$

$$\leq \max\,(C_5^{nr}\, Aw_1^{r+1/n}\, w_2^{1/n-B},\ C_5^{nr}\, A^{2r+1}\, w_1^{1/n+r-B(2r+1)}\, w_2^{1/n}).$$

By (12), $U_r = 0$ implies that $U_{r+1} \neq 0$. Hence we have for all $r \geq 1$, since $B > 1/2$,

(16) $$1 \leq \mathrm{Max}(C_5^{n(r+1)}\, Aw_1^{r+1+1/n}\, w_2^{1/n-B},\ C_5^{n(r+1)}\, A^{2r+3}\, w_1^{1/n+r-B(2r+1)}w_2^{1/n}).$$

Let k be the smallest positive integer with $k \geq \dfrac{2B-nB^2+2}{nB(B-\frac{1}{2}-1/n)}$ and suppose that

(17) $$w_1 > (C_5^{3n}A^5)^{(B-\frac{1}{2}-1/n)^{-1}}, \qquad w_2 > (C_5^{n(k+1)}Aw_1^{k+1+1/n})^{(B-1/n)^{-1}}.$$

We shall show that (17) is impossible. This proves Lemma 3, since

$B - 1/n \geq \frac{1}{2}$, $B \leq 1$ and

$$k + 1 + \frac{1}{n} \leq \mathrm{Max}(0, \frac{2B-nB^2+2}{nB(B-\frac{1}{2}-1/n)}) + 2 + \frac{1}{n}$$

$$= \mathrm{Max}(1, \frac{B-\frac{1}{2}nB+2}{nB(B-\frac{1}{2}-1/n)}) + 1 + \frac{1}{n}$$

$$\leq \mathrm{Max}(1, \frac{5-n/2}{n})(B-\tfrac{1}{2}-1/n)^{-1} + 1 + \frac{1}{n} \leq \frac{2}{B-\frac{1}{2}-1/n} .$$

By assumption of (17), there is an integer r with $r \geq k$ such that

$$(18) \qquad C_5^{n(r+1)} A w_1^{r+1+1/n} < w_2^{B-1/n} \leq C_5^{n(r+2)} A w_1^{r+2+1/n}.$$

For this integer r we have firstly,

$$C_5^{n(r+1)} A w_1^{r+1+1/n} w_2^{1/n-B} < 1$$

and secondly, since $r \geq k$ and $B > \frac{1}{2} + 1/n$,

$$C_5^{n(r+1)} A^{2r+3} w_1^{1/n+r-B(2r+1)} w_2^{1/n}$$
$$\leq (C_5^{n(nB-1)(r+1)+n(r+2)} A^{(nB-1)(2r+3)+1} w_1^{(nB-1)(1/n+r-B(2r+1)+r+2+1/n)})^{(nB-1)^{-1}}$$
$$= (C_5^{n^2B(r+1)+n} A^{(nB-1)2r+3nB-2} w_1^{2nB(\frac{1}{2}+\frac{1}{n}-B)r+2B-nB^2+2})^{(nB-1)^{-1}}$$
$$\leq (C_5^{3n} A^5 w_1^{\frac{1}{2}+1/n-B})^{\frac{nBr}{nB-1}} < 1.$$

This contradicts (16). Hence (17) is impossible. This completes the proof of Lemma 3. □

PROOF OF THEOREM 2. By Lemma 1 and Lemma 3 with $A = (2^n/n)|c|$, $B = 1$ and by $n \geq 3$, there are certain absolute constants C_6, C_7, such that for any two primitive solutions (x_1,y_1), (x_2,y_2) of (4), with

$$(19) \qquad w(x_2,y_2) \geq w(x_1,y_1) \geq C_6^n |c|^{30}$$

we have

$$(20) \qquad w(x_2,y_2) \leq C_7^n |c|^2 \, w(x_1,y_1)^{24}.$$

Let U be the set of primitive solutions of (4) belonging to a given congruence class. We divide U into three classes.

