Printed at the Mathematical Centre, Kruislaan 413, Amsterdam, The Netherlands.

The Mathematical Centre, founded 11 February 1946, is a non-profit institution for the promotion of pure and applied mathematics and computer science. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

MATHEMATICAL CENTRE TRACTS 168

UPPER BOUNDS FOR THE NUMBERS OF SOLUTIONS OF DIOPHANTINE EQUATIONS

J.H. EVERTSE

MATHEMATISCH CENTRUM AMSTERDAM 1983

1980 Mathematics subject classification: 10B10, 10B15, 10B25, 10C10, 10F25, 10F39, 10F45

ISBN 90 6196 265 X

ACKNOWLEDGEMENT

The present monograph is a version of my Ph.D. thesis, which was written as a result of investigations done at the University of Leiden, under supervision of professor R. Tijdeman. Dr. F. Beukers also played an important role in these investigations. I wish to express my thanks to prof. Tijdeman and dr. Beukers, for without their great support and helpful suggestions I would not have been able to write this dissertation.

I am grateful to the Mathematical Centre for publishing this monograph in the present form.

J.H. Evertse

CONTENTS

LIST OF SYMBOLS AND NOTATIONS, OTHER THAN OF LOCAL USE.

Apart from the notations listed here, we shall use the notations introduced in chapter 4.

$\mathbb{N}$	the set of natural numbers (i.e. $\{1,2,\ldots\}$)
$\mathbb{Z}$	the set of (rational) integers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
$\mathbb{Q}_p$	the set of p-adic numbers, i.e. the p-adic completion of $\mathbb{Q}$
$\mathbb{C}$	the set of complex numbers
$\mathbb{A}$	the set of algebraic numbers (i.e. the algebraic closure of $\mathbb{Q}$)
$\mathbb{Z}_{\geq 0}$, $\mathbb{Z}_{\leq 0}$, etc.	the set of non-negative integers, the set of non-positive integers, etc.
$\emptyset$	the empty set
$A \subset B$, $B \supset A$	A is a subset of B
$a \in A$	a belongs to A
$a \notin A$	a does not belong to A
$A \setminus B$	the elements of A not belonging to B
$A_1 \cup A_2 \cup \ldots \cup A_n$	the union of $A_1,\ldots,A_n$
$A_1 \cap A_2 \cap \ldots \cap A_n$	the intersection of $A_1,\ldots,A_n$
$\lvert A \rvert$	the number of elements of the finite set A
R^*	the set of all non-zero elements of R, where R is a ring, field etc.
$R[x_1,\ldots,x_n]$	the set of polynomials in the variables $x_1,\ldots,x_n$ with coefficients in R
K,L,M, etc.	algebraic number fields
$\mathcal{O}_K$	the ring of integers of the algebraic number field K
$K(\alpha_1,\ldots,\alpha_n)$	the smallest field extension of K containing $\alpha_1,\ldots,\alpha_n$
$[L:K]$	the degree of L over K, where L is a field extension

	of K
a,b, etc.	ideals in some algebraic number field
p,P, etc.	prime ideals in some algebraic number field
$<\alpha_1,\ldots,\alpha_n>_K$	the ideal in K generated by $\alpha_1,\ldots,\alpha_n$ (if confusion is unlikely we omit the subscript K)
σ,τ	isomorphisms (by these we mean injective homomorphisms) of an algebraic number field in $\mathbb{C}$
$\|.\|_v, \|.\|_V, \|.\|_p, \|.\|_p$	valuations
$[\alpha]$	the largest integer not exceeding α
$\overline{\alpha}$	the complex conjugate of the complex number α
$(m_1,\ldots,m_n)$	the positive gcd of the integers $m_1,\ldots,m_n$
$m_1 \mid m_2 \mid m_3 \ldots$	the integer m_1 divides m_2, m_2 divides m_3, ...
$a_1 \supset a_2 \supset a_3 \ldots$	the ideal a_1 divides a_2, a_2 divides a_3, ...
$f(x_1,\ldots,x_n)^c$	the value of the real function f in the variables x_1, $\ldots,x_n$ taken to the power c, where $c\in\mathbb{R}$
f^{-1}	the inverse function (mapping) of the bijective function (mapping) f
$\binom{\alpha}{n}$	$= \alpha(\alpha-1)\ldots(\alpha-n+1)/n!$ for $\alpha\in\mathbb{C}$, $n\in\mathbb{N}$ $= 1$ for $\alpha\in\mathbb{C}$, $n=0$ $= 0$ for $\alpha\in\mathbb{C}$, $n\in\mathbb{Z}_{<0}$
$\sum_{p\mid n}, \prod_{p\mid n}$	the sum, product respectively taken over all primes p dividing n
$\sum_{\alpha\in A}, \prod_{\alpha\in A}, \max_{\alpha\in A}, \min_{\alpha\in A}$	the sum, product, maximum, minimum respectively taken over all elements α of A
$\sum_{\alpha\notin A}, \prod_{\alpha\notin A}, \max_{\alpha\notin A}, \min_{\alpha\notin A}$	the sum, product, maximum, minimum respectively taken over all elements α of some given set which do not belong to A
$\square$	end of a proof
[Si 1] (example)	reference

$|ax^n-by^n| = c$ in $x,y\in\mathbb{Z}$, $(x,y)=1$ ($a>0, b\neq 0, c>0, n\geq 3$) (example)

the equation $|ax^n-by^n|=c$ in coprime integers x,y, where a,b,c,n are integers with $a>0, b\neq 0, c>0, n\geq 3$.

LIST OF SYMBOLS INTRODUCED IN EACH CHAPTER

For each page we give the symbols which are introduced or defined on that page and which are used throughout the remainder of the chapter. The symbols introduced in chapter 4 will also be used in the chapters thereafter.

CHAPTER 0.

p.1 F,m,D; p.3 n,κ; p.4 K,γ; p.5 $p_1,\ldots,p_t,\Psi(F,K,p_1,\ldots,p_t)$

CHAPTER 1.

p.8 $m,n,\nu,r,g,A_m(z),B_m(z),\alpha_m,\beta_m,\gamma_m$; p.9 $E_m(z),F_m(z)$; p.10 $q(m),n_*,C_{im}(z)$, $D_{im}(z)$; p.11 $V_m(z)$

CHAPTER 2.

p.15 $a,b,n,C,T_n,\mu_n,\alpha_n$; p.17 $c,R(n,c)$; p.19 $S(c)$; p.20 $w(x),w(x,y)$; p.22 β, f,ν,κ; p.23 σ_n,w_1,w_2; p.24 $z_1,A_m(z),B_m(z),S_m,r,g,s(m),t(m),P_m,Q_m$; p.25 h,u, $\tilde{E}_m(z),\tilde{F}_m(z),\tilde{E}^*_m(x,y),\tilde{F}^*_m(x,y),d,K_m(z)$; p.27 v,h',w',b_m; p.29 ℓ; p.34 $K(n),A,B$

CHAPTER 3.

p.36 $F(x,y)$; p.37 k; p.38 $H(x,y),A,B,C,D$; p.42 $a,b,c,d,G(x,y),a',b',c',d'$; p.43 M,α,β,ξ,η; p.44 O_0; p.45 Δ,ω; p.46 $\theta_1,\theta_2,\theta_3,\theta$; p.48 $\omega_i,\xi_i,\eta_i,z_1,A_m(z)$, $B_m(z)$; p.49 $r,g,\Sigma_m,\sigma(m),\tau(m),\Xi_m,\P_m,\gamma,\delta,\Lambda_m$; p.52 ℓ_1,ℓ_2

CHAPTER 4.

p.55 $I(K),S(K),w_p(\alpha),w_p(\alpha)$; p.56 $E(K),\overline{\sigma},S_\infty(K),\overline{S}(K),p,v,V,r_1,r_2$; p.57 $c_K(f)$, $N_{K/\mathbb{Q}}(\alpha),N_K(\alpha)$; p.58 $T(\alpha),F_\alpha(z),D(f),d_K(f)$; p.59 $p_\infty,|\alpha|_{p_\infty},|\alpha|_p,K,m,|\alpha|_p$; p.60 $|\alpha|_v,d(v)$; p.61 $s(v),h(\alpha),L(\alpha)$

CHAPTER 5.

p.64 $K,\omega,n,L,S,\{\theta_v\}_{v\in S},B,C,\{\Gamma_v\}_{v\in S},W(z)$; p.65 $|.|_v,\ell_0,k$; p.66 ν,U_n,D; p.67 $W_i,r,A_{2r+1}(z),B_{2r+1}(z),\Phi_r,\Psi_r$; p.68 $G_r(z),H_r(z),T_r(z),F_v$; p.69 ℓ

CHAPTER 6.

p.73 $K,m,r_1,r_2,F,n,p_1,\ldots,p_t,f(z)$; p.75 $\omega,U(n)$; p.76 A; p.77 γ; p.78 $f^*(x,y)$, $D,M,S_0,T_0,\alpha,\beta,\xi,\eta,\xi_1,\eta_1,\omega,a$; p.79 S,T,Δ_S,P; p.80 $K_0,\zeta(z),\Omega_S(z)$; p.81 θ_1,θ_2, $\theta_3,L,|.|_v,m_v(z)$; p.82 $B,R(B)$; p.85 T^+,T^-,θ_v; p.86 Γ_v; p.89 T,U_0,U_1,r; p.93 $K'',g(z)$; p.94 K'

CHAPTER 7.

p.102 $K,m,r_1,r_2,S,\lambda,\mu$; p.104 $a,b,p_1,\ldots,p_t,p_1,\ldots,p_t$; p.106 S_1; p.108 m,n; p.109 r,K_r,h_r; p.110 ρ,p; p.111 ξ,b,G,a,η_1; p.112 $H,U(n)$

CHAPTER 0. INTRODUCTION.

In this monograph we shall derive upper bounds for the numbers of solutions of diophantine equations taken from several classes. One of these classes consists of equations of the type

$$F(x,y) = m \qquad \text{in } x,y\in\mathbb{Z}, \tag{0.1}$$

where F is an irreducible binary form with coefficients in $\mathbb{Z}$ (i.e. a homogeneous polynomial in two variables which is irreducible over $\mathbb{Q}$) and m a non-zero integer.

If F is a linear form, $F(x,y)=ax+by$ say, then (0.1) is solvable if and only if the gcd d of a and b divides m. Moreover, if (x_0,y_0) is one solution of (0.1), then the other solutions of (0.1) are given by $x=x_0+tb/d$, $y=y_0-ta/d$, where t runs through the non-zero integers.

Also if F is a quadratic form of positive discriminant D, then (0.1) has either none or infinitely many solutions. Using the continued fractions expansion of $\sqrt{D}$ one can decide, whether (0.1) is solvable or not and compute the solutions of (0.1) if there are any. (cf [Hu],§§10.8,10.9,11.4, 11.5)

If F is a quadratic form of negative discriminant D, $F(x,y)=ax^2+bxy+cy^2$ say, then (0.1) has at most finitely many solutions. For then each solution (x,y) of (0.1) satisfies

$$(2ax+by)^2-Dy^2 = 4am,$$

hence $|y|\le|4am/D|^{1/2}$. Dirichlet ([Dir]§§86-91, see also [Hu], §12.4) gave an upper bound for the number of solutions of (0.1). Let D be a negative integer with $D\equiv 0$ or $1 \pmod 4$. There are quadratic forms of discriminant D which have integral coefficients with gcd 1. These can be divided into equivalence classes, where equivalence is defined by unimodular transformations. There are at most finitely many of such classes and in each one we choose a fixed representative. Thus we obtain a set $\{F_1,\dots,F_h\}$ of pairwise non-equivalent quadratic forms. For odd primes p, let $\left(\frac{\cdot}{p}\right)$ be the usual Legendre symbol. Moreover, put $\left(\frac{D}{2}\right)=1$ if $D\equiv 1 \pmod 8$ and $\left(\frac{D}{2}\right)=-1$ if $D\equiv 5 \pmod 8$. Put $w=6$ if $D=-3$, $w=4$ if $D=-4$ and $w=2$ if $D<-4$. Let $p_1,\dots,p_t$ be

distinct primes not dividing D and $k_1,\dots,k_t$ positive integers. Dirichlet proved that the number of solutions of

$$F_i(x,y) = p_1^{k_1}\dots p_t^{k_t} \qquad \text{in } x,y\in\mathbb{Z} \text{ and } i\in\{1,\dots,h\}$$

is equal to

$$w \prod_{i=1}^{t} \sum_{j=0}^{k_i} \left(\frac{D}{p_i}\right)^j .$$

The number of solutions of (0.1) does not change when F is replaced by an equivalent form. This implies that for a quadratic form with integral coefficients and discriminant $D<0$ and for an integer m with $(m,D)=1$ and $m=p_1^{k_1}\dots p_t^{k_t}$ for distinct primes p_i and positive integers k_i the equation (0.1) has at most

$$(0.2) \qquad 6(k_1+1)\dots(k_t+1)$$

solutions. In fact, this holds true also if $(m,D)>1$. If F is equivalent to x^2+xy+y^2 and if the primes p_i dividing m satisfy $p_i \equiv 1 \pmod 3$ then (0.2) can not be improved. In the other cases, the bound (0.2) is not optimal but it has the advantage of being independent of the coefficients of F and of the primes dividing m. For historical information on (0.2) in case F has degree ≤ 2 we refer to [Di 2], ch.2,12,13.

From now on, we assume that the form F appearing in (0.1) has degree at least 3. Equation (0.1) is often called the *Thue equation*, after A. Thue, who showed in 1909 [Th 1] that (0.1) has at most finitely many solutions. We shall discuss his method later on. Other proofs were given by Th. Skolem in 1935 [Sk 3] using p-adic power series, however under weak restrictions imposed on F, and by A. Baker in 1967 [B 2,3], using lower bounds for linear forms in logarithms. The methods of Thue and Skolem have the disadvantage of being *ineffective*, i.e. in general they do not supply an algorithm to compute all solutions of (0.1). Baker's method however, is *effective*. Baker gave an explicit upper bound for the solutions of (0.1). The estimates in his arguments have been improved later. Using a modification of Baker's method by Stark [St] and explicit estimates of Loxton and van der Poorten [L/P] on linear forms in logarithms and of Siegel [Si 5] and Györy [Gy] on units and regulators, one can show that every solution of (0.1) satisfies

$$(0.3)\qquad \max(|x|,|y|) < \exp\Big((4n)^{50(n+2)}|D|^{1/2}(\log|D|)^{n+1}\cdot \cdot\big(|D|^{1/2}(\log|D|)^{n-1}+\log A+\log|m|\big)\Big)\ ,$$

where n is the degree, D the discriminant and A the maximum of the absolute values of the coefficients of F. In this thesis we shall be mainly interested in upper bounds for the *number* of solutions of (0.1). We shall apply ineffective methods similar to that of Thue, since they seem to lead to far better estimates.

Thue derived his result on the number of solutions of (0.1) from his own theorem on the approximation of algebraic numbers by rationals [Th 1]:

let α *be an algebraic number of degree* n *and let* $\kappa>n/2+1$. *Then the inequality*

$$(0.4)\qquad \Big|\frac{x}{y}-\alpha\Big| < |y|^{-\kappa} \qquad \textit{in } x,y\in\mathbb{Z} \textit{ with } y\neq 0$$

has at most finitely many solutions.

The argument is as follows. Suppose that (0.1) has infinitely many solutions. Since F is irreducible, we have

$$F(x,y) = \beta(x-\alpha_1 y)(x-\alpha_2 y)\ldots(x-\alpha_n y)\ ,$$

where $\beta\in\mathbb{Z}$ and where $\alpha_1,\alpha_2,\ldots,\alpha_n$ are algebraic numbers of degree $n\geq 3$. There is no loss of generality in assuming that (0.1) has infinitely many solutions (x,y) with

$$y\neq 0, \qquad \Big|\frac{x}{y}-\alpha_1\Big| \leq \Big|\frac{x}{y}-\alpha_i\Big| \qquad \text{for } i=2,3,\ldots,n.$$

These solutions satisfy

$$\Big|\frac{x}{y}-\alpha_i\Big| \geq \frac{1}{2}\Big(\Big|\frac{x}{y}-\alpha_i\Big|+\Big|\frac{x}{y}-\alpha_1\Big|\Big) \geq \frac{1}{2}|\alpha_i-\alpha_1| \qquad \text{for } i=2,3,\ldots,n,$$

and hence

$$|m| = |F(x,y)| \geq |\beta||y|^n\Big|\frac{x}{y}-\alpha_1\Big|\Big|\frac{x}{y}-\alpha_2\Big|\ldots\Big|\frac{x}{y}-\alpha_n\Big|$$
$$\geq c|y|^n\Big|\frac{x}{y}-\alpha_1\Big|,$$

where c is a positive constant depending on F only. But this implies that

$$|\frac{x}{y} - \alpha_1| \leq \frac{|m|c^{-1}}{|y|^n},$$

which is in view of Thue's result on (0.4) and the inequality $n>n/2+1$ for $n\geq 3$, possible for at most finitely many pairs (x,y). This contradicts our assumption. Hence (0.1) has at most finitely many solutions.

Thue's results on (0.1) and (0.4) have been improved and generalised by several mathematicians. In his thesis, C.L. Siegel [Si 1] showed, that (0.4) has at most finitely many solutions if $\kappa>2n^{1/2}$. In 1947/48, F.J. Dyson [Dy] and A.O. Gel'fond [Ge 2] independently improved this to $\kappa>(2n)^{1/2}$. Finally, in 1955, K.F. Roth [Ro] reduced this condition to $\kappa>2$. The methods of Thue, Siegel,..., Roth are all ineffective. However, for some special equations of type (0.1) modifications of these methods have led or can lead to considerable improvements of (0.3). (cf. [Th 2],[B 1],[Bo],[Chu 2]).

Also in his thesis, Siegel considered the approximation of algebraic numbers by numbers from a fixed algebraic number field and the consequences for diophantine equations. Let F be a binary form of degree n with coefficients in some algebraic number field K of degree m and with non-zero discriminant and let γ be an integer in K. Siegel([Si 1],Satz 5) showed that if

$$n \geq m \cdot \min_{s=1,\ldots,n} (s+n/(s+1))$$

then there are at most finitely many pairs of integers (x,y) in K^2 satisfying

$$F(x,y) = \gamma. \tag{0.5}$$

In 1929, Siegel ([Si 3], zweiter Teil) proved the following extension. Let G(x,y) be an absolutely irreducible polynomial with algebraic coefficients such that the curve C defined by G(x,y)=0 has genus ≥ 1. Then C contains at most finitely many points (x,y) for which both x and y belong to the algebraic number field K and for which at least one of x,y is an algebraic integer. This result implies that (0.5) has only finitely many solutions in integers x,y of K if $\deg F \geq 3$.

In 1933, K. Mahler [Ma 1,2] generalised Thue's result in another direction. He studied the simultaneous approximation of real algebraic

numbers and p-adic algebraic numbers for finitely many primes p by rationals. His investigations ([Ma 2],Satz 6) led to this result: for every irreducible binary form F of degree ≥3 with rational integral coefficients there exists a positive constant c, depending on F only, such that the number of solutions of

$$|F(x,y)| = p_1^{k_1}\cdots p_t^{k_t} \qquad \text{in } x,y,k_1,\ldots,k_t \in \mathbb{Z} \text{ with } (x,y)=1,\ k_1\geq 0,\ldots,k_t\geq 0, \tag{0.6}$$

where $p_1,\ldots p_t$ are distinct primes, is finite and at most equal to c^{t+1}. Equation (0.6) is often called the *Thue-Mahler equation*.

In 1950, C.J. Parry [Pa] studied the simultaneous approximation of complex algebraic numbers and of algebraic numbers in the algebraic closure of $\mathbb{Q}_p$ for finitely many primes p by numbers taken from a fixed algebraic number field K. As a consequence he proved a theorem which is formulated precisely in chapter 6.(see also [Pa],pp 77/78). Here we mention a result which is in fact equivalent to that theorem: let F be a binary form of degree n≥3 with integral coefficients in K and non-zero discriminant and let $p_1,\ldots p_t$ be distinct prime numbers. Define $\Psi(F,K,p_1,\ldots,p_t)$ to be the number of fractions x/y such that x and y are integers in K with y≠0 and

$$|N_{K/\mathbb{Q}}(F(x,y))| = p_1^{k_1}\cdots p_t^{k_t} \tag{0.7}$$

for some non-negative integers $k_1,\ldots k_t$. Then $\Psi(F,K,p_1,\ldots,p_t)$ is finite and bounded above by c_0^{t+1}, where c_0 is a positive constant, depending on F and K only. This implies earlier stated results on (0.1),(0.5),(0.6). For by Parry's result there are finitely many fractions x/y for which x and y are integers in K satisfying (0.5) and if (x,y) is a solution of (0.5) with y≠0 then $\gamma=y^n F(x/y,1)$. Furthermore, each solution of (0.6) with y≠0 is completely determined by x/y up to the sign of y.

Very recently, the German mathematician G. Faltings [Fa] proved the so-called *Mordell conjecture*: let K be an algebraic number field and let $G(x,y)\in K[x,y]$ be an absolutely irreducible polynomial such that the curve C:G(x,y)=0 has genus at least 2. Then C contains at most finitely many points $(x,y)\in K^2$. As a consequence, equation (0.5) has at most finitely many (not necessarily integral) solutions in $x,y\in K$ if F has degree at least 4. From this, it follows easily that the number $\Psi(F,K,p_1,\ldots,p_t)$ which was defined relative to (0.7) is finite in case that n≥4.

We shall now give a survey of the contents of this monograph. An important rôle will be played by an approximation method which deals with the approximation of numbers of the type $\sqrt[n]{b/a}$ (where a,b,n are non-zero integers with $n \geq 3$) by rationals. This method is originally due to Thue [Th 2] but has been modified later by Siegel [Si 4]. Therefore, we shall refer to it as the Thue-Siegel method. For historical remarks about this method we refer to [Si 6]. We shall follow Siegel's arguments but instead of Siegel's hypergeometric functions we use polynomials. This has the advantage of not having to worry about convergence. The essential properties of these polynomials are discussed in chapter 1.

In chapter 2, in which only some knowledge of elementary number theory is presupposed, we use the Thue-Siegel method to obtain information about the solutions of

$$|ax^n - by^n| = c \qquad \text{in } x,y \in \mathbb{N} \text{ with } (x,y)=1, \tag{0.8}$$

where a,b,c,n are integers with $a>0, b\neq 0, c>0, n\geq 3$. It is shown that the number of solutions of (0.8) is at most $2n^{\omega(c)}+4$, where $\omega(c)$ is the number of distinct primes dividing c.

In chapter 3 we consider the equation

$$F(x,y) = 1 \qquad \text{in } x,y \in \mathbb{Z}, \tag{0.9}$$

where F is a binary cubic form with rational integral coefficients and positive discriminant D. We show that elements α,β of the field $M=\mathbb{Q}(\sqrt{-3D})$ exist, as well as linear forms $\xi,\eta \in M[x,y]$, such that

$$\alpha\xi^3 - \beta\eta^3 = 3\sqrt{-3D}\cdot F(x,y)$$

identically in x,y. By using this fact in combination with a modified version of the Thue-Siegel method we show that (0.9) has at most *twelve* solutions.

In chapter 4 we develop some algebraic tools which are needed in the chapters thereafter. In particular we introduce valuations and a height function similar to Bombieri's in [Bo].

In chapter 5 we generalise the Thue-Siegel method. We prove a result on the approximation of n-th roots (where $n\geq 3$) of a fixed number in an algebraic number field K by elements of K, in which both archimedean and

non-archimedean valuations are involved.

The result of chapter 5 is used in chapter 6. Let K be an algebraic number field of degree m. Further, let F be a binary form of degree $n \geq 3$ with integral coefficients in K such that $F(1,0) \neq 0$ and such that the polynomial $F(x,1)$ has at least three distinct zeros. Let $p_1,\ldots,p_t$ be distinct primes. We shall show that the number $\Psi(F,K,p_1,\ldots,p_t)$, which was defined relative to (0.7), does not exceed

$$7^{15\left(\binom{n}{3}m+1\right)^2} + 6\times 7^{2\binom{n}{3}m(t+1)} . \tag{0.10}$$

This is an improvement of Parry's result since (0.10) depends on m,n and t only. From (0.10) we derive an upper bound for the number of solutions of (0.1) which depends on the degree of F and the number of primes dividing m only. Such a bound does not exist when F is a positive definite quadratic form (cf (0.2)). We shall prove (0.10) firstly for n=3 by generalising the method of chapter 3 and then in general by taking a cubic divisor of F in some extension of K. In the derivation of (0.10) we actually use only results on the approximation of cubic roots of a fixed number in an algebraic number field by numbers of that field, whereas Parry considered the approximation of more general algebraic numbers.

In chapter 7 we prove some results on diophantine equations which can be reduced to a finite number of Thue or Thue-Mahler equations. For example we show that if $p_1,\ldots p_t$ are distinct primes and if a,b are non-zero integers, then the number of pairs $(x,y)\in\mathbb{Q}^2$ such that both the numerators and denominators of x,y are composed of primes from $p_1,\ldots,p_t$ and such that

$$ax+by = 1$$

is at most 296×7^{2t}. We shall also show that the number of solutions of the equation

$$x^m - y^n = 1 \qquad \text{in } x,y\in\mathbb{N} \qquad (m\geq 2, n\geq 2, mn\geq 6)$$

is at most $(mn)^{\min(m,n)}$.

CHAPTER 1. PROPERTIES OF THE AUXILIARY POLYNOMIALS.

In this chapter we shall study some polynomials which will be used in the chapters hereafter. Let m,n be integers with $m \geq 0$ and $n \geq 3$ and put $\nu = n^{-1}$. To each m we associate integers r,g with $g \in \{0,1\}$ such that $m = 2r+g-1$. We define

$$(1.1) \qquad A_m(z) = \sum_{k=0}^{r} \binom{r-g+\nu}{k}\binom{r-\nu}{r-k} z^k \ , \quad B_m(z) = \sum_{k=0}^{r-g} \binom{r-\nu}{k}\binom{r-g+\nu}{r-g-k} z^k \quad \text{for } m \geq 1,$$

$$A_0(z) = 1 \ , \quad B_0(z) = 0 \ .$$

Here it is supposed that the variable z assumes its values in some field of characteristic 0. Many of the properties of these polynomials can be derived from the theory of hypergeometric functions. Instead of doing this, we extend an elementary method of Faddeev. ([D/F], ch.5)

LEMMA 1.1. *(i) For* $m = 1, 2, \ldots$ *we have*

$$(1.2) \qquad \begin{aligned} A_{m+1}(z) &= \alpha_m A_m(z) - \beta_m (1-z) A_{m-1}(z) \ , \\ B_{m+1}(z) &= \alpha_m B_m(z) - \beta_m (1-z) B_{m-1}(z) \ , \end{aligned}$$

where

$$(1.3) \qquad \begin{aligned} \alpha_m &= 2, \qquad \beta_m = \frac{r-\nu}{r} \ \textit{if} \ m = 2r, \\ \alpha_m &= \frac{2r+1}{r+1}, \quad \beta_m = \frac{r+\nu}{r+1} \ \textit{if} \ m = 2r+1. \end{aligned}$$

(ii) For $m = 2, 3, \ldots$ *we have*

$$\begin{aligned} zA_m''(z) + (1-\nu)A_m'(z) &= \gamma_m A_{m-2}(z) \ , \\ zB_m''(z) + (1+\nu)B_m'(z) &= \gamma_m B_{m-2}(z) \ , \end{aligned}$$

where

$$\gamma_m = (r-g+\nu)(r-\nu) \ .$$

PROOF. These identities can be proved easily by showing that the left- and

the right-hand sides of the expressions given in (1.2), (1.3) are polynomials with equal coefficients. For example, we shall prove that

$$A_{2r+1}(z) = 2A_{2r}(z) - \frac{r-\nu}{r}(1-z)A_{2r-1}(z) \text{ for } r=1,2,\ldots,$$

that is

$$\text{(1.4)} \qquad \binom{r+\nu}{k}\binom{r-\nu}{r-k} =$$

$$2\binom{r-1+\nu}{k}\binom{r-\nu}{r-k} - \frac{r-\nu}{r}\binom{r-1+\nu}{k}\binom{r-1-\nu}{r-1-k} + \frac{r-\nu}{r}\binom{r-1+\nu}{k-1}\binom{r-1-\nu}{r-k}$$

for $k=0,1,\ldots,r$.

The right-hand side of (1.4) is equal to

$$\binom{r+\nu}{k}\binom{r-\nu}{r-k}\left(2\frac{r-k+\nu}{r+\nu} - \frac{r-\nu}{r}\frac{r-k+\nu}{r+\nu}\frac{r-k}{r-\nu} + \frac{r-\nu}{r}\frac{k}{r+\nu}\frac{k-\nu}{r-\nu}\right) =$$

$$\binom{r+\nu}{k}\binom{r-\nu}{r-k}\left(\frac{2r(r-k+\nu)-(r-k+\nu)(r-k)+k(k-\nu)}{r(r+\nu)}\right) = \binom{r+\nu}{k}\binom{r-\nu}{r-k}. \quad \square$$

Put

$$E_m(z) = \sum_{k=0}^{r}\binom{r-g+\nu}{k}\binom{2r-g-k}{r-g}(-z)^k, \quad F_m(z) = \sum_{k=0}^{r-g}\binom{r-\nu}{k}\binom{2r-g-k}{r}(-z)^k$$

$$\text{(1.5)} \qquad \text{for } m=1,2,\ldots,$$

$$E_0(z) = 1, \quad F_0(z) = 0.$$

LEMMA 1.2. $E_m(z)=A_m(1-z)$, $F_m(z)=B_m(1-z)$ *for* $m=0,1,\ldots$.

PROOF. We shall proceed by induction on m. The lemma can be verified easily for m=0,1. Suppose it has been proved for all $m\le t$, where $t\ge 2$. An easy computation shows that

$$E_{t+1}(z) = \alpha_t E_t(z) - \beta_t z E_{t-1}(z), \quad F_{t+1}(z) = \alpha_t F_t(z) - \beta_t z F_{t-1}(z).$$

Hence by (1.2) and by the induction hypothesis lemma 1.2 is valid for m=t+1. $\square$

LEMMA 1.3. *(i) Put* $q(m)=n^r(n^r,r!)$. *Then* $q(m)A_m(z)$ *and* $q(m)B_m(z)$ *have rational integral coefficients.*
(ii) Suppose that n *is odd and let* n_* *be the maximal positive square-free divisor of* n. *Then there are polynomials* $C_{im}(z), D_{im}(z)$ *for* $m=0,1,2,\ldots$ *and* $i=1,2$ *with rational integral coefficients depending on* n *such that*

$$\begin{aligned} A_m(1-n^{3/2}z) &= C_{1m}(z^2)+n_*^{1/2}zC_{2m}(z^2), \\ B_m(1-n^{3/2}z) &= D_{1m}(z^2)+n_*^{1/2}zD_{2m}(z^2). \end{aligned} \tag{1.6}$$

PROOF. Firstly, we shall show that for every pair of integers a,k,

$$d_1 := \binom{a\nu}{k} n^k (n^k,k!) \in \mathbb{Z}, \tag{1.7}$$

that is, d_1 is a p-adic integer for all primes p. Note that there exists an integer d_2 such that

$$d_1 = d_2 \frac{(n^k,k!)}{k!} .$$

Hence d_1 is a p-adic integer for all primes p dividing n. But for primes p not dividing n, $\binom{a\nu}{k}$ is even p-adically integral. This shows (1.7) completely.

(1.7) clearly implies that $q(m)E_m(z)$ and $q(m)F_m(z)$, whence $q(m)A_m(z)$ and $q(m)B_m(z)$ have rational integral coefficients. By (1.7) we have also that $E_m(n^{3/2}z)$ and $F_m(n^{3/2}z)$ have algebraic integral coefficients for odd n. For let p be a prime such that p^t divides n for some positive integer t, but p^{t+1} does not. Then $p\geq 3$. Hence the number of times that p divides $(n^k,k!)$ equals

$$\sum_{j=1}^{\infty} [kp^{-j}] < k \sum_{j=1}^{\infty} p^{-j} = \frac{k}{p-1} \leq \frac{k}{2} \leq \frac{kt}{2} .$$

Together with (1.7) this implies that

$$\binom{a\nu}{k}(n^{3/2})^k = \binom{a\nu}{k}(n^k(n^k,k!))(n^k(n^k,k!))^{-1}(n^{3/2})^k$$

is an algebraic integer. Therefore the coefficients of $E_m(n^{3/2}z)$, $F_m(n^{3/2}z)$ are algebraic integers. But we have also that the coefficients of these polynomials corresponding to even powers of z are rational numbers, while the coefficients corresponding to odd powers of z are the product of $n_*^{1/2}$ and a rational number. By lemma 1.2 this proves lemma 1.3 completely. □

LEMMA 1.4. *For every non-negative integer* m *there exists a polynomial* $V_m(z)$ *with non-negative coefficients such that*

$$A_m(z^n)-zB_m(z^n) = (1-z)^m V_m(z), \tag{1.8}$$

$$V_m(1) = n^m \binom{r-g+\nu}{r+1-g}\binom{r-\nu}{r}\Big/\binom{m}{r}. \tag{1.9}$$

PROOF. We shall proceed by induction on m. For m=0,1 we may take $V_m(z)=1$. Suppose our lemma has been proved for all $m\le t$, where $t\ge 1$. We define the rational function

$$V_{t+1}(z) = \frac{A_{t+1}(z^n)-zB_{t+1}(z^n)}{(1-z)^{t+1}} .$$

We have to show that $V_{t+1}(z)$ is a polynomial with non-negative coefficients.

By (1.2) we have

$$(1-z)^{t+1}V_{t+1}(z) = A_{t+1}(z^n)-zB_{t+1}(z^n) =$$

$$\alpha_t(A_t(z^n)-zB_t(z^n)) - \beta_t(1-z^n)(A_{t-1}(z^n)-zB_{t-1}(z^n)) =$$

$$(1-z)^t(\alpha_t V_t(z)-\beta_t(1+z+\ldots+z^{n-1})V_{t-1}(z)) .$$

Hence, on dividing by $(1-z)^t$,

$$(1-z)V_{t+1}(z) = \alpha_t V_t(z)-\beta_t(1+z+\ldots+z^{n-1})V_{t-1}(z). \tag{1.10}$$

It follows from (1.9) that $\alpha_t V_t(1)=n\beta_t V_{t-1}(1)$. Hence the right-hand side of (1.10) is a polynomial divisible by 1-z. This implies that $V_{t+1}(z)$ is a polynomial.

Note that by (1.3)

$$\frac{d^2}{dz^2}(A_{t+1}(z^n)-zB_{t+1}(z^n))$$

$$= n^2z^{2n-2}A''_{t+1}(z^n)+n(n-1)z^{n-2}A'_{t+1}(z^n) -$$

$$- n^2z^{2n-1}B''_{t+1}(z^n)-n(n+1)z^{n-1}B'_{t+1}(z^n)$$

$$= n^2z^{n-2}\Big((1-\nu)A'_{t+1}(z^n)+z^nA''_{t+1}(z^n)-z\{(1+\nu)B'_{t+1}(z^n)+z^nB''_{t+1}(z^n)\}\Big)$$

$$= n^2 z^{n-2} \gamma_{t+1}(A_{t-1}(z^n)-zB_{t-1}(z^n))$$

$$= n^2 \gamma_{t+1} z^{n-2}(1-z)^{t-1} V_{t-1}(z),$$

while on the other side,

$$\frac{d^2}{dz^2}(A_{t+1}(z^n)-zB_{t+1}(z^n)) = \frac{d^2}{dz^2}((1-z)^{t+1}V_{t+1}(z)) =$$

$$(t+1)t(1-z)^{t-1}V_{t+1}(z)-2(t+1)(1-z)^t V'_{t+1}(z)+(1-z)^{t+1}V''_{t+1}(z) .$$

Hence, on dividing by $(1-z)^{t-1}$,

$$(1.11) \qquad (1-z)^2 V''_{t+1}(z)-2(t+1)(1-z)V'_{t+1}(z)+(t+1)tV_{t+1}(z)=n^2\gamma_{t+1}z^{n-2}V_{t-1}(z).$$

This shows that $(t+1)tV_{t+1}(1)=n^2\gamma_{t+1}V_{t-1}(1)$. By our induction hypothesis this implies that (1.9) holds for $m=t+1$.

We shall now show that $V_{t+1}(z)$ has non-negative coefficients. Put

$$(1.12) \qquad W_{t+1}(z) = (t+1)V_{t+1}(z)-(1-z)V'_{t+1}(z).$$

Then, by (1.11),

$$(1.13) \qquad tW_{t+1}(z)-(1-z)W'_{t+1}(z) = n^2\gamma_{t+1}z^{n-2}V_{t-1}(z).$$

Put

$$V_{t+1}(z) = \sum_{k=0}^{\infty} a_k z^k \ , \ V_{t-1}(z) = \sum_{k=0}^{\infty} b_k z^k \ , \ W_{t+1}(z) = \sum_{k=0}^{\infty} c_k z^k.$$

Then $a_k=b_k=c_k=0$ for sufficiently large values of k. By (1.13) we have for every $k\geq 0$

$$(k+t)c_k = (k+1)c_{k+1}+n^2\gamma_{t+1}b_{k-n+2}$$

where $b_{k-n+2}:=0$ for $k<n-2$. By the induction hypothesis we have $c_k\geq 0$ if $c_{k+1}\geq 0$. Hence $c_k\geq 0$ for all k. By (1.12) we have

$$(k+t+1)a_k = (k+1)a_{k+1}+c_k,$$

which shows that $a_k \geq 0$ for all k. This completes the proof of lemma 1.4. □

LEMMA 1.5. $A_m(z)B_{m+h}(z) \neq A_{m+h}(z)B_m(z)$ *for* $z \neq 1$, $m, h \in \mathbb{Z}$, $m \geq 0$, $h \in \{1,2\}$.

PROOF. From

$$A_m(z^n)-zB_m(z^n) = (1-z)^m V_m(z),$$

$$A_{m+h}(z^n)-zB_{m+h}(z^n) = (1-z)^{m+h} V_{m+h}(z)$$

we obtain

$$U_{mh}(z^n) := A_m(z^n)B_{m+h}(z^n)-A_{m+h}(z^n)B_m(z^n) = R_{mh}(z)(1-z)^m, \tag{1.14}$$

where $R_{mh}(z)$ is some polynomial. Since the left-hand side of (1.14) is a polynomial in z^n it must be divisible by $(1-z^n)^m$. But one verifies easily that $U_{mh}(z)$ has degree at most m. Hence $R_{mh}(z)$ is a constant. A substitution of z=0 in (1.14) yields that this constant is non-zero. Hence z=1 is the only zero of $U_{mh}(z)$. □

LEMMA 1.6. *(i) For* $z \in \mathbb{C}$ *we have*

$$\begin{aligned} &|A_m(z)| \leq \binom{2r-g}{r}\max(1,|z|)^r, \quad |B_m(z)| \leq \binom{2r-g}{r}\max(1,|z|)^{r-g}, \\ &|V_m(z)| \leq n^m \binom{r-g+\nu}{r+1-g}\binom{r-\nu}{r}\binom{m}{r}^{-1}\max(1,|z|)^{r(n-2)}. \end{aligned} \tag{1.15}$$

(ii) For $z \in \mathbb{C}$ *with* $|1-z| \leq 1$ *we have*

$$|A_m(z^n)| \leq \binom{2r-g}{r}2^{nr}, \quad |B_m(z^n)| \leq \binom{2r-g}{r}2^{nr}, \quad |V_m(z)| \leq \binom{2r-g}{r}2^{nr}. \tag{1.16}$$

PROOF. Note that $A_m(z), B_m(z), V_m(z)$ have non-negative coefficients and degrees $r, r-g, r(n-2)$ respectively. Hence the sums of the absolute values of the coefficients of these polynomials are equal to their values in 1. Hence

$$\begin{aligned} &|A_m(z)| \leq A_m(1)\max(1,|z|)^r, |B_m(z)| \leq B_m(1)\max(1,|z|)^{r-g}, \\ &|V_m(z)| \leq V_m(1)\max(1,|z|)^{r(n-2)}. \end{aligned} \tag{1.17}$$

By lemma 1.2 we have $A_m(1)=B_m(1)=\binom{2r-g}{r}$. Together with (1.9) this implies (i).