I. The solutions $(x,y) \in U$ with $w(x,y) < (\frac{2^{2n}}{n})^{\frac{n\beta}{n\beta-2}}$;

II. The solutions $(x,y) \in U$ with $(\frac{2^{2n}}{n})^{n\beta/(n\beta-2)} \leq w(x,y) < C_6^n |c|^{30}$;

III. The solutions $(x,y) \in U$ with $w(x,y) \geq C_6^n |c|^{30}$.

Here we choose β such that $2/3 < \beta < 1$ and β does not depend on n. Since $w(x,y) \geq \max(x,y)^n$ the number of elements of I can be estimated from above by an absolute constant. Using Lemma 2, (ii) we can also estimate the cardinality of II from above by an absolute constant, on noting that $|c|$ can be eliminated due to the strictly positive exponent of $|c|$ in the expression for $U(\beta)$ in Lemma 2 and that n can be eliminated by the factor $\log(n\beta-1)$ appearing in the denominator of the expression in Lemma 2(ii). Let (x_0,y_0) be an element of III for which $w(x_0,y_0)$ is minimal. Then all solutions in III satisfy $w(x_0,y_0) \leq w(x,y) \leq C_7^n |c|^2 w(x_0,y_0)^{24}$. Using Lemma 2(ii) it is again easy to show the number of solutions in III can be bounded above by an absolute constant. This completes the proof of Theorem 2. □

§ 3 - On the equation $|ax^n - by^n| = cp_1^{k_1} \ldots p_t^{k_t}$.

Let a,b,c,n be non-zero integers with $n \geq 3$, $c > 0$ and let $\{p_1,\ldots,p_t\}$ be a set of distinct primes. We shall consider the equation

(21) $|ax^n - by^n| = cp_1^{k_1} \ldots p_t^{k_t}$ in $x,y \in \mathbb{Z}$ with $(x,y) = 1$ and $xy \neq 0$.

Solutions of (21) are shortly denoted by (x,y). We call two solutions $(x_1,y_1),(x_2,y_2)$ congruent mod c if $x_1y_2 - y_2y_1 \equiv 0 \pmod{c}$. $C_1,C_2,\ldots$ will denote absolute constants.

THEOREM 3. (21) has at most $C_1(C_2n)^t$ solutions belonging to a fixed congruence class mod c.

Theorem 3 can be proved by generalising the techniques in the proof of Theorem 2 to p-adic valuations. We shall not give a complete proof of Theorem 3 but we shall point out how the estimates in the proof of Theorem 2 can be generalised to estimates involving p-adic valuations.

Let p be a prime number (i.e. a "finite" prime). We define the

absolute value $|.|_p$ by $|p|_p = p^{-1}$. Moreover, we denote the usual absolute value on $\mathbb{Q}$ by $|.|_\infty$. (∞ is called the infinite prime). Thus we have a set of absolute values on $\mathbb{Q}$ satisfying the *product formula*

$$\prod_{p\in M} |\alpha|_p = 1 \quad \text{for} \quad \alpha \in \mathbb{Q}\setminus\{0\}, \tag{22}$$

where M is the set consisting of ∞ and the prime numbers. For $p \in M$ we denote the completion of $\mathbb{Q}$ at p by $\mathbb{Q}_p$ and the algebraic closure of $\mathbb{Q}_p$ by $\overline{\mathbb{Q}_p}$ (thus $\mathbb{Q}_\infty = \mathbb{R}$, $\overline{\mathbb{Q}_\infty} = \mathbb{C}$). Finally we put $s(p) = 1$ if $p = \infty$ and $s(p) = 0$ if $p \neq \infty$.

Let $S = \{\infty, p_1, \ldots, p_t\}$, let (x,y) be a solution of (21) and let θ_p ($p \in S$) that n-th root of b/a in $\mathbb{Q}_p$ such that $|1-\theta_p y/x|_p \leq |1-\theta y/x|_p$ for each other n-th root θ of b/a. Then one can show, similar to (6),

$$\text{Min}\,(1, |1-\theta_p \tfrac{y}{x}|_p) \leq \frac{2^{ns(p)}}{|n|_p}\, |ax^n - by^n|_p\, \text{Max}(|ax^n|_p, |by^n|_p)^{-1}.$$

Hence by (22)

$$\prod_{p\in S} \text{Min}(1, |1-\theta_p \tfrac{y}{x}|_p) \leq 2^n C\, w_S(x,y)^{-1}, \tag{23}$$

where

$$C = \prod_{p\in S} |c|_p, \quad w_S(x,y) = \prod_{p\in S} \text{Max}(|ax^n|_p, |by^n|_p). \tag{24}$$

Note that we have at most n possibilities for each θ_p, where $p \in \{p_1, \ldots, p_t\}$. Moreover, $|\text{Arg}\,\theta_\infty - \text{Arg}\,(y(x)| \leq \pi/n$. Thus we have at most two possibilities for θ_∞. Hence each solution (x,y) of (21) satisfies one of at most $2n^t$ inequalities of type (23).

We shall now "split up" (23) by using the following lemma, a proof of which can be found in Evertse [10], Chapter 6.

LEMMA 4. Let B be a real number with $\frac{1}{2} < B < 1$ and let q be a positive integer. Let $F_1, \ldots, F_q$, Λ be positive real numbers with $F_j \leq 1$ for $j = 1, \ldots, q$ and $\prod_{j=1}^q F_j \leq \Lambda$. Put

$$R(B) = (1-B)^{-1} B^{B/(B-1)}.$$

There exists a q-tuple $(\Gamma_1,\ldots,\Gamma_q)$ with $\Gamma_j \geq 0$ for $j=1,\ldots,q$ and $\Sigma_{j=1}^{q}\Gamma_j = B$ which can be chosen from a set of at most $R(B)^{q-1}$ of such tuples which depends on B and q only and does not depend on the F_j and Λ, such that for $j=1,\ldots,q$,

$$F_j \leq \Lambda^{\Gamma_j}.$$

As an immediate consequence of Lemma 4 we have for $B \in (\frac{1}{2},1)$:

LEMMA 5. Every solution (x,y) of (21) satisfies one of at most $2\times(nR(B))^t$ systems of inequalities of the type

$$\text{(25)} \qquad \text{Min}(1,|1-\theta_p \tfrac{y}{x}|_p) \leq (2^n C w_S(x,y)^{-1})^{\Gamma_p} \qquad (p \in S),$$

where $\theta_p^1 = b/a$ and $\Gamma_p \geq 0$ for $p \in S$ and $\Sigma_{p\in S}\Gamma_p = B$.

Similar to Theorem 2 one can show that the number of solutions of (21) in a fixed congruence class which satisfy a fixed system (25) can be bounded above by a constant depending on B only. One needs the following analogues of Lemmas 2 and 3. For convenience we denote the set of solutions of (21) which belong to a fixed congruence class mod c and which satisfy a fixed system (25) by $\mathcal{U}$. We assume that $\frac{1}{2} + 1/n < B < 1$. Moreover, we put

$$U_0 = U_0(B) = \left(\frac{C^{1-B}}{2^{nB+1}}\right)^{\frac{n}{nB-2}}$$

LEMMA 6 (i). Let $(x_1,y_1),(x_2,y_2)$ be distinct elements of $\mathcal{U}$ with $w_S(x_2,y_2) \geq w_S(x_1,y_1)$. Then

$$w_S(x_2,y_2) \geq U_0^{nB-2} w_S(x_1,y_1)^{nB-1}.$$

(ii) Let M_1,M_2 be constants with $U_0 < M_1 < M_2$. Then the number of pairs $(x,y) \in \mathcal{U}$ with

$$M_1 \leq w_S(x,y) \leq M_2$$

is at most

$$1 + \frac{\log\{\log(U_0M_2)/\log(U_0M_1)\}}{\log(nB-1)}$$

LEMMA 7. There are explicitly computable absolute constants $C_3 \geq 1$, $C_4 \geq 1$ with the following property. If $(x_1,y_1),(x_2,y_2)$ are two solutions of U with

$$w_S(x_2,y_2) \geq w_S(x_1,y_1) \geq (C_3^n C^5)^{(B-\frac{1}{2}-1/n)^{-1}}$$

then

$$w_S(x_1,y_1) \leq w_S(x_2,y_2) \leq C^2(C_4^n w_S(x_1,y_1)^4)^{(B-\frac{1}{2}-1/n)^{-1}}.$$

Lemma 6 (i) can be proved similarly to Lemma 2 (i) by estimating $|x_1y_2 - x_2y_1|_\rho$ from above similarly to the proof of Lemma 2 (i) for each $p \in S$ and by noticing that

$$\prod_{p\in S} |x_1y_2 - x_2y_1|_p = \prod_{p\in M\setminus S} |x_1y_2 - x_2y_1|_p^{-1} \geq \prod_{p\in M\setminus S} |C|_p^{-1} = C.$$

Lemma 6 (ii) can be derived from Lemma 6 (i) in exactly the same way as Lemma 2 (ii) is derived from Lemma 2 (i). Lemma 7 can be proved in a similar way as Lemma 3, by estimating the expression $|U_r|_p$ from above for each $p \in S$, where U_r is defined by (15) and by noting that $U_r \neq 0$ implies that $\prod_{p\in S} |U_r|_p \geq 1$. Now Theorem 3 can be derived from Lemmas 6 and 7 in just the same way as Theorem 2 has been derived from Lemmas 2 and 3. □

§ 4 - On the equation $aX + bY + cZ = 0$ in integers X, Y, Z composed of fixed primes.