To show (ii) we note that $|1-z|\le 1$ implies that $|z|\le 2$. Hence

$$|A_m(z^n)|\le A_m(2^n),\quad |B_m(z^n)|\le B_m(2^n),\quad |V_m(z)|\le V_m(2)\ . \tag{1.18}$$

Note that by (1.2)

$$A_{m+1}(2^n) = \alpha_m A_m(2^n)+\beta_m(2^n-1)A_{m-1}(2^n),$$

$$B_{m+1}(2^n) = \alpha_m B_m(2^n)+\beta_m(2^n-1)B_{m-1}(2^n).$$

Since clearly $A_0(2^n)\ge B_0(2^n)$, $A_1(2^n)\ge B_1(2^n)$ this implies that $A_m(2^n)\ge B_m(2^n)$ for all m. Hence by (1.8),

$$V_m(2) = |A_m(2^n)-2B_m(2^n)| \le A_m(2^n) \le A_m(1)2^{nr} = \binom{2r-g}{r}2^{nr}.$$

By (1.18) this implies (ii). □

CHAPTER 2. ON THE EQUATION $ax^n-by^n=c$.

§2.1. Introduction.

In this chapter we shall deal with the diophantine inequality

$$|ax^n-by^n| \le C \quad \text{in } x,y\in\mathbb{N},\ (x,y)=1 \quad (a,b,n\in\mathbb{Z},\ a>0,b\neq 0,\ n\ge 3, C\in\mathbb{R},\ C\ge 1)\ . \tag{2.1}$$

By an approximation method in which the polynomials from the preceding chapter are used we shall show the following:

THEOREM 2.1. *Put*

$$T_n = 3^{-(n-2)/n} \prod_{p\mid n} p^{1/(p-1)},$$

$$\mu_3 = T_3^{11/2}, \mu_n = T_n^{\max((n+2)/2(n-3),n/(n-2))} \text{ for } n\ge 4,$$

$$\alpha_3 = 9, \quad \alpha_n = \max((3n-2)/2(n-3),2(n-1)/(n-2)) \text{ for } n\ge 4.$$

Then the inequality (2.1) *has at most* one *solution with*

$$\max(ax^n,|by^n|) \ge \mu_n C^{\alpha_n}. \tag{2.2}$$

In the table below we have written down some values of μ_n and α_n, rounded off to two decimals.

n	3	4	5	6	7	8	9	10
μ_n	1152.20	98.53	10.67	31.59	8.00	13.44	11.39	23.31
α_n	9.00	5.00	3.25	2.67	2.40	2.33	2.29	2.25

α_n decreases monotonically to 2 if n tends to infinity but μ_n behaves irregularly. However, we have

$$\mu_n < n^2 \text{ for } n\ge 5. \tag{2.3}$$

This is clear for $5\le n\le 8$ while for $n\ge 8$

$$\mu_n = T_n^{n/(n-2)} = \frac{1}{3}\Big(n \prod_{p|n} p^{1/(p-1)}\Big)^{n/(n-2)}$$

$$\leq \frac{2^{n/(n-2)}}{3}\Big(n \prod_{p|n} p^{1/2}\Big)^{n/(n-2)} < n^{3n/2(n-2)} \leq n^2.$$

For most of the applications of theorem 1.2 this upper bound will suffice.

Theorem 2.1 is an improvement of theorem 3 of [Ev 1](p.291), especially in the case n=3. There we showed, that for n=3 (2.1) has at most three solutions with $\max(ax^3, |by^3|) \geq (1.71\times 10^7)C^{11}$. In the proof of theorem 2.1 we shall use the polynomials constructed in the preceding chapter. In [Ev 1] we used hypergeometric functions which are closely related to the polynomials from chapter 1. Also by means of these hypergeometric functions, Siegel [Si 4] showed, that (2.1) has at most one solution if

$$|ab|^{n/2-1} \geq 4\Big(n \prod_{p|n} p^{1/(p-1)}\Big)^n C^{2n-2}.$$

Hyyrö ([Hy 2],Satz 1,p.11) generalised Siegel's result in the following way: there are constants $\sigma_0=\sigma_0(n)\in(0,1]$, $C_0=C_0(n,ab)>0$ with the following property: for any pair of real numbers σ,C with $\sigma_0\leq\sigma\leq 1, C>0$ such that $\sigma=\sigma_0$, $C>C_0$ do not hold simultaneously, the equation

$$|ax^n-by^n| = z \quad \text{in } x,y,z\in\mathbb{N} \qquad (a,b,n\in\mathbb{N},\ n\geq 3)$$

has at most one solution with $(x,y)=1$, $z<C\max(ax^n,by^n)^{1-\sigma}$ and $\max(ax^n,by^n) > G=G(n,\sigma,C,ab)$. By choosing $\sigma=1$ for those values of n for which $\sigma_0(n)<1$, i.e. $n\geq 4$, Hyyrö obtained a result similar to but somewhat weaker than theorem 2.1.

We shall also deal with the equation

$$(2.4) \qquad ax^n-by^n = c \qquad \text{in } x,y\in\mathbb{Z} \qquad (a,b,c,n\in\mathbb{Z},\ n\geq 3, abc\neq 0)$$

For some small values of n and c sharp estimates for the number of solutions of (2.4) can be given. Nagell showed that the number of solutions of (2.4) in integers x,y with $xy\neq 0$ is at most 1 if n=3,c=1,3 (with the exception of $2x^3+y^3=3$ which has solutions (1,1),(4,-5))[Na 1] and at most 2 if n=3,c=2,4 and a,b odd [Na 3]. Ljunggren [Lj 1,4] showed that (2.4) has at most one solution in positive integers x,y if n=4,c=1,2,4,8 and if n=6, c=1,2,3,4,6,a>0,b>0,(ab,c)=1, ab is not a square or cube of an integer and

and not divisible by the sixth power of a prime. Domar [Do] showed that

$$(2.5) \qquad |ax^n - by^n| = 1 \qquad \text{in } x,y \in \mathbb{N} \qquad (a,b,n \in \mathbb{N}, n \geq 5)$$

has at most two solutions. While the methods of Nagell and Ljunggren were algebraic, Domar showed his result by improving some of the estimates Siegel used in [Si 4]. In fact, Domar's result follows immediately from theorem 2.1. For this theorem implies, together with (2.3) and $2^n \geq n^2$ for $n \geq 5$, that (2.5) has at most one solution with $\max(x,y) \geq 2$.

Let $R(n,c)$ denote the number of residue classes $Z \pmod c$ with $Z^n \equiv 1 \pmod c$. We shall derive an upper bound for the number of solutions of (2.4) in terms of $R(n,c)$.

THEOREM 2.2. *The number of solutions of*

$$(2.6) \qquad |ax^n - by^n| = c \qquad \textit{in } x,y \in \mathbb{N}, (x,y)=1$$
$$(a,b,c,n \in \mathbb{Z}, a>0, b \neq 0, c>0, n \geq 3)$$

is bounded above by

$$\begin{aligned} &2R(3,c)+4 && \textit{if } n=3, \\ &R(4,c)+3 && \textit{if } n=4, \\ &R(5,c)+2 && \textit{if } n=5 \quad (R(5,c)+1 \textit{ if } c \geq 25), \\ &R(n,c)+1 && \textit{if } n \geq 6. \end{aligned}$$

This is an improvement of theorem 1 of [Ev 1] for n=3,5,6. Using theorem 2.1 one can show that (2.6) can not have many "large" solutions and by congruence considerations one can estimate the number of "small" solutions of (2.6) from above. Doing so, one obtains theorem 2.2.

The following theorem, which is stated without proof, is another consequence of theorem 2.1.

THEOREM 2.3. *The number of solutions of*

$$ax^n - by^n = dz \qquad (a,b,d,n \in \mathbb{Z}, a>0, b \neq 0, d>0, n \geq 3, (a,d)=(b,d)=1)$$

in integers x,y,z *with* $x>0, y>0, (x,y)=1, 0<|z| \leq d^{2n/5-1}$ *is bounded above by*

$$3R(3,d)+4 \qquad \textit{if } n=3,$$

$$\begin{cases} 2R(4,d)+2 & \text{if } n=4, \\ 2R(n,d)+1 & \text{if } n=5,6, \\ R(7,d)+3 & \text{if } n=7, \\ R(n,d)+2 & \text{if } n\geq 8. \end{cases}$$

Apart from an improvement in case n=3, this result is the same as theorem 2 of [Ev 1]. One can derive theorem 2.3 from theorem 2.1 similarly as theorem 2 is derived from theorem 3 in [Ev 1].

Let m,n be given positive integers. We shall give an upper bound for R(n,m) in order to replace the bounds in theorem 2.2 by simpler ones. Let $\omega(m)$ be the number of primes dividing m and let $\phi(m)$ be the number of positive integers not exceeding m and coprime to m. Let $m=2^{k_0}p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$ where k_0 is a non-negative integer, $k_1,\ldots,k_s$ are positive integers and $p_1,\ldots,p_s$ are distinct, odd primes. By elementary number theory we have

$$R(n,m) = R(n,2^{k_0}) \prod_{i=1}^{s} R(n,p_i^{k_i}) . \tag{2.7}$$

Furthermore, it is easy to verify that $R(n,p_i^{k_i})=(n,\phi(p_i^{k_i}))$ for $i\in\{1,\ldots,k\}$ and that $R(n,2^{k_0})$ is equal to 1 if $k_0\in\{0,1\}$ and to $(n,2)(n,2^{k_0-2})$ if $k_0\geq 2$. Hence $R(n,2^{k_0})$ divides $((n,2)n,\phi(2^{k_0}))$. Together with (2.7) this implies that R(n,m) divides

$$((n,m,2)n^{\omega(m)},\phi(2^{k_0})\prod_{i=1}^{s}\phi(p_i^{k_i})) = ((n,m,2)n^{\omega(m)},\phi(m)) .$$

Substituting this into theorem 2.2 we obtain

COROLLARY. *Let* $a,b,n,k_1,k_2,\ldots,k_t$ *be integers with* $a>0, b\neq 0, n\geq 3, k_i\geq 0$ *for* $i\in\{1,2,\ldots,t\}$ *and let* $p_1,p_2,\ldots,p_t$ *be distinct primes. Then the equation*

$$|ax^n-by^n| = p_1^{k_1}p_2^{k_2}\ldots p_t^{k_t} \tag{2.8}$$

has at most $2n^t+4$ *solutions in integers* x,y *with* $x>0, y>0, (x,y)=1$.

In chapter 6 we shall see that the number of solutions of (2.8) can be estimated from above by a constant depending only on n and t even if the exponents $k_1,\ldots,k_t$ are considered as variables.

§2.2. Lemmas and special cases.

In this section we shall prove some auxiliary results for the proofs of theorems 2.1 and 2.2. We shall also deal with some special cases of these theorems. a,b,c,n will denote integers with $a>0, b\neq 0, c>0, n\geq 3$ and C will denote a real with $C\geq 1$.

LEMMA 2.1. *There are non-zero integers* a_1, b_1, c_1, *having the same signs as* a, b, c *respectively, with* c_1 *dividing* c *and with* $(a_1,c_1)=(b_1,c_1)=1$ *such that the number of solutions of* (2.6) *does not exceed the number of solutions of* $|a_1x^n-b_1y^n|=c_1$ *in positive integers* x,y *with* $(x,y)=1$.

PROOF. We may assume that (a,b) divides c, for otherwise (2.6) is not solvable. Put $a_2=a/(a,b), b_2=b/(a,b), c_2=c/(a,b), f_1=(a_2,c_2), f_2=(b_2,c_2)$. Let (x_0,y_0) be a solution of (2.6). From $(a_2,b_2)=(x_0,y_0)=1$ it follows easily, that $(a_2,y_0^n)=f_1, (b_2,x_0^n)=f_2, (a_2x_0^n,b_2y_0^n)=(a_2,y_0^n)(b_2,x_0^n)=f_1f_2=(a_2b_2,c_2)$. Let F_1,F_2 be the smallest positive integers such that $f_1|F_1^n, f_2|F_2^n$. Then $F_1|y_0$, $F_2|x_0$. Put $a_1=a_2F_2^n/f_1f_2, b_1=b_2F_1^n/f_1f_2, c_1=c_2/f_1f_2$. Then a_1,b_1,c_1 are non-zero integers having the same signs as a,b,c respectively such that $c_1|c$ and such that $(a_1,c_1)=(b_1,c_1)=1$. Furthermore, every solution (x_0,y_0) of $|ax^n-by^n|=c$ corresponds to a solution $(x_0/F_2, y_0/F_1)$ of $|a_1x^n-b_1y^n|=c_1$. Hence the number of solutions of (2.6) is at most equal to the number of solutions of $|a_1x^n-b_1y^n|=c_1$ in positive integers x,y with $(x,y)=1$ which proves our lemma. □

By lemma 2.1 and by the fact that $R(n,c_1)\leq R(n,c)$ we may assume that $(a,c)=(b,c)=1$, whence $(x,c)=(y,c)=1$ for every solution (x,y) of (2.6). We shall do so in the sequel. Furthermore, we shall distinguish between the cases $b>0$ and $b<0$. There we use the fact that the numbers a_1,b_1 mentioned in lemma 2.1 have the same signs as a,b respectively.

Let S(c) be the set $\{(x,y)\in\mathbb{N}^2 \mid (x,c)=(y,c)=1\}$. On S(c) we define the following congruence relation: $(x_1,y_1),(x_2,y_2)$ are congruent mod c if $x_1y_2\equiv x_2y_1 \pmod c$, i.e. if $x_1/y_1\equiv x_2/y_2 \pmod c$. We denote this by $(x_1,y_1)\equiv(x_2,y_2) \pmod c$. By our assumption on a,b,c all solutions of (2.6) belong to S(c). Hence we can divide them into congruence classes mod c. In fact, we have

LEMMA 2.2. *The solutions of* (2.6) *belong to at most* R(n,c) *congruence classes* mod c.

PROOF. Let (x_0,y_0) be a fixed solution of (2.6). Then $(x_0,c)=(y_0,c)=(a,c)=(b,c)=1$, hence

$$(x_0/y_0)^n \equiv (b/a) \pmod{c}.$$

Let (x,y) be an arbitrary solution of (2.6). Then

$$\left(\frac{xy_0}{yx_0}\right)^n \equiv 1 \pmod{c}.$$

This shows that the number of congruence classes of solutions of (2.6) is at most equal to the number of solutions of the congruence equation $Z^n \equiv 1 \pmod{c}$ in residue classes $Z \pmod{c}$, i.e. $R(n,c)$. □

We put $w(x)=ax^n$ for every positive integer x and $w(x,y)=\max(ax^n,|by^n|)$ for every pair of positive integers x,y.

LEMMA 2.3. *Let* $(x_1,y_1),(x_2,y_2)$ *be solutions of* (2.6) *such that* $(x_1,y_1) \equiv (x_2,y_2) \pmod{c}$ *and* $w(x_2) \geq w(x_1)$. *If* $ab=1$ *then* $w(x_2) \geq c^{n-1}/2$ *and if* $ab \neq 1$ *then* $w(x_2) \geq c^{n-1}$.

PROOF. We have $ax_1^n-by_1^n=h_1, ax_2^n-by_2^n=h_2$, with $|h_1|=|h_2|=c$. On solving b from this system of linear equations in the unknowns a and b, we obtain

$$b = \frac{h_2x_1^n-h_1x_2^n}{x_2^ny_1^n-x_1^ny_2^n}$$

Since x_2y_1, x_1y_2 are positive integers with $|x_1y_2-x_2y_1| \geq c$ we have $|x_2^ny_1^n-x_1^ny_2^n| \geq c^n$, hence

$$|h_2w(x_1)-h_1w(x_2)| \geq |ab|c^n.$$

For $b>0$ we have

$$|h_2w(x_1)-h_1w(x_2)| \leq c(w(x_1)+w(x_2)) \leq 2cw(x_2),$$

hence

$$w(x_2) \geq \frac{ab}{2}c^{n-1}.$$

If $b<0$ then both h_1 and h_2 are positive and we even have

$$|h_2 w(x_1) - h_1 w(x_2)| \le c w(x_2),$$

hence

$$w(x_2) \ge |ab| c^{n-1}.$$

Since $ab \neq 1$ for $b<0$ this proves our lemma. □

We shall now prove theorem 2.1 in some special cases.

LEMMA 2.4. *If* (x,y) *is a solution of* (2.1), *then* $w(x,y)<C$ *if* $b<0$ *and* $w(x,y)<C^{n/(n-1)}/2$ *if* $a=b=1$.

PROOF. The lemma is trivial if $b<0$. If $a=b=1$, we may assume that $x>y$. Then we have

$$C \ge x^n - y^n \ge x^n - (x-1)^n.$$

Hence it suffices to show that $x^n-(x-1)^n > 2^{1-1/n} x^{n-1}$ for all $x \ge 2, n \ge 3$. The function $f(z)=((z^n-(z-1)^n)z^{-n+1}$ has the derivative $(z^n-(z-1)^n-n(z-1)^{n-1})z^{-n}$. For $z>1$ this derivative is positive, hence $f(z)$ is monotonically increasing. This implies that

$$(x^n-(x-1)^n)x^{-n+1} \ge (2^n-1)2^{-n+1}$$

for $x \ge 2, n \ge 3$. But from this fact our lemma follows immediately, since

$$(2^n-1)2^{-n+1} = 2(1-2^{-n}) > 2\exp(-(2^n-1)^{-1}) > 2^{1-1/n}$$

for $n \ge 3$. □

We see that theorem 2.1 is valid for $ab \le 1$. We shall now prove theorem 2.2 in this case.

LEMMA 2.5. *If* $ab \le 1$ *then* (2.6) *has at most* $R(n,c)$ *solutions*.

PROOF. By our assumption that $(a,c)=(b,c)=1$ and by lemma 2.2 it suffices to show that (2.6) has at most one solution in each congruence class mod c, i.e. that for any two distinct solutions $(x_1,y_1),(x_2,y_2)$ of (2.6) we have $(x_1,y_1) \not\equiv (x_2,y_2) \pmod{c}$.

Suppose to the contrary that (2.6) has two congruent solutions mod c, $(x_1,y_1),(x_2,y_2)$ say, ordered such that $w(x_1)\le w(x_2)$. Then by lemma 2.3, $w(x_2)\ge c^{n-1}$ if $b<0$ and $w(x_2)\ge c^{n-1}/2$ if $a=b=1$. But this is contradictory to lemma 2.4 since $c^{n-1}\ge c, c^{n-1}/2\ge c^{n/(n-1)}/2$ for $c\ge 1, n\ge 3$. □

In the proofs of theorems 2.1 and 2.2 we shall use the following lemma. It is assumed that $ab\ge 2$.

LEMMA 2.6. *Let* β, f *be constants with* $\beta>1, f\ge 1$. *Put* $\nu=n^{-1}, \kappa=(n-1)/2$.
(i) If (x,y) *is a solution of* (2.1) *with* $w(x)\ge\beta C$, *then*

$$\left|1-\left(\frac{b}{a}\right)^{\nu}\frac{y}{x}\right| < \frac{C(\beta/(\beta-1))^{\kappa\nu}}{nw(x)} . \tag{2.9}$$

(ii) If $(x_1,y_1),(x_2,y_2)$ *are two solutions of* (2.1) *with* $|x_1y_2-x_2y_1|\ge f$ *and* $w(x_2)\ge w(x_1)\ge\beta C$, *then*

$$w(x_2) \ge 2\left(\frac{nf}{2C}\right)^{n}\left(\frac{\beta-1}{\beta}\right)^{\kappa} w(x_1)^{n-1}. \tag{2.10}$$

PROOF. (i) We have

$$|a^{\nu}x-b^{\nu}y| = \frac{|ax^n-by^n|}{(ax^n)^{1-\nu}+(ax^n)^{2-\nu}(by^n)^{\nu}+\ldots+(by^n)^{1-\nu}} .$$

Using the inequality of the arithmetic and the geometric mean, it follows that

$$|a^{\nu}x-b^{\nu}y| < \frac{C}{n(ax^n)^{\kappa\nu}(by^n)^{\kappa\nu}} ,$$

hence

$$\left|1-\left(\frac{b}{a}\right)^{\nu}\frac{y}{x}\right| < \frac{C}{n(ax^n)^{(1+\nu)/2}(by^n)^{\kappa\nu}} .$$

Since $ax^n/by^n\le\beta/(\beta-1)$ this implies that

$$\left|1-\left(\frac{b}{a}\right)^{\nu}\frac{y}{x}\right| < \frac{C(\beta/(\beta-1))^{\kappa\nu}}{nw(x)} .$$

(ii) We have by (i) and by the fact that $ab\ge 2$,

$$\frac{f}{w(x_1)^{\nu}w(x_2)^{\nu}} \le \frac{\left|x_1y_2-x_2y_1\right|}{a^{2\nu}x_1x_2} = a^{-2\nu}\left|\frac{y_1}{x_1}-\frac{y_2}{x_2}\right|$$

$$\le a^{-2\nu}(a/b)^{\nu}\left(\left|1-\left(\frac{b}{a}\right)^{\nu}\frac{y_1}{x_1}\right|+\left|1-\left(\frac{b}{a}\right)^{\nu}\frac{y_2}{x_2}\right|\right)$$

$$\le (ab)^{-\nu}\nu C(\beta/(\beta-1))^{\kappa\nu}(w(x_1)^{-1}+w(x_2)^{-1})$$

$$\le 2^{1-\nu}\nu C(\beta/(\beta-1))^{\kappa\nu}w(x_1)^{-1}.$$

Hence

$$w(x_2) \ge 2\left(\frac{nf}{2C}\right)^{n}\left(\frac{\beta-1}{\beta}\right)^{\kappa} w(x_1)^{n-1}. \qquad \square$$

§2.3. Proof of theorem 2.1.

We assume that a,b,n are integers with $a>0, b>0, n\ge 3, a/b\ne(u/v)^n$ for all $u,v\in\mathbb{Z}$ (whence $ab\ge 2$) and that C is a real with $C\ge 1$. We shall show that for these values of a,b,n,C, inequality (2.1) has at most one solution with $w(x,y)\ge\mu_n C^{\alpha_n}$. This completes the proof of theorem 2.1, for if $a>0$, $b<0$, then by lemma 2.4 $w(x,y)\le C$, while if $a/b=(u/v)^n$ for some $u,v\in\mathbb{Z}$ with $(u,v)=1$, then $a=du^n, b=dv^n$ for some integer d, whence by lemma 2.4,

$$w(x,y) = |d|\max(|ux|^n,|vy|^n) \le |d||C/d|^{n/(n-1)}/2 \le C^{n/(n-1)}/2.$$

Assume on the contrary that (2.1) has two solutions with $w(x,y) \ge \mu_n C^{\alpha_n}$, $(x_1,y_1),(x_2,y_2)$ say, ordered such that $w(x_2,y_2)\ge w(x_1,y_1)$. As in §2.2, we put $\nu=n^{-1}, \kappa=(n-1)/2$ and we put also $\sigma_n=(\mu_n/(\mu_n-1))^{\kappa\nu}$. By symmetry we may assume that $w(x_1,y_1)=w(x_1)$. Put $w_1=w(x_1), w_2=w(x_2)$. Then

$$w_1 \ge \mu_n C^{\alpha_n} \tag{2.11}$$

and also

$$w_2 \ge 2\left(\frac{n}{2\sigma_n C}\right)^{n} w_1^{n-1} . \tag{2.12}$$

(2.12) follows from 2.6 (ii) with $\beta=\mu_n, f=1$ when we have shown that $w_2\ge w_1$. This holds true indeed for suppose $w_2<w_1$. Then by $w_2^n\ge ax_1^n>ax_2^n$. Hence

$$C \leqq by_2^n - ax_2^n \geq ax_1^n - ax_2^n \geq nax_2^n \geq w_2^{(n-1)/n}.$$

Therefore, by (2.11),

$$\mu_n C^{\alpha_n} \leq w_1 \leq w(x_2,y_2) \leq w_2 + C \leq 2C^{n/(n-1)}.$$

But this is impossible, since $\alpha_n > n/(n-1)$ and

(2.13) $$\mu_n \geq 8.$$

The latter inequality, which will also be used later, is easy to check for $n<24$ and for $n\geq 24$ it follows from $\mu_n \geq n/3$.

Put

$$z_1 = \left(\frac{b}{a}\right)^{\nu} \frac{y_1}{x_1}, \qquad S_m = \frac{y_2}{x_2} A_m(z_1^n) - \frac{y_1}{x_1} B_m(z_1^n) \text{ for } m=1,2,\ldots,$$

where $A_m(z), B_m(z)$ are the polynomials defined in chapter 1. Let r,g be the integers defined by $m=2r+1-g$ with $g\in\{0,1\}$. Put $q(m)=n^r(n^r,r!)$. We assume that $m\geq 2$.

LEMMA 2.7. *Put*

$$s(m) := q(m)\binom{2r-g}{r}\sigma_n 2^{\nu(g-1)},$$

$$t(m) := q(m)2^{\nu(g-1)}(1-\nu)^{-1}\sigma_n^m \binom{r+\nu}{r+1}\binom{r-\nu}{r}\Big/\binom{m}{r},$$

$$P_m := s(m)Cw_2^{\nu-1}w_1^{r+\nu(1-g)}, \quad Q_m := t(m)C^m w_2^{\nu} w_1^{-r-(1-\nu)(1-g)}.$$

If $S_m \neq 0$ *then*

(2.14) $$1 < \nu P_m + (1-\nu)Q_m.$$

PROOF. Note that $A_m(z)$ has degree r and that $B_m(z)$ has degree $r-g$. Hence by lemma 1.3 (i) $q(m)x_2x_1^{1-g}w_1^r S_m$ is a rational integer. If $S_m\neq 0$ we therefore have, by $w_1=w(x_1,y_1)$, whence $|z_1|\leq 1$ and by lemma 1.4, lemma 2.6 (i), $ab\geq 2$ and lemma 1.6 (i),

$$1 \leq q(m)w_2^{\nu}w_1^{r+\nu(1-g)}a^{-\nu(2-g)}|S_m|$$

$$= q(m)w_2^{\nu}w_1^{r+\nu(1-g)}a^{-\nu(2-g)}\left(\frac{a}{b}\right)^{\nu}\left|\left(\left(\frac{b}{a}\right)^{\nu}\frac{y_2}{x_2}-1\right)A_m(z_1^n)+(1-z_1)^m V_m(z_1)\right|$$

$$< q(m)w_2^{\nu}w_1^{r+\nu(1-g)}2^{\nu(g-1)}\left(\binom{2r-g}{r}\frac{\sigma_n C}{nw_2}+\binom{m}{n}\binom{r+\nu}{r+1}\binom{r-\nu}{r}\binom{m}{r}^{-1}\left(\frac{\sigma_n C}{nw_1}\right)^m\right)$$

$$= \nu P_m + (1-\nu)Q_m. \qquad \square$$

LEMMA 2.8. $S_3\neq 0$ *for* $n\geq 3$; $S_m\neq 0$ *for* $n=3, m=2, 5, 7$.

PROOF. Put $h=ax_1^n-by_1^n$, $u=1-z_1^n=h/w_1$, $\tilde{E}_m(z)=q^*(m)A_m(1-z)$, $\tilde{F}_m(z)=q^*(m)B_m(1-z)$, where $q^*(m)$ is the smallest positive rational number such that both $q^*(m)A_m(1-z)$ and $q^*(m)B_m(1-z)$ have integral coefficients. Let $\tilde{E}^*_m(x,y),\tilde{F}^*_m(x,y)$ be binary forms which are for $x\neq 0$ equal to $x^r\tilde{E}_m(y/x),x^r\tilde{F}_m(y/x)$ respectively.

Suppose that $S_m=0$. Then

$$\frac{y_2}{x_2}\tilde{E}_m(u) = \frac{y_1}{x_1}\tilde{F}_m(u),$$

hence

$$\frac{by_2^n}{ax_2^n} = \frac{(1-u)\tilde{F}_m(u)^n}{\tilde{E}_m(u)^n} = \frac{(w_1-h)\tilde{F}^*_m(w_1,h)^n}{w_1\tilde{E}^*_m(w_1,h)^n}$$

Put $d=\left((w_1-h)\tilde{F}^*_m(w_1,h)^n, w_1\tilde{E}^*_m(w_1,h)^n\right)$. Then

$$w_1^{nr+1}\tilde{E}_m(u)^n-(1-u)\tilde{F}_m(u)^n = w_1\tilde{E}^*_m(w_1,h)^n-(w_1-h)\tilde{F}^*_m(w_1,h)^n \tag{2.15}$$
$$\Big| d(ax_2^n-by_2^n) .$$

Now we have

$$\tilde{E}_m(z)^n-(1-z)\tilde{F}_m(z)^n = z^m K_m(z)$$

for some polynomial $K_m(z)$. For put $z=1-w^n$. $(\tilde{E}_m(1-w^n))^n-w^n(\tilde{F}_m(1-w^n))^n$ is a polynomial in w^n which is divisible by $A_m(w^n)-wB_m(w^n)$, hence by $(1-w)^m$ in view of lemma 1.4. But then it must be divisible by $(1-w)^m=z^m$. Hence by (2.15)

$$w_1^{(n-2)r+g}h^m K_m(u) = w_1^{nr+1}u^m K_m(u) \Big| d(ax_2^n-by_2^n). \tag{2.16}$$

We shall show that this is impossible for the values of m,n stated in the

lemma, by estimating $K_m(u)$ from below and d from above.

Firstly, we estimate $K_m(u)$ from below. If n=3 we have

$$\tilde{E}_2(z)=3-z, \quad \tilde{F}_2(z)=3, \quad K_2(z)=9-z,$$
$$\tilde{E}_3(z)=3-2z, \quad \tilde{F}_3(z)=3-z, \quad K_3(z)=2-z,$$
$$\tilde{E}_5(z)=54-63z+14z^2, \quad \tilde{F}_5(z)=54-45z+5z^2, \quad K_5(z)=756-756z+125z^2,$$
$$\tilde{E}_7(z)=81-135z+63z^2-7z^3, \quad \tilde{F}_7(z)=81-108z+36z^2-2z^3, \quad K_7(z)=162-243z+97z^2-8z^3.$$

Since $|u|<\mu_3^{-1}$ for n=3 we have

$$|K_2(u)|>8, \quad |K_3(u)|>1, \quad |K_5(u)|>755, \quad |K_7(u)|>161. \tag{2.17}$$

In case $n\geq 4$ we have

$$\tilde{E}_3(z) = \frac{2n-(n+1)z}{(n-1,2)}, \quad \tilde{F}_3(z) = \frac{2n-(n-1)z}{(n-1,2)}.$$

We shall not compute $K_3(z)$ explicitly but we shall derive a lower bound for $K_3(u)$ by another method. Note that $|u|<1$, whence that $(1-u)^\nu=\sum_{k=0}^{\infty}\binom{\nu}{k}(-u)^k$ converges. Moreover, since h>0 and u>0,

$$\begin{aligned} u^{-3}&\left(\tilde{E}_3(u)-(1-u)^\nu\tilde{F}_3(u)\right) \\ &= u^{-3}(n-1,2)^{-1}\left(2n-(n+1)u-(1-u)^\nu(2n-(n-1)u)\right) \\ &= (n-1,2)^{-1}\sum_{k=0}^{\infty}(-1)^{k+1}\binom{\nu}{k+2}\frac{(n+1)(k+1)}{k+3}u^k \\ &> -(n-1,2)^{-1}\binom{\nu}{2}\frac{n+1}{3} = \frac{n^2-1}{(n-1,2)6n^2}. \end{aligned}$$

By (2.13) we have $|u|<1/8$, hence

$$|\tilde{E}_3(u)| > (n-1,2)^{-1}15(n-1)/8, \quad |\tilde{F}_3(u)| > (n-1,2)^{-1}15(n-1)/8.$$

Therefore,

$$\begin{aligned} K_3(u) &= u^{-3}\left(\tilde{E}_3(u)-(1-\nu)\tilde{F}_3(u)\right)\sum_{k=0}^{n-1}\tilde{E}_3(u)^k(1-u)^{(n-1-k)\nu}\tilde{F}_3(u)^{n-1-k} \\ &> (1-u)(n-1,2)^{-n}\left((n^2-1)/6n^2\right)n\left(15(n-1)/8\right)^{n-1} \\ &\geq (n-1,2)^{-n}\frac{7}{8}\frac{8}{15}\frac{n+1}{6n}\left(15(n-1)/8\right)^n. \end{aligned}$$

Since $n \geq 4$ this implies that

$$(2.18) \qquad K_3(u) \geq \frac{7}{72}(n-1,2)^{-n}\left(15(n-1)/8\right)^n .$$

We shall now estimate d from above. Put $v=(h,w_1)$, $h=vh'$, $w_1=vw'$. Firstly, we consider the case $n=3,m=2$. Then d divides

$$\begin{aligned}
&\left(w_1\tilde{E}_2^*(w_1,h)^3,(w_1-h)\tilde{F}_2^*(w_1,h)^3\right)= \left(w_1^2h^2K_2(h/w_1),(w_1-h)\tilde{F}_2^*(w_1,h)^3\right)\\
&= w_1\left(h^2(9w_1-h),27(w_1-h)w_1^2\right) = w_1v^3\left(27(w'-h')w'^2,h'^2(9w'-h')\right)\\
&\mid 3^3w_1v^3(w'-h',h'^2)(w'-h',9w'-h')(w'^2,9w'-h')(w',h')^2\\
&= 3^3w_1v^3(w'-h',9w'-h') = 3^3w_1v^3(w'-h',8h')\\
&\mid 6^3w_1h^3.
\end{aligned}$$

Here we used that for $a_1,a_2,a_3,a_4 \in \mathbb{Z}$, (a_1a_2,a_3a_4) divides $(a_1,a_3)(a_1,a_4)(a_2,a_3)(a_2,a_4)$. Hence if $S_2=0$ for $n=3$ we have by (2.16) and (2.17), on noting that $ax_2^n-by_2^n \neq 0$,

$$8w_1^2h^2 \leq 6^3w_1h^3C, \quad w_1 \leq 27hC \leq 27C^2 \leq \mu_3C^9,$$

which is contradictory to (2.11).

We shall now consider the other possibilities for m,n. Note that m is odd, hence for $z \neq 0$ $A_m(z)=z^rB_m(z^{-1})$, i.e. $\tilde{E}_m(1-z)=z^r\tilde{F}_m(1-z^{-1})$ (cf (1.1)). Put $b_m=\tilde{E}_m^*(w',h'),\tilde{F}_m^*(w',h')$. Then d divides

$$\begin{aligned}
&v^{nr+1}\left(w'\tilde{E}_m^*(w',h')^n,(w'-h')\tilde{F}_m^*(w',h')^n\right)\\
&\mid v^{nr+1}(w',w'-h')\left(w',\tilde{F}_m^*(w',h')^n\right)\left(w'-h',\tilde{E}_m^*(w',h')^n\right)b_m^n\\
&= v^{nr+1}\left(w',\tilde{F}_m^*(0,h')^n\right)\left(w'-h',\tilde{E}_m^*(h',h')^n\right)b_m^n\\
&= v^{nr+1}\left(w',\tilde{F}_m^*(0,1)^n\right)\left(w'-h',\tilde{F}_m^*(0,1)^n\right)b_m^n \quad .
\end{aligned}$$

Hence

$$(2.19) \qquad d \mid v^{nr+1}\tilde{F}_m^*(0,1)^nb_m^n .$$

In the case n=3, we shall use the following identities:

$$\tilde{E}_3^*(x,y)-\tilde{F}_3^*(x,y) = -y,$$
$$(3x-y)\tilde{E}_5^*(x,y)-(3x-2y)\tilde{F}_5^*(x,y) = -4y^3,$$
$$(27x-5y)\tilde{E}_5^*(x,y)-(27x-14y)\tilde{F}_5^*(x,y) = -72xy^2,$$
$$\tilde{E}_7^*(x,y)-\tilde{F}_7^*(x,y) = (-27x^2+27xy-5y^2)y,$$
$$(3x-y)\tilde{E}_7^*(x,y)-(3x-2y)\tilde{F}_7^*(x,y) = (-6x+3y)y^3.$$

These imply

$$\begin{aligned} b_3 &\mid (3w'-h',h') \mid h', \\ b_5 &\mid (72w'h'^2,4h'^3) \mid (72w',4h')h'^2 \mid 72h'^2, \\ b_7 &\mid \{(6w'-3h')h'^3, 27w'^2h'-27h'^2w'+5h'^3\} \\ &\quad \mid 3h'^3(2w'-h', 27w'^2-27w'h'+5h'^2) \\ &\quad \mid 3h'^3(2w'-h', 7h'^2) \\ &\quad \mid 42h'^3 . \end{aligned}$$

Therefore, by (2.19),

$$\begin{aligned} &d \mid v^4h'^3 \mid h^4 && \text{if } m=3, \\ (2.20)\qquad &d \mid v^7 5^3 (72h'^2)^3 \mid 360^3 h^7 && \text{if } m=5, \\ &d \mid v^{10} 2^3 (42h'^3)^3 \mid 84^3 h^{10} && \text{if } m=7. \end{aligned}$$

Since $|ax_2^n-by_2^n|\le C$ this yields, together with (2.16),(2.17),

$$\begin{aligned} &w_1h^3 \le h^4C, && w_1 \le hC \le C^2 \text{ if } m=3, \\ &755w_1^2h^5 \le 360^3h^7C, && w_1 \le (360^3/755)^{1/2}hC^{1/2} \le 249C^{3/2} \text{ if } m=5, \\ &161w_1^3h^7 \le 42^3h^{10}C, && w_1 \le (84/(161)^{1/3})hC^{1/3} \le 16C^{4/3} \text{ if } m=7. \end{aligned}$$

These inequalities are clearly impossible.

Finally, we estimate d from above for m=3,n≥4. Note that

$$b_3 = (n-1,2)^{-1}(2nw'-(n+1)h', 2nw'-(n-1)h') \mid (n-1,2)^{-1}2h'.$$

Hence by (2.19),

$$d \mid (n-1,2)^{-n}\,(2(n-1))^{n}v^{n+1}h',^{n} \mid (n-1,2)^{-n}(2(n-1))^{n}h^{n+1}.$$

Together with (2.16) and (2.18) this implies that for $n\geq 4$,

$$w_1^{n-2}h^{3}\frac{7}{72}(n-1,2)^{-n}(15(n-1)/8)^{n} \leq (n-1,2)^{-n}(2(n-1))^{n}h^{n+1}C,$$

hence

$$\begin{aligned} w_1 &\leq \left(\frac{72}{7}\right)^{1/(n-2)}\left(\frac{16}{15}\right)^{n/(n-2)}(h^{n-2}C)^{1/(n-2)} \\ &\leq \left(\frac{72}{7}\right)^{1/2}\left(\frac{16}{15}\right)^{2}C^{(n-1)/(n-2)} < 4C^{3/2} < \mu_n C^{\alpha_n}, \end{aligned}$$

which is clearly impossible. □

LEMMA 2.9. *There is a positive integer ℓ such that*

$$s(2\ell+1)w_1^{\ell} \leq \frac{w_1^{-\nu}w_2^{1-\nu}}{C} < s(2\ell+3)w_1^{\ell+1}. \tag{2.21}$$

PROOF. We suppose the contrary. Then, by the fact that the sequence $s(2\ell+1)w_1^{\ell}$ increases monotonically to infinity,

$$\frac{w_1^{-\nu}w_2^{1-\nu}}{C} < s(3)w_1 = 2^{1-\nu}n\sigma_n w_1,$$

hence

$$w_2 < 2(n\sigma_n C)^{n/(n-1)}w_1^{(n+1)/(n-1)}. \tag{2.22}$$

Firstly we consider the case $n\geq 4$. By (2.12) we have that

$$\left(\frac{n}{2\sigma_n C}\right)^{n}w_1^{n-1} \leq (n\sigma_n C)^{n/(n-1)}w_1^{(n+1)/(n-1)},$$

hence

$$w_1^{n-1-(n+1)/(n-1)} = w_1^{n(n-3)/(n-1)} < \frac{\sigma_n^{n^2/(n-1)}\cdot 2^{n}}{n^{n(n-2)/(n-1)}}\cdot C^{n^2/(n-1)}.$$

Therefore,

$$w_1 < \frac{\sigma_n^{n/(n-3)}\cdot 2^{(n-1)/(n-3)}}{n^{(n-2)/(n-3)}}\cdot C^{n/(n-3)} \tag{2.23}$$

Since $\mu_n \geq 8$ we have

$$\frac{\sigma_n^{n/(n-3)} \cdot 2^{(n-1)/(n-3)}}{n^{(n-2)/(n-3)}} \leq \left(\left(\frac{8}{7}\right)^{(n-1)/2} \cdot 2^{n-1} 4^{-n+2} \right)^{1/(n-3)} < \mu_n .$$

Moreover, $\alpha_n > n/(n-3)$. Hence by (2.23),

$$w_1 < \mu_n C^{\alpha_n}.$$

But this contradicts (2.11), which proves our lemma for $n \geq 4$.

We now assume that $n=3$. We infer from lemma 2.7 and lemma 2.8 with $m=2$ that $3 < P_2 + 2Q_2$. However, by (2.11), (2.12) we have

$$P_2 = 3\sigma_3 C w_1 w_2^{-2/3} \leq 3\sigma_3 C w_1 2^{-2/3} \left(\frac{2\sigma_3 C}{3}\right)^2 w_1^{-4/3}$$
$$= 3\sigma_3 2^{-2/3} \left(\frac{2\sigma_3 C}{3}\right) C^3 w_1^{-1/3} < 2C^3 w_1^{-1/3} < 1,$$

whereas by (2.22),

$$Q_2 = \frac{1}{3} \cdot \sigma_3^2 C^2 w_2^{1/3} w_1^{-1} < \frac{1}{3} \cdot 2^{1/3} \sigma_3^2 (3\sigma_3)^{1/2} C^{5/2} < C^{5/2} w_1^{-1/3} < 1.$$

This contradiction proves our lemma completely. □

LEMMA 2.10. $s(2(r+j)+1)t(2r+1)^{n-1} < T_n^{nr+j}$ *for* $r \in \mathbb{N}, j \in \{1,2\}$.

PROOF. Note that

$$s(2(r+j)+1)t(2r+1)^{n-1} = R_{rj}^{(n)} n^{nr+j} (n^{r+j}, (r+j)!) (n^r, r!)^{n-1},$$

where

$$R_{rj}^{(n)} = \frac{1}{2} \cdot \sigma_n \left(\binom{2(r+j)}{r+j} \left(\frac{\sigma_n^{2r+1}}{1-\nu} \binom{r+\nu}{r+1} \binom{r-\nu}{r} \right) \binom{2r+1}{r}^{-1} \right)^{n-1}.$$

For every positive integer k we have

$$(n^k, k!) = \prod_{p \mid n} p^{\delta(p)},$$

with

$$\delta(p) = \sum_{j=1}^{\infty} [kp^{-j}] < \frac{k}{p-1} ,$$

hence

$$(2.24) \qquad n^k(n^k,k!) < \Big(n \prod_{p|n} p^{1/(p-1)}\Big)^k .$$

Therefore, it suffices to show that

$$(2.25) \qquad R_{rj}^{(n)} < (3^{-(n-2)/n})^{nr+j}.$$

Since $R_{r1}^{(n)} \le R_{r2}^{(n)}$ we may restrict ourselves to the case j=2.

Note that

$$\mu_n \ge 8 > \frac{(4/3)^{3/4}}{(4/3)^{3/4}-1} \ge \frac{(4/3)^{n(n-2)/(n-1)^2}}{(4/3)^{n(n-2)/(n-1)^2}-1} ,$$

hence

$$(2.26) \qquad \sigma_n < \Big(\frac{8}{7}\Big)^{(n-1)/2n} < \Big(\frac{4}{3}\Big)^{(n(n-2)/(n-1)^2)(n-1)/2n} = \Big(\frac{4}{3}\Big)^{(n-2)/2(n-1)}$$

First of all we have for $n \ge 3$, by (2.26),

$$R_{12}^{(n)} = 10\sigma_n\Big(\frac{\sigma_n^3(n+1)}{6n^2}\Big)^{n-1} < 10\Big(\frac{8}{7}\Big)^{1/2}\Big(\frac{(8/7)^{3/2}\times 4}{54}\Big)^{n-1} \le 11^{-n+2}$$
$$< (3^{-(n-2)/n})^{n+2}.$$

Furthermore we have for $r \ge 1$, by (2.26),

$$\frac{R_{r+1,2}^{(n)}}{R_{r,2}^{(n)}} = \frac{(2r+6)(2r+5)}{(r+3)^2}\Big(\sigma_n^2 \frac{r+1+\nu}{r+2}\cdot\frac{r+1-\nu}{r+1}\cdot\frac{(r+2)(r+1)}{(2r+3)(2r+2)}\Big)^{n-1}$$
$$< 4\cdot\sigma_n^2\Big(\frac{(r+1)^2-\nu^2}{(2r+2)(2r+3)}\Big)^{n-1} < 4(\sigma_n^2/4)^{n-1} = \sigma_n^{2(n-1)}4^{-(n-2)}$$
$$< 3^{-(n-2)}.$$

This proves (2.25), whence lemma 2.10 completely. □

We shall now complete the proof of theorem 2.1. If ℓ is the integer from lemma 2.9 then we choose $r=\ell$ if $S_{2\ell+1} \neq 0$, and $r=\ell-1$ if otherwise. Then

$r=\ell-j+1$ for some $j\in\{1,2\}$. By lemma 2.8 and lemma 2.9 we always have $r\geq 1$ and in case $n=3$ we can have $j=2$ only if $r\geq 3$. By lemma 1.5 with $h=2$ we always have $S_{2r+1}\neq 0$. Note that by our choice of r and by the left-hand side inequality of (2.21),

$$(2.27)\qquad P_{2r+1} = s(2r+1)w_1^r C w_2^{\nu-1} w_1^{\nu} \leq s(2\ell+1)w_1^{\ell} C w_2^{\nu-1} w_1^{\nu} < 1.$$

Furthermore by the right-hand side inequality of (2.21) and by lemma 2.10,

$$\begin{aligned} Q_{2r+1}^{n-1} &= \left(t(2r+1)C^{2r+1}w_2^{\nu}w_1^{\nu-r-1}\right)^{n-1} \\ &< s(2(r+j)+1)t(2r+1)^{n-1}C^{(2r+1)(n-1)+1}w_1^{r+j+1-(n-1)(r+1)} \\ &< T_n^{nr+j}C^{(2n-2)r+n}w_1^{-(n-2)(r+1)+j} =: G_j. \end{aligned}$$

If $n\geq 4$ we have by (2.11)

$$G_j \leq G_2 = \left(T_n^n C^{2n-2} w_1^{-(n-2)}\right)^{r-1} T_n^{n+2} C^{3n-2} w_1^{-2(n-3)} \leq 1,$$

if $n=3$ we have in case $j=1$,

$$G_j = G_1 = (T_3^3 C^4 w_1^{-1})^{r-1} T_3^4 C^7 w_1^{-1} \leq 1,$$

while in case $j=2$,

$$G_j = G_2 = (T_3^3 C^4 w_1^{-1})^{r-3} T_3^{11} C^{15} w_1^{-2} \leq 1.$$

Hence $Q_{2r+1}<1$ for $n\geq 3$. Together with (2.27) this contradicts (2.14). But then our assumption that (2.1) has two solutions with $w(x,y)\geq \mu_n C^{\alpha n}$ must be wrong. This completes the prove of theorem 2.1. □

§2.4. Proof of theorem 2.2.

Let a,b,c,n be integers with $a>0, b\neq 0, c>0, n\geq 3$. By lemma 2.1 and lemma 2.5 we may assume that $ab\geq 2$, $(a,c)=(b,c)=1$. Moreover, by the results of Nagell, Ljunggren and Domar (cf §2.1) we may assume that $c\geq 2$.

By lemma 2.3, each congruence class of solutions of (2.6) contains at most one solution (x,y) with $w(x)<c^{n-1}$. Hence by lemma 2.2, (2.6) has at most $R(n,c)$ solutions with $w(x)<c^{n-1}$. If $n=3$ then each congruence class mod c contains at most two solutions with $w(x)<27c^4/8$, whence (2.6) has at

most $2R(3,c)$ solutions for which $w(x)<27c^4/8$. For suppose that (x_1,y_1), $(x_2,y_2),(x_3,y_3)$ are solutions of (2.6) in the same congruence class, ordered such that $w(x_1)\le w(x_2)\le w(x_3)$. Then by lemma 2.3 we have $w(x_2)\ge c^2$ and by lemma 2.6 (ii) with $f=C=c,\beta=2$,

$$w(x_3) \ge 2\left(\frac{3}{2}\right)^3 \cdot \frac{1}{2} w(x_2)^2 \ge 27c^4/8,$$

a contradiction.

By theorem 2.1 (with C=c) (2.6) has at most one solution with $w(x)\ge\mu_n c^{\alpha_n}$. Hence we have only to estimate the number of solutions of (2.6) with $c^{n-1}\le w(x)<\mu_n c^{\alpha_n}$ if $n\ge4$ and $27c^4/8\le w(x)<\mu_3 c^{\alpha_3}$ if $n=3$.

If $c^{n-1}\ge\mu_n c^{\alpha_n}$ then (2.6) has at most $R(n,c)+1$ solutions. This is the case if $n=5,c\ge25$ or $n\ge6,c\ge5$. For by (2.3) we have

$$\mu_n < n^2 \le 5^{n-1-\alpha_6} \le 5^{n-1-\alpha_n} \le c^{n-1-\alpha_n} \quad \text{for } n\ge6,c\ge5.$$

We have also

$$\mu_n 4^{\alpha_n} \le 4^n \quad \text{for } n\ge6.$$

Hence if $c\le4,n\ge6$, then (2.6) has, by theorem 2.1, at most one solution with $\max(x,y)\ge4$. It is easy to check that at most one of the pairs $(1,1)$, $(1,2),(1,3),(2,1),(2,3),(3,1),(3,2)$ can be a solution of (2.6). For suppose that two of these pairs are solutions, $(x_1,y_1),(x_2,y_2)$ say. Then

$$1 \le |a| = \frac{c|y_1^n \pm y_2^n|}{|x_1^n y_2^n - x_2^n y_1^n|}, \quad 1 \le |b| = \frac{c\,|x_1^n \pm x_2^n|}{|x_1^n y_2^n - x_2^n y_1^n|}.$$

However, it is easy to verify that for all possibilities of $(x_1,y_1),(x_2,y_2)$,

$$|x_1^n y_2^n - x_2^n y_1^n| > 4\cdot\min(x_1^n+x_2^n, y_1^n+y_2^n) \quad \text{for } n\ge6,$$

a contradiction. This proves theorem 2.2 for $n\ge6$.

In the remaining cases, i.e. $n=5,c\le24$ and $n\in\{3,4\}$ we have to show that (2.6) has at most one solution if $n=5$ and at most two solutions if $n=4$ for which $c^{n-1}\le w(x)<\mu_n c^{\alpha_n}$, and at most three solutions for which $27c^4/8\le w(x)<\mu_3 c^{\alpha_3}$ if $n=3$. Therefore we need the following lemma.

LEMMA 2.11. *Put* $K(n)=\left(2^{3/2}(2^{-3/2}n)^n\right)^{1/(n-2)}$. *Let* A, B *be constants with*

$$B > A > \max\left(2c, K(n)^{-1}c^{n/(n-2)}\right).$$

Let r *be the smallest positive integer with*

$$r \geq S=S(A,B,c) := \log\left(\frac{\log(K(n)c^{-n/(n-2)}B)}{\log(K(n)c^{-n/(n-2)}A)}\right)\Big/\log(n-1) .$$

Then (2.6) *has at most* r *solutions with* $A\leq w(x)<B$.

PROOF. Let $(x_1,y_1),(x_2,y_2),\ldots,(x_r,y_r)$ be solutions of (2.6) such that $A\leq w(x_1)\leq w(x_2)\leq\ldots\leq w(x_r)<B$. We apply lemma 2.6 (ii) with $\beta=2, f=1, C=c$. For convenience we put

$$T = K(n)c^{-n/(n-2)}.$$

Then we have for $i\in\{1,2,\ldots,r-1\}$,

$$w(x_{i+1}) \geq 2\left(\frac{n}{2c}\right)^n 2^{-\kappa}w(x_i)^{n-1} = T^{n-2}w(x_i)^{n-1},$$

hence

$$Tw(x_{i+1}) \geq (Tw(x_i))^{n-1}.$$

This implies that

$$TB > Tw(x_r) \geq (Tw(x_1))^{(n-1)^{r-1}} \geq (TA)^{(n-1)^{r-1}},$$

hence

$$(n-1)^{r-1} < \log(TB)/\log(TA),$$

and therefore

$$r-1 < \log\left(\log(TB)/\log(TA)\right)/\log(n-1),$$

which implies lemma 2.11. □

We shall apply lemma 2.11 with $A=c^{n-1}$ if $n\in\{4,5\}$ but $A=27c^4/8$ if $n=3$, while $B=\mu_n c^{\alpha_n}$. Then clearly the conditions imposed on A,B in lemma 2.11 are satisfied. If $n\in\{4,5\}$ we have

$$S = \log\left(\frac{\log(K(n)\mu_n)+(\alpha_n-n/(n-2))\log c}{\log K(n)+(n-1-n/(n-2))\log c}\right)\Big/\log(n-1) \ .$$

If n=5, then S<1, since $4\log K(5) > \log(K(5)\mu_5)$, $4(4-5/3)>\alpha_5-5/3$. If n=4, then S<2, since $3^2\log K(4) > \log(K(4)\mu_4)$, $3^2(3-4/2)>\alpha_4-4/2$. Finally, if n=3, then

$$S = \log\left(\frac{\log(K(3)\mu_3)+6\log c}{\log(K(3)27/8)+\log c}\right)\Big/\log 2 < 3,$$

since $2^3\log(K(3)27/8)>\log(K(3)\mu_3)$, $2^3>6$. This proves theorem 2.2 completely. □

CHAPTER 3. ON THE REPRESENTATION OF INTEGERS BY BINARY CUBIC FORMS OF POSITIVE DISCRIMINANT.

§ 3.1. Introduction.

Let $F(x,y)$ be an irreducible binary cubic form with integral coefficients and of negative discriminant. Nagell [Na 2] and Delone [De] independently showed, that the equation

$$F(x,y) = 1 \tag{3.1}$$

has at most *five* solutions in integers x,y. This can not be improved, for if $F(x,y)$ equals $x^3-xy^2+y^3$ then F has discriminant -23 and (3.1) is satisfied by the pairs $(1,0),(0,1),(-1,1),(1,1),(4,-3)$. Delone and Nagell proved their result by considering units in the algebraic number field $\mathbb{Q}(\varepsilon)$, where ε is the real root of $F(x,1)=0$. In both the proofs of Delone and Nagell the fact that $\mathbb{Q}(\varepsilon)$ has only one fundamental unit is essential.

Now suppose that F satisfies the same conditions as above, except that its discriminant is positive. Let $L=\mathbb{Q}(\varepsilon)$, where ε is some root of $F(x,1)=0$. We can not apply the methods of Delone and Nagell since L has two fundamental units. However, it is possible to reduce (3.1) to a set of exponential equations to which a p-adic method of Skolem can be applied. (cf. [Lj 2],[Av 1,2],[Mo]ch.23,[Sk 1,2,3,4]). In this way (3.1) was solved for the forms $F(x,y)=x^3-3xy^2+y^3$ of discriminant 81 and $F(x,y)=x^3+x^2y-2xy^2-y^3$ of discriminant 49 by respectively Ljunggren [Lj 2] and Baulin [Ba]. For the first form the six solutions of (3.1) are $(1,0),(0,1),(-1,-1),(1,3),(-3,-2),(2,-1)$, while for the second form (3.1) is satisfied by the nine pairs $(1,0),(0,-1),(-1,+1),(-1,1),(2,-1),(-1,2),(5,4),(4,-9),(-9,5)$. Note that for the first form $L=\mathbb{Q}(e^{2\pi i/9}+e^{-2\pi i/9})$, while for the second form $L=\mathbb{Q}(e^{2\pi i/7}+e^{-2\pi i/7})$. In the proofs of Ljunggren and Baulin, use is made of the explicit values of some fundamental units in a quadratic extension of L. So it does not seem easy to derive general results on (3.1) by their method.

It is possible to derive more general, though ineffective results by means of a modification of the Thue-Siegel method used in chapter 2. In this way, Siegel [Si 3,6] showed that the number of solutions of the

inequality

$$|F(x,y)| \leq k \qquad (k \in \mathbb{N}) \tag{3.2}$$

in integers x,y with (x,y)=1,y>0 or x=1,y=0 is at most 18 if the discriminant of F is sufficiently large compared with k. In a student paper from 1949, A.E. Gel'man showed, by refining Siegel's estimates, that 18 can be replaced by 10.(For a proof we refer to [D/F],ch.5). In particular this implies that (3.1) has at most ten solutions if the discriminant of F is large enough. We shall give a uniform upper bound for the number of solutions of (3.1).

THEOREM 3.1. *Let F be a binary cubic form with integral coefficients and non-zero discriminant. Then the equation*

$$F(x,y) = 1 \tag{3.1}$$

has at most twelve *solutions in integers* x,y.

As far as I know, no cubic forms F are known for which (3.1) has more than nine solutions and it is likely, that our result can be improved. Note that the upper bound given in theorem 3.1 does not depend on the coefficients of F. As we already mentioned in chapter 0, we shall prove a similar result also for forms of degree higher than 3 in chapter 6.

We shall also derive an analogue of theorem 2.1. Before we can state it, we have to introduce some notions. Let F be an arbitrary binary form (whose coefficients belong to some field of characteristic zero) and let $T:(x,y)\mapsto(X,Y)$ be a linear transformation of determinant unity. Put $F^T(x,y)=F(X,Y)$. An *invariant* of F is a rational function I(F) in the coefficients of F such that $I(F^T)=I(F)$ for any choice of T. A *covariant* $C_F(x,y)$ is a binary form whose coefficients are rational functions in the coefficients of F such that $C_{F^T}(x,y)=C_F(X,Y)$. (cf. [Di 1],[Mo] ch.18). In particular, the discriminant of a binary form is an invariant. If a form C(x,y) is a covariant of a binary form F then we say that it has the *covariance property*. We now suppose that F is a cubic form, $F(x,y)=ax^3+bx^2y+cxy^2+dy^3$ say. It is easy to check, that

$$H(x,y) = -\frac{1}{4}\left(\frac{\partial^2 F}{\partial x^2}\frac{\partial^2 F}{\partial y^2} - \left(\frac{\partial^2 F}{\partial x \partial y}\right)^2\right) = (bx+cy)^2-(3ax+by)(cx+3dy)$$
$$= Ax^2+Bxy+Cy^2$$

say, is a covariant of F, the so-called *quadratic covariant*. Since the discriminant D of F equals

$$b^2c^2-4ac^3-4b^3d+18abcd-27a^2d^2,$$

H is a quadratic form of discriminant $B^2-4AC=-3D$. If $D>0$ and $a,b,c,d\in\mathbb{R}$, then H is positive definite since $H(b,-3a)=(b^2-3ac)^2\geq 0$.

DEFINITION. A cubic form F with integral coefficients and of positive discriminant is called *reduced* if its quadratic covariant H is reduced, i.e. if $C\geq A\geq |B|$.

Two binary forms F_1,F_2 with integral coefficients are called *equivalent* if a unimodular transformation $X:=a_{11}x+a_{12}y, Y:=a_{21}x+a_{22}y$ (with $a_{11},\ldots,a_{22}\in\mathbb{Z}$ and $a_{11}a_{22}-a_{12}a_{21}=1$) exists such that $F_2(X,Y)=F_1(x,y)$. If two cubic forms with integral coefficients are equivalent under a unimodular transformation then their quadratic covariants are equivalent under the same transformation by the covariance property. Hence, since every positive definite quadratic form is equivalent to a reduced quadratic form, every cubic form of positive discriminant is equivalent to a reduced cubic form. (cf. [Mo],ch.24).

THEOREM 3.2. *Let* F *be a reduced, irreducible binary cubic form with integral coefficients and of positive discriminant. Let* k *be a positive integer. Then the inequality*

$$|F(x,y)| \leq k \tag{3.2}$$

has at most nine *solutions in integers* x,y *with* $(x,y)=1, y\geq 1$ $2^{1/4}k^{3/2}$.

In fact, both theorem 3.1 and theorem 3.2 are consequences of

THEOREM 3.3. *Let* F *be an irreducible binary cubic form with integral coefficients, positive discriminant* D *and quadratic covariant* H. *Let* k *be a positive integer. Then the number of solutions of the inequality*

(3.2) $\quad |F(x,y)| \leq k$

in integers x,y *with*

(3.3) $\quad H(x,y) \geq \frac{3}{2}(3D)^{1/2}k^3$, $(x,y)=1$, $y>0$ *or* $x=1,y=0$

is at most 9.

In the proof of theorem 3 we have used ideas from [D/F],ch.5 and [Si 3,4]. It will be similar to the proof of theorem 2.1 in case n=3.

§3.2. Proofs of theorem 3.1 and theorem 3.2.

In this section we shall derive theorem 3.1 and theorem 3.2 from theorem 3.3. In the sequel, let F be a binary cubic form with integral coefficients, discriminant D and quadratic covariant H. Theorem 3.2 is an immediate consequence of theorem 3.3 and the lemma below.

LEMMA 3.1. *If* $D>0$ *and if* F *is reduced and irreducible, then*

(3.4) $\quad H(x,y) \geq \frac{3}{4}D^{1/2}y^2$ *for* $x,y\in\mathbb{Z}$,

(3.5) $\quad H(x,y) \geq \frac{3}{2}(3D)^{1/2}y^2$ *for* $x,y\in\mathbb{Z}$ *with* $|x|\geq|2y|$.

PROOF. We may assume that $y\neq 0$. Put $H(x,y)=Ax^2+Bxy+Cy^2=y^2f(z)$, where $z=x/y$ and $f(z)=Az^2+Bz+C$. Note that for $z=-B/2A$, $f(z)$ assumes a minimum on the reals which is equal to $3D/4A$. Furthermore F, whence H, is reduced, hence

$$A^2 \leq AC \leq \frac{1}{3}(4AC-B^2) = D.$$

This implies that $f(z)\geq 3D/4D^{1/2}=3D^{1/2}/4$ which is equivalent to (3.4).

We are now going to prove (3.5). Since $f(z)$ assumes its minimum in a point with absolute value not exceeding 1/2, it follows that for $|x|\geq|2y|$,

$$f(z) \geq \min(f(2),f(-2)) = 4A-2|B|+C = 4A+C-2(4AC-3D)^{1/2} =: g(A,C).$$

We shall minimalise $g(A,C)$ on the (A,C)-plane. Since H is reduced, (A,C) belongs to the set

$$G = \{(A,C)\in\mathbb{R}^2 \mid 1\le A\le C,\ A^2\ge 4AC-3D\ge 0\}.$$

(cf. figure 3.1). In G, $g(A,C)$ assumes its minimum in the point $((3D)^{1/2}/3, 5(3D)^{1/2}/6)$. This minimum is equal to $3(3D)^{1/2}/2$ and this proves our lemma completely. □

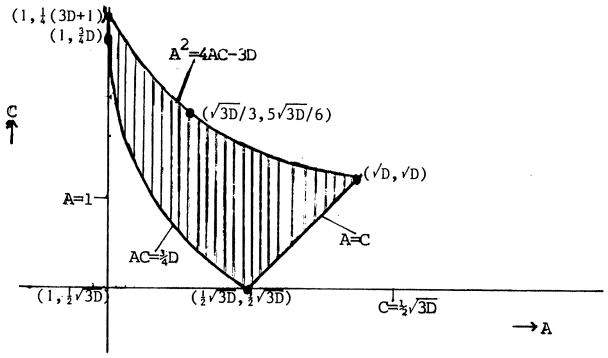

figure 3.1. The set G.

We shall now prove theorem 3.1. Suppose, that $D\neq 0$. We may assume, that F is irreducible for otherwise we can write

$$F(x,y) = (a_1x+a_2y)(b_1x^2+b_2xy+b_3y^2)$$

for some integers a_1,a_2,b_1,b_2,b_3. Hence solutions of (3.1) must satisfy

$$a_1x+a_2y = \pm 1,\ b_1x^2+b_2xy+b_3y^2 = \pm 1.$$

Therefore,

$$a_2^2b_1x^2+a_2b_2x(a_1x\overline{+}1)+b_3(a_1x\overline{+}1)^2 = \pm a_2^2 .$$

It is easy to check, that these relations can be satisfied by at most four pairs $(x,y)\in\mathbb{Z}^2$.

From now on, we assume that $D>0$, that F is irreducible and reduced and that its coefficient of x^3 is positive. By the result of Delone and Nagell and by the fact that the number of solutions of (3.1) does not change when F is replaced by an equivalent form, these are no restrictions.

Note that for every pair of integers (x_1,y_1) with $|F(x_1,y_1)|=1$ and

$y_1>0$ or $(x_1,y_1)=(1,0)$ exactly one pair of integers (x_0,y_0) exists with $F(x_0,y_0)=1$ and $(x_0,y_0)=\pm(x_1,y_1)$. Hence by theorem 3.3, (3.1) has at most nine solutions with $H(x,y)\geq 3\sqrt{3D}/2$. Note that by lemma 3.1, $H(x,y)\geq 3\sqrt{3D}/2$ if $|xy|\geq 2$. We shall show that (3.1) has at most three solutions with $|xy|\leq 1$ if F is not equivalent to the form $x^3+x^2y-2xy^2-y^3$. In view of Baulin's result this suffices to prove theorem 3.1.

First of all, there are at most three solutions of (3.1) in the set $\{(x,y)\in\mathbb{Z}^2 \mid |x|\leq 1, |y|=1\}$. For if (x_0,y_0) is a solution of (3.1) belonging to this set then the pair $(-x_0,-y_0)$, which is clearly no solution, also belongs to it. Hence we may restrict ourselves to the case that (1,0) is a solution of (3.1) and we shall do so in the sequel.

We assume that the number of solutions with $y=-1$ and $|x|\leq 1$ is not less than the number of solutions with $y=1$ and $|x|\leq 1$ and moreover, that there are at least two solutions with $y=-1$ and $|x|\leq 1$. These are no restrictions. Since $F(1,0)=1$ we have as a consequence, that

$$F(x,y) = (x+py)(x+qy)(x+ry)-y^3 \quad \text{where } p,q\in\{-1,0,1\}, p>q, r\in\mathbb{Z}.$$

If there is a third solution with $y=-1, |x|\leq 1$ then $F(x,y)=x(x-y)(x+y)-y^3=x^3-xy^2-y^3$ has discriminant -23. Hence this is impossible. If there is a solution with $y=1, |x|\leq 1$ then

$$(x+p)(x+q)(x+r) = 2.$$

If $x=-1$, then $p=0, q=-1, r=2$ and $F(x,y)=x^3+x^2y-2xy^2-y^3$. If $x=0$ then $p=1, q=-1$, $r=-2$ and F has discriminant -87. Finally, if $x=1$, then $p=1, q=0, r=0$ and F has discriminant -23. Hence there are no solutions with $y=1, |x|\leq 1$. It follows that (3.1) has at most three solutions with $|xy|\leq 1$ if F satisfies the conditions mentioned above. This completes the proof of theorem 1. □

For the sake of completeness we mention that there are infinitely many reduced forms F for which (3.1) has three solutions with $H(x,y)<3\sqrt{3D}/2$. Take

$$F(x,y) = x^3+ax^2y-(a+3)xy^2+y^3 \qquad (a\in\mathbb{Z}).$$

Then F has quadratic covariant $(a^2+3a+9)(x^2-xy+y^2)$ and discriminant $(a^2+3a+9)^2$. It is easy to check that F is irreducible and that $(1,0),(0,1)$, $(-1,-1)$ are solutions of (3.1). For these solutions one has $H(x,y)=D^{1/2}$.

(3.1) has at most one solution with $H(x,y)<\frac{1}{2}(3D)^{1/2}$ if F is irreducible and of positive discriminant. For by the covariance property of H we may assume that F is reduced. Hence, by lemma 3.1, $H(x,y)\geq 3(3D)^{1/2}/2$ if $|xy|\geq 2$. Furthermore, $H(\pm 1,0)=A, H(0,\pm 1)=C, H(\pm 1,\pm 1)\geq A-|B|+C$ and

$$A-|B|+C \geq C \geq (AC)^{1/2} = \frac{1}{2}(3D+B^2)^{1/2} \geq \frac{1}{2}(3D)^{1/2}.$$

If D exceeds some absolute constant, D_0 say, then one can prove, similar to theorem 3.3, that theorem 3.3 with k=1 holds true even if the lower bound $(3/2)(3D)^{1/2}$ in (3.3) is replaced by $\frac{1}{2}(3D)^{1/2}$. Hence for $D\geq D_0$, (3.1) has at most ten solutions. In fact, one can show that D_0 can be taken equal to 6×10^{10} but we shall not work this out here.

§3.3. Preliminaries to the proof of theorem 3.3.

Also for later purposes, we shall state some general properties of binary cubic forms. Let K be a field of characteristic 0 and let F(x,y) be a cubic form with coefficients in K, say

$$F(x,y) = ax^3+bx^2y+cxy^2+dy^3.$$

The quadratic covariant of F was defined by

$$H(x,y) = -\frac{1}{4}\left(\frac{\partial^2 F}{\partial x^2}\frac{\partial^2 F}{\partial y^2} - \left(\frac{\partial^2 F}{\partial x \partial y}\right)^2\right) = Ax^2+Bxy+Cy^2,$$

where

$$A = b^2-3ac,\quad B = bc-9ad,\quad C = c^2-3bd. \tag{3.6}$$

Let D denote the discriminant of F. Then H has discriminant -3D. Another covariant of F, the *cubic covariant*, is defined by

$$G(x,y) = \frac{\partial F}{\partial x}\frac{\partial H}{\partial y} - \frac{\partial F}{\partial y}\frac{\partial H}{\partial x} = a'x^3+3b'x^2y+3c'xy^2+d'y^3,$$

where

(3.7) $$a'=9abc-2b^3-27a^2d,\ b'=6ac^2-b^2c-9abd,$$
$$c'=9acd+bc^2-6b^2d,\ d'=27ad^2+2c^3-9bcd.$$

LEMMA 3.2. *In the above notation, let* $M=K(\sqrt{-3D})$. *There are a pair of constants* $\alpha,\beta\in M$ *and a pair of linear forms* $\xi,\eta\in M[x,y]$ *of determinant unity such that for some choice of the square root of* $-3D$*:*

(3.8) $$\alpha\xi^3 = \frac{G+3\sqrt{-3D}\,F}{2},\quad \beta\eta^3 = \frac{G-3\sqrt{-3D}\,F}{2},$$

(3.9) $$\alpha\xi^3-\beta\eta^3 = 3\sqrt{-3D}\,F,$$

(3.10) $$H^3=\alpha\xi^3\beta\eta^3,\quad H = -\sqrt{-3D}\,\xi\eta.$$

PROOF. Choose $\sqrt{-3D}$ such that $B+\sqrt{-3D}\neq 0$ and put

$$\xi(x,y) = \frac{-1}{\sqrt{-3D}}\left(Ax+\frac{B+\sqrt{-3D}}{2}y\right),\quad \eta(x,y) = x+\frac{2C}{B+\sqrt{-3D}}y.$$

Since H has discriminant $-3D$ it follows that the linear transformation $(x,y)\mapsto(\xi,\eta)$ has determinant unity and that

$$H = -\sqrt{-3D}\,\xi\eta.$$

Put

$$\tilde{F}(\xi,\eta) = \tilde{a}\xi^3+\tilde{b}\xi^2\eta+\tilde{c}\xi\eta^2+\tilde{d}\eta^3 := F(x,y).$$

Then $\tilde{a},\tilde{b},\tilde{c},\tilde{d}\in M$ and by the covariance property of H and by (3.6),

(3.11) $$\tilde{b}^2-3\tilde{a}\tilde{c} = 0,\ \tilde{c}^2-3\tilde{b}\tilde{d} = 0,\ \tilde{b}\tilde{c}-9\tilde{a}\tilde{d} = -\sqrt{-3D}.$$

Hence

$$0 = \tilde{b}^2\tilde{c}^2-9\tilde{a}\tilde{b}\tilde{c}\tilde{d} = \tilde{b}\tilde{c}(\tilde{b}\tilde{c}-9\tilde{a}\tilde{d}) = -\tilde{b}\tilde{c}\sqrt{-3D}.$$

Therefore, $\tilde{b}\tilde{c}=0$ and together with (3.11) this yields that $\tilde{b}=\tilde{c}=0$, $\tilde{a}\tilde{d}=\sqrt{-3D}/9$. Thus we have, by the invariance of D and the covariance property of G,

$$F(x,y) = \tilde{F}(\xi,\eta) = \tilde{a}\xi^3+\tilde{d}\eta^3,\ G(x,y) = 3\sqrt{-3D}(\tilde{a}\xi^3-\tilde{d}\eta^3),\ D= -27\tilde{a}^2\tilde{d}^2.$$

Now we put $\alpha=3\sqrt{-3D}\ \tilde{a}$, $\beta=-3\sqrt{-3D}\ \tilde{d}$. Then clearly $\alpha,\beta\in M$,

$$\alpha\xi^3-\beta\eta^3 = 3\sqrt{-3D}\ F,\ \alpha\xi^3+\beta\eta^3 = G,\ \alpha\xi^3\beta\eta^3 = H^3.$$

This proves our lemma. Note that as a by-product we obtained the well-known identity

$$4H^3 = G^2+27DF^2.$$ □

In the sequel we shall use some facts about quadratic fields. (cf [La],ch.1,4). We shall apply the preceding theory with $K=\mathbb{Q}$, $a,b,c,d\in\mathbb{Z}$, $D>0$. Thus $M=\mathbb{Q}(\sqrt{-3D})$ is an imaginary quadratic field, which is supposed to be contained in $\mathbb{C}$. Furthermore we put

$$\mathcal{O}_0 = \{\frac{m+n\sqrt{-3D}}{2}\in\mathcal{O}_M \mid m,n\in\mathbb{Z}\}.$$

It is easy to check that $\mathcal{O}_0$ is a subring of $\mathcal{O}_M$, on noting that $D\equiv B^2 \pmod 4$, i.e. $D\equiv 0,1 \pmod 4$ and that $(m+n\sqrt{-3D})/2\in\mathcal{O}_M$ if and only if $m\equiv nD \pmod 2$. Furthermore,

(3.12) $\lambda\in\mathcal{O}_0$ if and only if $\lambda\in\mathcal{O}_M$, $\lambda-\bar{\lambda}\in\mathbb{Z}\sqrt{-3D}$.

This implies that

(3.13) $|\lambda| \geq |\mathrm{Im}\ \lambda| \geq \frac{1}{2}\sqrt{3D}$ if $\lambda\in\mathcal{O}_0\setminus\mathbb{Z}$.

Note that by (3.8) and (3.10) $\alpha\xi(x,y)^3$ and $\beta\eta(x,y)^3$ are complex conjugate elements of $\mathcal{O}_0$ for every pair of rational integers (x,y). Furthermore we have

LEMMA 3.3. *Let* $(x_1,y_1),(x_2,y_2)$ *be pairs of rational integers. Then the numbers* $\sqrt{-3D}\cdot\xi(x_1,y_1)\eta(x_2,y_2)$, $\alpha\xi(x_1,y_1)^2\xi(x_2,y_2)$, $\beta\eta(x_1,y_1)^2\eta(x_2,y_2)$ *belong to* $\mathcal{O}_0$.

PROOF. For convenience, we put $\xi_i=\xi(x_i,y_i)$, $\eta_i=\eta(x_i,y_i)$ for $i=1,2$. Note that $-\sqrt{-3D}\xi_1\eta_2$ and $-\sqrt{-3D}\xi_2\eta_1$ are cube roots of the complex conjugate algebraic integers $\alpha\xi_1^3\beta\eta_2^3$ and $\alpha\xi_2^3\beta\eta_1^3$ respectively which belong to M and that the product of these numbers is equal to $H(x_1,y_1)H(x_2,y_2)>0$. Hence $\sqrt{-3D}\xi_1\eta_2$ and $\sqrt{-3D}\xi_2\eta_1$ are complex conjugate elements of $\mathcal{O}_M$. Furthermore, since the

transformation $(x,y)\mapsto(\xi,\eta)$ has determinant unity,

$$(3.14)\qquad \sqrt{-3D}\xi_1\eta_2-\sqrt{-3D}\xi_2\eta_1 = \sqrt{-3D}(x_1y_2-x_2y_1) \in \mathbb{Z}\sqrt{-3D}.$$

By (3.12) this implies that $\sqrt{-3D}\xi_1\eta_2\in\mathcal{O}_0$.