Let $\{p_1,\ldots,p_t\}$ be a set of distinct prime numbers, let S be the set of those $\alpha \in \mathbb{Z}$ for which $|\alpha|$ is composed of primes from $\{p_1,\ldots,p_t\}$ and let a,b,c be rational integers with $abc \neq 0$ and $(abc, p_1\ldots p_t) = 1$. Then we have

THEOREM 4. The equation

$$aX + bY + cZ = 0 \quad \text{in} \quad X,Y,Z \in S \quad \text{with} \quad (X,Y,Z) = 1 \tag{26}$$

has at most

$$6 \times 7^{2t+3}$$

solutions.

Although this equation seems to be totally different from the equations mentioned in the previous sections it can be dealt with by similar techniques. We shall give a very rough sketch of the proof below.

We assume that $(a,b,c) = 1$ which is clearly no restriction. Let $\rho = e^{2\pi i/3}$ and let (X,Y,Z) be a solution of (26). Put

$$\xi = aX - \rho bY, \quad \eta = aX - \rho^2 bY.$$

Then

$$\xi^3 - \eta^3 = 3(\rho-\rho^2)abcXYZ.$$

Hence there are rational, non-negative integers $k_1,\ldots,k_t$ such that

$$\xi^3 - \eta^3 = 3(\rho-\rho^2)abc\, p_1^{k_1}\ldots p_t^{k_t}. \tag{27}$$

Let (X_1,Y_1,Z_1), (X_2,Y_2,Z_2) be two solutions of (26) and let (ξ_1,η_1), (ξ_2,η_2) be the corresponding (ξ,η)-values. Then

$$\xi_1\eta_2 - \xi_2\eta_1 = ab(\rho-\rho^2)(X_1Y_2-X_2Y_1). \tag{28}$$

Moreover, by (26),

$$a(X_1Y_2-X_2Y_1) = c(Z_2Y_1-Z_1Y_2), \quad b(X_1Y_2-X_2Y_1) = c(X_2Z_1-X_1Z_2).$$

Hence, since $(a,b) = 1$,

$$X_1Y_2 - X_2Y_1 \equiv 0 \pmod{c}.$$

Together with (28) this shows that

$$\xi_1\eta_2 - \xi_2\eta_1 \equiv 0 \pmod{(\rho-\rho^2)abc}. \tag{29}$$

Hence the solutions of (26) correspond, roughly speaking, to solutions of (27) belonging to the same congruence class mod $(\rho-\rho^2)abc$. Moreover, the gcd of ξ,η need not be equal to 1 but is in any case a divisor of $1-\rho$. Now we can prove, using similar techniques as in paragraphs 2 and 3, that (26) has at most $C_1 \times C_2^t$ solutions, where C_1,C_2 are cer-

tain absolute constants. A precise computation yields Theorem 4. □

It is possible to generalise Theorem 4 to algebraic number fields. Let K be an algebraic number field of degree m with ring of integers $\mathcal{O}_K$ and let r be the rank of the unit group of $\mathcal{O}_K$. Let $\{p_1,\ldots,p_t\}$ be a (possibly empty) set of prime ideals and let S^* be the set of those $\delta \in \mathcal{O}_K$ such that the ideal generated by δ is composed solely of prime ideals from $\{p_1,\ldots,p_1\}$. Let α,β,γ be non-zero elements of $\mathcal{O}_K$. We shall consider the equation

$$\alpha X + \beta Y + \gamma Z = 0 \quad \text{in} \quad X,Y,Z \in S^*. \tag{30}$$

If (X,Y,Z) is a solution of (31) and if $u \in S^*$, then (uX, uY, uZ) is also a solution of (30). We say that (uX, uY, uZ) is derived from (X,Y,Z) by multiplication with an element of S^*. Without proof we state

THEOREM 5. Up to multiplication by elements of S^*, (30) has at most

$$3 \times 7^{m+2(r+t+1)}$$

solutions.

For a proof we refer to Evertse [11].

§ 5 - On the Thue-Mahler equation and some generalisations.

In this section we shall discuss some applications of Theorem 5. First of all it is possible to derive an upper bound for the number of solutions of the Thue-Mahler equation (3) which does not depend on the coefficients of the binary form involved. Let $\{p_1,\ldots,p_t\}$ be a set of primes and let $F(x,y) \in \mathbb{Z}[x,y]$ be a binary form of degree $n \geq 3$ which has at least three distinct linear factors in $\mathbb{C}[x,y]$. Then we have

THEOREM 6. The number of solutions of the equation

$$|F(x,y)| = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t} \quad \text{in} \quad x,y,k_1,\ldots,k_t \in \mathbb{Z} \quad \text{with} \quad (x,y) = 1 \tag{31}$$

is at most

$$7^{n^3(2t+3)}.$$

Note that this bound depends on n and t only. A complete proof of

Theorem 6 can be found in Evertse [11].

In fact, it is not difficult to derive Theorem 6 from Theorem 5. We assume that $F(1,0) = 1$ which is in fact no restriction. For suppose that (31) is solvable. Then we may assume that $a := F(1,0)$ is a positive integer which is composed of primes from $\{p_1,\ldots,p_t\}$, by replacing F by an equivalent form and by multiplying all coefficients of F with -1 if necessary. Put $G(x,y) = a^{n-1}F(x/a,y)$. Then $G(x,y) \in \mathbb{Z}[x,y]$, $G(1,0) = 1$ and moreover, the number of solutions of (31) will not decrease when F is replaced by G.

By our assumption on F, we have

$$F(x,y) = (x-\alpha_1 y)\ldots(x-\alpha_n y), \tag{32}$$

where $\alpha_1,\ldots,\alpha_n$ are algebraic integers of which at least three are pairwise distinct, α_1, α_2, α_3 say. Let $L = \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$ and let $\mathfrak{p}_1,\ldots,\mathfrak{p}_u$ be the prime ideals in L which divide $p_1\ldots p_t$. Denote solutions of (31) by (x,y). For each solution (x,y) of (31), $x-\alpha_1 y$, $x-\alpha_2 y$, $x-\alpha_3 y$ are algebraic integers composed of prime ideals from $\mathfrak{p}_1,\ldots,\mathfrak{p}_u$. Moreover we have

$$(\alpha_2-\alpha_3)(x-\alpha_1 y) + (\alpha_3-\alpha_1)(x-\alpha_2 y) + (\alpha_1-\alpha_2)(x-\alpha_3 y) = 0\ . \tag{33}$$

If $(x_1,y_1),(x_2,y_2)$ are two solutions of (31) with $(x_1-\alpha_i y_1)/(x_2-\alpha_i y_2) = (x_1-\alpha_j y_1)/(x_2-\alpha_j y_2)$ for $i,j \in \{1,2,3\}$ then $(x_2,y_2) = \pm(x_1,y_1)$. Hence by Theorem 5, on noting that $u \le [L:\mathbb{Q}]t$ and $[L:\mathbb{Q}] \le n(n-1)(n-2)$, the number of solutions of (31) is at most

$$2 \times 3 \times 7^{n(n-1)(n-2)(2t+3)} \le 7^{n^3(2t+3)}. \qquad \square$$

By similar arguments it is possible to derive results on the Thue-Mahler equation with variables in the ring of integers of a given algebraic number field, cf. Evertse [11]. By applying similar approximation techniques as discussed in the previous sections to function fields of characteristic zero it is possible to give upper bounds for the number of solutions of the Thue-Mahler equation over function fields. We shall state a result only for rational function fields although it can be generalised to albebraic function fields. Let $\mathbb{K}$ be a field of characteristic 0, let $K = \mathbb{K}(X_1,\ldots,X_r)$ and $\mathcal{O} = \mathbb{K}[X_1,\ldots,X_r]$ where $X_1,\ldots,X_r$ are alge-

braically independent over $\mathbb{K}$. Let $\pi_1,\ldots,\pi_t$ be distinct, pairwise non associated irreducible polynomials in O and let $F(x,y) \in O[x,y]$ be a binary form of degree $n \geq 3$ which has at least three distinct linear factors in some extension of K and which has the following additional property : there are no $\alpha,\beta,\gamma,\delta \in O$ with $\alpha\delta - \beta\gamma \neq 0$, $\ell_1,\ldots,\ell_t \in \mathbb{Z}$ and a binary form $f(x,y) \in \mathbb{K}[x,y]$ such that .