Since $\alpha\beta(\xi_1\eta_1)^2\xi_2\eta_2=H(x_1,y_1)^2H(x_2,y_2)>0$ and $|\alpha\xi_i^3|=|\beta\eta_i^3|$ for i=1,2 we have $|\alpha\xi_1^2\xi_2|=|\beta\eta_1^2\eta_2|$, and hence $\alpha\xi_1^2\xi_2,\beta\eta_1^2\eta_2$ are complex conjugates. Therefore it suffices to show that $\alpha\xi_1^2\xi_2\in\mathcal{O}_0$. We put $\varepsilon_1=\xi(1,0),\varepsilon_2=\xi(0,1)$. Then $\alpha\xi_1^2\xi_2$ can be written as a linear combination of $\alpha\varepsilon_1^3,\alpha\varepsilon_1^2\varepsilon_2,\alpha\varepsilon_1\varepsilon_2^2,\alpha\varepsilon_2^3$ with rational integral coefficients. Hence it suffices to show that $\alpha\varepsilon_1^3,\alpha\varepsilon_1^2\varepsilon_2$, $\alpha\varepsilon_1\varepsilon_2^2,\alpha\varepsilon_2^3$ belong to $\mathcal{O}_0$. Note that $\alpha\varepsilon_1^3,\alpha\varepsilon_2^3$ are algebraic integers and that $\alpha\varepsilon_1^2\varepsilon_2,\alpha\varepsilon_1\varepsilon_2^2$ are also algebraic integers since they are cube roots of $(\alpha\varepsilon_1^3)^2\alpha\varepsilon_2^3,\alpha\varepsilon_1^3(\alpha\varepsilon_2^3)^2$ respectively. Furthermore by (3.8),

$$\alpha\varepsilon_1^3x^3+3\alpha\varepsilon_1^2\varepsilon_2x^2y+3\alpha\varepsilon_1\varepsilon_2^2xy^2+\alpha\varepsilon_2^3y^3 = \alpha(\varepsilon_1x+\varepsilon_2y)^3 = \alpha\xi(x,y)^3$$
$$= \frac{a'+3a\sqrt{-3D}}{2}x^3+3\frac{b'+b\sqrt{-3D}}{2}x^2y+3\frac{c'+c\sqrt{-3D}}{2}xy^2+\frac{d'+3d\sqrt{-3D}}{2}y^3.$$

Since a,b,c,d,a',b',c',d' are rational integers, $\alpha\varepsilon_1^3,\alpha\varepsilon_1^2\varepsilon_2,\alpha\varepsilon_1\varepsilon_2^2,\alpha\varepsilon_2^3$ belong to $\mathcal{O}_0$. This completes the proof of lemma 3.3. □

§3.4. Proof of theorem 3.3.

We shall prove theorem 3.3 similarly to theorem 2.1 for n=3 but we have to be more careful in our estimates. We put $\Delta=3D$ and for every pair of rational integers (x,y),

$$\omega = \omega(x,y) = |\alpha\xi(x,y)^3| = |\beta\eta(x,y)^3| = H(x,y)^{3/2}.$$

We have to show that there are at most nine pairs of rational integers (x,y) such that

$$(3.15)\qquad \omega \geq \left(\frac{3}{2}\right)^{3/2}\Delta^{3/4}k^{9/2},\quad |\alpha\xi^3-\beta\eta^3| \leq 3k\Delta^{1/2},$$
$$(x,y)=1 \text{ and } y>0 \text{ or } x=1 \text{ and } y=0.$$

It is known that 49,81,148 are the three smallest positive integers which are discriminant of an irreducible cubic form and that for these values of D only one equivalence class of cubic forms exists. (cf. footnote† on p.46)

Hence by the results of Ljunggren and Baulin, we may assume that $D \geq 148$ if $k=1$ and $D \geq 49$ otherwise, i.e. $\Delta \geq 444$ if $k=1$ and $\Delta \geq 147$ if $k \geq 2$.

Let $\theta_1, \theta_2, \theta_3$ be the three cube roots of β/α. We say that a solution (x,y) of (3.5) is related to θ_i if

$$\left|1-\theta_i \frac{\eta(x,y)}{\xi(x,y)}\right| = \min_{j\in\{1,2,3\}} \left|1-\theta_j \frac{\eta(x,y)}{\xi(x,y)}\right| .$$

We shall show that at most three solutions of (3.15) can be related to a θ_i. We assume the contrary, i.e. that there is a cube root θ of β/α to which at least four solutions of (3.15) are related, $(x_{-1},y_{-1}),(x_0,y_0)$, $(x_1,y_1),(x_2,y_2)$ say, ordered such that $\omega(x_{i+1},y_{i+1}) \geq \omega(x_i,y_i)$ for $i=-1,0,1$.

LEMMA 3.4. *(i) If* (x,y) *is a solution of* (3.15) *related to* θ, *then*

$$(3.16) \qquad \left|1-\theta\frac{\eta}{\xi}\right| < \frac{\pi}{3}\frac{k\sqrt{\Delta}}{\omega} .$$

(ii) If $(x',y'),(x'',y'')$ *are distinct solutions of* (3.15) *related to* θ *and if* $\omega(x'',y'') \geq \omega(x',y')$, *then*

$$(3.17) \qquad \omega(x'',y'') \geq \left(\frac{0.948}{k}\right)^3 \omega(x',y')^2 .$$

PROOF. I shall use an argument which was suggested to me by F. Beukers. Note that by (3.15),

$$(3.18) \qquad \left|1-\frac{\beta\eta^3}{\alpha\xi^3}\right| \leq \frac{3k\sqrt{\Delta}}{\omega^3} .$$

Since $\Delta^{1/4}k^{7/2} \geq 444^{1/4} > 2^{3/2}3^{-1/2}$, we have by (3.18) and the lower bound for

---

†In [D/F] on p.159 a table is given of rings of discriminant D with $0<D\leq 1296$ with a unit element which are contained in rings of integers of cubic fields. This table can also be considered as a table of equivalence classes of cubic forms of positive discriminant for Delone and Faddeev showed in ch.2 of [D/F] that there exists a bijective mapping of equivalence classes of irreducible cubic forms onto the rings described above which preserves the discriminant. This table shows that the class of discriminant 49 is represented by $x^3-x^2y-2xy^2+y^3$, the class of discriminant 81 by $x^3-3xy^2-y^3$ and that of 148 by $x^3-x^2y-3xy^2+y^3$.

ω given in (3.15),

$$\left|1-\frac{\beta\eta^3}{\alpha\xi^3}\right| \le \frac{2^{3/2}}{3^{1/2}\Delta^{1/4}k^{7/2}} < 1.$$

Since $|\beta\eta^3/\alpha\xi^3| = 1$, this implies that $|\arg(\beta\eta^3/\alpha\xi^3)| < \pi/3$. (cf. figure 3.2 below). Hence, by the fact that (x,y) is related to θ,

$$|1-\theta\tfrac{\eta}{\xi}| \le |\arg(\theta\tfrac{\eta}{\xi})| = \tfrac{1}{3}|\arg\left(\frac{\beta\eta^3}{\alpha\xi^3}\right)| < \tfrac{1}{3}\tfrac{\pi}{3}|1-\frac{\beta\eta^3}{\alpha\xi^3}| \le \frac{\pi}{3}\frac{k\sqrt{\Delta}}{\omega}.$$

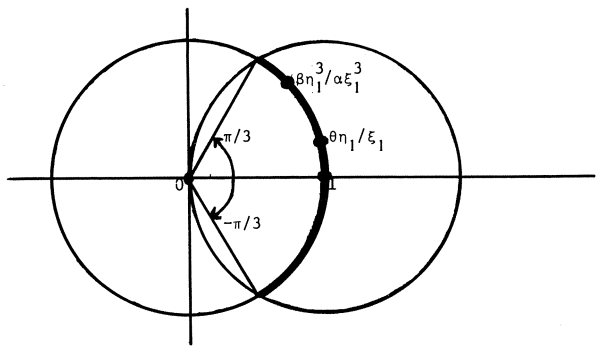

figure 3.2.

(ii) Put $\xi'=\xi(x',y')$, $\eta'=\eta(x',y')$, $\omega'=\omega(x',y')$, $\xi''=\xi(x'',y'')$, $\eta''=\eta(x'',y'')$, $\omega''=\omega(x'',y'')$. We have $|\alpha\beta|=\Delta^{3/2}$, hence by (3.14) and (3.16),

$$\sqrt{\Delta} = |\alpha\beta|^{1/3} \le |\alpha\beta|^{1/3}|\xi'\eta''-\xi''\eta'| = (\omega'\omega'')^{1/3}|\theta\frac{\eta'}{\xi'}-\theta\frac{\eta''}{\xi''}|$$
$$\le (\omega'\omega'')^{1/3}\left(|1-\theta\frac{\eta'}{\xi'}|+|1-\theta\frac{\eta''}{\xi''}|\right) < (\omega'\omega'')^{1/3}\frac{\pi}{3}k\sqrt{\Delta}(\omega'^{-1}+\omega''^{-1}).$$

This implies that

$$\omega'+\omega'' > \frac{3}{\pi k}(\omega'\omega'')^{2/3}.$$

Put $p=k\omega''^{1/3}\omega'^{-2/3}$, $h(z)=z^3-3z^2/\pi+k^3/\omega'$. Then $h(p)>0$. Note that $h(z)$ assumes a local maximum for $z=0$ and a local minimum for $z=2/\pi$. Clearly, $h(0)>0$. (cf. figure 3.3 on the following page). By (3.15) and the fact that $k^{3/2}\Delta^{3/4}\ge 444^{3/4}$ we have

(3.19) $\qquad \omega' \ge 999^{3/4}k^3.$

Hence

$$h(2/\pi) = (2/\pi)^3-(3/\pi)(2/\pi)^2+k^3/\omega' < 0.$$

Therefore, $h(z)$ has two zeros, p_1,p_2 say, with $p_1<p_2$, such that $h(z)$ is positive for $0<z<p_1$ and $z>p_2$, and negative for $p_1<z<p_2$. It is impossible that $p<p_1$. For since $\omega''\geq\omega'$ we have $p\geq k\omega'^{-1/3}$ and, by (3.19),

$$h(k\omega'^{-1/3}) = \frac{3}{\pi}\frac{k^3}{\omega'}\left(\frac{2\pi}{3}-\frac{\omega'^{1/3}}{k}\right) < 0.$$

Hence $p>p_2$. Furthermore we have $p_2\geq 0.948$ since by (3.19),

$$h(0.948) = 0.948^3-(3/\pi)0.948^2+k^3/\omega' < 0.$$

This proves lemma 3.4 completely. □

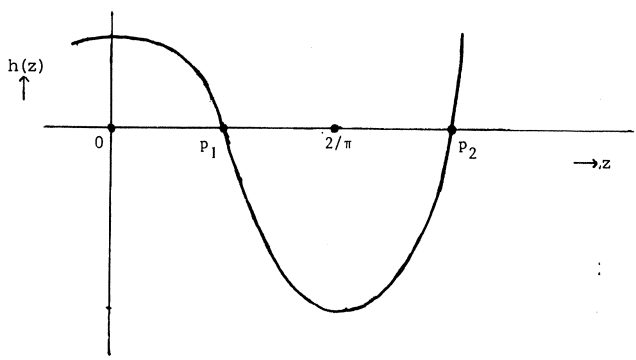

figure 3.3. Graph of $h(z)$.

Put $\omega_i=\omega(x_i,y_i),\xi_i=\xi(x_i,y_i),\eta_i=\eta(x_i,y_i)$ for $i=1,2$ and $z_1=\theta\eta_1/\xi_1$. On applying lemma 3.4 (ii) twice we have, by the lower bound for ω in (3.15),

$$\omega_1 \geq \left(\frac{0.948}{k}\right)^9 \omega(x_{-1},y_{-1})^4 \geq \frac{0.948^9}{k^9}\left(\left(\frac{3}{2}\right)^{3/2}\Delta^{3/4}k^{9/2}\right)^4 > 7\Delta^3k^9. \tag{3.20}$$

Furthermore, on applying lemma 3.4 (ii) once again,

$$\omega_2 \geq \left(\frac{0.948}{k}\right)^3 \omega_1^2. \tag{3.21}$$

Let $A_m(z),B_m(z)$ be the polynomials defined in chapter 1 (with $n=3$)

and let r,g be the integers defined by $m=2r+1-g$ with $g\in\{0,1\}$. We assume that $m\geq 2$.

LEMMA 3.5. *Put*

$$\Sigma_m = \frac{\eta_2}{\xi_2} A_m(z_1^3) - \frac{\eta_1}{\xi_1} B_m(z_1^3),$$

$$\sigma(m) = \pi 2^{-2g/3}\binom{2r}{r}, \tau(m) = 2^{g/3-1}3\pi^m\binom{r-g+1/3}{r-g+1}\binom{r-1/3}{r}\binom{m}{r}^{-1},$$

$$\Xi_m = \sigma(m)k\Delta^{g/3}\omega_1^{r+(1-g)/3}\omega_2^{-2/3}, \quad \P_m = \tau(m)k^m\Delta^{r-g/6}\omega_2^{1/3}\omega_1^{-r-2(1-g)/3}.$$

If $\Sigma_m\neq 0$, *then*

$$1 < \frac{1}{3}\cdot\Xi_m + \frac{2}{3}\cdot\P_m . \tag{3.22}$$

PROOF. Put $\gamma=-\alpha\theta/\sqrt{-3D}, \delta=-\beta/\theta\sqrt{-3D}$. Then, by the fact that $\alpha\beta=-(\sqrt{-3D})^3$ (cf. (3.10)), $\gamma^3=\alpha, \delta^3=\beta, \gamma\delta=-\sqrt{-3D}, \delta/\gamma=\theta$. Furthermore, we put $F=F(x_1,y_1)$, $\zeta=F\sqrt{-D}/\alpha\xi_1^3$. We shall consider the number

$$\Lambda_m = (\alpha\xi_1^3)^r(\gamma\xi_1)^{1-g}\gamma\xi_2(\theta\Sigma_m).$$

We assume that Σ_m, whence Λ_m is non-zero. The numbers $(\alpha\xi_1^3)^r A_m(z_1^3)$ and $(\alpha\xi_1^3)^{r-g}B_m(z_1^3)$ belong to $\mathcal{O}_0$. For by lemma 1.3 (ii) with n=3 we have, using that $\max(2\deg C_{1m}, 2\deg C_{2m}+1)\leq r, \sqrt{-3D}\in\mathcal{O}_0$,

$$(\alpha\xi_1^3)^r A_m(z_1^3) = (\alpha\xi_1^3)^r A_m(1-3^{3/2}\zeta) = (\alpha\xi_1^3)^r C_{1m}(\zeta^2) - \zeta\sqrt{3}(\alpha\xi_1^3)^r C_{2m}(\zeta^2)$$

$$= (\alpha\xi_1^3)^r C_{1m}(-F^2D/(\alpha\xi_1^3)^2) - F\sqrt{-3D}(\alpha\xi_1^3)^{r-1}C_{2m}(-F^2D/(\alpha\xi_1^3)^2) \in \mathcal{O}_0$$

and similarly, $(\alpha\xi_1^3)^{r-g}B_m(z_1^3)\in\mathcal{O}_0$.

Firstly, we consider the case that m is odd. Then, by (1.1), $B_m(z)=z^r A_m(z^{-1})$ for $z\neq 0$. Hence, by $\alpha\xi_1^3=\beta\eta_1^3$, $(\alpha\xi_1^3)^r A_m(z_1^3)$ and $(\alpha\xi_1^3)^r B_m(z_1^3)$ are conjugate elements of $\mathcal{O}_0$. Furthermore, by the proof of lemma 3.3, $\sqrt{-3D}\xi_1\eta_2$ and $\sqrt{-3D}\xi_2\eta_1$ are conjugate elements of $\mathcal{O}_0$. Hence, by (3.12),

$$\Lambda_m = \sqrt{-3D}\xi_1\eta_2(\alpha\xi_1^3)^r A_m(z_1^3) - \sqrt{-3D}\xi_2\eta_1(\alpha\xi_1^3)^r B_m(z_1^3) \in \mathbb{Z}\sqrt{-3D}. \tag{3.23}$$

Secondly, we assume that m is even. It follows at once from lemma 3.3 and $\delta^3=\beta$, that

$$\Lambda_m^3 = \left(\delta\eta_2(\alpha\xi_1^3)^r A_m(z_1^3) - \delta\eta_1\alpha\xi_1^2\xi_2(\alpha\xi_1^3)^{r-1}B_m(z_1^3)\right)^3 \in \mathcal{O}_0.$$

Furthermore we may assume that $\Lambda_m^3 \notin \mathbb{Z}$. For suppose the contrary. Then $\Lambda_m = \rho\overline{\Lambda_m}$ for some third root of unity ρ. Furthermore, by (3.10) and $\gamma\delta = -\sqrt{-3D}$, $\gamma\xi_i$ and $\delta\eta_i$ are complex conjugates for $i \in \{1,2\}$. Hence by lemma 3.3,

$$\begin{aligned}\theta\Sigma_m &= \rho(\alpha\xi_1^3)^{-r}(\gamma\xi_2)^{-1}\,\overline{\Lambda_m} \\ &= \rho(\alpha\xi_1^3)^{-r}(\gamma\xi_2)^{-1}\left(\gamma\xi_2(\beta\eta_1^3)^r A_m(z_1^{-3}) - \gamma\xi_1\beta\eta_1^2\eta_2(\beta\eta_1^3)^{r-1}B_m(z_1^{-3})\right) \\ &= \rho\left(z_1^{3r}A_m(z_1^{-3}) - (\beta\eta_1^2\eta_2/\alpha\xi_1^2\xi_2)z_1^{3(r-1)}B_m(z_1^{-3})\right) \in M(\rho).\end{aligned}$$

Hence $\theta\Sigma_m$ has degree at most 2 over M. But this is impossible, since $\Sigma_m \in M^*$, since F is irreducible and since $M(\theta)$ contains a zero of $F(x,1)$. Hence $\Lambda_m^3 \notin \mathbb{Z}$. This implies by (3.13) that

$$|\Lambda_m^3| \geq \tfrac{1}{2}\Delta^{1/2}.$$

Together with (3.23) this yields that for all values of m with $m \geq 2$,

$$|\Lambda_m| \geq 2^{-g/3}\Delta^{1/2-g/3}. \tag{3.24}$$

We shall now estimate $|\Lambda_m|$ from above. By $|z_1| = 1$, lemma 1.4, lemma 3.4 (i) and lemma 1.6 (i) we have

$$\begin{aligned}|\Lambda_m| &= \omega_1^{r+(1-g)/3}\omega_2^{1/3}\left|\left(\theta\frac{\eta_2}{\xi_2} - 1\right)A_m(z_1^3) + \left(1-\theta\frac{\eta_1}{\xi_1}\right)^m V_m(z_1)\right| \\ &< \omega_1^{r+(1-g)/3}\omega_2^{1/3}\binom{2r-g}{r}\frac{\pi k}{3}\Delta^{1/2}\omega_2^{-1} + \\ &\quad + \omega_1^{r+(1-g)/3}\omega_2^{1/3}\left(\frac{\pi k}{3}\right)^m\Delta^{m/2}\omega_1^{-m}\cdot 3^m\binom{r-g+1/3}{r-g+1}\binom{r-1/3}{r}\binom{m}{r}^{-1} \\ &= \frac{1}{3}\cdot 2^{-g/3}\sigma(m)k\Delta^{1/2}\omega_1^{r+(1-g)/3}\omega_2^{-2/3} + \\ &\quad + \frac{2}{3}\cdot 2^{-g/3}\tau(m)k^m\Delta^{r+1/2-g/2}\omega_2^{1/3}\omega_1^{-r-2(1-g)/3}.\end{aligned}$$

Together with (3.24) this proves lemma 3.5. □

LEMMA 3.6. $\Sigma_m \neq 0$ *for* $m \in \{2,3,5,7\}$.

PROOF. We shall proceed similarly as in lemma 2.8. Put $h=\alpha\xi_1^3-\beta\eta_1^3, w_1=\alpha\xi_1^3$, $u=h/w_1=1-z_1^3$. Then $h,w_1 \in \mathcal{O}_M$. Note that by (3.18), (3.20) and the fact that $\Delta^{5/2}k^8 \geq 444^{5/2}$,

$$(3.25) \qquad |u| \leq \frac{3k\Delta^{1/2}}{7\Delta^3 k^9} = \frac{3}{7\Delta^{5/2}k^8} < \frac{3}{7\times 444^{5/2}} < 10^{-6}.$$

As in lemma 2.8 we put $\tilde{E}_m(z)=q^*(m)A_m(1-z), \tilde{F}_m(z)=q^*(m)B_m(1-z)$, where $q^*(m)$ is the smallest positive rational number such that both $q^*(m)A_m(1-z)$ and $q^*(m)B_m(1-z)$ have rational integral coefficients. The forms $\tilde{E}_m^*(x,y), \tilde{F}_m^*(x,y)$ are defined similarly as in lemma 2.8. Finally, let $K_m(z)$ be the polynomial defined by $\tilde{E}_m(z)^n-(1-z)\tilde{F}_m(z)^n=z^m K_m(z)$. Let d be the ideal in $\mathcal{O}_M$ generated by $(w_1-h)\tilde{F}_m^*(w_1,h)^3$ and $w_1\tilde{E}_m^*(w_1,h)^3$. If $\Sigma_m=0$ then we have, completely similar as in the proof of lemma 2.8,

$$(3.26) \qquad \langle w_1^{r+g}h^m K_m(u)\rangle \supset d\langle\alpha\xi_2^3-\beta\eta_2^3\rangle,\ w_1^{r+g}h^m K_m(u) \in \mathcal{O}_M.$$

By (3.25) we have, similar to (2.17),

$$(3.27) \qquad |K_2(u)| > 8,\ |K_3(u)| > 1,\ |K_5(u)| > 755,\ |K_7(u)| > 161.$$

The arguments used in the proof of lemma 2.8 in order to estimate d from above can be used here as well if we work in a finite extension of M in which the ideal generated by w_1 and h is principal. Thus we obtain

$$(3.28) \qquad d \supset \langle 6^3 w_1 h^3\rangle \text{ if } m=2,\ d \supset \langle h^4\rangle \text{ if } m=3,$$
$$d \supset \langle 360^3 h^7\rangle \text{ if } m=5,\ d \supset \langle 84^3 h^{10}\rangle \text{ if } m=7.$$

Note that if γ_1,γ_2 are elements of $\mathcal{O}_M$ with $\langle\gamma_1\rangle\supset\langle\gamma_2\rangle$, then $|\gamma_1|\leq|\gamma_2|$. Hence by (3.26),(3.27),(3.28) and

$$0 < |\alpha\xi_2^3-\beta\eta_2^3| \leq 3k\Delta^{1/2},\ |w_1| = \omega_1,\ |h| \leq 3k\Delta^{1/2},$$
$$\Delta \geq 147,\ \Delta \geq 444 \text{ if } k=1$$

we have

$$8\omega_1^2|h|^2 \le 6^3\omega_1|h|^3\cdot 3k\Delta^{1/2}\ ,$$
$$\omega_1 \le 3^3|h|\cdot 3k\Delta^{1/2} \le 3^5k^2\Delta \le 3^5444^{-2}k^9\Delta^3 < k^9\Delta^3 \qquad \text{if } m=2,$$

$$\omega_1|h|^3 \le |h|^4\cdot 3k\Delta^{1/2}\ ,$$
$$\omega_1 \le 9k^2\Delta \le 9\times 444^{-2}k^9\Delta^3 < k^9\Delta^3 \qquad \text{if } m=3,$$

$$\omega_1^2|h|^5 \le |h|^7 360^3\cdot 3k\Delta^{1/2}\ ,$$
$$\omega_1 \le (3k\Delta^{1/2})^{3/2}360^{3/2} \le (3\times 360)^{3/2}444^{-9/4}k^9\Delta^3 < k^9\Delta^3 \qquad \text{if } m=5,$$

$$\omega_1^3|h|^7 \le |h|^{10}84^3\cdot 3k\Delta^{1/2}\ ,$$
$$\omega_1 \le (3k\Delta^{1/2})^{4/3}84 \le 3^{4/3}\times 84\times 444^{-7/3}k^9\Delta^3 < k^9\Delta^3 \qquad \text{if } m=7,$$

provided that $\Sigma_m=0$ for one of the values of m given in the lemma. But these inequalities clearly contradict (3.20). This proves lemma 3.6. □

LEMMA 3.7. *There are rational integers* ℓ_1,ℓ_2 *with* $1\le\ell_1\le\ell_2\le\ell_1+1$ *such that*

$$\sigma(2\ell_1+1)\omega_1^{\ell_1+1/3} \le k^{-1}\omega_2^{2/3} < \sigma(2\ell_1+3)\omega_1^{\ell_1+4/3}\ ,$$
$$\sigma(2\ell_2)\omega_1^{\ell_2} \le k^{-1}\Delta^{-1/3}\omega_2^{2/3} < \sigma(2\ell_2+2)\omega_1^{\ell_2+1}\ . \tag{3.29}$$

PROOF. For the sake of completeness, we put $\sigma(0)=\sigma(1)=0$. Then the sequences $\sigma(2\ell+1)\omega_1^{\ell+1/3}$ and $\sigma(2\ell)\omega_1^{\ell}$ increase monotonically to infinity and their terms with $\ell=0$ are equal to 0. Hence there exist non-negative integers ℓ_1,ℓ_2 satisfying (3.29). Firstly, we shall show that $\ell_1\ge 1$. We assume the contrary, i.e.

$$\omega_2 < (\sigma(3)k)^{3/2}\omega_1^2 = (2\pi k)^{3/2}\omega_1^2. \tag{3.30}$$

Note that by (3.21),(3.20) and $\Delta\ge 147$,

$$\Xi_2 = \sigma(2)k\Delta^{1/3}\omega_1\omega_2^{-2/3} \le \sigma(2)k^3\Delta^{1/3}0.948^{-2}\omega_1^{-1/3}$$
$$\le \sigma(2)0.948^{-2}\times 147^{-2/3}k^3\Delta\omega_1^{-1/3} < k^3\Delta\omega_1^{-1/3} < 1.$$

Furthermore, by (3.30),(3.20) and $k^{1/2}\Delta^{1/6}\ge 444^{1/6}$,

$$\P_2 = \tau(2)k^2\Delta^{5/6}\omega_2^{1/3}\omega_1^{-1} \le \tau(2)(2\pi)^{1/2}k^{5/2}\Delta^{5/6}\omega_1^{-1/3}$$

$$\leq \tau(2)(2\pi)^{1/2}444^{-1/6}k^{3}\Delta\omega_1^{-1/3} < (6.7k^{9}\Delta^{3}\omega_1^{-1})^{1/3} < 1.$$

But these facts are contradictory to lemma 3.5 and lemma 3.6 in case m=2.

We shall now show that $\ell_1 \leq \ell_2 \leq \ell_1+1$. Suppose that $\ell_1 \geq \ell_2+1$. Then

$$\binom{2\ell_2+2}{\ell_2+1}\pi\omega_1^{\ell_2+4/3} \leq k^{-1}\omega_2^{2/3} \leq 2^{-2/3}\Delta^{1/3}\binom{2\ell_2+2}{\ell_2+1}\pi\omega_1^{\ell_2+1},$$

hence

$$\omega_1 < \Delta/4,$$

which is clearly impossible. If $\ell_2 \geq \ell_1+2$ then

$$\binom{2\ell_1+1}{\ell_1+1}\pi\omega_1^{\ell_1+2} \leq 2^{-2/3}\pi\binom{2\ell_1+4}{\ell_1+2}\omega_1^{\ell_1+2} \leq k^{-1}\Delta^{-1/3}\omega_2^{2/3}$$
$$< \Delta^{-1/3}\pi\binom{2\ell_1+2}{\ell_1+1}\omega_1^{\ell_1+4/3},$$

hence

$$\omega_1 < \Delta^{-1/2} < 1,$$

which is also impossible. This completes the proof of lemma 3.7. □

Now we shall prove theorem 3.3. Let ℓ_1, ℓ_2 be the integers defined in lemma 3.7. We choose $r=\ell_1, g=0, m=2\ell_1+1$ if $\Sigma_{2\ell_1+1} \neq 0$, but $r=\ell_2, g=1, m=2\ell_2$ otherwise. Then we have by lemma 3.7 that $|m-(2\ell_1+1)| \leq 1$. Hence, by lemma 1.5, $\Sigma_m \neq 0$. Note that by lemma 3.6, m is even implies that $r \geq 4$ and $m \geq 8$. Furthermore we have, by our definitions of ℓ_1, ℓ_2, r, g, m,

$$\sigma(m)\omega_1^{r+(1-g)/3} \leq k^{-1}\Delta^{-g/3}\omega_2^{2/3} < \sigma(m+2)\omega_1^{r+1+(1-g)/3}. \tag{3.31}$$

The left-hand side inequality of (3.31) clearly implies that $\Xi_m \leq 1$. We shall now show that $\P_m \leq 1$. Then we have a contradiction with lemma 3.5. This shows that (3.15) can not have four solutions which are related to θ, i.e. that theorem 3.3 is valid. Note that, by $k^2\Delta \geq 444$, $r-3g>0$, and by the right-hand side inequality of (3.31),

$$\P_m = \tau(m)k^{m}\Delta^{r-g/6}\omega_2^{1/3}\omega_1^{-r-2(1-g)/3}$$

$$< \left(\sigma(m+2)\tau(m)^2 k^{4r+3-2g} \Delta^{2r} \omega_1^{g-r}\right)^{1/2}$$
$$\leq \left(\sigma(m+2)\tau(m)^2 (k^2\Delta)^{3g-r} (k^9\Delta^3)^{r-g} \omega_1^{g-r}\right)^{1/2} \leq \left(\Omega_m k^9 \Delta^3 \omega_1^{-1}\right)^{(r-g)/2},$$

where

$$\Omega_m = \left(\sigma(m+2)\tau(m)^2 444^{3g-r}\right)^{1/(r-g)}$$
$$= \left(\binom{2r+2}{r+1}\left(\frac{3}{2}\binom{r-g+1/3}{r-g+1}\binom{r-1/3}{r}\binom{2r+1-g}{r}^{-1}\right)^2 \pi^{4r+3-2g} 444^{3g-r}\right)^{\frac{1}{r-g}}.$$

By (3.20) it suffices to show that $\Omega_m \leq 7$. But this is easy, since for every integer n with $n=2s+1-h$, where s and h are integers with $h \in \{0,1\}$ and $s>0$,

$$\Omega_{n+2}^{s+1-h} \Big/ \Omega_n^{s-h}$$
$$= \frac{(2s+4)(2s+3)}{(s+2)(s+2)}\left(\frac{(s+1-h+1/3)(s+1-1/3)}{(s+2-h)(s+1)} \Big/ \frac{(2s+3-h)(2s+2-h)}{(s+2-h)(s+1)}\right)^2 \pi^4 444^{-1}$$
$$< 4\pi^4 444^{-1}\left(\frac{(s-h+4/3)(s-2/3)}{(2s-h+3)(2s-h+2)}\right)^2 < 4\pi^4 444^{-1} < 1,$$

whereas

$$\Omega_3 = \binom{4}{2}\left(\frac{3}{2}\binom{4/3}{2}\binom{2/3}{1}\binom{3}{1}^{-1}\right)^2 \pi^7 444^{-1} < 0.3,$$
$$\Omega_8 = \left(\binom{10}{5}\left(\frac{3}{2}\binom{10/3}{4}\binom{11/3}{4}\binom{8}{4}^{-1}\right)^2 \pi^{17} 444^{-1}\right)^{1/3} < 6.8.$$

This completes the proof of theorem 3.3. □

CHAPTER 4. SOME FACTS FROM ALGEBRAIC NUMBER THEORY.

From this chapter on, it is supposed that the reader is familiar with the basic concepts of algebraic number theory, as can be found in the first six chapters of Lang's book [La 1]. In this chapter we shall develop some techniques which will be needed later. Apart from the notations listed at the beginning of this monograph, we shall use the notations introduced in this chapter throughout the remainder of this thesis.

§4.1. Ideals and primes.

Let K be an algebraic number field. By ideals in K we shall mean fractional ideals, i.e. finitely generated $\mathcal{O}_K$-modules, whereas integral ideals will mean ideals in the ring $\mathcal{O}_K$ in the usual sense. We put

I(K): the multiplicative group of ideals in K;
S(K): the set of prime ideals in K.

As is well-known, I(K) is generated by S(K). That is, for every $\mathfrak{a}\in I(K)$ we have

$$\mathfrak{a} = \prod_{\mathfrak{p}\in S(K)} \mathfrak{p}^{w_{\mathfrak{p}}(\mathfrak{a})}, \tag{4.1}$$

where the numbers $w_{\mathfrak{p}}(\mathfrak{a})$ are integers, uniquely determined by $\mathfrak{a}$, of which at most finitely many are non-zero. If $\mathfrak{a}=<\alpha>$ we shortly write $w_{\mathfrak{p}}(\alpha)$ instead of $w_{\mathfrak{p}}(<\alpha>)$.

Let L be a finite extension of K. Let $\mathfrak{p},\mathfrak{P}$ be prime ideals in K,L respectively, such that $\mathfrak{P}$ divides $\mathfrak{p}\mathcal{O}_L$. We say that $\mathfrak{P}$ *lies above* $\mathfrak{p}$ and we denote this by $\mathfrak{P}|\mathfrak{p}$. Furthermore we put

$e(\mathfrak{P}/\mathfrak{p}) = w_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_L)$, the *ramification index* of $\mathfrak{P}$,
$f(\mathfrak{P}/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P}:\mathcal{O}_K/\mathfrak{p}]$, the *residue class degree* of $\mathfrak{P}$.

Then

$$\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) = [L:K], \tag{4.2}$$

where $\mathfrak{P}$ runs through all prime ideals in L lying above $\mathfrak{p}$. If L is a Galois-extension of K, then all prime ideals $\mathfrak{P}$ lying above $\mathfrak{p}$ are conjugate over K, i.e. they can be transformed into each other by means of a K-automorphism of L. Then the numbers $e(\mathfrak{P}/\mathfrak{p}), f(\mathfrak{P}/\mathfrak{p})$ do not depend on $\mathfrak{P}$.

Let $E(K)$ be the set of $\mathbb{Q}$-isomorphisms of K into $\mathbb{C}$. Such an isomorphism is called *real* if it maps K into $\mathbb{R}$ and *complex* otherwise. If $\sigma \in E(K)$ is complex, its conjugate $\overline{\sigma}$ is defined by $\overline{\sigma}(\alpha)=\overline{\sigma(\alpha)}$ for $\alpha \in K$. We divide $E(K)$ into subsets consisting of either one real or a pair of conjugate complex isomorphisms. Such subsets are called *infinite primes*, whereas prime ideals are called *finite primes*. Thus we have

$S(K)$: the set of finite primes,

and we put

$S_\infty(K)$: the set of infinite primes,
$\overline{S}(K) = S(K) \cup S_\infty(K)$: the set of all primes on K.

We shall denote primes, either finite or infinite on $\mathbb{Q}$ by the letter p, on a fixed algebraic number field by v and, if confusion may arise, on an extension of this field by V. An infinite prime is called *real* if it consists of a real isomorphism and *complex* otherwise. If r_1 denotes the number of real, and r_2 the number of complex primes on an algebraic number field K we clearly have

$$r_1+2r_2 = [K:\mathbb{Q}]. \tag{4.3}$$

We say that a prime V on an extension L of K lies above the prime v on K if it lies above v in the sense of prime ideals in the finite case or if it contains continuations of $\mathbb{Q}$-isomorphisms of K belonging to v in the infinite case. We denote this by $V|v$. Note that by (4.2) and by the fact that each $\mathbb{Q}$-isomorphism of K can be extended to exactly [L:K] $\mathbb{Q}$-isomorphisms of L, at most [L:K] primes on L ly above a fixed prime on K. If L/K is Galois all primes on L lying above a fixed prime on K are conjugate over K. In the infinite case this means the following: two infinite primes V_1, V_2 on L are called conjugate if a K-automorphism τ of L exists such that all elements of V_2 are given by $\tau\sigma$, where σ runs through

the elements of V_1. Finally we note that for Galois-extensions L/K either all primes on L lying above a fixed infinite prime on K are real or they are all complex.

§4.2. Norms, polynomials, discriminants.

Let K be an algebraic number field as usual and let $f(x_1,\ldots,x_r)$ be a polynomial in r variables with coefficients in K. The *content of* f *with respect to* K, denoted by $c_K(f)$, is defined to be the ideal in K generated by the coefficients of f. If $c_K(f)=\mathcal{O}_K$ then we call f *primitive*. If L is a finite extension of K then

$$c_L(f) = c_K(f)\mathcal{O}_L. \tag{4.4}$$

Moreover, if $f,g\in K[x_1,\ldots,x_r]$ then

$$c_K(fg) = c_K(f)c_K(g). \tag{4.5}$$

In case that both f and g are primitive, this can be proved similarly to Gauss' lemma. In the general case one can extend K to a field L in which both $c_L(f)$ and $c_L(g)$ are principal ideals with generators δ_1,δ_2 say. Then both f/δ_1 and g/δ_2 are primitive, hence their product $fg/\delta_1\delta_2$ is. This shows the general case.

As is well-known, the norm of an element $\alpha\in K$ is defined as

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma\in E(K)} \sigma(\alpha) .$$

There is a suitable generalisation for ideals. The norm of an integral ideal a is defined as

$$N_K(a) = |\mathcal{O}_K/a|.$$

If a is not integral, then a is the quotient of two integral ideals, b/c say. We put

$$N_K(a) = N_K(b)/N_K(c).$$

This is well-defined and we have

(4.6) $N_K(ab) = N_K(a)N_K(b)$ for $a,b\in I(K)$,

(4.7) $N_K(<\alpha>) = |N_{K/\mathbb{Q}}(\alpha)|$ for $\alpha\in K^*$,

(4.8) $N_L(a\mathcal{O}_L) = N_K(a)^{[L:K]}$ for $a\in I(K)$, L/K finite,

(4.9) $N_K(a)\mathcal{O}_M = \prod_{\sigma\in E(K)} \sigma(a)\mathcal{O}_M$ for $a\in I(K)$, M/$\mathbb{Q}$ Galois, $M\supset\sigma(K)$ for $\sigma\in E(K)$.

We shall apply this together with (4.5) to the following situation. Let $\alpha\in\mathbb{A}^*$ and put $k=\mathbb{Q}(\alpha)$,

$$T(\alpha) = N_k(<1,\alpha>)^{-1}\ ,\ F_\alpha(z) = T(\alpha)\prod_{\sigma\in E(k)}(z-\sigma(\alpha)).$$

F_α is called the *minimal polynomial* of α. Clearly F_α is an irreducible polynomial with coefficients in $\mathbb{Q}$. By the preceding theory, one can show that F_α is primitive, whence has integral coefficients. For in general we have by (4.5) for every polynomial $f(z)=\beta(z-\alpha_1)\ldots(z-\alpha_r)$ with $\beta,\alpha_1,\ldots,\alpha_r$ in some algebraic number field K,

(4.10) $$c_K(f) = <\beta><1,\alpha_1>\ldots<1,\alpha_r>.$$

Hence, if M is an extension of k containing all conjugates of α, we have by (4.9),

$$c_M(F_\alpha) = N_k(<1,\alpha>_k)^{-1}\mathcal{O}_M\prod_{\sigma\in E(k)}<1,\sigma(\alpha)>_M = \mathcal{O}_M.$$

We shall use (4.10) also in order to derive a useful identity involving discriminants of polynomials. Let r be an integer with $r\geq 2$ and let $\beta,\alpha_1,\ldots,\alpha_r$ be algebraic numbers. The discriminant of $f(z)=\beta(z-\alpha_1)\ldots(z-\alpha_r)$ is given by

$$D(f) = \beta^{2r-2}\prod_{i>j}(\alpha_i-\alpha_j)^2.$$

Since D(f) is symmetrical in $\alpha_1,\ldots,\alpha_r$ it can be expressed entirely in terms of the coefficients of f. Now suppose that $f(z)\in K[z]$ for some algebraic number field K and that $\alpha_1,\ldots,\alpha_r$ are pairwise distinct. The *primitive discriminant* of f with respect to K is defined as the ideal

(4.11) $$d_K(f) = c_K(f)^{-2r+2}<D(f)>_K.$$

Let M be an algebraic number field containing $\alpha_1,\ldots,\alpha_r$. By (4.10) we have the following identity of ideals in M:

$$(4.12)\qquad d_M(f) = \left(<\beta>\prod_{i=1}^{r}<1,\alpha_i>\right)^{-2r+2}<\beta>^{2r-2}\prod_{i>j}<\alpha_i-\alpha_j>^2$$
$$= \prod_{i>j}\left(<1,\alpha_i>^{-1}<1,\alpha_j>^{-1}<\alpha_i-\alpha_j>\right)^2.$$

This implies that $d_M(f)$ is an integral ideal not depending on β. It follows easily that $d_K(f)$ is an integral ideal not depending on β for every algebraic number field K containing the coefficients of f.

§4.3. Valuations.

On $\mathbb{Q}$ we have the following primes: the prime numbers which are usually identified with the finite primes and the infinite prime consisting of the identity on $\mathbb{Q}$ which is usually denoted by p_∞. For every prime we define a valuation:

$|\alpha|_{p_\infty} = |\alpha|$ for $\alpha\in\mathbb{Q}$, the ordinary absolute value;
$|\alpha|_p = p^{-w_p(\alpha)}$ for $\alpha\in\mathbb{Q}^*$, $|0|_p = 0$, the ordinary p-adic valuation, if p is a prime number.

By the unique factorisation on $\mathbb{Q}$ we have the *product formula*:

$$(4.13)\qquad \prod_{p\in\overline{S}(\mathbb{Q})}|\alpha|_p = 1 \quad \text{for } \alpha\in\mathbb{Q}^*.$$

It is possible to generalise this for algebraic number fields. Firstly, we define valuations for ideals. Let K be an algebraic number field of degree m. We define for $p\in S(K)$ and $a\in I(K)$:

$$|a|_p = N_K(p)^{-w_p(a)/m}.$$

By this definition, we have

$$(4.14)\qquad |<\alpha_1,\ldots,\alpha_r>_K|_p = \max(|\alpha_1|_p,\ldots,|\alpha_r|_p) \text{ for } \alpha_1,\ldots,\alpha_r\in K.$$

By (4.1) and (4.6) we have the *product formula for ideals*:

$$(4.15) \qquad N_K(a)^{1/m} \prod_{p\in S(K)} |a|_p = 1 .$$

We now define valuations on K. For $\alpha\in K$ we put

$$\text{for } v=p\in S(K): \ |\alpha|_v = N_K(p)^{-w_p(\alpha)/m} \text{ if } \alpha\neq 0, \ |0|_v = 0;$$

$$\text{for } v\in S_\infty(K): \ |\alpha|_v = |\sigma(\alpha)|^{d(v)/m} \text{ for some } \sigma\in v, \text{ where } d(v)=1$$
$$\text{if v is real and } d(v)=2 \text{ otherwise.}$$

Since by (4.7),

$$(4.16) \qquad N_K(<\alpha>) = |N_{K/\mathbb{Q}}(\alpha)| = \prod_{v\in S_\infty(K)} |\alpha|_v^m,$$

we have by (4.15) the *product formula*:

$$(4.17) \qquad \prod_{v\in \overline{S}(K)} |\alpha|_v = 1 \text{ for } \alpha\in K^* .$$

We shall often use the following corollaries of the product formula. If S is a finite collection of primes containing all infinite ones and if α is a so-called *S-unit*, i.e. $|\alpha|_v=1$ for $v\notin S$ then clearly

$$(4.18) \qquad \prod_{v\in S} |\alpha|_v = 1.$$

If $\alpha\in O_K^*$ and S is a collection of primes which contains all infinite primes but is not necessarily finite then

$$(4.19) \qquad \prod_{v\in S} |\alpha|_v \geq 1.$$

The following important properties of these valuations may be noted. If $\alpha\in K^*$, then $|\alpha|_v\neq 1$ for at most finitely many v. If L/K is a Galois extension, if $v\in\overline{S}(K)$, and if V_1,V_2 are primes on L lying above v, then either V_1,V_2 are conjugate prime ideals, or conjugate real primes, or conjugate complex primes. Hence we have for some K-automorphism τ of L:

$$(4.20) \qquad |\alpha|_{V_2} = |\tau(\alpha)|_{V_1} \quad \text{for } \alpha\in L.$$

In order to simplify estimates in which both finite and infinite primes appear, we introduce the following notations:

(4.21) $s(v) = 0$ if $v \in S(K)$; $s(v) = d(v)/m$ if $v \in S_\infty(K)$.

Then we have

(4.22) $$\sum_{v \in S(K)} s(v) = \sum_{v \in S_\infty(K)} s(v) = 1,$$

(4.23) $$|\alpha_1 + \ldots + \alpha_r|_v \leq r^{s(v)} \max(|\alpha_1|_v, \ldots, |\alpha_r|_v) \quad \text{for } \alpha_1, \ldots, \alpha_r \in K \text{ and } v \in \overline{S}(K).$$

§4.4. Heights.

Let K be an algebraic number field. The *height* of $\alpha \in K^*$ is defined as

(4.24) $$h(\alpha) = \prod_{v \in \overline{S}(K)} \max(1, |\alpha|_v).$$

In fact, the height does not depend on K, hence it can be considered as a height function on $\mathbf{A}^*$. For put $k = \mathbb{Q}(\alpha)$,

$$d = \deg \alpha = [k:\mathbb{Q}], \quad L(\alpha) = \prod_{\sigma \in E(k)} \max(1, |\sigma(\alpha)|).$$

Each $\mathbb{Q}$-isomorphism σ of k can be extended to exactly $[K:k]$ $\mathbb{Q}$-isomorphisms of K. Hence

$$\prod_{v \in S_\infty(K)} \max(1, |\alpha|_v) = \Big(\prod_{\tau \in E(K)} \max(1, |\tau(\alpha)|) \Big)^{1/[K:\mathbb{Q}]} = L(\alpha)^{1/d},$$

whereas by (4.14), (4.15) and (4.8),

$$\prod_{v \in S(K)} \max(1, |\alpha|_v) = \prod_{v \in S(K)} |\langle 1, \alpha \rangle|_v = N_K(\langle 1, \alpha \rangle)^{-1/[K:\mathbb{Q}]}$$
$$= N_k(\langle 1, \alpha \rangle_k)^{-1/d} = T(\alpha)^{1/d}.$$

Therefore,

(4.25) $$h(\alpha) = \Big(L(\alpha) T(\alpha) \Big)^{1/d}.$$

Note that by (4.25), algebraic numbers which are conjugate over $\mathbb{Q}$ have the same height. Furthermore, if $r, s \in \mathbb{Z}^*$ with $(r,s) = 1$ then $T(r/s) = |s|$, $L(r/s) = \max(1, |r/s|)$, hence

$$h(r/s) = \max(|r|,|s|). \tag{4.26}$$

Finally, we mention another useful expression for the height. Let $\xi,\eta\in K^*$. Then it follows easily from the product formula (4.17) that

$$h(\xi/\eta) = \prod_{v\in\overline{S}(K)} \max(|\xi|_v,|\eta|_v). \tag{4.27}$$

LEMMA 4.1. *Let* $\alpha,\beta,\alpha_1,\ldots,\alpha_r\in\mathbf{A}^*$, $n\in\mathbb{Z}$. *Then*

$$h(\alpha^n) = h(\alpha)^{|n|}, \tag{4.28}$$

$$h(\alpha_1\alpha_2\ldots\alpha_r) \le h(\alpha_1)h(\alpha_2)\ldots h(\alpha_r), \tag{4.29}$$

$$h(\alpha\beta)\ge h(\alpha)/h(\beta),\ h(\alpha/\beta)\ge h(\alpha)/h(\beta), \tag{4.30}$$

$$h(\alpha_1+\ldots+\alpha_r) \le rh(\alpha_1)\ldots h(\alpha_r) \quad \textit{if } \alpha_1+\ldots+\alpha_r\neq 0. \tag{4.31}$$

PROOF. Let K be an algebraic number field containing $\alpha,\beta,\alpha_1,\ldots,\alpha_r$. Let $v\in\overline{S}(K)$. Note that by (4.27), $h(\alpha^{-1})=h(\alpha)$. Hence in the proof of (4.28) we may assume that $n\ge 0$. By (4.23) and (4.22) we have

$$\max(1,|\alpha^n|_v) = \max(1,|\alpha|_v)^n,$$

$$\max(1,|\alpha_1\alpha_2\ldots\alpha_r|_v) \le \max(1,|\alpha_1|_v)\max(1,|\alpha_2|_v)\ldots\max(1,|\alpha_r|_v),$$

$$\max(1,|\alpha_1+\ldots\alpha_r|_v) \le \max\{1,r^{s(v)}\max(|\alpha_1|_v,\ldots,|\alpha_r|_v)\}$$

$$\le r^{s(v)}\max(1,|\alpha_1|_v,\ldots,|\alpha_r|_v)$$

$$\le r^{s(v)}\max(1,|\alpha_1|_v)\ldots\max(1,|\alpha_r|_v).$$

Now (4.28), (4.29) and (4.31) follow by taking the product over all v. (4.30) follows from (4.29) by noting that $h(\beta)=h(\beta^{-1})$ and

$$h(\alpha) = h(\alpha\beta\beta^{-1}) \le h(\alpha\beta)h(\beta). \qquad \square$$

LEMMA 4.2. *Let* C *be a positive number and let* d *be a positive integer. Then the number of algebraic numbers of degree at most* d *and height at most* C *is bounded above by*

$$\frac{d}{2}\left((2C)^{d}+1\right)^{d+1}.$$

PROOF. Let α be an algebraic number of degree $d'\le d$ and height $\le C$. Let $\alpha_1,\ldots,\alpha_{d'}$ be the conjugates of α and suppose that these numbers belong to $\mathbb{C}$.

Put $f(z)=(z-\alpha_1)\dots(z-\alpha_{d'})$. Then $f(z)=z^{d'}+a_1z^{d'-1}+\dots+a_{d'}$, say, where

$$a_r = \pm \sum_{1\le i_1<\dots<i_r\le d'} \alpha_{i_1}\dots\alpha_{i_r} \qquad \text{for } r=1,2,\dots,d'.$$

Since there are at most $\binom{d'}{r}$ tuples $(i_1,\dots,i_r)$, we have that

$$|a_r| \le \binom{d'}{r} \max_{1\le i_1<\dots<i_r\le d'} |\alpha_{i_1}\dots\alpha_{i_r}| \le 2^{d-1}L(\alpha). \tag{4.32}$$

Let $G_\alpha(z)=\delta F_\alpha(z)$, where $F_\alpha(z)$ is the minimal polynomial of α and where $\delta\in\{-1,1\}$ is chosen such that $G_\alpha(0)>0$. Suppose that $G_\alpha(z)=b_0+b_1z+\dots+b_dz^d$, where $b_{d'+1}=\dots=b_d=0$ if $d>d'$. By (4.32) and (4.25) we have

$$\begin{aligned} |b_i| &\le T(\alpha)\max(1,|a_1|,\dots,|a_{d'}|) \\ &\le 2^{d-1}L(\alpha)T(\alpha) \le 2^{d-1}h(\alpha)^d \le \tfrac{1}{2}(2C)^d \qquad \text{for } i=0,1,\dots,d. \end{aligned}$$

Moreover, $b_i\in\mathbb{Z}$ for $i=0,\dots,d$ and $b_0>0$. Hence we have at most

$$\tfrac{1}{2}(2C)^d\left((2C)^d+1\right)^d \le \tfrac{1}{2}\left((2C)^d+1\right)^{d+1}$$

possibilities for the polynomial $G_\alpha(z)$. Since every polynomial $G_\alpha(z)$ has at most d zeros, this proves lemma 4.2. □

CHAPTER 5. AN APPROXIMATION THEOREM.

§5.1. Introduction.

In chapter 2 we considered the equation $ax^n-by^n=c$ in integers x,y. We showed that solutions of this equation satisfy the inequality

$$|1-\left(\frac{b}{a}\right)^{1/n}\frac{y}{x}| \leq c_1 \max(|ax^n|,|by^n|)^{-1}, \tag{5.1}$$

where c_1 is some positive constant depending on n and c. In chapter 3 we met a similar inequality. The equation $F(x,y)=1$ in integers x,y, where F is a binary cubic form of positive discriminant D was transformed into an equation $\alpha\xi^3-\beta\eta^3=3\sqrt{-3D}$, where α,β are constants and ξ,η variables in the field $\mathbb{Q}(\sqrt{-3D})$. We showed that ξ,η satisfy

$$|1-\theta\frac{\eta}{\xi}| \leq c_2|\alpha\xi^3|^{-1}, \tag{5.2}$$

where $\theta^3=\beta/\alpha$ and where c_2 is some absolute constant. In this chapter we shall consider systems of diophantine inequalities which may be considered as generalisations of (5.1),(5.2). The result we obtain here will be used to derive upper bounds for the number of solutions of equations of the Thue-Mahler type.

Apart from the notations in chapter 4 we shall use the notations below.

K is an algebraic number field;
ω is a non-zero element of K;
n is an integer with $n\geq 3$;
L is a finite extension of K containing all n-th roots of ω;
S is a finite set of primes on K;
$\{\theta_v\}_{v\in S}$ is a set of fixed n-th roots of ω which belong to L;
B,C are constants with $B>1/2+1/n$ and $C\geq 1$;
$\{\Gamma_v\}_{v\in S}$ is a set of positive constants with $\sum_{v\in S}\Gamma_v=B$;
$W(z)$ is a function on K^* such that $W(z)\geq h(\omega z^n)$ for all $z\in K^*$.

(The reader is warned that S and S(K) are distinct sets). For every $v\in S$,

we choose a continuation of $|.|_v$ to L and this continuation is fixed in the sequel. This continuation is also denoted by $|.|_v$.

We consider the following system of inequalities:

$$(5.3) \qquad |1-\theta_v z|_v \le (CW(z)^{-1})^{\Gamma_v} \qquad (v\in S) \qquad \text{in } z\in K^*.$$

We shall derive an upper bound for the number of solutions of (5.3) with W(z) sufficiently large, by applying a generalisation of the method used in chapter 2 and chapter 3. Since this method is a modification of Thue's method [Th 1,2], we have to assume that $B>n^{-1}(1+n/2)$. It is very likely, that by an adaptation of Roth's method ([Ro], see also [D/R],[Ri]) results can be obtained on (5.3) for all $B>2/n$.

THEOREM 5.1. *Suppose* ℓ_0 *is the smallest integer such that*

$$(5.4) \qquad \ell_0 \ge \max\left(2, -\frac{1}{4}\left(n-6+\frac{n^2-8n-4}{2nB-n-2}\right)\right)$$

and k *is the largest integer such that*

$$(5.5) \qquad k < \frac{\log\left(1+2n\ell_0(nB-2)/(n-2)\right)}{\log(nB-1)} .$$

Then (5.3) *has at most* k *solutions with*

$$(5.6) \qquad W(z) \ge \left(2^{(n+1)(n+4)}(nC^B)^{2n}\right)^{(2nB-n-2)^{-1}} .$$

REMARK 1. For specific choices of n,B,C,W(z) it might be possible to obtain a better result than the one given in theorem 5.1, but that would not essentially improve upon the results which we shall derive from theorem 5.1.

REMARK 2. For $n\ge 9$, we have $\ell_0=2$,k=1. To prove this, it suffices to show that

$$(5.7) \qquad \frac{4n}{n-2}(nB-2)+1 \le (nB-1)^2 \qquad \text{for } n\ge 9,\ B > 1/2 + 1/n.$$

Note that the left-hand side of (5.7) is a function in B with derivative $4n^2/(n-2)$, whereas the right-hand side has derivative $2n(nB-1)$. It is easy to check that for $n\ge 9$ and $B>1/2+1/n$,

$$\frac{4n^2}{n-2} \le 2n(nB-1)$$

and that for $n\ge 9$ and $B=1/2+1/n$,

$$\frac{4n}{n-2}(nB-2)+1 = 2n+1 \le \frac{n^2}{4} = (nB-1)^2.$$

This proves (5.7).

§5.2. Proof of theorem 5.1.

We shall use the same notations as in §5.1. Furthermore, we put

$$\nu = n^{-1},\quad U_n = 2^{n+2}n\prod_{p\mid n} p^{1/(p-1)},\quad D=2C^B.$$

The following lemma will be used in chapter 6 as well.

LEMMA 5.1. *Suppose* z', z'' *are two distinct solutions of* (5.3) *such that* $W(z')\le W(z'')$. *Then*

$$W(z'') \ge D^{-n}W(z')^{nB-1}. \tag{5.8}$$

PROOF. Put $W'=W(z'), W''=W(z'')$ and for every $v\in\overline{S}(K)$

$$E_v = \frac{|\omega|_v^{\nu}|z'-z''|_v}{\left(\max(1,|\omega z'^n|_v)\max(1,|\omega z''^n|_v)\right)^{\nu}}$$

$$= \frac{|\theta_v z'-\theta_v z''|_v}{\max(1,|\theta z'|_v)\max(1,|\theta z''|_v)} \qquad \text{for } v\in S.$$

By (4.23), (5.3) and the fact that $W''\ge W'$ we have for $v\in S$,

$$E_v \le 2^{s(v)}\max\left(|1-\theta_v z'|_v,\ |1-\theta_v z''|_v\right)$$

$$\le 2^{s(v)}\max(CW'^{-1}, CW''^{-1})^{\Gamma_v} = 2^{s(v)}(CW'^{-1})^{\Gamma_v}.$$

For $v\notin S$ we have the trivial estimate $E_v\le 2^{s(v)}$. Hence by the fact that $z'\ne z''$ and by (4.17), (4.22),

$$(W'W'')^{-\nu} \le \left(h(\omega z'^n)h(\omega z''^n)\right)^{-\nu} = \prod_{v\in\overline{S}(K)} E_v \le 2(CW'^{-1})^B \le DW'^{-B},$$

which proves lemma 5.1. □

We now assume that (5.3) has k+1 solutions satisfying (5.6), $z_1, z_2, \ldots, z_{k+1}$ say, ordered such that $W(z_{j_1}) \le W(z_{j_2}) \ldots \le W(z_{j_{k+1}})$, where $(j_1, \ldots, j_{k+1})$ is some permutation of $(1,2,\ldots,k+1)$ with $j_1=1, j_{k+1}=2$. Put

$$W_i = W(z_i) \text{ for } i=1,2.$$

We have

$$\prod_{p|n} p^{1/(p-1)} \le n^{(n-1)/(n+1)}. \tag{5.9}$$

This is clear for $n \le 6$. For $n \ge 7$ we have

$$\prod_{p|n} p^{1/(p-1)} \le (n,2) \prod_{\substack{p|n \\ p\neq 2}} p^{1/(p-1)} \le (2n)^{1/2} \le n^{3/4} \le n^{(n-1)/(n+1)}.$$

By (5.9) we have

$$2^{(n+4)(n+1)} n^{2n} \ge 4 \times 2^{2n} U_n^{n+1}.$$

Hence, by (5.6),

$$W_1 \ge \left(4U_n^{n+1} D^{2n}\right)^{(2nB-n-2)^{-1}}. \tag{5.10}$$

By lemma 5.1 we have for $i \in \{1,\ldots,k\}$,

$$D^{-n/(nB-2)} W_{j_{i+1}} \ge \left(D^{-n/(nB-2)} W_{j_i}\right)^{nB-1},$$

hence

$$D^{-n/(nB-2)} W_2 \ge \left(D^{-n/(nB-2)} W_1\right)^{(nB-1)^k}. \tag{5.11}$$

LEMMA 5.2. *Let* r *be a positive integer and let* $A_{2r+1}(z), B_{2r+1}(z)$ *be the polynomials constructed in chapter 1. Put*

$$\Phi_r = U_n^r C^B W_2^{\nu-B} W_1^{\nu+r}, \quad \Psi_r = U_n^r C^{B(2r+1)} W_2^{\nu} W_1^{\nu+r-B(2r+1)}.$$

If $z_2A_{2r+1}(\omega z_1^n) \neq z_1 B_{2r+1}(\omega z_1^n)$, *then*

$$1 \leq \max(\Phi_r, \Psi_r) . \tag{5.12}$$

PROOF. Put

$$G_r(z) = q(2r+1)A_{2r+1}(z),\ H_r(z) = q(2r+1)B_{2r+1}(z),$$
$$T_r(z) = q(2r+1)V_{2r+1}(z),$$

where $q(2r+1)=n^r(n^r,r!)$ and where $V_{2r+1}(z)$ is the polynomial constructed in lemma 1.4. By lemma 1.3 (i), $G_r(z)$ and $H_r(z)$ have rational integral coefficients and as a consequence of Gauss' lemma, $T_r(z)$ also has. Note that by (2.24),

$$q(2r+1)\binom{2r}{r}2^{nr} \leq \left(n \prod_{p|n} p^{1/(p-1)}\right)^r 2^{(n+2)r-1} = \frac{1}{2}U_n^r . \tag{5.13}$$

Furthermore, by (5.6), $W_2 \geq W_1 \geq C$ and hence, by (5.3),

$$|1-\theta_v z_1|_v \leq 1,\ |1-\theta_v z_2|_v \leq 1 \quad \text{for } v \in S.$$

These inequalities imply that

$$\max\left(|G_r(\omega z_1^n)|_v, |T_r(\theta_v z_1)|_v\right) \leq \left(\frac{1}{2}U_n^r\right)^{s(v)} \quad \text{for } v \in S. \tag{5.14}$$

If v is finite, this follows immediately from the fact that $s(v)=0$, that $|\theta_v z_1|_v \leq 1, |\theta_v z_2|_v \leq 1$ and that G_r and T_r have v-adically integral coefficients. If v is infinite, then (5.14) follows from (5.13), lemma 1.6 (ii), the fact that G_r, T_r have rational coefficients and that $|\alpha|_v = |\sigma(\alpha)|^{s(v)}$ for all $\alpha \in K$ and for some $\mathbb{Q}$-isomorphism σ of K in $\mathbb{C}$. Similarly, we have by lemma 1.6 (i),

$$\max\left(|G_r(\omega z_1^n)|_v, |H_r(\omega z_1^n)|_v\right) \leq \left(\frac{1}{2}U_n^r\right)^{s(v)} \cdot \max(1, |\omega z_1^n|_v)^r \quad \text{for } v \notin S. \tag{5.15}$$

Put

$$F_v = |\omega|_v^{\nu} |z_2 G_r(\omega z_1^n) - z_1 H_r(\omega z_1^n)|_v \quad \text{for } v \in \overline{S}(K).$$

Then

$$F_v = |\theta_v z_2 G_r((\theta_v z_1)^n) - \theta_v z_1 H_r((\theta_v z_1)^n)|_v \quad \text{for } v \in S.$$

Firstly, we assume that $v \in S$. Then by lemma 1.4, (4.23) and (5.14),

$$\begin{aligned} F_v &= |(\theta_v z_2 - 1) G_r(\omega z_1^n) + (1-\theta_v z_1)^{2r+1} T_r(\theta_v z_1)|_v \\ &\le 2^{s(v)} \max\{|1-\theta_v z_2|_v |G_r(\omega z_1^n)|_v, |1-\theta_v z_1|_v^{2r+1} |T_r(\theta_v z_1)|_v\} \\ &\le (U_n^r)^{s(v)} \max\{|1-\theta_v z_2|_v, |1-\theta_v z_1|_v^{2r+1}\}. \end{aligned}$$

Hence by (5.3),

$$F_v \le (U_n^r)^{s(v)} \max\{CW_2^{-1}, (CW_1^{-1})^{2r+1}\}^{\Gamma_v} \quad \text{for } v \in S. \tag{5.16}$$

Secondly, we assume that $v \notin S$. Then by (5.15) and (4.23),

$$\begin{aligned} F_v &\le 2^{s(v)} \max\{|\omega z_2^n|_v^{\nu} |G_r(\omega z_1^n)|_v, |\omega z_1^n|_v^{\nu} |H_r(\omega z_1^n)|_v\} \\ &\le (U_n^r)^{s(v)} \{\max(1, |\omega z_1^n|_v) \max(1, |\omega z_2^n|_v)\}^{\nu} \max(1, |\omega z_1^n|_v)^r. \end{aligned}$$

Hence

$$F_v \le (U_n^r)^{s(v)} \max(1, |\omega z_1^n|_v)^{r+\nu} \max(1, |\omega z_2^n|_v)^{\nu} \quad \text{for } v \notin S. \tag{5.17}$$

By the assumption of lemma 5.2 we have $F_v \neq 0$. Hence by the product formula (4.17), (4.22), (5.16) and (5.17),

$$\begin{aligned} 1 &= \prod_{v \in \overline{S}(K)} F_v = \prod_{v \in S} F_v \cdot \prod_{v \notin S} F_v \\ &\le U_n^r \max\{CW_2^{-1}, (CW_1^{-1})^{2r+1}\}^B \prod_{v \notin S} \{\max(1, |\omega z_1^n|_v)^{\nu+r} \max(1, |\omega z_2^n|_v)^{\nu}\} \\ &\le U_n^r \max\{CW_2^{-1}, (CW_1^{-1})^{2r+1}\}^B h(\omega z_1^n)^{\nu+r} h(\omega z_2^n)^{\nu} \\ &\le U_n^r W_1^{\nu+r} W_2^{\nu} \max\{CW_2^{-1}, (CW_1^{-1})^{2r+1}\}^B = \max(\Phi_r, \Psi_r). \end{aligned}$$

□

LEMMA 5.3. *There is a unique integer ℓ with $\ell \ge \ell_0$ such that*

(5.18) $$(U_n W_1)^{\ell} < C^{-B} W_1^{-\nu} W_2^{B-\nu} \le (U_n W_1)^{\ell+1}.$$

PROOF. Since the sequence $(U_n W_1)^{\ell}$ increases monotonically to infinity if ℓ tends to infinity, it suffices to show that

$$D^{-1} W_1^{-\nu} W_2^{B-\nu} > (U_n W_1)^{\ell_0}.$$

This is equivalent to

$$D^{-n(nB-1)/(nB-2)} W_2^{nB-1} > D^{-n/(nB-2)} U_n^{n\ell_0} W_1^{n\ell_0+1}.$$

By (5.11) it suffices to show that

$$\left(D^{-n/(nB-2)} W_1\right)^{(nB-1)^{k+1}} > D^{-n/(nB-2)} U_n^{n\ell_0} W_1^{n\ell_0+1},$$

which is the same as

$$W_1^{(nB-1)^{k+1}-n\ell_0-1} > U_n^{n\ell_0} D^{n((nB-1)^{k+1}-1)/(nB-2)}.$$

By (5.10) it is sufficient to show, comparing the exponents of U_n, D respectively and neglecting the factor 4,

$$\frac{n+1}{2nB-n-2}\left((nB-1)^{k+1}-n\ell_0-1\right) \ge n\ell_0,$$
$$\frac{n+1}{2nB-n-2}\left((nB-1)^{k+1}-n\ell_0-1\right) \ge \frac{n((nB-1)^{k+1}-1)}{nB-2}.$$

These inequalities are equivalent to

(5.19) $$(nB-1)^{k+1} \ge 1+n\ell_0\frac{2nB-1}{n+1},$$

(5.20) $$(nB-1)^{k+1} \ge 1+2n\ell_0\frac{nB-2}{n-2}$$

respectively. Note that (5.19) is weaker than (5.20) since

$$\frac{2nB-1}{n+1} < \frac{2(nB-2)}{n-2} \qquad \text{for } B > 1/2 + 1/n.$$

But (5.20) follows from (5.5). This proves our lemma. □

Let ℓ be the integer defined in lemma 5.3. We put $r=\ell$ if $z_2 A_{2\ell+1}(\omega z_1^n)$

$\neq z_1 B_{2\ell+1}(\omega z_1^n)$ and $r=\ell-1$ otherwise. Note that always $r\geq 1$. By lemma 1.5 with $h=2$ we have $z_2 A_{2r+1}(\omega z_1^n)\neq z_1 B_{2r+1}(\omega z_1^n)$, hence we may apply lemma 5.2. Note that by (5.18),

$$\Phi_r \leq \Phi_\ell < 1.$$

We shall now show that $\Psi_r<1$, thus contradicting lemma 5.2 and thus showing that (5.3) can not have k+1 solutions satisfying (5.6). By the right-hand side inequality of (5.18) we have

$$\begin{aligned}\Psi_r &\leq U_n^r C^{B(2r+1)} W_1^{\nu+r-B(2r+1)} \left(W_1^\nu C^B (U_n W_1)^{\ell+1}\right)^{(nB-1)^{-1}} \\ &\leq U_n^r C^{B(2r+1)} W_1^{r-B(2r+1)} \left(C^B U_n^{r+2} W_1^{r+2+B}\right)^{(nB-1)^{-1}} \\ &= \left(U_n^{nBr+2} C^{B((2nB-2)r+nB)} W_1^{-B(2nB-n-2)r-(nB^2-2B-2)}\right)^{(nB-1)^{-1}}. \end{aligned} \tag{5.21}$$

Put $A=U_n^{nB/(2nB-2)} C^B$. Note that $n+2>2n^2B/(2nB-2)$ for $B>1/2+1/n$ and that

$$U_3 < 4\times 2^6, \quad U_n = 2^{n+2} n \prod_{p|n} p^{1/(p-1)} \leq 2^{n+2} n^2 \leq 4\times 2^{2n} \text{ for } n\geq 4.$$

Hence by (5.10),

$$\begin{aligned} W_1 &\geq \left(U_n 2^{-2n} U_n^{n+1} (2C^B)^{2n}\right)^{(2nB-n-2)^{-1}} = \left(U_n^{n+2} C^{2nB}\right)^{(2nB-n-2)^{-1}} \\ &> \left(U_n^{2n^2B/(2nB-2)} C^{2nB}\right)^{(2nB-n-2)^{-1}} = A^{2n/(2nB-n-2)} \end{aligned} \tag{5.22}$$

Furthermore we know, by (5.4), $B>2/n$ and $r\geq \ell_0-1$, that

$$nBr+2 \leq nBr + \frac{(nB)^2}{2nB-2} = \frac{nB}{2nB-2}((2nB-2)r+nB),$$

$$\begin{aligned}&(2nB-2)r+nB - \frac{2n}{2nB-n-2}(B(2nB-n-2)r+nB^2-2B-2) \\ &\quad = -2r-(n-2)/2 - \frac{n^2-8n-4}{2(2nB-n-2)} \leq -2(r-\ell_0+1) \leq 0,\end{aligned}$$

and hence

$$B(2nB-n-2)r+nB^2-2B-2 > 0.$$

Together with (5.21),(5.22) this yields

$$\Psi_r < \left(A^{(2nB-2)r+nB}\left(A^{-2n/(2nB-n-2)}\right)^{B(2nB-n-2)r+nB^2-2B-2}\right)^{(nB-1)^{-1}}$$

$$\leq 1.$$

This completes the proof of theorem 5.1. □

CHAPTER 6. ON THE NUMBER OF SOLUTIONS OF THE THUE-MAHLER EQUATION.

§6.1. Introduction.

Let K be an algebraic number field of degree m and let r_1, r_2 denote the numbers of real and complex primes on K respectively. Let F be a binary form of degree n with coefficients in $\mathcal{O}_K$ such that $F(1,0)\neq 0$ and such that the polynomial $F(x,1)$ has at least three distinct zeros in $\mathbf{A}$. Furthermore, let $p_1,\ldots,p_t$ be t distinct prime ideals in K. (t might be zero, now and in the sequel). We shall deal with the generalised Thue-Mahler equation

$$(6.1) \qquad <F(x,y)> = p_1^{k_1}\ldots p_t^{k_t} \quad \text{in } x,y\in\mathcal{O}_K^*,\ k_1,\ldots,k_t\in\mathbb{Z}_{\geq 0}.$$

We call $z\in K^*$ a *solution fraction* of (6.1) if there is a solution $(x,y,k_1,\ldots,k_t)$ of (6.1) with $x/y=z$. Note that in case $K=\mathbb{Q}$ there is a one-to-one correspondence between solutions of (6.1) with $(x,y)=1$ and $y>0$ and solution fractions x/y of (6.1). Apart from the case that $t=0$ and $K=\mathbb{Q}$ or an imaginary quadratic number field, there are infinitely many solutions of (6.1) corresponding to a given solution fraction. In this chapter we shall show that the number of solution fractions of (6.1) can be bounded above by a number depending only on m,n,t and not on the coefficients of F, the prime ideals $p_1,\ldots,p_t$ and invariants of K other than its degree. For technical reasons, it is more convenient to consider instead of (6.1),

$$(6.2) \qquad \frac{<F(x,y)>}{c_K(F)<x,y>^n} = p_1^{k_1}\ldots p_t^{k_t} \quad \text{in } x,y\in\mathcal{O}_K^*,\ k_1,\ldots,k_t\in\mathbb{Z}_{\geq 0}.$$

Solution fractions of (6.2) are defined in a similar way as solution fractions of (6.1) and clearly, the number of solution fractions of (6.1) is at most equal to the number of solution fractions of (6.2).

Let f(z) be a polynomial with coefficients in K which has degree n and at least three distinct zeros in $\mathbf{A}$. Instead of (6.2) we may consider the equation

$$(6.3) \qquad \frac{<f(z)>}{c_K(f)<1,z>^n} = p_1^{k_1}\ldots p_t^{k_t} \quad \text{in } z\in K^*,\ k_1,\ldots,k_t\in\mathbb{Z}_{\geq 0}.$$

For suppose that $f(z)=F(z,1)$. Then f(z) has degree n since $F(1,0)\neq 0$. Furthermore, there is a one-to-one correspondence between solutions

$(z,k_1,\ldots,k_t)$ of (6.3) and solution fractions z of (6.2). We shall prove the following

THEOREM 6.1. *Let* $f(z)\in K[z]$ *be a polynomial of degree* n *which has at least three distinct zeros in* $\mathbb{A}$. *Then the number of solutions of* (6.3) *is at most*

$$7^{15\left(\binom{n}{3}m+1\right)^2} + 6\times 7^{2\binom{n}{3}(r_1+r_2+t)}.$$

Let $F(x,y)\in\mathbb{Z}[x,y]$ be a binary form of degree n such that $F(x,1)$ is a polynomial with at least three distinct zeros and let $p_1,\ldots,p_t$ be distinct prime numbers. Theorem 6.1 implies that the number of solutions of

$$|F(x,y)| = p_1^{k_1}\ldots p_t^{k_t} \quad \text{in } x,y\in\mathbb{Z} \text{ with } (x,y)=1, x\neq 0, y>0 \text{ and } k_1,\ldots,k_t\in\mathbb{Z}_{\geq 0} \tag{6.4}$$

is at most

$$7^{15\left(\binom{n}{3}+1\right)^2} + 6\times 7^{2\binom{n}{3}(t+1)}.$$

Under the restrictions that F has non-zero discriminant and that $F(1,0)\neq 0$, $F(0,1)\neq 0$, Lewis and Mahler [L/M] showed, using Mahler's p-adic generalisation [Ma 1,2] of Siegel's approximation method [Si 1], that the number of solutions of (6.4) is at most

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

where c_1,c_2,c_3 are absolute constants and where H is the maximum of the absolute values of the coefficients of F. Lewis and Mahler gave explicit, but very complicated expressions for c_1,c_2,c_3. In contrast to our bound, the bound of Lewis and Mahler depends on the coefficients of F, but if n is large compared with H the bound of Lewis and Mahler is sharper than ours. By theorem 6.1 with $K=\mathbb{Q}$ and $t=0$, the equation

$$F(x,y) = 1 \quad \text{in } x,y\in\mathbb{Z}^* \tag{6.5}$$

(where F is as in (6.4)) has at most

$$2\left(7^{15\left(\binom{n}{3}+1\right)^2} + 6\times 7^{2\binom{n}{3}}\right)$$

solutions, where we have taken under consideration both possibilities for the sign of y if n is even. Tartakovskiĭ [Ta] stated without proof that for irreducible forms F of degree $n \geq 4$, (6.5) has at most $235n^6$ solutions.

In case that $K \neq \mathbb{Q}$, no other explicit bound for the number of solutions of (6.3) is known. Only Parry [Pa](pp.77/78) has proved some results in this direction, by an algebraic generalisation of Mahler's p-adic approximation method. For example he proved the following:

let F *be a binary form as in* (6.1), *let* $p_1,\ldots,p_t$ *be given prime numbers and let* D_K *be the discriminant of* K. *Let* S *be a set of pairs* (x,y) *with* $x,y \in O_K^*$ *such that no two pairs* $(x_1,y_1),(x_2,y_2)$ *both belong to* S *if* $x_1/x_2 = y_1/y_2 = \varepsilon$ *for some unit* ε. *Then the number of pairs* $(x,y) \in S$ *with* $N_K(\langle x,y\rangle) \leq |D_K|^{1/2}$ *such that* $|N_{K/\mathbb{Q}}(F(x,y))|$ *is composed solely of* $p_1,\ldots,p_t$ *is at most* C_0^{t+1}, *where* C_0 *is a constant depending on* F *and* K *only and not on the number and choice of* $p_1,\ldots,p_t$.

Parry did not give an explicit value for C_0. Note that by theorem 6.1, C_0 can be replaced by a constant depending on K and the degree of F only.

In case that $f(z) = 1-\omega z^n$, where $\omega \in K^*$, theorem 6.1 can be improved.

THEOREM 6.2. *Let* n *be an integer with* $n \geq 3$, *let* $\omega \in K^*$ *and let* $p_1,\ldots,p_t$ *be given prime ideals. Put*

$$U(n) = \frac{16n-2}{8n-17}\left(\frac{16n-2}{8n+15}\right)^{(8n+15)/(8n-17)}.$$

Then
(i) the number of solutions of the equation

$$\frac{\langle 1-\omega z^n\rangle}{\langle 1,\omega z^n\rangle} = p_1^{k_1}\ldots p_t^{k_t} \quad \text{in } z \in K^*,\ k_1,\ldots,k_t \in \mathbb{Z}_{\geq 0} \tag{6.6}$$

with $h(\omega z^n) \geq 3^{n+10}$ *is at most*

$$2\left(nU(n)\right)^{r_1+r_2+t}$$

and
(ii) the number of solutions of (6.6) *with* $h(\omega z^n) < 3^{n+10}$ *is at most*

$$\left(2\times 3^{n+10}\right)^{(m+1)^2}.$$

The number U(n) decreases to 4 if n tends to infinity. In the table below some values of U(n) are given, rounded off to two decimals.