$$F(\alpha x+\beta y,\gamma x+\delta y) = \pi_1^{\ell_1},\ldots,\pi_t^{\ell_t} f(x,y). \tag{34}$$

Then we have

THEOREM 7. The equation

$$F(x,y) = \pi_1^{k_1},\ldots,\pi_t^{k_t} \text{ in } x,y \in O \text{ with } (x,y) = 1 \text{ and } k_1,\ldots,k_t \in \mathbb{Z} \tag{35}$$

(where $(x,y) = 1$ means that x,y are not both divisible by the same non-constant polynomial in O) has at most

$$7^{n^3(2t+3)}$$

solutions.

For a proof we refer to Evertse [12]. We mention that Mason [24] has derived an effective analogue of this theorem in case that $r = 1$.

Finally we mention that Theorem 5 can also be applied to a special class of norm-form equations. Let $\alpha_1,\ldots,\alpha_r$ be algebraic numbers such that $[\mathbb{Q}(\alpha_1):\mathbb{Q}] \geq 3$ and $[\mathbb{Q}(\alpha_1,\ldots,\alpha_{i+1}) : \mathbb{Q}(\alpha_1,\ldots,\alpha_i)] \geq 3$ for $i = 1,\ldots,r-1$. Let $K = \mathbb{Q}(\alpha_1,\ldots,\alpha_r)$ and $n = [K:\mathbb{Q}]$. If $\beta \in K$ then we denote the conjugates of β by $\beta^{(1)},\ldots,\beta^{(n)}$. Put

$$F(x_0,\ldots,x_r) = a \prod_{i=1}^{n} (x_0+\alpha_1^{(i)}x_1+\ldots+\alpha_r^{(i)}x_r)$$

where $a \in \mathbb{Q} \setminus \{0\}$ is chosen such that $F(x_0,\ldots,x_r)$ has coefficients in $\mathbb{Z}$. Let $p_1,\ldots,p_t$ be distinct prime numbers and let g be the degree of the normal closure of K over $\mathbb{Q}$.

THEOREM 8. The equation

$$|F(x_0,\ldots,x_r)| = p_1^{k_1},\ldots,p_t^{k_t} \text{ in } x_0,\ldots,x_r,k_1,\ldots,k_t \in \mathbb{Z} \text{ with } (x_0,\ldots,x_r)=1$$

has at most

$$2(4 \times 7^{g(2t+3)})^{r-1}$$

solutions.

For a proof we refer to Evertse and Győry [13]. In fact, Evertse and Győry proved a generalisation of Theorem 8 dealing with norm form equations over rings which are finitely generated over $\mathbb{Z}$.

REFERENCES

[1] A. Baker.- Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers, Quart. J. Math. Oxford 15 (1964), 375-383.

[2] A. Baker.- Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms, Philos. Trans. Roy. Soc. London, Ser. A 263 (1968), 173-191.

[3] A. Baker.- Contributions to the theory of Diophantine equations. II. The Diophantine equation $y^2 = x^3+k$, Philos. Trans. Roy. Soc. London, Ser. A 263 (1968), 193-208.

[4] G.V. Choodnovsky.- The Gel'fond-Baker method in problems of diophantine approximation, Coll. Math. Soc. János Bolyai 13 (1974), 19-30.

[5] G.V. Choodnovsky.- On the method of Thue-Siegel, Ann. of Math. 117 (1983), 325-382.

[6] B.N. Delone.- Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante, Math. Zeitschr. 31 (1930), 1-26.

[7] B.N. Delone and D.K. Faddeev.- The theory of irrationalities of the third degree, Am. Math. Soc. Transl. of Math. monographs 10, Providence, USA (1964).

[8] J.H. Evertse.- On the equation $ax^n-by^n = c$, Compositio Math. 47 (1982), 289-315.

[9] J.H. Evertse.- On the representation of integers by binary cubic forms of positive discriminant, Invent. Math. 73 (1983), 117-138. Erratum, Invent. Math. 75 (1984), p. 379.

[10] J.H. Evertse.- Upper bounds for the numbers of solutions of diophantine equations, Thesis, Leiden, 1983. MC-tract 168, Mathematical Centre, Amsterdam, 1983.