(6.7)

n	3	4	5	6	7	8	9
U(n)	16.49	9.85	7.82	6.84	6.26	5.88	5.60

Using the result of theorem 6.2, it is possible to derive upper bounds for the number of solutions of equations of the type $y^m=f(x)$ in $x,y \in \mathbb{Z}$ (where $m\in\mathbb{Z}, m\geq 2, f(x)\in\mathbb{Z}[x]$) and for $|ax^r-by^s|=p_1^{k_1}\ldots p_t^{k_t}$ in $x,y\in\mathbb{Z}$ with (x^r,y^s) not divisible by an lcm(r,s)-th power >1 and $k_1,\ldots,k_t\in\mathbb{Z}_{\geq 0}$ (where $r,s\in\mathbb{N}, rs\geq 6, a,b\in\mathbb{Z}^*$ and $p_1,\ldots,p_t$ are fixed prime numbers.). By methods described in [Si 2]and[LeV 2], $y^m=f(x)$ can be reduced to finitely many equations of the type $\alpha x^n-\beta y^n=\gamma$ with α,β,γ constants and x,y integral variables in some algebraic number field K. Mahler [Ma 5]pointed out, that $|ax^r-by^s|=p_1^{k_1}\ldots p_t^{k_t}$ can be reduced to finitely many equations of the type $<\alpha x^n-\beta y^n>=p_1^{\ell_1}\ldots p_t^{\ell_t}$ where x,y are integral variables, α,β constants and $p_1,\ldots,p_t$ fixed prime ideals in some algebraic number field K and where $\ell_1,\ldots,\ell_t$ are non-negative, integral variables.

First of all, we shall prove theorem 6.1 for n=3. By combining some techniques Mahler introduced in p-adic approximation theory (cf.[Ma 1,2], [L/M]) with techniques from chapter 3 we shall reduce (6.3) to finitely many systems of inequalities of type (5.3) with n=3 and then apply theorem 5.1. The general result is derived from the result in case n=3. Equations of type (6.6) can be reduced to systems of inequalities of type (5.3) for all values of n with $n\geq 3$. This brings about the fact that our upper bound for the number of solutions of (6.6) has a better dependence on n than that of (6.3). The proof of theorem 6.2 follows the same lines as that of theorem 6.1 and we shall sketch it briefly at the end of this chapter.

Furthermore we shall prove the following result in a similar way as theorem 6.1.

THEOREM 6.3. *Let* f *be a polynomial of degree* $n\geq 3$ *with coefficients in* K *and non-zero discriminant. Let* A *be a constant with* $A\geq 1$. *If*

$$N_K(d_K(f)) \geq (13^m A)^{5n(n-1)/6} \tag{6.8}$$

then the inequality

(6.9) $$N_K\left(\frac{<f(z)>}{c_K(f)<1,z>^n}\right) \leq A \quad \textit{in } z\in K^*$$

has at most

$$6\times 7^{2\binom{n}{3}(r_1+r_2)}$$

solutions.

This generalises previous results of Siegel [Si 4] on the inequality $|ax^n-by^n|\leq C$ (cf.§2.1) and Siegel [Si 3], Delone, Faddeev and Gel'man [D/F] on the inequality $|F(x,y)|\leq k$, where F is a binary form with coefficients in $\mathbb{Z}$ and positive discriminant (cf.§3.1). For a discussion of possible refinements in case $n>3$ we refer to the remarks after the proof of theorem 6.3.

Using theorems 6.1 and 6.3 it is also possible to derive results on the number of solutions of the equation

(6.10) $$F(x,y) = \gamma \quad \text{in } x,y\in \mathcal{O}_K^*,$$

where $\gamma\in\mathcal{O}_K^*$ and where F is as in (6.1). In the theorem below, $\omega_K(\gamma)$ denotes the number of distinct prime ideals in K dividing $<\gamma>$.

THEOREM 6.4. *(i) The number of solutions of* (6.10) *is at most*

$$n\left(7^{15\left(\binom{n}{3}m+1\right)^2} + 6\times 7^{2\binom{n}{3}(r_1+r_2+\omega_K(\gamma))}\right).$$

(ii) Suppose that F *has non-zero discriminant* D(F). *If*

(6.11) $$|N_{K/\mathbb{Q}}(D(F))| \geq |13^m N_{K/\mathbb{Q}}(\gamma)|^{5n(n-1)/6},$$

then (6.10) *has at most*

$$6n\times 7^{2\binom{n}{3}(r_1+r_2)}$$

solutions.

Note that the bound given in the first part of theorem 6.4 depends on $\omega_K(\gamma)$, n,m,r_1,r_2 only, while the second part of theorem 6.4 states that if $|N_{K/\mathbb{Q}}(D(F))|$ exceeds some constant depending on m,n and $|N_{K/\mathbb{Q}}(\gamma)|$, then the

number of solutions of (6.10) can be estimated from above by a constant depending on n, r_1, r_2 only. In 1974, Chudnovsky [Chu 1] claimed that bounds of similar type could be derived under similar conditions by means of a method of Gel'fond[Ge 1] from 1934 on linear forms of two logarithms of algebraic numbers near to unity. As far as I know, Chudnovsky has never published a proof of his claim. Theorem 6.4 will be derived as a corollary from theorems 6.1 and 6.3 later.

§6.2. Preliminaries to the proofs of theorems 6.1 and 6.3 in the case n=3.

As before, K is an algebraic number field of degree m with r_1 real and r_2 complex primes, $p_1,\dots,p_t$ are distinct prime ideals in K and A is a real constant with $A \geq 1$. We consider

$$\frac{\langle f(z)\rangle}{c_K(f)\langle 1,z\rangle^3} = p_1^{k_1}\dots p_t^{k_t} \quad \text{in } z\in K^*, k_1,\dots,k_t \in \mathbb{Z}_{\geq 0} \tag{6.12}$$

and

$$N_K\left(\frac{\langle f(z)\rangle}{c_K(f)\langle 1,z\rangle^3}\right) \leq A \quad \text{in } z\in K^* \tag{6.13}$$

simultaneously, where in both (6.12) and (6.13), $f(z)\in K[z]$ is a polynomial of degree 3 with only simple zeros. We define the binary form $f^*(x,y)$ such that $f^*(x,y)=y^3 f(x/y)$ for $y\neq 0$. Then f and f^* have the same discriminant, which we denote by D. Let $M=K(\sqrt{-3D})$. Let $S_0=S_\infty(K)\cup\{p_1,\dots,p_t\}$, where $p_1,\dots p_t$ are the prime ideals from (6.12) and let T_0 be the set of primes on M lying above the primes from S_0.

We apply lemma 3.2 to $f^*(x,y)$. Let α,β be the constants, and let ξ,η be the linear forms constructed there. Then $\alpha,\beta \in M$ and $\xi,\eta\in M[x,y]$. We put, if confusion can not arise,

$$\xi_1 = \xi(z,1),\ \eta_1 = \eta(z,1),\ \omega = \beta/\alpha.$$

Let $\mathfrak{a}$ be the ideal in M defined by

$$\mathfrak{a} = c_M(f)^{-2}\langle\sqrt{-3D}\rangle_M. \tag{6.14}$$

Then by (3.9),

$$(6.15)\qquad \frac{<\alpha\xi_1^3-\beta\eta_1^3>_M}{c_M(f)^3<1,z>_M^3} = 3a\frac{<f(z)>_M}{c_M(f)<1,z>_M^3}\ .$$

Solutions $(z,k_1,\ldots,k_t)$ of (6.12) will be shortly denoted by z. Let z be such a solution. Then we have by (4.14),(6.12) and (6.15), for every $V\notin T_0$,

$$|\alpha\xi_1^3-\beta\eta_1^3|_V = |3a|_V|c_M(f)|_V^3\max(1,|z|_V)^3.$$

Hence by the product formula (cf.(4.17)) and (4.14),

$$(6.16)\qquad \prod_{V\in T_0}|\alpha\xi_1^3-\beta\eta_1^3|_V\cdot\prod_{V\notin T_0}\left(|c_M(f)|_V\max(1,|z|_V)\right)^3\prod_{V\notin T_0}|3a|_V = 1.$$

If z is a solution of (6.13) then by (6.15) and (4.8),

$$N_M\left(\frac{<\alpha\xi_1^3-\beta\eta_1^3>}{c_M(f)^3<1,z>^3}\right)\le N_M(3a)A^{[M:K]}.$$

Hence by (4.14),(4.16) and the product formula for ideals (4.15),

$$(6.17)\qquad \prod_{V\in S_\infty(M)}|\alpha\xi_1^3-\beta\eta_1^3|_V\cdot\prod_{V\in S(M)}\left(|c_M(f)|_V\max(1,|z|_V)\right)^3 \le N_M(3a)^{1/[M:\mathbb{Q}]}A^{1/[K:\mathbb{Q}]}.$$

Let S be an arbitrary, but finite subset of $\overline{S}(K)$ containing all infinite primes. Let T be the set of primes on M lying above the primes in S. Put

$$\Delta_S = \prod_{V\notin T}|a|_V^{-2} = \prod_{V\notin T}|3d_M(f)|_V^{-1}.$$

Note that (6.12),(6.13) are equivalent to (6.16), (6.17) respectively. These inequalities are special cases of

$$(6.18)\qquad \prod_{V\in T}|\alpha\xi_1^3-\beta\eta_1^3|_V\cdot\prod_{V\notin T}\left(|c_M(f)|_V\max(1,|z|_V)\right)^3\le\left(\prod_{V\in T}|3|_V\right)P\Delta_S^{1/2},$$

where P is a constant with $P\ge 1$. For we obtain (6.16) by taking $P=1,S=S_0$ and applying the product formula (4.17) and (6.17) by taking $P=A^{1/m},S=S_\infty(K)$. In the remainder of this section we shall study (6.18). We shall consider

only solutions of (6.18) belonging to the set

$$K_0 = \{z \in K \mid \xi(z,1)\eta(z,1) \neq 0\}.$$

Since ξ,η are linear forms, we exclude at most two solutions of (6.18).

For every $z \in K_0$ we put

$$\zeta = \zeta(z) = \eta_1/\xi_1 \tag{6.19}$$

and

$$\Omega_S(z) = \prod_{V \in T} \max(|\alpha\xi_1^3|_V, |\beta\eta_1^3|_V) \cdot \prod_{V \notin T} \left(|c_M(f)|_V \max(1,|z|_V)\right)^3. \tag{6.20}$$

$\Omega_S(z)$ is a kind of height function with the property that

$$\Omega_S(z) \geq h(\omega\zeta^3). \tag{6.21}$$

This can be proved as follows. Let the ideals b_1, b_2 be defined by

$$b_1 = \frac{<\alpha\xi_1^3>_M}{c_M(f)^3 <1,z>_M^3}, \quad b_2 = \frac{<\beta\eta_1^3>_M}{c_M(f)^3 <1,z>_M^3}.$$

Let M' be an extension of M in which $<1,z>_{M'}$ and $c_{M'}(f)$ are principal ideals, with generators λ_1, λ_2 respectively. Let $G(x,y), H(x,y)$ be the cubic and quadratic covariant of $f^*(x,y)$ respectively. It is easy to check that the numbers $G_* = \lambda_2^{-3} G(\lambda_1^{-1}z, \lambda_1^{-1}), H_* = \lambda_2^{-2} H(\lambda_1^{-1}z, \lambda_1^{-1})$ are algebraic integers. By (3.8) and (3.10) the numbers $\lambda_2^{-3}\alpha\xi(\lambda_1^{-1}z, \lambda_1^{-1})^3$, $\lambda_2^{-3}\beta\eta(\lambda_1^{-1}z, \lambda_1^{-1})^3$ are the roots of the equation

$$x^2 - G_* x + H_*^3 = 0,$$

whence are algebraic integers. These numbers generate $b_1 O_{M'}, b_2 O_{M'}$ respectively, hence b_1, b_2 are integral ideals in M. But this implies by (4.27) that

$$h(\omega\zeta^3) = \prod_{V \in \overline{S}(M)} \max(|\alpha\xi_1^3|_V, |\beta\eta_1^3|_V)$$

$$= \prod_{V\in T} \max(|\alpha\xi_1^3|_V, |\beta\eta_1^3|_V) \times$$
$$\times \prod_{V\notin T} \left(\max(|b_1|_V, |b_2|_V)(|c_M(f)|_V \max(1, |z|_V))^3\right)$$
$$\leq \Omega_S(z).$$

Let $\theta_1, \theta_2, \theta_3$ be the cube roots of ω and let L be the smallest Galois extension of K containing $M(\theta_1, \theta_2, \theta_3)$. For every $V\in T$ we choose a fixed continuation of $|.|_V$ to L which is also denoted by $|.|_V$.

LEMMA 6.1. *Let z be a solution of* (6.18) *with* $z\in K_0$. *Put*

$$m_V = m_V(z) = \max\left(\min_{1\leq i\leq 3}(1, |1-\theta_i\zeta|_V), \min_{1\leq j\leq 3}(1, |1-\theta_j^{-1}\zeta^{-1}|_V)\right)$$

for $V\in T$. *Then*

$$\prod_{V\in T} m_V(z) \leq 8P\Delta_S^{1/2}\Omega_S(z)^{-1}. \tag{6.22}$$

PROOF. First of all, we prove that for each $V\in T$,

$$|1-\omega\zeta^3|_V \geq |3|_V 2^{-3s(V)} \max(1, |\omega\zeta^3|_V) \min_i (1, |1-\theta_i\zeta|_V). \tag{6.23}$$

We suppose that $|1-\theta_1\zeta|_V \leq |1-\theta_i\zeta|_V$ and that $\theta_i = \rho^{i-1}\theta_1$ for i=2,3, where ρ is a primitive third root of unity. This is clearly no restriction. By (4.23) we have for i=2,3,

$$\begin{aligned} |1-\theta_i\zeta|_V &= \max(|1-\theta_i\zeta|_V, |1-\theta_1\zeta|_V) \\ &= \max(|1-\rho^{i-1}\theta_1\zeta|_V, |\rho^{1-i}-\theta_1\zeta|_V, |1-\theta_1\zeta|_V) \\ &\geq 2^{-s(V)} \max(|1-\rho^{i-1}|_V |\theta_1\zeta|_V, |1-\rho^{1-i}|_V) \\ &= 2^{-s(V)} |1-\rho^{i-1}|_V \max(1, |\theta_1\zeta|_V). \end{aligned} \tag{6.24}$$

Furthermore, we have either $|\theta_1\zeta|_V \leq 2^{s(V)}$, which implies that $2^{-s(V)}\max(1, |\theta_1\zeta|_V) \leq 1$; or $|\theta_1\zeta|_V > 2^{s(V)}$, which implies by (4.23) that

$$|\theta_1\zeta|_V = |1-\theta_1\zeta-1|_V \leq 2^{s(V)} \max(1, |1-\theta_1\zeta|_V) = 2^{s(V)} |1-\theta_1\zeta|_V.$$

Therefore,

$$|1-\theta_1\zeta|_V \geq 2^{-s(V)}\max(1,|\theta_1\zeta|_V)\min(1,|1-\theta_1\zeta|_V).$$

Together with (6.24) this yields that

$$\begin{aligned}|1-\omega\zeta^3|_V &= |1-\theta_1\zeta|_V|1-\theta_2\zeta|_V|1-\theta_3\zeta|_V \\ &\geq 2^{-3s(V)}|1-\rho|_V|1-\rho^2|_V\max(1,|\theta_1\zeta|_V)^3\min(1,|1-\theta_1\zeta|_V) \\ &= 2^{-3s(V)}|3|_V\max(1,|\omega\zeta^3|_V)\min(1,|1-\theta_1\zeta|_V).\end{aligned}$$

This proves (6.23). As a consequence we have

$$\begin{aligned}U_V &:= |\alpha\xi_1^3-\beta\eta_1^3|_V\cdot 2^{3s(V)}|3|_V^{-1}\max(|\alpha\xi_1^3|_V,|\beta\eta_1^3|_V)^{-1} \\ &\geq \min_{1\leq i\leq 3}(1,|1-\theta_i\zeta|_V).\end{aligned}$$

It follows in a similar way, by interchanging α,β and ξ_1,η_1, that

$$U_V \geq \min_{1\leq j\leq 3}(1,|1-\theta_j^{-1}\zeta^{-1}|_V).$$

Hence $m_V\leq U_V$ for $V\in T$. Therefore, by (6.20) and (6.18),

$$\begin{aligned}\prod_{V\in T} m_V &\leq \prod_{V\in T} U_V \\ &= 8\Big(\prod_{V\in T}|3|_V\Big)^{-1}\cdot\prod_{V\in T}|\alpha\xi_1^3-\beta\eta_1^3|_V\cdot\prod_{V\notin T}\Big(|c_M(f)|_V\max(1,|z|_V)\Big)^3\times \\ &\qquad\qquad\times\,\Omega_S(z)^{-1} \\ &\leq 8P\Delta_S^{1/2}\Omega_S(z)^{-1}\ .\end{aligned}$$

□

We shall now show that every solution of (6.22) satisfies one of finitely many given systems of inequalities of type (5.3). Therefore we use the following technical lemma, which is a slight improvement of a result used by Mahler in [Ma 1,2].

LEMMA 6.2. *Let* B *be a real number with* $1/2 < B < 1$ *and let* q *be a positive integer. Let* $F_1,\ldots,F_q,\Lambda$ *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* $\sum_{j=1}^{q}\Gamma_j = B$, *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* F_j, Λ, *such that for* $j=1,\ldots,q$:

$$F_j \leq \Lambda^{\Gamma_j}. \tag{6.25}$$

PROOF. If q=1 we may take the 1-tuple (B), so we shall restrict ourselves to the case $q \geq 2$. Let u be the integer defined by

$$(q-1)B/(1-B) \leq u < (q-1)B/(1-B) + 1. \tag{6.26}$$

Then $u \geq 1$. We shall show that the set of q-tuples

$$V_0 = \{(\Gamma_1,\ldots\Gamma_q) \mid \Gamma_j = f_j B/u,\ f_j \in \mathbb{Z}_{\geq 0} \text{ for } j=1,\ldots,q,\ \sum_{j=1}^{q} f_j = u\}$$

satisfies the conditions of our lemma. Clearly, V_0 does not depend on F_j, Λ and moreover, $\Gamma_j \geq 0$ for $j=1,\ldots,q$, $\sum_{j=1}^{q}\Gamma_j = B$ for $(\Gamma_1,\ldots,\Gamma_q)\in V_0$. In the remainder of the proof we shall assume that $\Lambda<1$, which is no restriction at all.

Now we show that (6.25) holds for some tuple $(\Gamma_1,\ldots,\Gamma_q)\in V_0$. There are non-negative reals $\phi_1,\ldots,\phi_q$ such that $F_j = \Lambda^{\phi_j}$ and $\sum_{j=1}^{q}\phi_j \geq 1$. Define integers g_j by

$$u\phi_j/B - 1 < g_j \leq u\phi_j/B \quad \text{for } j=1,\ldots,q. \tag{6.27}$$

Then $g_j \geq 0$ and by (6.26),

$$\sum_{j=1}^{q} g_j > uB^{-1}\cdot\Big(\sum_{j=1}^{q}\phi_j\Big) - q \geq uB^{-1} - q \geq u-1.$$

Hence

$$\sum_{j=1}^{q} g_j \geq u.$$

There are integers f_j such that $0 \leq f_j \leq g_j$ and $\sum_{j=1}^{q} f_j = u$. For these integers we have $(Bf_1/u,\ldots,Bf_q/u)\in V_0$ and by (6.27),

$$F_j \leq \Lambda^{Bf_j/u}.$$

In order to complete the proof of lemma 6.2, we shall estimate the number of elements of V_0 from above. Note that by (6.26),

$$|V_0| = \binom{u+q-1}{q-1} \leq \binom{(q-1)/(1-B)+1}{q-1} .$$

Hence it suffices to show that

$$\binom{(q-1)/(1-B)+1}{q-1} \leq R(B)^{q-1} \quad \text{for } 1/2 < B < 1, q \in \mathbb{Z}, q \geq 2. \tag{6.28}$$

It is possible to show (6.28) for large values of q by means of Stirling's formula

$$\Gamma(x) \sim \sqrt{2\pi x}\left(\frac{x-1}{e}\right)^{x-1} \quad \text{for } x \to \infty,$$

where $\Gamma(x)$ denotes Euler's Γ-function. Proceeding like this, one can even show that

$$\lim_{q\to\infty} \log\binom{(q-1)/(1-B)+1}{q-1} \Big/ \log q = R(B)$$

hence (6.28) can not be essentially improved. However, we shall prove (6.28) completely in an elementary way.

Put $x=B/(1-B)$, $h=q-1$. Then (6.28) is equivalent to

$$\binom{h(x+1)+1}{h} \leq \left((1+x)(1+x^{-1})^x\right)^h \quad \text{for } x>1,\ h \in \mathbb{N}. \tag{6.29}$$

Note that for $h=1$,

$$\binom{h(x+1)+1}{h} = x+2 < 2(x+1) \leq (1+x)(1+x^{-1})^x,$$

while for $h=2$,

$$\binom{h(x+1)+1}{h} = (2x+3)(2x+2)/2 < 4(x+1)^2 \leq \left((1+x)(1+x^{-1})^x\right)^2.$$

Hence we may assume that $h \geq 3$. We shall use the following inequality:

$$\binom{y}{g} \leq \frac{3}{7} \frac{y^y}{(y-g)^{y-g} g^g} \quad \text{for } y \in \mathbb{R}, g \in \mathbb{N} \text{ with } y \geq g+4. \tag{6.30}$$

(6.30) can be proved by induction on g. First of all, suppose $g=1$. Then

$x \geq 5$, hence

$$\frac{y^y}{(y-1)^{y-1}} = y\left(1+(y-1)^{-1}\right)^{y-1} \geq y(5/4)^4 > \frac{7}{3}\binom{y}{1}.$$

Suppose that (6.30) has been proved for $g=p-1$, where $p \geq 2$. Then we have for $g=p$, by the fact that the function $(1-w^{-1})^{w-1}$ decreases monotonically for $w>1$,

$$\binom{y}{p} = \frac{y}{p}\binom{y-1}{p-1} \leq \frac{3}{7}\frac{y}{p}\frac{(y-1)^{y-1}}{(y-p)^{y-p}(p-1)^{p-1}} = \frac{3}{7}\frac{y^y}{(y-p)^{y-p}p^p}\frac{(1-y^{-1})^{y-1}}{(1-p^{-1})^{p-1}}$$
$$\leq \frac{3}{7}\frac{y^y}{(y-p)^{y-p}p^p}.$$

We shall now prove (6.29) for $h \geq 3$. Note that $h(x+1)=h+xh \geq h+3$, hence by (6.30)

$$\binom{h(x+1)+1}{h} = \frac{h(x+1)+1}{h}\binom{h(x+1)}{h-1} \leq (x+4/3)\binom{h(x+1)}{h-1}$$
$$\leq \frac{3}{7}(x+4/3)\frac{(h(x+1))^{h(x+1)}}{(hx+1)^{hx+1}(h-1)^{h-1}}$$
$$= \frac{3}{7}(x+4/3)\frac{h^{h-1}}{(h-1)^{h-1}}\frac{(hx)^{hx+1}}{(hx+1)^{hx+1}}(1+x)^{h(1+x)}x^{-hx-1}$$
$$= \frac{3}{7}(1+4/3x)\left(1+(h-1)^{-1}\right)^{h-1}\left(1-(hx+1)^{-1}\right)^{hx+1} \times$$
$$\times \left((1+x)(1+x^{-1})^x\right)^h$$
$$\leq e \times e^{-1}\left((1+x)(1+x^{-1})^x\right)^h = \left((1+x)(1+x^{-1})^x\right)^h.$$

This proves lemma 6.2 completely. □

For each $v \in S$ we choose a fixed prime in T lying above v and the set of these primes is denoted by T^+. Furthermore, we put $T^- = T \setminus T^+$. Note that $T^- = \emptyset$ if $M=K$.

Let $z \in K_0$ and choose for each $V \in T^+$ $\theta_V \in \{\theta_1, \theta_2, \theta_3\}$ such that $|1-\theta_V \zeta|_V$ is minimal. Let $v \in S$ and suppose that there are two primes V, V' in T lying above v, where $V \in T^+$ and $V' \in T^-$. Then $[M:K]=2$ and there is a unique K-automorphism σ of M which maps $\sqrt{-3D}$ onto $-\sqrt{-3D}$. By (3.8) we have $\sigma(\alpha\xi_1^3) = \beta\eta_1^3$, hence

$$\sigma(\omega\zeta^3) = \omega^{-1}\zeta^{-3}, \quad N_{M/K}(\omega\zeta^3) = 1, \tag{6.31}$$

(where $N_{M/K}$ denotes the norm of M over K). By (4.20) we have

$$|\lambda|_{V'} = |\sigma(\lambda)|_V \quad \text{for } \lambda\in M.$$

Moreover, since L/K is a Galois extension and since the continuations of $|.|_V$ and $|.|_{V'}$ to L which were chosen on p.81 are equal on K, there are primes W,W' on L which are conjugate over K and a constant c such that $|.|_V = |.|_W^c$, $|.|_{V'} = |.|_{W'}^c$. Hence by (4.20) there exists a continuation τ_v of σ to L such that

$$|\lambda|_{V'} = |\tau_v(\lambda)|_V \quad \text{for } \lambda\in L.$$

By (6.31) there is a permutation (j_1,j_2,j_3) of (1,2,3) such that $\tau_v(\theta_{j_i}\zeta) = \theta_i^{-1}\zeta^{-1}$, i.e. $\theta_{j_i} = \left(\tau_v^{-1}(\theta_i)N_{M/K}(\zeta)\right)^{-1}$. Put $\theta_{V'} = \left(\tau_v^{-1}(\theta_V)N_{M/K}(\zeta)\right)^{-1}$. Then

$$|1-\theta_{j_i}\zeta|_{V'} = |1-\theta_i^{-1}\zeta^{-1}|_V = |\omega\zeta^3|_V^{-1/3}|1-\theta_i\zeta|_V ,$$
$$|1-\theta_{j_i}^{-1}\zeta^{-1}|_{V'} = |1-\theta_i\zeta|_V \qquad \text{for } i=1,2,3.$$

Hence, on noting that $|1-\theta_i^{-1}\zeta^{-1}|_V$ is minimal if and only if $|1-\theta_i\zeta|_V$ is minimal,

$$(6.32) \qquad m_V(z) = m_{V'}(z) = \max\left(\min(1,|1-\theta_V\zeta|_V),\min(1,|1-\theta_{V'}\zeta|_{V'})\right).$$

We now apply lemma 6.2 to (6.22). Let s be the number of primes in S. Then we have for every B with $1/2 < B < 1$ and for every $z\in K_0$ satisfying (6.22) that there exists a tuple $(\Gamma_v)_{v\in S}$ of non-negative numbers with $\sum_{v\in S}\Gamma_v = B$, belonging to a set of at most $R(B)^{s-1}$ of such tuples which depends on B and s but not on z, such that

$$\prod_{V|v} m_V \le \left(8P\Delta_S^{1/2}\Omega_S(z)^{-1}\right)^{\Gamma_v} \quad \text{for } v\in S.$$

(where the product in the left-hand side is taken over all primes V lying above v). For every $V\in T$ lying above $v\in S$ we put $\Gamma_V = \Gamma_v/n(v)$, where n(v) is the number of primes lying above v. Then, by (6.32),

$$m_V \le \left(8P\Delta_S^{1/2}\Omega_S(z)^{-1}\right)^{\Gamma_V},$$

hence

$$\min(1, |1-\theta_V\zeta|_V) \le \left(8P\Delta_S\Omega_S(z)^{-1}\right)^{\Gamma_V} \quad \text{for } V\in T. \tag{6.33}$$

The tuple $(\Gamma_V)_{V\in T}$ can be chosen from at most $R(B)^{s-1}$ possibilities. The tuple $(\theta_V)_{V\in T}$ is completely determined by the tuple $(\theta_V)_{V\in T^+}$ and by $N_{M/K}(\zeta)$. Note that $|T^+|=s$ and that for each $V\in T^+$, θ_V is equal to one of the three cube roots of ω in L. By (6.31), $N_{M/K}(\zeta)$ is equal to one of the three cube roots of $N_{M/K}(\omega^{-1})$. Hence the tuple $(\theta_V)_{V\in T}$ can be chosen from at most 3^{s+1} possibilities. Combining the above arguments we obtain:

LEMMA 6.3. *Let* B *be a real with* $1/2<B<1$, *let* $s=|S|$ *and put* $R(B)=(1-B)^{-1}B^{B/(B-1)}$. *There exists a set consisting of at most* $3^{s+1}R(B)^{s-1}$ *tuples of the type* $((\theta_V)_{V\in T},(\Gamma_V)_{V\in T})$ *with* $\theta_V\in L$, $\theta_V^3=\omega$, $\Gamma_V\ge 0$ *for* $V\in T$ *and* $\sum_{V\in T}\Gamma_V=B$, *with the following property: every* $z\in K_0$ *satisfying* (6.18) *satisfies* (6.33) *for at least one of these tuples.*

We shall need the following improvement of lemma 5.1.

LEMMA 6.4. *Let* z', z'' *be distinct solutions of* (6.33) *with* $z', z''\in K_0$ *and* $\Omega_S(z'')\ge\Omega_S(z')$. *Then*

$$\Omega_S(z'') \ge \left(\frac{\Delta_S^{(1-B)/2}}{2^{3B+1}P^B}\right)^3 \Omega_S(z')^{3B-1} \tag{6.34}$$

and

$$\Omega_S(z'') \ge \Delta_S/64P\ . \tag{6.35}$$

PROOF. Put $\xi_1'=\xi(z',1)$, $\eta_1'=\eta(z',1)$, $\zeta'=\zeta(z')$, $\Omega'=\Omega_S(z')$, $\xi_1''=\xi(z'',1)$, $\eta_1''=\eta(z'',1)$, $\zeta''=\zeta(z'')$, $\Omega''=\Omega_S(z'')$. For each $V\in T$ we put

$$\omega_V' = \max(|\alpha\xi_1'^3|_V, |\beta\eta_1'^3|_V),\quad \omega_V'' = \max(|\alpha\xi_1''^3|_V, |\beta\eta_1''^3|_V).$$

Note that the linear transformation $(x,y)\to(\xi,\eta)$ has determinant unity and that $\alpha\beta=-(\sqrt{-3}D)^3$ (cf. lemma 3.2). Hence by the product formula (4.17) and (6.14),

$$\prod_{V\in T}\left(|\alpha\beta|_V^{1/3}|\xi_1'\eta_1''-\xi_1''\eta_1'|_V\right) = \prod_{V\in T}\left(|\alpha\beta|_V^{1/3}|z'-z''|_V\right)$$

$$= \prod_{V\notin T} \left(|\alpha\beta|_V^{1/3}|z'-z''|_V\right)^{-1}$$
$$\geq \prod_{V\notin T} |\alpha|_V^{-1} \cdot \prod_{V\notin T} \left(|c_M(f)|_V^2 \max(1,|z'|_V)\max(1,|z''|_V)\right)^{-1}$$
$$= \Delta_S^{1/2} \prod_{V\notin T} \left(|c_M(f)|_V^2 \max(1,|z'|_V)\max(1,|z''|_V)\right)^{-1}.$$

Hence, by (6.20),

$$\Delta_S^{1/2} \leq \prod_{V\in T} \left(|\alpha\beta|_V^{1/3}|\xi_1'\eta_1''-\xi_1''\eta_1'|_V\right) \cdot (\Omega'\Omega'')^{1/3} \cdot \prod_{V\in T} (\omega_V'\omega_V'')^{-1/3}. \tag{6.36}$$

Note that for each $V\in T$, by a trivial estimate,

$$|\alpha\beta|_V^{1/3}|\xi_1'\eta_1''-\xi_1''\eta_1'|_V \leq 2^{s(V)}(\omega_V'\omega_V'')^{1/3}. \tag{6.37}$$

For each $V\in T$ we have also

$$|\alpha\beta|_V^{1/3}|\xi_1'\eta_1''-\xi_1''\eta_1'|_V = |\alpha\xi_1'^3|_V|\alpha\xi_1''^3|_V|\theta_V\zeta'-\theta_V\zeta''|_V$$
$$\leq 2^{s(V)}(\omega_V'\omega_V'')^{1/3}\max(|1-\theta_V\zeta'|_V,|1-\theta_V\zeta''|_V).$$

This implies, together with (6.37),(6.33), $\Omega''\geq\Omega'$ and the fact that for real numbers a,b,c $\min(a,\max(b,c))=\max(\min(a,b),\min(a,c))$,

$$|\alpha\beta|_V^{1/3}|\xi_1'\eta_1''-\xi_1''\eta_1'|_V$$
$$\leq 2^{s(V)}(\omega_V'\omega_V'')^{1/3}\min(1,\max(|1-\theta_V\zeta'|_V,|1-\theta_V\zeta''|_V))$$
$$\leq 2^{s(V)}(\omega_V'\omega_V'')^{1/3}\max(\min(1,|1-\theta_V\zeta'|_V),\min(1,|1-\theta_V\zeta''|_V))$$
$$\leq 2^{s(V)}(\omega_V'\omega_V'')^{1/3}\left(8P\Delta_S\Omega'^{-1}\right)^{\Gamma V}.$$

Therefore, by (6.36), on taking the product over all $V\in T$,

$$\Delta_S^{1/2}(\Omega'\Omega'')^{-1/3} \leq 2\left(8P\Delta_S^{1/2}\Omega'^{-1}\right)^B,$$

which proves (6.34),

We are now going to prove (6.35). Note that by (6.36) and (6.37), on taking the product over all $V\in T$,

$$\Delta_S^{1/2} \leq 2(\Omega'\Omega'')^{1/3}.$$

Hence, by (6.34),

$$1 \le 2\Omega''^{1/3}\Delta_S^{-1/2}\left(2^{3B+1}P^B\Delta_S^{-(1-B)/2}\Omega''^{1/3}\right)^{1/(3B-1)}$$
$$= \left(2^6 P\Delta_S^{-1}\Omega''\right)^{B/(3B-1)}.$$

This proves (6.35). □

From lemma 6.4 the following useful corollary can be derived (compare lemma 2.11).

LEMMA 6.5. *Put* $T = \left(\Delta_S^{(1-B)/2}2^{-3B-1}P^{-B}\right)^{3/(3B-2)}$. *Let* U_0, U_1 *be constants with* $T^{-1} < U_0 < U_1$. *Then the number of solutions of* (6.33) *with* $U_0 \le \Omega_S(z) < U_1$ *is at most* r, *where* r *is the largest integer with*

$$r < 1 + \frac{\log(\log(TU_1)/\log(TU_0))}{\log(3B-1)}.$$

PROOF. Let $z_1,\ldots,z_{r_0}$ be solutions of (6.33) with $z_i \in K_0$ for $i=1,\ldots,r_0$ and

$$U_0 \le \Omega_S(z_1) \le \ldots \le \Omega_S(z_{r_0}) < U_1.$$

Put $\Omega_i = \Omega_S(z_i)$ for $i=1,\ldots,r_0$. By (6.34) we have

$$T\Omega_{i+1} \ge (T\Omega_i)^{3B-1} \quad \text{for } i=1,\ldots,r_0,$$

hence

$$TU_1 > T\Omega_{r_0} \ge (T\Omega_1)^{(3B-1)^{r_0-1}} \ge (TU_0)^{(3B-1)^{r_0-1}}.$$

Therefore,

$$r_0^{-1} < \frac{\log(\log(TU_1)/\log(TU_0))}{\log(3B-1)},$$

which proves our lemma. □

§6.3. Proofs of theorems 6.1 and 6.3 in the case n=3.

In this section the same notations are used as in the preceding

sections. Furthermore we choose B=0.846. Note that $B>1/2+1/3=5/6$. We shall deduce theorems 6.1 and 6.3 from the lemma below. To avoid confusion we agree that when speaking of (6.33) we shall always mean (6.33) with B=0.846.

LEMMA 6.6. *(i)* (6.33) *has at most* 30 *solutions in* $z\in K_0$ *with*

$$\Omega_S(z) \geq \tfrac{1}{2}\times 7^{7.5}P^5. \tag{6.38}$$

(ii) If $\Delta_S\geq(13P)^5$ *then the number of solutions of* (6.33) *in* $z\in K_0$ *is at most* 32.

PROOF. We apply theorem 5.1 with n=3, B=0.846, $C=8P\Delta_S^{1/2}$ and $W(\zeta)=\Omega_S(z)$ to (6.33). Note that by (6.22), $W(\zeta)\geq h(\omega\zeta^3)$. Also ζ is a bilinear function of z, hence to each value of ζ corresponds at most one value of z. If we restrict ourselves to those solutions of (6.33) with $\Omega_S(z)\geq C=8P\Delta_S^{1/2}$, then (6.33) is equivalent to a system of inequalities of type (5.3) in the variable ζ. For our choice of B we have that $\ell_0=64$ (where ℓ_0 is defined by (5.4)) and k=12 (where k is defined by (5.5)). Hence by theorem 5.1, (6.33) has at most *twelve* solutions in $z\in K_0$ with

$$\Omega_S(z) \geq U_1 := \left(2^{28}\left(3(8P\Delta_S^{1/2})^B\right)^6\right)^{1/(6B-5)}. \tag{6.39}$$

We shall now count the solutions of (6.33) with $\Omega_S(z)<U_1$. Note that if T is the constant defined in lemma 6.5 then

$$\begin{aligned}\log(TU_1) &= \left(\frac{3(1-B)}{2(3B-2)}+\frac{3B}{6B-5}\right)\log\Delta_S + \left(\frac{6B}{6B-5}-\frac{3B}{3B-2}\right)\log P + \\ &+ \left(\frac{18B+28}{6B-5}-\frac{3(3B+1)}{3B-2}\right)\log 2 + \frac{6\log 3}{6B-5} \\ &\leq 33.8251\log\Delta_S + 62.0731\log P + 467.313.\end{aligned} \tag{6.40}$$

Firstly we prove (i). We apply lemma 6.5 with U_1 as defined in (6.39) and with $U_0=(1/2)7^{7.5}P^5$, B=0.846. Then

$$\begin{aligned}\log(TU_0) &= \frac{3(1-B)}{2(3B-2)}\log\Delta_S + (5-\frac{3B}{3B-2})\log P + (7.5\log 7-\frac{12B+1}{3B-2}\log 2) \\ &\geq 0.421\log\Delta_S + 0.281\log P + 0.226,\end{aligned}$$

$$3B-1 = 1.538. \tag{6.41}$$

Hence by (6.40),

$$1 + \frac{\log(\log(TU_1)/\log(TU_0))}{\log(3B-1)}$$
$$< 1 + \log\left(\frac{33.825\log\Delta_S+62.073\log P+467.313}{0.42\log\Delta_S+0.28\log P+0.226}\right)\Big/\log 1.538$$
$$\le 1 + \log(467.313/0.226)/\log 1.538 = 18.73...$$

This implies that (6.33) has at most 12+18=30 solutions satisfying (6.38).

Now we prove (ii). Note that, by (6.35), (6.33) has at most one solution with $\Omega_S(z)<\Delta_S/64P$. We apply lemma 6.5 with U_1 as in (6.39) and with $U_0=\Delta_S/64P, B=0.846$. Put $Q=\Delta_S/P^4$. Then

(6.42) $\qquad Q \ge 13^5 P.$

On noting that $P\le 13^{-5}Q$, $\Delta_S\ge 13^{-20}Q^5$, we deduce from (6.40) that

$$\log(TU_1) \le 33.825(5\log Q - 20\log 13) + 62.073(\log Q - 5\log 13) + 467.313$$
$$\le 231.198\log Q - 2063.945.$$

Moreover,

$$\log(TU_0)$$
$$= \left(\frac{3(1-B)}{2(3B-2)}+1\right)\log\Delta_S - \left(\frac{3B}{3B-2}+1\right)\log P - \left(\frac{3(3B+1)}{3B-2}+6\right)\log 2$$
$$= \frac{3B-1}{2(3B-2)}\log Q - \left(6+\frac{3(3B+1)}{3B-2}\right)\log 2 \ge 1.42\log Q - 17.834 .$$

Hence by (6.41),(6.42) and $P\ge 1$,

$$1 + \frac{\log(\log(TU_1)/\log(TU_0))}{\log(3B-1)}$$
$$\le 1 + \log\left(\frac{231.198\log Q - 2063.945}{1.42\log Q - 17.834}\right)\Big/\log 1.538$$
$$\le 1 + \log\left(\frac{231.198\times 5\log 13 - 2063.945}{1.42\times 5\log 13 - 17.834}\right)\Big/\log 1.538 = 19.06...$$

Therefore, (6.33) has at most 12+1+19=32 solutions in $z\in K_0$ if $\Delta_S\ge(13P)^5$. This completes the proof of lemma 6.6. □

PROOF OF THEOREM 6.3 FOR n=3. Let $P=A^{1/m}$ (where m is the degree of the algebraic number field K) and $S=S_\infty(K)$. Suppose that (6.8) holds with n=3. Then we have by (4.15), (4.8) and (6.14) that

$$\Delta_S = N_M(a)^{2/[M:\mathbb{Q}]} = N_M(3d_M(f))^{1/[M:\mathbb{Q}]} = N_K(3d_K(f))^{1/m}$$
$$\geq N_K(d_K(f))^{1/m} \geq (13A^{1/m})^5.$$

Hence by lemma 6.6 (ii), (6.33) has at most 32 solutions in $z\in K_0$. Note that for B=0.846, $R(B)=(1-B)^{-1}B^{B/(B-1)}<49/3$. Hence by lemma 6.3, there are at most $(9/49)7^{2(r_1+r_2)}$ distinct systems (6.33) such that each solution z of (6.13) (or (6.17)) belonging to K_0 satisfies at least one among these. Hence the total number of solutions of (6.13) (including the ones with $\xi_1\eta_1=0$) is at most

$$2 + \frac{9}{49}\times 32\times 7^{2(r_1+r_2)} < 6\times 7^{2(r_1+r_2)}.$$

This proves theorem 6.3 for n=3. □

PROOF OF THEOREM 6.1 FOR n=3. We apply lemma 6.6 (i) with P=1 and $S=S_0$, where S_0 is the set consisting of the prime ideals appearing in (6.12) and the infinite primes on K. Thus we obtain, in combination with lemma 6.3, $R(B)<49/3$ and (6.21), that the number of solutions of (6.12) with $z\in K_0$, $h(\omega\zeta^3)\geq 7^{7.5}/2$ is at most

$$\frac{9}{49}\times 30\times 7^{2(r_1+r_2+t)} < 6\times 7^{2(r_1+r_2+t)}.$$

We state this as a lemma for later purposes.

LEMMA 6.7. *Let* $f(z)$ *be a polynomial with coefficients in* K *and of degree* 3 *with only simple zeros. Let* α,β *be the constants and let* ξ,η *be the linear forms corresponding to the cubic form* $y^3f(x/y)$ *as constructed in lemma* 3.2. *Let* $p_1,\dots,p_t$ *be distinct prime ideals in* K. *Then the number of solutions of*

$$\frac{<f(z)>_K}{c_K(f)<1,z>_K^3} = p_1^{k_1}\dots p_t^{k_t} \quad \text{in } z\in K^*,\ k_1,\dots,k_t\in\mathbb{Z}_{\geq 0} \tag{6.12}$$

with

(6.43) $\qquad \xi(z,1)\eta(z,1) \neq 0\ ,\ h\left(\frac{\beta\eta(z,1)^3}{\alpha\xi(z,1)^3}\right) \geq \frac{1}{2}\times 7^{7.5}$

is at most

$$6\times 7^{2(r_1+r_2+t)}.$$

It is possible to derive an upper bound for the number of remaining solutions of (6.12) by counting the algebraic numbers of degree at most 2m and height at most $7^{7.5}/2$. However, by another method it is possible to improve this. Note that either $\omega\zeta^3 \in K$ or, by (6.31), $\omega\zeta^3$ and $(\omega\zeta^3)^{-1}$ are conjugate over K. In both cases, the number $\kappa := \omega\zeta^3 + (\omega\zeta^3)^{-1}$ belongs to K, provided that $z \in K_0$. Observe that for given κ, there are at most two possible values for $\omega\zeta^3$, hence at most six for ζ and therefore at most six for z. Furthermore, by (4.28) and (4.31), we have for the solutions of (6.12) not satisfying (6.43) that either $z \in K\backslash K_0$ or

$$h(\kappa) \leq 2h(\omega\zeta^3)^2 \leq \frac{1}{2}\times 7^{15}.$$

Hence by lemma 4.2 the number of solutions of (6.12) which do not satisfy (6.43) is at most

$$2 + 6\times\frac{m}{2}((7^{15})^m+1))^{m+1} \leq 7^{15(m+1)^2}.$$

This completes the proof of theorem 6.1 for n=3. □

§6.4. Proofs of theorems 6.1, 6.3 and 6.4.

First of all, we shall prove theorems 6.1 and 6.3 in the general case, i.e. for all integers n with $n \geq 3$. As usual, K is an algebraic number field with r_1 real and r_2 complex primes. We shall assume that the polynomial f(z) appearing in both theorem 6.1 and theorem 6.3 is monic, i.e. has leading coefficient equal to 1, which is clearly no restriction. When speaking of a *divisor* of f we shall mean a monic polynomial with coefficients in some extension of K which divides f.

Let K" be the smallest extension of K containing the zeros of f. In order to prove theorems 6.1 and 6.3 in the general case, we choose a suitable divisor g of f. In the case of theorem 6.1 we choose for g(z) an arbitrary cubic divisor of f with non-zero discriminant. Clearly, we may

assume that g(z) has its coefficients in K". In the case of theorem 6.3 we have to be more careful. Note that in that case, f has non-zero discriminant. Since f has degree n, f has n distinct zeros in K", $\zeta_1,\ldots,\zeta_n$ say. For each pair of zeros ζ_i,ζ_j with $i\neq j$ we put

$$d_{ij} = \frac{<\zeta_i-\zeta_j>_{K"}}{<1,\zeta_i>_{K"}<1,\zeta_j>_{K"}} .$$

Then by (4.12),

$$d_{K"}(f) = \prod_{i>j} d_{ij}^2 . \tag{6.44}$$

Let g(z) be an arbitrary cubic divisor of f(z), $g(z)=(z-\zeta_{i_1})(z-\zeta_{i_2})(z-\zeta_{i_3})$ say. Then

$$d_{K"}(g) = d_{i_1i_2}^2 d_{i_2i_3}^2 d_{i_3i_1}^2 . \tag{6.45}$$

Let G be the collection of all cubic divisors of f. Then by (6.44) and (6.45),

$$\prod_{g\in G} d_{K"}(g) = \prod_{1\le i<j<k\le n} d_{ij}^2 d_{jk}^2 d_{ki}^2 = d_{K"}(f)^{n-2}.$$

Now we choose g as the cubic divisor of f for which $N_{K"}(d_{K"}(g))$ is maximal. Then, by the fact that $|G|=\binom{n}{3}$,

$$N_{K"}(d_{K"}(g)) \ge N_{K"}(d_{K"}(f))^{6/n(n-1)}. \tag{6.46}$$

Thus we have chosen a suitable divisor g of f both in the case of theorem 6.1 and of theorem 6.3.

Let K' be the smallest extension of K containing the coefficients of g. Then

$$[K':K] \le \binom{n}{3}. \tag{6.47}$$

For let $g(z)=z^3+\alpha z^2+\beta z+\gamma$ and let σ be a K-isomorphism of K'. Then σ is completely determined by its action on α,β,γ. Since $\sigma(\alpha),\sigma(\beta),\sigma(\gamma)$ are the elementary symmetrical functions of three of the zeros of f, we have at most $\binom{n}{3}$ possibilities for the triple $(\sigma(\alpha),\sigma(\beta),\sigma(\gamma))$ and hence at most $\binom{n}{3}$ for σ.

Note that $f(z)=g(z)k(z)$ for some polynomial $k(z)\in K'[z]$. Hence, by (4.5),

$$\frac{<f(z)>_{K'}}{c_{K'}(f)<1,z>_{K'}^{n}} = \left(\frac{<g(z)>_{K'}}{c_{K'}(g)<1,z>_{K'}^{3}}\right)\left(\frac{<k(z)>_{K'}}{c_{K'}(k)<1,z>_{K'}^{n-3}}\right) .$$

Both ideals in the right-hand side of this equality are integral, hence

$$\frac{<g(z)>_{K'}}{c_{K'}(g)<1,z>_{K'}^{3}} \supset \frac{<f(z)>_{K'}}{c_{K'}(f)<1,z>_{K'}^{n}} . \tag{6.48}$$

Using (6.46), (6.47), (6.48) it is not difficult to complete the proofs of theorem 6.1 and theorem 6.3.

PROOF OF THEOREM 6.1. Let $P_1,\dots,P_u$ be the prime ideals in K' lying above the prime ideals $p_1,\dots,p_t$ appearing in (6.3). By (6.48), for each solution $(z,k_1,\dots,k_t)$ of (6.3) there are non-negative integers $\ell_1,\dots,\ell_u$ such that

$$\frac{<g(z)>_{K'}}{c_{K'}(g)<1,z>_{K'}^{3}} = P_1^{\ell_1}\dots P_u^{\ell_u} . \tag{6.49}$$

By (6.47), $[K':\mathbb{Q}]\le\binom{n}{3}m, u\le\binom{n}{3}t$ and K' has at most $\binom{n}{3}(r_1+r_2)$ infinite primes. Hence by theorem 6.1 in case n=3 the number of solutions of (6.49) in $z\in K^*$ (even in $z\in K'^*$) and $\ell_1,\dots,\ell_u\in\mathbb{Z}_{\ge 0}$ is at most

$$7^{15\left(\binom{n}{3}m+1\right)^2} + 6\times 7^{2\binom{n}{3}(r_1+r_2+t)} .$$

This completes the proof of theorem 6.1. □

PROOF OF THEOREM 6.3. Put $A'=A^{[K':K]}$. Then by (6.48) and (4.8), we have for each solution z of (6.9),

$$N_{K'}\left(\frac{<g(z)>_{K'}}{c_{K'}(g)<1,z>_{K'}^{3}}\right) \le A'. \tag{6.50}$$

Furthermore, by (6.46), (4.8) and (6.8),

$$\begin{aligned} N_{K'}(d_{K'}(g)) &\ge N_{K'}(d_{K'}(f))^{6/n(n-1)} = N_K(d_K(f))^{6[K':K]/n(n-1)} \\ &\ge \left(13^{[K':\mathbb{Q}]}A'\right)^5. \end{aligned}$$

Since K' has at most $\binom{n}{3}(r_1+r_2)$ infinite primes, we have by theorem 6.3 in case n=3 that (6.50) has at most

$$6\times 7^{2\binom{n}{3}(r_1+r_2)}$$

solutions in $z\in K^*$ (even in $z\in K'^*$). This proves theorem 6.3 completely. □

We have just made some very rough estimates. Firstly, we counted in fact the solutions of (6.49),(6.50) respectively in K' instead of K. It would be of interest to refine our arguments in such a way that an upper bound for the number of solutions in K can be derived which is essentially better than ours. Secondly, it is possible to improve theorem 6.3 in several cases. For if f(z) has all its zeros in K then the factor $\binom{n}{3}$ in the upper bound for the number of solutions of (6.9) can be dropped. If we have the other extremal case, i.e. $[K'':K]=n!$ then all ideals $\langle g(z)\rangle_{K''}c_{K''}(g)^{-1}\langle 1,z\rangle_{K''}^{-3}$ with g belonging to the set G of cubic divisors of f are conjugate over K for $z\in K$. Hence the number

$$N_{K''}\left(\frac{\langle g(z)\rangle_{K''}}{c_{K''}(g)\langle 1,z\rangle_{K''}^{3}}\right)$$

does not depend on the choice of g. We have also that

$$\prod_{g\in G} g(z) = f(z)^{\binom{n-1}{2}}.$$

Hence, if g is any cubic divisor of f and if K' is the smallest extension of K containing the coefficients of g, we have by (6.47) and $\binom{n-1}{2}/\binom{n}{3}=3/n$,

$$N_{K'}\left(\frac{\langle g(z)\rangle_{K'}}{c_{K'}(g)\langle 1,z\rangle_{K'}^{3}}\right) = N_{K'}\left(\frac{\langle f(z)\rangle_{K'}}{c_{K'}(f)\langle 1,z\rangle_{K'}^{n}}\right)^{3/n}.$$

Therefore, the constant A' appearing in (6.50) can be replaced by $A'^{3/n}$. Furthermore, we have that (6.46) holds for all $g\in G$ (even with equality). Hence, arguing similarly as in the proof of theorem 6.3, we have that (6.9) has at most

$$6\times 7^{2\binom{n}{3}(r_1+r_2)}$$

solutions in $z\in K^*$ even if

$$N_K(d_K(f)) \geq \left(13^m A^{3/n}\right)^{5n(n-1)/6},$$

provided that $[K'':K]=n!$.

PROOF OF THEOREM 6.4. Let $F(x,y)$ be the binary form appearing in (6.1). Then $F(1,0)\neq 0$. Put $f(z)=F(z,1)$, $A=|N_{K/\mathbb{Q}}(\gamma)|/N_K(c_K(f))$. Then f has degree n and at least three distinct zeros. We assume that (6.10) is solvable. Then $A\geq 1$. Clearly for each solution (x,y) of (6.10) we have

$$N_K\left(\frac{<f(x/y)>}{c_K(f)<1,x/y>^n}\right) \leq A. \tag{6.51}$$

Moreover, if $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ are the prime ideals in K dividing $<\gamma>$ then for each solution (x,y) of (6.10) there are non-negative integers $k_1,\ldots,k_t$ such that

$$\frac{<f(x/y)>}{c_K(f)<1,x/y>^n} = \mathfrak{p}_1^{k_1}\ldots\mathfrak{p}_t^{k_t}. \tag{6.52}$$

For every $z\in K^*$ there are at most n solutions (x,y) of (6.10) such that $x/y=z$. For suppose $(x_1,y_1),(x_2,y_2)$ are solutions of (6.10) with $x_1/y_1=x_2/y_2$. Then there is a $\delta\in K^*$ such that $x_2=\delta x_1, y_2=\delta y_1$. But then

$$\gamma = F(x_2,y_2) = \delta^n F(x_1,y_1) = \delta^n\gamma,$$

hence $\delta^n=1$. Therefore, we have at most n possibilities for δ. In view of (6.52), the first part of theorem 6.4 follows easily from theorem 6.1.

Now we suppose that F has non-zero discriminant $D(F)$. Then, by (4.11),

$$\begin{aligned} N_K(d_K(f)) &= N_K(c_K(f))^{-2n+2}\,|N_{K/\mathbb{Q}}(D(F))| \\ &\geq \left(13^m|N_{K/\mathbb{Q}}(\gamma)|/N_K(c_K(f))\right)^{5n(n-1)/6} = (13^m A)^{5n(n-1)/6}. \end{aligned}$$

Now the second part of theorem 6.4 follows easily from (6.51) and theorem 6.3. □

§6.5. Sketch of the proof of theorem 6.2.

As before, let K be an algebraic number field of degree m with r_1 real and r_2 complex primes, let $\omega\in K^*$, let $n\in\mathbb{Z}$ with $n\geq 3$ and let $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ be distinct prime ideals in K. Put $S=S_\infty(K)\cup\{\mathfrak{p}_1,\ldots,\mathfrak{p}_t\}$. Let $\theta_1,\ldots,\theta_n$ be

the n-th roots of ω and put $L=K(\theta_1,\ldots,\theta_n)$. For every valuation $|.|_v$ on K with $v\in S$ we choose a fixed extension to L which is also denoted by $|.|_v$. We consider the equation

$$\frac{<1-\omega z^n>}{<1,\omega z^n>} = p_1^{k_1}\ldots p_t^{k_t} \quad \text{in } z\in K^*, k_1,\ldots,k_t\in\mathbb{Z}_{\geq 0}. \tag{6.6}$$

Solutions $(z,k_1,\ldots,k_t)$ of (6.6) are shortly denoted by z.

For every solution z of (6.6) we have that $|1-\omega z^n|_v=\max(1,|\omega z^n|_v)$ for $v\notin S$. By the product formula (4.17), every solution z of (6.6) satisfies

$$\prod_{v\in S}|1-\omega z^n|_v \prod_{v\notin S}\max(1,|\omega z^n|_v) = 1. \tag{6.53}$$

Completely similar to (6.23) one can show that for $z\in K^*, v\in S$,

$$|1-\omega z^n|_v \geq |n|_v 2^{-ns(v)}\max(1,|\omega z^n|_v)\min_{1\leq i\leq n}(1,|1-\theta_i z|_v).$$

Hence by (6.53), solutions of (6.6) satisfy

$$\prod_{v\in S}\left(|n|_v 2^{-ns(v)}\min_{1\leq i\leq n}(1,|1-\theta_i z|_v)\right)\prod_{v\in\overline{S}(K)}\max(1,|\omega z^n|_v) \leq 1.$$

Therefore, by (4.19) and (4.22),

$$\prod_{v\in S}\min_{1\leq i\leq n}(1,|1-\theta_i z|_v) \leq 2^n h(\omega z^n)^{-1}. \tag{6.54}$$

Let B be a real with $1/2<B<1$ and put $s=r_1+r_2+t$. By lemma 6.2 there exists a set of at most $R(B)^{s-1}=\left((1-B)^{-1}B^{B/(B-1)}\right)^{s-1}$ s-tuples $(\Gamma_v)_{v\in S}$ with $\Gamma_v\geq 0$ for $v\in S$ and $\sum_{v\in S}\Gamma_v=B$, such that each solution z of (6.54) with $z\in K^*$ satisfies at least one of the systems of inequalities

$$\min_{1\leq i\leq n}(1,|1-\theta_i z|_v) \leq \left(2^n h(\omega z^n)^{-1}\right)^{\Gamma_v} \quad \text{for } v\in S.$$

We finally obtain, that each solution z of (6.6) satisfies a system of inequalities of the type

$$\min(1,|1-\theta_v z|_v) \leq \left(2^n h(\omega z^n)^{-1}\right)^{\Gamma_v} \quad \text{for } v\in S, \tag{6.55}$$

where θ_v is an n-th root of ω, belonging to L. Clearly, for each θ_v we have

at most n possibilities. Since we have at most $R(B)^{s-1}$ possibilities for the tuple $(\Gamma_v)_{v\in S}$, the tuple $((\theta_v)_{v\in S},(\Gamma_v)_{v\in S})$ can be chosen from a set of at most $R(B)^{-1}(nR(B))^s$ of such tuples, which does not depend on z.

Put $B=1/2+1/(n-1/8)$, $C=2^n$. Then $R(B)=U(n)$. Hence the first part of theorem 6.2 follows if we have shown that each system of inequalities (6.55) has at most 2U(n) solutions in $z\in K^*$ with $h(\omega z^n)\geq 3^{n+10}$. The proof of this fact is rather elaborate and we shall give only a brief sketch of it.

Put $A=\left(2^{(n+1)(n+4)}(nC^B)^{2n}\right)^{1/(2nB-n-2)}$ (with the just chosen values for B and C). The solutions z of (6.55) with $h(\omega z^n)\geq 3^{n+10}$ are divided into two classes:

I: the solutions with $h(\omega z^n)\geq A$;
II: the solutions with $3^{n+10}\leq h(\omega z^n)<A$.

The number of solutions in class I can be estimated from above by means of theorem 5.1, on noting that all solutions of (6.55) in class I satisfy $h(\omega z^n)>C$, whence $|1-\theta_v z|_v \leq 1$ for $\Gamma_v>0$. By remark 2 of §5.1, class I contains at most one solution if $n\geq 9$. The number of solutions in class II can be estimated from above by means of lemma 5.1, using the same type of argument as in lemma 2.11 or lemma 6.6. It follows in fact, that the number of solutions in class II is at most 6 if $n\geq 9$. Since $U(n)>4$ for all $n\geq 3$, it suffices to prove that the union of the classes I and II contains at most 2U(n) solutions for $3\leq n\leq 8$. This can be done by straightforward computation.

The proof of the second part of theorem 6.2 is an immediate consequence of lemma 4.2, for by that lemma, the number of algebraic numbers with degree at most m and height at most 3^{n+10} does not exceed

$$\frac{m}{2}\left((2\times 3^{n+10})^m+1\right)^{m+1} \leq \frac{1}{n}(2\times 3^{n+10})^{(m+1)^2},$$

while for each given value of ωz^n, there are at most n solutions z of (6.6).

□

REMARK. From the sketch of the proof given above it is clear that it is advantageous, to choose B as small as possible, for then R(B) is small. By the result given in theorem 5.1, we have to choose B larger than $1/2+1/n$. If we would have a result of the same type as theorem 5.1, but with a lower bound for B in the order of $o(1)$ (e.g. $B>2n^{-1/2}$ in case of Siegel's method or $B>2/n$ in case of Roth's method) B could be chosen such that R(B)

decreases to 1 for n going to infinity.

CHAPTER 7. SOME APPLICATIONS.

In the first part of this chapter we shall consider linear equations in two S-units. These can be transformed into certain Thue-Mahler equations. In the second part we shall deal with a special case of Catalan's equation $x^m-y^n=1$ in $x,y,m,n\in\mathbb{N}\setminus\{1\}$, namely the case where m,n are fixed. We shall reduce this equation to finitely many equations of the type (6.6). The same procedure can be followed for equations of the type $y^m=f(x)$ in $x,y\in\mathbb{Z}$ (where $f(x)\in\mathbb{Z}[x]$ and $m\in\mathbb{N}\setminus\{1\}$) and $|ax^m-by^n|=p_1^{k_1}\ldots p_t^{k_t}$ in $x,y,k_1,\ldots,k_t\in\mathbb{Z}$ (where $a,b,m,n\in\mathbb{Z}$, $ab\neq 0, m>1, n>1, mn\geq 6$ and $p_1,\ldots,p_t$ are distinct primes). (cf.§6.1). However, in case of Catalan's equation we have less technical difficulties.

PART I. ON EQUATIONS IN S-UNITS.

§7.1. Introduction.

In 1961, Lewis and Mahler proved the following ([L/M],pp.360-362):

let $p_{11},\ldots,p_{1r},p_{21},\ldots,p_{2s},p_{31},\ldots,p_{3t}$ *be fixed distinct primes of which the smallest and the largest are* P *and* Q *say. Then the equation*

$$p_{11}^{x_{11}}\ldots p_{1r}^{x_{1r}}+p_{21}^{x_{21}}\ldots p_{2s}^{x_{2s}}=p_{31}^{x_{31}}\ldots p_{3t}^{x_{3t}} \quad \textit{in } x_{11},\ldots,x_{3t}\in\mathbb{Z}_{\geq 0} \tag{7.1}$$

has at most

$$\left(c_1(r+s)\,\frac{\log Q}{\log P}\right)^{r+s}+c_2^{r+s+t+1}$$

solutions, where c_1,c_2 *are absolute constants.*

In the proof of this fact they proceeded in the following way. Let n be a fixed integer with $n\geq 3$. For each integer x_{ij} appearing in (7.1) define integers X_{ij},Y_{ij} with $Y_{ij}\in\{0,1,\ldots,n-1\}$ such that $x_{ij}=nX_{ij}+Y_{ij}$. Then, on putting $a=p_{11}^{Y_{11}}\ldots p_{1r}^{Y_{1r}}, b=p_{21}^{Y_{21}}\ldots p_{2s}^{Y_{2s}}, X=p_{11}^{X_{11}}\ldots p_{1r}^{X_{1r}}, Y=p_{21}^{X_{21}}\ldots p_{2s}^{X_{2s}}$, one obtains

$$aX^n+bY^n=p_{31}^{x_{31}}\ldots p_{3t}^{x_{3t}}. \tag{7.2}$$

Note that we have at most n^{r+s} possibilities for the pair (a,b). Clearly, from upper bounds for the number of solutions of equations of the type (7.2) one can derive an upper bound for the number of solutions of (7.1).

Lewis and Mahler considered it as a problem of great interest to decide whether the number of solutions of (7.1) can be bounded above by a constant depending on r,s,t only and not on the primes $p_{11},\dots,p_{3t}$. However there is a second method of dealing with (7.1) which together with the result of Lewis and Mahler on the number of solutions of the Thue-Mahler equation (cf.§6.1 or [L/M]) yields such a bound. Put $X=p_{11}^{x_{11}}\dots p_{1r}^{x_{1r}}$, $Y=p_{21}^{x_{21}}\dots p_{2s}^{x_{2s}}$, $F(X,Y)=XY(X+Y)$, where $(x_{11},\dots,x_{3t})$ is a solution of (7.1). Then clearly,

$$F(X,Y) = p_{11}^{x_{11}}\dots p_{1r}^{x_{1r}} p_{21}^{x_{21}}\dots p_{2s}^{x_{2s}} p_{31}^{x_{31}}\dots p_{3t}^{x_{3t}}. \tag{7.3}$$

Note that F(X,Y) is a binary cubic form of non-zero discriminant and that an upper bound for the number of solutions of (7.3) in positive integers X,Y with (X,Y)=1 induces the same upper bound for the number of solutions of (7.1). We can not directly apply the result of Lewis and Mahler on the Thue-Mahler equation since F is divisible by both X and Y. But this difficulty can be solved by replacing F by an equivalent form which is not divisible by X or Y, for example (X+Y)(X+2Y)(2X+3Y). Now the result of Lewis and Mahler yields, that the number of solutions of (7.1) can be estimated from above by a constant depending on r+s+t only.

We shall generalise the second method of dealing with (7.1) and apply it to more general equations. Let K be an algebraic number field of degree m with r_1 real and r_2 complex primes. Let S be a finite set of primes on K, containing the infinite primes. An S-unit is an element $\alpha\in K$ with the property that $|\alpha|_v=1$ for every $v\notin S$. We shall deal with the following equation:

$$\lambda x+\mu y = 1 \quad \text{in S-units } x,y\in K, \tag{7.4}$$

where λ,μ are, for the time being, non-zero elements of K. When both sides of (7.1) are divided by the right-hand side of (7.1) we obtain an equation of type (7.4) with $K=\mathbb{Q}$, $\lambda=\mu=1$ and $S=\{p_\infty,p_{11},\dots,p_{3t}\}$ where p_∞ denotes the infinite prime on $\mathbb{Q}$.

Under very restrictive conditions imposed on λ,μ, Györy [Gy] derived

a sharp upper bound for the number of solutions of (7.4), both in the archimedean and in the p-adic case. He showed the following:

let β *be an algebraic integer such that* $\alpha_1 := \beta\lambda, \alpha_2 := \beta\mu$ *are algebraic integers. Let* S *be a finite set of primes on* K *consisting of* r_1+r_2 *infinite and* t *finite primes. Suppose the finite primes of* S *ly above prime numbers in* $\mathbb{Z}$ *of which the largest equals* P. *Let* ε *be a real number with* $0<\varepsilon\leq 1$. *Put*

$$M_i = \prod_{v\in S} |\alpha_i|_v \quad \text{for } i=1,2, \quad M = \prod_{v\in S} |\beta|_v.$$

If $\min_i M_i \leq M^{1-\varepsilon}$ *and* $\log M > C$, *where* C *is an effectively computable constant depending on* ε, P, K *and* t *only, then* (7.4) *has at most* r_1+r_2+4t *solutions.*†

Györy gives an explicit, but very complicated expression for C. We shall derive an upper bound for the number of solutions of (7.4) which is not as sharp as that of Györy, but only under the restriction that λ,μ are algebraic integers in K.

THEOREM 7.1. *Let* S *be a finite set of primes on* K, *containing all infinite primes and exactly* t *finite primes. Let* λ,μ *be non-zero elements of* O_K. *Then*
(i) (7.4) *has at most*

$$6\times 7^{2(r_1+r_2+t)}$$

solutions with

$$h(\lambda x/\mu y) \geq 206$$

and
(ii) (7.4) *has at most*

$$412^{(m+1)^2}$$

†The reader is warned, that Györy's notations differ from ours. For example he uses valuations $\|.\|_v$ which are exactly the m-th powers of ours, where m is the degree of K. We have rewritten Györy's result in our notations.

solutions with

$$h(\lambda x/\mu y) < 206.$$

The upper bound in theorem 7.1 depends on r_1, r_2, t only and does not depend on λ, μ. It would be of interest to derive such an upper bound for the number of solutions of (7.4) if λ, μ are arbitrary non-zero numbers in K.

In the special case $K=\mathbb{Q}$ we have the following generalisation and improvement of the result of Lewis and Mahler on (7.1).

THEOREM 7.2. *Let* a, b *be non-zero rational integers. Let* $p_1, \ldots, p_t$ *be distinct prime numbers. Then the number of pairs of rational numbers* (x,y) *for which the absolute values of the numerators and denominators are composed of primes from* $\{p_1, \ldots, p_t\}$ *and for which*

$$ax+by = 1 \tag{7.5}$$

is at most

$$296 \times 7^{2t}.$$

§7.2. Proofs of theorems 7.1 and 7.2.

PROOF OF THEOREM 7.1. We shall use the same notations as in §7.1. Thus K is an algebraic number field of degree m with r_1 real and r_2 complex primes, λ, μ are non-zero integers in K and S is a finite collection of primes given by $S_\infty(K) \cup \{p_1, \ldots, p_t\}$, where $p_1, \ldots, p_t$ are distinct prime ideals. Put $F(x,y)=xy(\lambda x+\mu y)$. If (x,y) is a pair of S-units satisfying (7.4) then there exists an S-unit δ such that $\delta x, \delta y \in \mathcal{O}_K$. But δ must belong to the integral ideal generated by λ and μ, hence $\langle \lambda, \mu \rangle$ is solely composed of prime ideals from $p_1, \ldots, p_t$. This in turn implies that

$$\frac{\langle F(x,y) \rangle}{\langle \lambda, \mu \rangle \langle x, y \rangle^3} = p_1^{k_1} \ldots p_t^{k_t} \tag{7.6}$$

for certain non-negative integers $k_1, \ldots, k_t$. Since $F(1,0)=0$, we can not directly apply the theory of chapter 6. In order to avoid this difficulty, we choose a rational integer k such that $F(1,k) \neq 0$ and k is not an S-unit. Put $F^*(x,y)=F(x,kx+y)$. Then $F^*(1,0) \neq 0$. Furthermore, it is easy to check,

that $c_K(F^*)=c_K(F)=\langle\lambda,\mu\rangle_K$. For any solution (x,y) of (7.4), define numbers x',y' such that x'=x, y'=y-kx and put z=x'/y'. Then to every value of z corresponds at most one pair of S-units (x,y) with $\lambda x+\mu y=1$. In view of (7.6) we have for every pair of S-units (x,y) satisfying (7.4),

$$\frac{\langle F^*(z,1)\rangle}{c_K(F^*)\langle 1,z\rangle^3} = p_1^{k_1}\ldots p_t^{k_t} \tag{7.7}$$

for certain non-negative integers $k_1,\ldots,k_t$. Since $F^*(z,1)$ is a polynomial of degree 3 in z we can apply theorem 6.1. However, we can derive a better result by applying lemma 6.7 directly. Let α,β be the constants and let ξ, η be the linear forms corresponding to F(x,y) as constructed in lemma 3.2. Let $\alpha^*,\beta^*,\xi^*,\eta^*$ be the constants, linear forms respectively, corresponding in the same way to $F^*(x,y)$. By lemma 6.7, there are at most $6\times 7^{2(r_1+r_2+t)}$ numbers z in K^* satisfying (7.7) such that

$$\xi^*(z,1)\eta^*(z,1) \neq 0,\quad h\left(\frac{\alpha^*\xi^*(z,1)^3}{\beta^*\eta^*(z,1)^3}\right) \geq \tfrac{1}{2}\times 7^{7.5}. \tag{7.8}$$

Now $\alpha\xi^3,\beta\eta^3$ can be expressed in terms of invariants and covariants of F (cf. (3.8)). Hence

$$\alpha\xi(x,y)^3 = \alpha^*\xi^*(x',y')^3,\quad \beta\eta(x,y)^3 = \beta^*\eta^*(x',y')^3.$$

By (7.8),(7.7) and the fact that every z corresponds to at most one solution (x,y) of (7.4), the number of pairs of S-units (x,y) satisfying (7.4) and

$$\alpha\xi(x,y)^3\beta\eta(x,y)^3 \neq 0,\quad h\left(\frac{\alpha\xi(x,y)^3}{\beta\eta(x,y)^3}\right) \geq \tfrac{1}{2}\times 7^{7.5} \tag{7.9}$$

is at most

$$6\times 7^{2(r_1+r_2+t)}. \tag{7.10}$$

Note that F has a non-zero discriminant, namely $(\lambda\mu)^2$, and quadratic covariant

$$H(x,y) = \lambda^2x^2+\lambda\mu xy+\mu^2y^2 = (\lambda x-\rho\mu y)(\lambda x-\rho^2\mu y), \tag{7.11}$$

where ρ is a primitive third root of unity. By (3.10), $\alpha\xi^3$ and $\beta\eta^3$ are the

cubes of linear forms whose product equals H. Furthermore, by (3.9),

$$\alpha\xi^3-\beta\eta^3 = \pm 3\sqrt{-3}\lambda\mu F(x,y)$$

is a cubic form whose coefficient of x^3 equals 0. Hence we have by (7.11), for suitably chosen ρ,

$$\alpha\xi^3 = (\lambda x-\rho\mu y)^3,\ \beta\eta^3 = (\lambda x-\rho^2\mu y)^3. \tag{7.12}$$

Let L be a finite extension of K, containing the third roots of unity. Then, for every $V\in\overline{S}(L)$ and for $x,y\in K^*$ with $(\lambda x/\mu y)^3\neq 1$ we have by (4.23),

$$\begin{aligned}
&\max(|\lambda x-\rho\mu y|_V, |\lambda x-\rho^2\mu y|_V)\\
&\quad = \max(|\lambda x-\rho\mu y|_V, |\lambda x-\rho^2\mu y|_V, |\rho^2\lambda x-\rho\mu y|_V)\\
&\quad \geq 2^{-s(V)}\max(|1-\rho^{-1}|_V|\lambda x|_V, |\rho^2-\rho|_V|\mu y|_V)\\
&\quad \geq 2^{-s(V)}|1-\rho|_V\max(|\lambda x|_V, |\mu y|_V).
\end{aligned}$$

Hence, by (7.12),(4.27),(4.22) and the product formula (4.17),

$$\begin{aligned}
h\left(\frac{\alpha\xi^3}{\beta\eta^3}\right) &= \left(h\left(\frac{\lambda x-\rho\mu y}{\lambda x-\rho^2\mu y}\right)\right)^3 = \prod_{V\in\overline{S}(L)}\max(|\lambda x-\rho\mu y|_V^3, |\lambda x-\rho^2\mu y|_V^3)\\
&\geq \prod_{V\in\overline{S}(L)}\left(2^{-3s(V)}|1-\rho|_V^3\max(|\lambda x|_V^3, |\mu y|_V^3)\right)\\
&= \frac{1}{8}\,h(\lambda x/\mu y)^3.
\end{aligned}$$

By (7.9),(7.10) and the fact that $(8\times(1/2)\times 7^{7.5})^{1/3}=205.79\ldots$, (7.4) has at most $6\times 7^{2(r_1+r_2+t)}$ solutions with $h(\lambda x/\mu y)\geq 206$. This proves the first part of theorem 7.1. The second part follows immediately from lemma 4.2 for by that lemma, the number of algebraic numbers of degree at most m and height at most 206 is at most

$$\frac{m}{2}(412^m+1)^{m+1} \leq 412^{(m+1)^2}.$$ □

PROOF OF THEOREM 7.2. Let $S_1=\{p_1,\ldots,p_t\}$, $S=\{p_\infty\}\cup S_1$. We have to show that the number of solutions of

(7.13) $\quad ax+by = 1 \quad$ in S-units x,y

is at most 296×7^{2t}. If (7.13) is solvable, then the gcd of a and b must be composed solely of primes from S_1. Moreover, if a and b have divisors which are composed solely of primes from S_1, these can be absorbed by x,y respectively. Hence it is no restriction to assume that a,b are coprime to each other and to $p_1 \ldots p_t$ and we shall do so in the sequel.

Let (x,y) be a solution of (7.13). We define integers x',y' such that $x/y=x'/y'$, $y'>0$ and $(x',y')=1$. Then x',y' are uniquely determined by x,y. Moreover, every solution (x,y) of (7.13) is uniquely determined by x/y, whence by x',y'. By (4.26) and by our assumptions on a,b we have

$$h(ax/by) = \max(|ax'|,|by'|) \geq \max(|x'|,y').$$

Hence by theorem 7.1 (i) with $\lambda=a, \mu=b, K=\mathbb{Q}, S=S_1 \cup \{p_\infty\}$, the number of solutions of (7.13) with

$$\max(|x'|,y') \geq 206$$

is at most

$$6\times 7^{2t+2} = 294\times 7^{2t}.$$

Let S_0 be a fixed subset of S_1. We shall consider solutions of (7.13) with the following properties:

(7.14) $\quad \max(|x'|,y') \leq 205$, x' is composed solely of primes from S_0, y' is composed solely of primes from $S_1 \setminus S_0$.

Note that x',y' are completely determined by the integers $w_p(x'), w_p(y')$ for $p \in S_1$ (cf. §4.1) and by the sign of x'. For each solution of (7.13) satisfying (7.14) and for each $p \in S_1$ we have

$$0 \leq w_p(x') \leq \frac{\log 205}{\log 2}, \quad 0 \leq w_p(y') \leq \frac{\log 205}{\log 2}.$$

Let $s=|S_0|$. Then, taking into account the two possibilities for the sign of x', the number of solutions of (7.13) satisfying (7.14) is at most

$$2\left(1+\frac{\log 205}{\log 2}\right)^{s}\left(1+\frac{\log 205}{\log 2}\right)^{t-s} = 2\left(1+\frac{\log 205}{\log 2}\right)^{t}.$$

Since S_1 has at most 2^t possible subsets S_0, the number of solutions of (7.13) with $\max(|x'|,y')\leq 205$ is at most

$$2\left(2\left(1+\frac{\log 205}{\log 2}\right)\right)^{t} \leq 2\times 7^{2t}.$$

This completes the proof of theorem 7.2. □

PART II. ON THE EQUATION OF CATALAN.