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

[12] J.H. Evertse.- On equations in two S-units over function fields of characteristic zero, preprint, Leiden, 1983, has been submitted for publication.

[13] J.H. Evertse and K. Győry.- On unit equations and decomposable form equation, J.F. reine u. angew. Math., to appear.

[14] G. Faltings.- Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73, (1983), 349-366.

[15] K. Győry.- Résultats effectifs sur la représentation des entiers par des formes décomposables, Queen's Papers in Pure and Applied Math., N° 56, Kingston, Canada, 1980.

[16] K. Győry.- Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains, Acta Math. Hungar. 42 (1983), 45-80.

[17] K. Győry.- On norm form, discriminant form and index form equations. Coll. Math. Soc. J. Bolyai 34. Topics in Classical Number Theory, to appear.

[18] S.V. Kotov and V.G. Sprindžuk.- The Thue-Mahler equation in a relative field, and the approximation of algebraic numbers by algebraic numbers, Izv. Akad. SSSR 41 (1977), 723-751 (Russian) or Math. USSR Jzv. 11 (1977), 677-707.

[19] S. Lang.- Fundamentals of Diophantine Geometry, Springer Verlag, Berlin, Heidelberg, New York, Tokyo, 1983.

[20] D.J. Lewis and K. Mahler.- Representation of integers by binary forms, Acta Arith. 6 (1961), 333-363.

[21] K. Mahler.- Zur Approximation algebraischer Zahlen, I. (Über den gröszten Primteiler binärer Formen), Math. Ann. 107 (1933), 691-730.

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

[23] K. Mahler.- On Thue's theorem, Math. Scand., to appear.

[24] R.C. Mason.- On Thue's equation over function fields, J. London Math. Soc. 24 (1981), 414-426.

[25] R.C. Mason.- The hyperelliptic equation over function fields, Math. Proc. Cambridge Phil. Soc. 93 (1983), 219-230.

[26] L.J. Mordell.- Diophantine equations, Academic Press, London (1969).

[27] T. Nagell.- Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante, Math. Zeitschr. 28 (1928), 10-29.

[28] C.J. Parry.- The p-adic generalization of the Thue-Siegel theorem, Acta Math. 83 (1950), 1-99.

[29] K.F. Roth.- Rational approximations to algebraic numbers, Mathematika 2 (1955), 1-20. Corrigendum ibid, p. 168.

[30] C.L. Siegel.- Approximation algebraischer Zahlen, Math. Zeitschr. 10 (1921), 173-213.

[31] C.L. Siegel (under the pseudonym X).- The integer solutions of the equation $y^2 = ax^n+bx^{n-1}+\ldots+k$, J. London Math. Soc. 1 (1926), 66-68.

[32] C.L. Siegel.- Über einige Anwendungen diophantischer Approximationen, Abh. preuss. Akad. Wiss. phys.-math. K1. (1929), N°1.

[33] C.L. Siegel.- Die Gleichung $ax^n-by^n = c$, Math. Ann. 114 (1937), 57-68.

[34] C.L. Siegel.- Einige Erläuterungen zu Thues Untersuchungen über Annäherungswerte algebraischer Zahlen und diophantische Gleichungen. Nachr. Göttingen, math.-phys. K1 (1970), 169-195.

[35] J.H. Silverman.- Integer points and the rank of Thue elliptic curves, Invent. Math. 66 (1982), 395-404.

[36] J.H. Silverman.- Representations of integers by binary forms and the rank of the Mordell-Weil group, Invent. Math. 74 (1983), 281-292.

[37] J.H. Silverman.- Quantitative results in Diophantine geometry, preprint Cambridge, Massachusetts.

[38] V.G. Sprindžuk.- Achievements and problems in Diophantine approximation theory, Uspekhi Mat. Nank. 35 (4) (1980), 3-68 (Russian) or Russ. Math. Surv. 35 (4) (1980), 1-80.

[39] A. Thue.- Über Annäherungswerte algebraischer Zahlen, J. reine Angew. Math. 135 (1909), 284-305.

[40] A. Thue.- Berechnung aller Lösungen gewisser Gleichungen von der Form $ax^r-by^r = f$, Vid-Selsk. Skrifter, I. Math.-naturv. K1, Christiania (1918), 4.

J.H. EVERTSE
Mathematical Centre
Kruislaan 413
1098 SJ AMSTERDAM
The Netherlands