§7.3. Introduction.

In 1844, Catalan [Ca] conjectured that the equation

(7.15) $\qquad x^p-y^q = 1 \quad$ in $x,y,p,q\in\mathbb{Z}$, $x>1,y>1,p>1,q>1$

has no other solution than $x=3,y=2,p=2,q=3$. No one has been able to prove this yet. In 1953, Cassels [C 1] independently made the weaker conjecture that (7.15) has at most finitely many solutions and this was proved by Tijdeman [Tij] in 1976. Several special cases of (7.15) have been considered. Wall [W] showed in an elementary way that $(x,y,p,q)=(3,2,2,3)$ is the only solution of (7.15) for which $p>1,q>1$ and x,y are primes. LeVeque [LeV 1] showed that for each given pair of integers x,y at most one pair (p,q) exists with $p>1,q>1$ and $x^p-y^q=1$.

We shall consider the case that p,q are fixed integers, m,n respectively say, with $m>1,n>1$, i.e. we shall consider the equation

(7.16) $\qquad x^m-y^n = 1 \quad$ in $x,y\in\mathbb{Z}$, $x>1,y>1$.

Several results on special cases of this equation are known. In 1738, Euler [Eu] showed that for $m=2,n=3$ the only solution of (7.12) is $x=3,y=2$. V.A. Lebesgue [Le] showed in 1850 that (7.16) is unsolvable for $n=2$ (hence for n even) and $m\neq 3$. Nagell [Na 1] showed in 1921 that (7.16) ia unsolvable for $m=3$ or for $m\neq 2,n=3$. Chao Ko [ChK] showed in 1967 that (7.16) has no solutions for $m=2$ (hence for m even) and $n\neq 3$. Hyyrö [Hy 1] showed in 1964, by using a result of Davenport and Roth [D/R], that for $m\geq 2,n\geq 2,mn\geq 6$, (7.16) has no more than $\exp(631m^2n^2)$ solutions. As an application of

theorem 6.2 we shall improve Hyyrö's result.

THEOREM 7.3. *The number of solutions of*

$$x^m - y^n = 1 \quad \text{in } x,y \in \mathbb{Z} \text{ with } x>1, y>1, \tag{7.16}$$

where m,n *are integers with* $m>1, n>1$, *is at most*

$$(mn)^{\min(m,n)}.$$

§7.4. Proof of theorem 7.3.

In the proof of theorem 7.3 we shall assume that m,n are distinct. This is no restriction, for if x,y are positive integers with $x^n-y^n=1$, then $1 \geq (y+1)^n - y^n \geq ny^{n-1} \geq n$, which is impossible for $n \geq 2$. Secondly, we assume that m,n are prime numbers with $m \geq 5, n \geq 5$. By the historical remarks made in §7.3 this is also no restriction. For every integer $r \geq 3$ we put $K_r = \mathbb{Q}(e^{2\pi i/r})$ and we define h_r to be the class number of K_r. We shall need two lemmas. The first is due to Cassels and is stated without proof (for a proof we refer to [C 1] or [Hy 1]) and the second is a rather bad estimate for h_r in case that r is a prime.

LEMMA 7.1. *If* (x,y) *is a solution of* (7.16) *then* $n \mid x, m \mid y$.

LEMMA 7.2. *Let* r *be a prime number with* $r \geq 3$. *Then* $h_r \leq (r/3)^r$.

PROOF OF LEMMA 7.2. We shall prove the lemma by combining some estimates which can be found in literature. Let K denote an algebraic number field of degree m with r_1 real and r_2 complex primes. Let h,R,D denote the class number, regulator and discriminant of K respectively and let w denote the number of roots of unity in K. Then we have the following estimates:

$$\frac{2R}{w} \geq 0.04 \times e^{0.46r_1 + 0.1r_2}; \tag{7.17}$$

$$h < 4wR^{-1}2^{-r_1}(2\pi)^{-r_2}\left(\frac{be\log|D|}{m-1}\right)^{m-1}|D|^{1/2}, \tag{7.18}$$

$$\text{where } b = \left(1+(\log \pi)/2 + (r_2/m)\log 2\right)^{-1}.$$

The first is due to Zimmert ([Zi], Korollar, p.375) and the second to Siegel ([Si 5], Satz 1).

We now prove lemma 7.2. We assume that r is a prime with $r \geq 23$. Since $h_r = 1$ for $r < 23$ (cf [Wa], p.204) this is no restriction. Put $K_r^{\oplus} = \mathbb{Q}(e^{2\pi i/r} + e^{-2\pi i/r})$. Then $K_r^{\oplus}$ is the maximal totally real subfield of K_r. Let R_r be the regulator of K_r and $R_r^{\oplus}$ that of $K_r^{\oplus}$. Then

$$R_r \geq 2^{(r-3)/2} R_r^{\oplus}.$$

(For this, and the other properties of cyclotomic fields we shall use in the sequel, we refer to [Wa], ch. 1,2,4). On noting that for $K = K_r^{\oplus}$ we have $m = r_1 = (r-1)/2, r_2 = 0, w = 2$ this implies by (7.17) that

$$R_r \geq \frac{1}{50}\left(2^{1/2} e^{0.23}\right)^{r-1}. \tag{7.19}$$

For $K = K_r$ we have $w = 2r, r_1 = 0, r_2 = (r-1)/2, m = r-1, |D| = r^{r-2}, b = (1+(\log(2\pi))/2)^{-1}$, hence by (7.18) and (7.19),

$$\begin{aligned} h_r &< 400 r (2\pi)^{-(r-1)/2} \left(2^{-1/2} e^{-0.23}\right)^{r-1} \times \\ &\qquad \times \left(\frac{e(r-2)\log r}{(r-2)(1+(\log(2\pi))/2)}\right)^{r-2} r^{(r-2)/2} \\ &< 400 \left(\frac{1+(\log(2\pi))/2}{e}\right)^2 2^{1/2} e^{0.23} (2\pi)^{1/2} \times \\ &\qquad \times \left(\frac{2^{-1/2} e^{-0.23} e}{(2\pi)^{1/2}(1+(\log(2\pi)/2)}\right)^{r} r^{r/2} (\log r)^{r-2} \\ &< 890 \times 3^{-r} r^{r/2} (\log r)^{r-2}. \end{aligned}$$

It is easy to check that this is smaller than $(r/3)^r$ for $r \geq 23$. □

We are now going to prove theorem 7.3. Put $\rho = e^{2\pi i/m}$ and let $\mathfrak{p}$ be the prime ideal in K_m generated by $1-\rho$. Then all numbers $1-\rho^k$ $(k = 2, 3, \ldots, m-1)$ also generate $\mathfrak{p}$ and we have

$$\mathfrak{p}^{m-1} = \langle m \rangle. \tag{7.20}$$

Let (x,y) be a solution of (7.16). Then we have by lemma 7.1,

$$x - 1 \equiv x^m - 1 \equiv y^n \equiv 0 \pmod{m}.$$

Hence by (7.20), $w_{\mathfrak{p}}(x-1) \geq m-1$ and $w_{\mathfrak{p}}(x-\rho) = w_{\mathfrak{p}}(x-\rho^2) = \ldots = 1$. But this implies

by (7.20) that in $\mathbb{Z}$

$$(7.21) \qquad w_m\left(\frac{x^m-1}{x-1}\right) = 1, \quad w_m(x-1) \equiv -1 (\mathrm{mod}\ n).$$

Furthermore, by (7.20),

$$\langle x-1, \frac{x^m-1}{x-1}\rangle \supset \langle x-1, x-\rho\rangle\langle x-1, x-\rho^2\rangle \ldots \langle x-1, x-\rho^{m-1}\rangle$$
$$\supset p^{m-1} = \langle m\rangle$$

and similarly,

$$\langle x-\rho, \frac{x^m-1}{x-\rho}\rangle \supset \langle m\rangle.$$

Hence if q is a prime ideal in K_m with $q \neq p$ we have $w_q(x-1) \equiv w_q(x-\rho) \equiv 0 (\mathrm{mod}\ n)$. Together with (7.21) and the fact that $w_p(x-\rho)=1$ this yields that there exists a positive integer ξ and an integral ideal b in K_m such that

$$(7.22) \qquad x-1 = m^{n-1}\xi^n, \quad \langle x-\rho\rangle = \langle 1-\rho\rangle b^n.$$

There are at most h_m ideal classes in K_m whose n-th power is the principal ideal class. Choose in each of these classes a fixed ideal and choose a fixed generator of each of the n-th powers of these ideals. Let G be the set of these generators. Then G has cardinality at most h_m. Let a be the ideal which was chosen in the ideal class of b and let α be the chosen generator of a^n. Then $b=a\langle\eta_1\rangle$ for some $\eta_1 \in K_m$, hence by (7.22),

$$\langle x-\rho\rangle = \langle 1-\rho\rangle\langle \alpha\eta_1^n\rangle,$$

i.e.

$$(7.23) \qquad x-\rho = \varepsilon(1-\rho)\alpha\eta_1^n$$

for some unit ε in O_{K_m}.

Let $\rho_0 = e^{\pi i/m}$ and let $\{\varepsilon_1, \ldots, \varepsilon_s\}$ be a system of fundamental units in K_m, where $s=(m-3)/2$. There exist rational integers $k_0, k_1, \ldots, k_s$ with $0 \leq k_0 \leq 2m-1$ such that

$$\varepsilon = \rho_0^{k_0}\varepsilon_1^{k_1}\dots\varepsilon_s^{k_s}.$$

Put $k_i=n\ell_i+q_i$ for $i=0,1,\dots,s$, where $\ell_i\in\mathbb{Z}$, $q_i\in\{0,1,\dots,n-1\}$ and let $\varepsilon'=\rho_0^{q_0}\varepsilon_1^{q_1}\dots\varepsilon_s^{q_s}$, $\varepsilon''=\rho_0^{\ell_0}\varepsilon_1^{\ell_1}\dots\varepsilon_s^{\ell_s}$. Then, by (7.23),

$$x-\rho = (1-\rho)\varepsilon'\alpha\eta^n, \tag{7.24}$$

where $\eta=\varepsilon''\eta_1$. Put $z=\xi/\eta$, $\omega=m^{n-1}/(1-\rho)\varepsilon'\alpha$. Then ω belongs to the set

$$H = \{m^{n-1}/(1-\rho)\beta\rho_0^{u_0}\varepsilon_1^{u_1}\dots\varepsilon_s^{u_s} \mid \beta\in G, u_0,u_1,\dots,u_s\in\{0,1,\dots,n-1\}\ \}$$

which has cardinality at most $n^{(m-1)/2}h_m$. Now we have by (7.22),(7.24) and $\langle x-1,x-\rho\rangle=\langle 1-\rho\rangle$ that

$$\frac{\langle 1-\omega z^n\rangle}{\langle 1,\omega z^n\rangle} = \frac{\langle (1-\rho)\varepsilon'\alpha\eta^n - m^{n-1}\xi^n\rangle}{\langle (1-\rho)\varepsilon'\alpha\eta^n, m^{n-1}\xi^n\rangle} = \frac{\langle x-\rho-(x-1)\rangle}{\langle x-\rho,x-1\rangle} = \mathcal{O}_{K_m}. \tag{7.25}$$

By theorem 6.2 (i) with $K=K_m$, $t=0$, $r_1=0$, $r_2=(m-1)/2$ there are at most

$$2\left(nU(n)\right)^{(m-1)/2}$$

distinct values of z satisfying (7.25) for which

$$h(\omega z^n) \geq 3^{n+10},$$

where

$$U(n) = \frac{16n-2}{8n-17}\left(\frac{16n-2}{8n+15}\right)^{(8n+15)/(8n-17)}.$$

Now we have that $(x-1)/(x-\rho)=\omega z^n$, hence x and y are completely determined by ω and z. Moreover, since $(x-1)/(1-\rho),(x-\rho)/(1-\rho)$ are algebraic integers whose difference equals -1, we have by (4.22),(7.22),(4.16),$m\geq 5$, $|N_{K_m/\mathbb{Q}}(1-\rho)| = m$,

$$\begin{aligned} h\left(\frac{x-1}{x-\rho}\right) &= \prod_{v\in S(K)} \max\left(\left|\frac{x-1}{1-\rho}\right|_v, \left|\frac{x-\rho}{1-\rho}\right|_v\right) = \prod_{v\in S_\infty(K)} \max\left(\left|\frac{x-1}{1-\rho}\right|_v, \left|\frac{x-\rho}{1-\rho}\right|_v\right) \\ &\geq \prod_{v\in S_\infty(K)} \left|\frac{m^{n-1}\xi^n}{1-\rho}\right|_v = \left|N_{K_m/\mathbb{Q}}\left(\frac{m^{n-1}\xi^n}{1-\rho}\right)\right|^{1/(m-1)} \end{aligned}$$

$$= m^{n-1-1/(m-1)}\xi^n \geq m^{n-2}\xi^n.$$

Hence, in view of the upper bound for the cardinality of H, the number of solutions of (7.16) with

$$\xi \geq 3^{1+10/n}m^{2/n-1}$$

is at most

$$2\left(nU(n)\right)^{(m-1)/2}n^{(m-1)/2}h_m = 2U(n)^{(m-1)/2}n^{m-1}h_m.$$

Therefore, by the fact that $m\geq 5, n\geq 5, U(n)^{1/2}<3$ for $n\geq 5$, by lemma 7.2 and since x,y are completely determined by ξ, the total number of solutions of (7.16) is at most

$$3^{1+10/5}5^{2/5-1} + 2\times(3n)^{m-1}h_m \leq \left(\frac{3^3\times 5^{-3/5}}{(3\times 5)^5} + \frac{2}{3\times 5}\right)(3n)^m h_m$$

$$\leq (3n)^m h_m \leq (mn)^m.$$

It can be shown in a similar way, by factorising $x^m=y^n+1$ in K_n, that the number of solutions of (7.16) can also be bounded above by $(mn)^n$. Hence (7.16) has at most $(mn)^{\min(m,n)}$ solutions. This proves theorem 7.3. □

REFERENCES

In this list of references, we included the literature to which we referred in this book. Apart from that, we selected some books and articles on the Thue equation and the Thue-Mahler equation in order to give a survey of the most important results which have been obtained on these subjects. There are very many articles which are devoted to Thue equations or related subjects. It is hardly possible to insert everyone of these articles into this list. Many other references can be found in Mordell's book on diophantine equations [Mo]. Readers who are interested in effective results can find an enormous list of references in Sprindžuk's article [Sp].

AF EKENSTAM, A.

[AEk] *Contributions to the theory of the Diophantine equation* $Ax^n-By^n=C$, Inaugural Dissertation, Univ. of Uppsala, Almqvist & Wiksells Boktryckeri AB, Uppsala (1959) 63 pp.

AVANESOV, È.T.

[Av 1] *The representation of numbers by binary cubic forms of positive discriminant* (Russian), Acta Arith. 14 (1967/68) p. 13-25.

[Av 2] *A bound for the number of representations by a special class of binary cubic forms of positive discriminant* (Russian), Acta Arith. 20 (1972) p. 17-31.

BAKER, A.

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

[B 2] *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) p. 173-191.

[B 3] *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) p. 193-208.

[B 4] *Transcendental Number Theory*, Cambridge University Press (1975).

BAULIN, V.I.

[Ba] *On an indeterminate equation of the third degree with least positive discriminant* (Russian), Tul'sk Gos. Ped. Inst. U'čen Zap. Fiz. Math. Nauk. Vip. 7 (1960) p. 138-170.

BOMBIERI, E.

[Bo] *On the Thue-Siegel-Dyson theorem*, Acta Math. 148 (1982) p. 255-296.

CASSELS, J.W.S.

[C 1] *On the equation* $a^x-b^y=1$, Amer. J. Math. 75 (1953) p. 159-162.

[C 2] *On the equation* $a^x-b^y=1$, *II*, Proc. Cambridge Philos. Soc. 56 (1960) p. 97-103.

CATALAN, E.

[Ca] *Note extraite d'une lettre adressée à l'éditeur*, J. reine angew. Math. 27 (1844) p. 192.

CHABAUTY, C.

[Ch] *Démonstration nouvelle d'un théorème de Thue et Mahler sur les formes binaires*, Bull. Sci. Math (2) 65 (1941) p. 112-130.

CHAO KO

[ChK] *On the diophantine equation* $x^2=y^n+1, xy\neq 0$, Scientia Sinica (Notes) 14 (1964) p. 457-460.

CHUDNOVSKY, G.V. (ČUDNOVSKIĬ)

[Chu 1] *The Gel'fond-Baker method in problems of diophantine approximation*, Coll. Math. Soc. János Bolyai 13 (1974) p. 19-30.

[Chu 2] *On the method of Thue-Siegel*, Ann. of Math. 117 (1983) p. 325-382.

COATES, J.

[Co 1] *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1968/69) p. 279-305.

[Co 2] *An effective p-adic analogue of a theorem of Thue II*, Acta Arith. 16 (1969/70) p. 399-412.

DAVENPORT, H. & K.F. ROTH

[D/R] *Rational approximations to algebraic numbers*, Mathematika 2 (1955) p. 160-167

DELONE, B.N. (DELAUNAY)

[De] *Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante*, Math. Zeitschr. 31 (1930) p. 1-26.

DELONE, B.N. & D.K. FADDEEV

[D/F] *The theory of irrationalities of the third degree*, Am. Math. Soc. Transl. of math. monographs 10, Providence, USA (1964).

DEM'JANENKO, V.A.

[Dem] *The representation of numbers by binary biquadratic forms* (Russian) Mat. Sb. 80 (122) (1969) p. 445-452.

DICKSON, L.E.

[Di 1] *Algebraic Invariants*, Math. Monographs 14, Wiley & Sons, New York (1914).

[Di 2] *History of the theory of numbers*, vol.II, Chelsea Publ., New York (1952).

DIRICHLET, P.G.L.

[Dir] *Vorlesungen über Zahlentheorie*, 4th ed., Vieweg & Sohn, Braunschweig (1894).

DOMAR, Y.

[Do] *On the diophantine equation* $|Ax^n-By^n|=1, n\geq 5$, Math. Scand. 2 (1954) p. 29-32.

DYSON, F.J.

[Dy] *The approximation of algebraic numbers by rationals*, Acta Math. 79 (1947) p. 225-240.

ERDÖS, P. & K. MAHLER

[E/M] *On the number of integers which can be represented by a binary form*, J. London Math. Soc. 13 (1938) p. 134-139.

EULER, L.

[Eu] *Theorematum quorundam arithmeticorum demonstrationes*, Comm. Acad. Sci. Petropolitanae 10 (1738) p. 125-146. Reprinted in Comm. Arithm. Coll. 1 (1849) p. 24-34 and in Comm. Arithm. Coll. I (1915) p. 38-58 (Collected Works, vol. 2).

EVERTSE, J.H.

[Ev 1] *On the equation* $ax^n-by^n=c$, Compositio Math. 47 (1982) p. 289-315.

[Ev 2] *On the representation of integers by binary cubic forms of positive discriminant*, Invent. Math. 73 (1983), p. 117-138.

FALTINGS, G.

[Fa] *Einige Sätze zum Thema abelsche Varietäten über Zahlkörpern*, preprint, Univ. of Wuppertal, West Germany.

GEL'FOND, A.O.

[Ge 1] *Sur le septième problème de Hilbert*, Izv. Akad. Nauk. SSSR 7 (1934) p. 623-640.

[Ge 2] *Transcendental and algebraic numbers*, Dover Publ., New York (1960).

GYÖRY, K.

[Gy] *On the number of solutions of linear equations in units of an algebraic number field*, Comm. Math. Helv. 54 (1979) p. 583-600.

HOOLEY, C.

[Ho] *On binary cubic forms*, J. reine angew. Math. 226 (1967) p. 30-87.

HUA LO KENG

[Hu] *Introduction to number theory*, Springer Verlag, Berlin, Heidelberg, New York (1982).

HYYRÖ, S.

[Hy 1] *Über das Catalansche Problem*, Ann. Univ. Turku Ser.A1, No 79 (1964).

[Hy 2] *Über die Gleichung* $ax^n-by^n=z$ *und das Catalansche Problem*, Ann. Ac. Scient. Fenn. Ser.A1, No 355 (1964).

KOTOV, S.V. & V.G. SPRINDŽUK

[K/S] *The Thue-Mahler equation in a relative field, and the approximation of algebraic numbers by algebraic numbers*, Izv. Akad. SSSR 41 (1977) p. 723-751 (Russian) or Math. USSR Izv. 11 (1977) p. 677-707.

LANG, S.

[La 1] *Algebraic Number Theory*, Addison-Wesley Publ., Reading, Massachussets (1970).

[La 2] *Elliptic Curves, Diophantine Analysis*, Grundl. math. Wiss. 231 Springer Verlag, Berlin, Heidelberg, New York (1978).

LEBESGUE, V.A.

[Le] *Sur l'impossibilité en nombres entiers de l'équation* $x^m=y^2+1$, Nouv. Ann. Math. 9 (1850) p. 178-181.

LEVEQUE, W.J.

[LeV 1] *On the equation* $a^x-b^y=1$, Amer. J. Math. 74 (1952) p. 325-331.

[LeV 2] *On the equation* $y^m=f(x)$, Acta Arith. 9 (1964) p. 209-219.

LEWIS, D.J. & K. MAHLER

[L/M] *Representation of integers by binary forms*, Acta Arith. 6 (1961) p. 333-363.

LJUNGGREN, W.

[Lj 1] *Einige Eigenschaften der Einheiten reëller quadratischer und rein biquadratischer Zahlkörper*, Oslo Vid. Akad. Skrifter 1 (1936) No 12.

[Lj 2] *Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante*, Acta Math. 75 (1942) p. 1-21.

[Lj 3] *On the representation of integers by binary biquadratic forms of a special class* (Norwegian), Norsk Mat. Tidsskr. 26 (1944) p. 51-59.

[Lj 4] *Solutions complète de quelques équations du sixième degrée à deux indeterminées*, Arch. Math. Naturv. 48 (1946) No 7 p. 26-29.

LOXTON, J.H. & A.J. VAN DER POORTEN

[L/P] *Multiplicative relations in number fields*, Bull. Austr. Math. Soc. 16 (1977) p. 83-98. *Corrigendum and addendum*, ibid., 17 (1977) p. 151-156.

MAHLER, K.

[Ma 1] *Zur Approximation algebraischer Zahlen, I. (Über den grösszten Primteiler binärer Formen)*, Math. Ann. 107 (1933) p. 691-730.

[Ma 2] *Zur Approximation algebraischer Zahlen, II. (Über die Anzahl der Darstellungen ganzer Zahlen durch Binärformen)*, Math. Ann. 108 (1933) p. 37-55.

[Ma 3] *Zur Approximation algebraischer Zahlen, III. (Über die mittlere Anzahl der Darstellungen groszer Zahlen durch binäre Formen)*, Acta Math. 62 (1933) p. 91-166.

[Ma 4] *On the lattice points on curves of genus* 1, Proc. London Math. Soc. 2nd Ser. 39 (1935) p. 431-460.

[Ma 5] *On the greatest prime factor of* ax^m+by^n, Nieuw Arch. Wisk. Ser. 3, 1 (1953) p. 113-122.

[Ma 6] *On Thue's theorem*, Austral. Nation. Univ. research rep. No. 24 (1982).

MORDELL, L.J.

[Mo] *Diophantine equations*, Academic Press, London (1969).

NAGELL, T.

[Na 1] *Über einige kubische Gleichungen mit zwei Unbestimmten*, Math. Zeitschr. 24 (1926) p. 422-447.

[Na 2] *Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante*, Math. Zeitschr. 28 (1928) p. 10-29.

[Na 3] *Über die Anzahl der Lösungen gewisser diophantischer Gleichungen dritten Grades*, Math. Zeitschr. 52 (1950) p. 750-757.

PARRY, C.J.

[Pa] *The p-adic generalization of the Thue-Siegel theorem*, Acta Math. 83 (1950) p. 1-99.

PODSYPANIN, V.

[Po] *On the equation* $ax^4+bx^2y^2-cy^4=1$, Rec. Math. (Mat. Sbornik) N.S. 18 (60) (1946) p. 105-114 (Russian, English summary).

RIDOUT, P.

[Ri] *The p-adic generalization of the Thue-Siegel-Roth theorem*, Mathematika 5 (1958) p. 40-48.

ROTH, K.F.

[Ro] *Rational approximations to algebraic numbers*, Mathematika 2 (1955) p. 1-20. *Corrigendum*, ibid., p. 168.

SIEGEL, C.L.

[Si 1] *Approximation algebraischer Zahlen*, Math. Zeitschr. 10 (1921) p. 173-213.

[Si 2] (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) p. 66-68.

[Si 3] *Über einige Anwendungen diophantischer Approximationen*, Abh. preuss. Akad. Wiss. Phys. Math. Kl. (1929) No 1.

[Si 4] *Die Gleichung* $ax^n-by^n=c$, Math. Ann. 114 (1937) p. 57-68.

[Si 5] *Abschätzung von Einheiten*, Nachr. Göttingen Math. Phys. Kl. (1969) p. 71-86.

[Si 6] *Einige Erläuterungen zu Thues Untersuchungen über Annäherungswerte algebraischer Zahlen und diophantische Gleichungen*, Nachr. Göttingen Math. Phys. Kl. (1970) p. 169-195.

These articles can also be found in Siegel's *"Gesammelte Abhandlungen"*

(Springer Verlag, Berlin, vol. I-III 1966, vol. IV 1979): [Si 1]: vol.I, p. 6-46, [Si 2]: vol. I, p. 207-208, [Si 3]: vol. I, p. 209-266, [Si 4]: vol. II, p. 8-19, [Si 5]: vol. IV, p. 66-81, [Si 6]: vol. IV, p. 140-166.

SILVERMAN, J.H.

[Sil 1] *Integer points and the rank of Thue elliptic curves*, Invent. Math. 66 (1982) p. 395-404.

[Sil 2] *The Thue equation and height functions*, in D. Bertrand & M. Waldschmidt (eds.), Approximations Diophantienne et Nombres Transcendants, Coll. Luminy, 1982, p. 259-270. Progress in Math., vol. 31, Birkhäuser Verlag, Boston, Basel, Stuttgart (1983).

SKOLEM, Th.

[Sk 1] *Einige Sätze über gewisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen*, Oslo Vid. Akad. Skrifter I (1933) No 6 p. 1-61.

[Sk 2] *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8de Skand. mat. Kongr. förh. Stockholm (1934) p. 163-188.

[Sk 3] *Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen*, Math. Ann. 111 (1935) p. 399-424.

[Sk 4] *Diophantische Gleichungen*, Erg. d. Math. u. ihrer Grenzgeb., Hrsg. v.d. Schriftleitung d. Zbl. f. Math. Bd. 5, H. 4, Julius Springer, Berlin (1938).

SPRINDŽUK, V.G.

[Sp] *Achievements and problems in Diophantine approximation theory*, Uspekhi Mat. Nauk. 35(4) (1980) p. 3-68 (Russian) or Russ. Math. Surv. 35(4) (1980) p. 1-80.

STARK, H.M.

[St] *Effective estimates of solutions of some diophantine equations*, Acta Arith. 24 (1973) p. 251-259.

TARTAKOVSKĬI, V.A.

[Ta] *A uniform estimate of the number of representations of unity by a binary form of degree* n≥3, Dokl. Akad. Nauk. SSSR 193 (1970) p. 764 (Russian) or Soviet Math. Dokl. 11 (1970) p. 1026-1027.

THUE, A.

[Th 1] *Über Annäherungswerte algebraischer Zahlen*, J. reine angew. Math. 135 (1909) p. 284-305.

[Th 2] *Berechnung aller Lösungen gewisser Gleichungen von der Form* $ax^r-by^r=f$, Vid-Selsk. Skrifter, I. Math.-naturv. Kl., Christiania (1918) Nr. 4.

These articles can also be found in the *"Selected Mathematical Papers of Axel Thue"* (Universitetsforlaget, Oslo, 1977): [Th 1]: p. 232-254, [Th 2]: p. 565-572.

TIJDEMAN, R.

[Tij] *On the equation of Catalan*, Acta Arith. 29 (1976) p. 197-209.

WALL, C.T.C.

[W] *A theorem on prime powers*, Eureka no. 19 (1957) p. 10-11.

WASHINGTON, L.C.

[Wa] *Introduction to cyclotomic fields*, Graduate texts in mathematics 83, Springer Verlag, Berlin, Heidelberg, New York (1980).

ZIMMERT, R.

[Zi] *Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung*, Invent. Math. 62 (1981) p. 367-380.

INDEX

TITLES IN THE SERIES MATHEMATICAL CENTRE TRACTS

(An asterisk before the MCT number indicates that the tract is under preparation).

A leaflet containing an order form and abstracts of all publications mentioned below is available at the Mathematisch Centrum, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands. Orders should be sent to the same address.

MCT 1 T. VAN DER WALT, *Fixed and almost fixed points*, 1963. ISBN 90 6196 002 9.

MCT 2 A.R. BLOEMENA, *Sampling from a graph*, 1964. ISBN 90 6196 003 7.

MCT 3 G. DE LEVE, *Generalized Markovian decision processes, part I: Model and method*, 1964. ISBN 90 6196 004 5.

MCT 4 G. DE LEVE, *Generalized Markovian decision processes, part II: Probabilistic background*, 1964. ISBN 90 6196 005 3.

MCT 5 G. DE LEVE, H.C. TIJMS & P.J. WEEDA, *Generalized Markovian decision processes, Applications*, 1970. ISBN 90 6196 051 7.

MCT 6 M.A. MAURICE, *Compact ordered spaces*, 1964. ISBN 90 6196 006 1.

MCT 7 W.R. VAN ZWET, *Convex transformations of random variables*, 1964. ISBN 90 6196 007 X.

MCT 8 J.A. ZONNEVELD, *Automatic numerical integration*, 1964. ISBN 90 6196 008 8.

MCT 9 P.C. BAAYEN, *Universal morphisms*, 1964. ISBN 90 6196 009 6.

MCT 10 E.M. DE JAGER, *Applications of distrubutions in mathematical physics*, 1964. ISBN 90 6196 010 X.

MCT 11 A.B. PAALMAN-DE MIRANDA, *Topological semigroups*, 1964. ISBN 90 6196 011 8.

MCT 12 J.A.Th.M. VAN BERCKEL, H. BRANDT CORSTIUS, R.J. MOKKEN & A. VAN WIJNGAARDEN, *Formal properties of newspaper Dutch*, 1965. ISBN 90 6196 013 4.

MCT 13 H.A. LAUWERIER, *Asymptotic expansions*, 1966, out of print; replaced by MCT 54.

MCT 14 H.A. LAUWERIER, *Calculus of variations in mathematical physics*, 1966. ISBN 90 6196 020 7.

MCT 15 R. DOORNBOS, *Slippage tests*, 1966. ISBN 90 6196 021 5.

MCT 16 J.W. DE BAKKER, *Formal definition of programming languages with an application to the definition of ALGOL 60*, 1967. ISBN 90 6196 022 3.

MCT 17 R.P. VAN DE RIET, *Formula manipulation in ALGOL 60, part 1*, 1968. ISBN 90 6196 025 8.

MCT 18 R.P. VAN DE RIET, *Formula manipulation in ALGOL 60, part 2*, 1968. ISBN 90 6196 038 X.

MCT 19 J. VAN DER SLOT, *Some properties related to compactness*, 1968. ISBN 90 6196 026 6.

MCT 20 P.J. VAN DER HOUWEN, *Finite difference methods for solving partial differential equations*, 1968. ISBN 90 6196 027 4.

MCT 21 E. WATTEL, *The compactness operator in set theory and topology*, 1968. ISBN 90 6196 028 2.

MCT 22 T.J. DEKKER, *ALGOL 60 procedures in numerical algebra, part 1*, 1968. ISBN 90 6196 029 0.

MCT 23 T.J. DEKKER & W. HOFFMANN, *ALGOL 60 procedures in numerical algebra, part 2*, 1968. ISBN 90 6196 030 4.

MCT 24 J.W. DE BAKKER, *Recursive procedures*, 1971. ISBN 90 6196 060 6.

MCT 25 E.R. PAËRL, *Representations of the Lorentz group and projective geometry*, 1969. ISBN 90 6196 039 8.

MCT 26 EUROPEAN MEETING 1968, *Selected statistical papers, part I*, 1968. ISBN 90 6196 031 2.

MCT 27 EUROPEAN MEETING 1968, *Selected statistical papers, part II*, 1969. ISBN 90 6196 040 1.

MCT 28 J. OOSTERHOFF, *Combination of one-sided statistical tests*, 1969. ISBN 90 6196 041 X.

MCT 29 J. VERHOEFF, *Error detecting decimal codes*, 1969. ISBN 90 6196 042 8.

MCT 30 H. BRANDT CORSTIUS, *Exercises in computational linguistics*, 1970. ISBN 90 6196 052 5.

MCT 31 W. MOLENAAR, *Approximations to the Poisson, binomial and hypergeometric distribution functions*, 1970. ISBN 90 6196 053 3.

MCT 32 L. DE HAAN, *On regular variation and its application to the weak convergence of sample extremes*, 1970. ISBN 90 6196 054 1.

MCT 33 F.W. STEUTEL, *Preservation of infinite divisibility under mixing and related topics*, 1970. ISBN 90 6196 061 4.

MCT 34 I. JUHÁSZ, A. VERBEEK & N.S. KROONENBERG, *Cardinal functions in topology*, 1971. ISBN 90 6196 062 2.

MCT 35 M.H. VAN EMDEN, *An analysis of complexity*, 1971. ISBN 90 6196 063 0.

MCT 36 J. GRASMAN, *On the birth of boundary layers*, 1971. ISBN 90 6196 064 9.

MCT 37 J.W. DE BAKKER, G.A. BLAAUW, A.J.W. DUIJVESTIJN, E.W. DIJKSTRA, P.J. VAN DER HOUWEN, G.A.M. KAMSTEEG-KEMPER, F.E.J. KRUSEMAN ARETZ, W.L. VAN DER POEL, J.P. SCHAAP-KRUSEMAN, M.V. WILKES & G. ZOUTENDIJK, *MC-25 Informatica Symposium* 1971. ISBN 90 6196 065 7.

MCT 38 W.A. VERLOREN VAN THEMAAT, *Automatic analysis of Dutch compound words*, 1971. ISBN 90 6196 073 8.

MCT 39 H. BAVINCK, *Jacobi series and approximation*, 1972. ISBN 90 6196 074 6.

MCT 40 H.C. TIJMS, *Analysis of (s,S) inventory models*, 1972. ISBN 90 6196 075 4.

MCT 41 A. VERBEEK, *Superextensions of topological spaces*, 1972. ISBN 90 6196 076 2.

MCT 42 W. VERVAAT, *Success epochs in Bernoulli trials (with applications in number theory)*, 1972. ISBN 90 6196 077 0.

MCT 43 F.H. RUYMGAART, *Asymptotic theory of rank tests for independence*, 1973. ISBN 90 6196 081 9.

MCT 44 H. BART, *Meromorphic operator valued functions*, 1973. ISBN 90 6196 082 7.

MCT 45 A.A. BALKEMA, *Monotone transformations and limit laws* 1973. ISBN 90 6196 083 5.

MCT 46 R.P. VAN DE RIET, *ABC ALGOL, A portable language for formula manipulation systems, part 1: The language*, 1973. ISBN 90 6196 084 3.

MCT 47 R.P. VAN DE RIET, *ABC ALGOL, A portable language for formula manipulation systems, part 2: The compiler*, 1973. ISBN 90 6196 085 1.

MCT 48 F.E.J. KRUSEMAN ARETZ, P.J.W. TEN HAGEN & H.L. OUDSHOORN, *An ALGOL 60 compiler in ALGOL 60, Text of the MC-compiler for the EL-X8*, 1973. ISBN 90 6196 086 X.

MCT 49 H. KOK, *Connected orderable spaces*, 1974. ISBN 90 6196 088 6.

MCT 50 A. VAN WIJNGAARDEN, B.J. MAILLOUX, J.E.L. PECK, C.H.A. KOSTER, M. SINTZOFF, C.H. LINDSEY, L.G.L.T. MEERTENS & R.G. FISKER (eds), *Revised report on the algorithmic language ALGOL 68*, 1976. ISBN 90 6196 089 4.

MCT 51 A. HORDIJK, *Dynamic programming and Markov potential theory*, 1974. ISBN 90 6196 095 9.

MCT 52 P.C. BAAYEN (ed.), *Topological structures*, 1974. ISBN 90 6196 096 7.

MCT 53 M.J. FABER, *Metrizability in generalized ordered spaces*, 1974. ISBN 90 6196 097 5.

MCT 54 H.A. LAUWERIER, *Asymptotic analysis, part 1*, 1974. ISBN 90 6196 098 3.

MCT 55 M. HALL JR. & J.H. VAN LINT (eds), *Combinatorics, part 1: Theory of designs, finite geometry and coding theory*, 1974. ISBN 90 6196 099 1.

MCT 56 M. HALL JR. & J.H. VAN LINT (eds), *Combinatorics, part 2: Graph theory, foundations, partitions and combinatorial geometry*, 1974. ISBN 90 6196 100 9.

MCT 57 M. HALL JR. & J.H. VAN LINT (eds), *Combinatorics, part 3: Combinatorial group theory*, 1974. ISBN 90 6196 101 7.

MCT 58 W. ALBERS, *Asymptotic expansions and the deficiency concept in statistics*, 1975. ISBN 90 6196 102 5.

MCT 59 J.L. MIJNHEER, *Sample path properties of stable processes*, 1975. ISBN 90 6196 107 6.

MCT 60 F. GÖBEL, *Queueing models involving buffers*, 1975. ISBN 90 6196 108 4.

*MCT 61 P. VAN EMDE BOAS, *Abstract resource-bound classes, part 1*, ISBN 90 6196 109 2.

*MCT 62 P. VAN EMDE BOAS, *Abstract resource-bound classes, part 2*, ISBN 90 6196 110 6.

MCT 63 J.W. DE BAKKER (ed.), *Foundations of computer science*, 1975. ISBN 90 6196 111 4.

MCT 64 W.J. DE SCHIPPER, *Symmetric closed categories*, 1975. ISBN 90 6196 112 2.

MCT 65 J. DE VRIES, *Topological transformation groups 1 A categorical approach*, 1975. ISBN 90 6196 113 0.

MCT 66 H.G.J. PIJLS, *Locally convex algebras in spectral theory and eigenfunction expansions*, 1976. ISBN 90 6196 114 9.

*MCT 67 H.A. LAUWERIER, *Asymptotic analysis, part 2*, ISBN 90 6196 119 X.

MCT 68 P.P.N. DE GROEN, *Singularly perturbed differential operators of second order*, 1976. ISBN 90 6196 120 3.

MCT 69 J.K. LENSTRA, *Sequencing by enumerative methods*, 1977. ISBN 90 6196 125 4.

MCT 70 W.P. DE ROEVER JR., *Recursive program schemes: Semantics and proof theory*, 1976. ISBN 90 6196 127 0.

MCT 71 J.A.E.E. VAN NUNEN, *Contracting Markov decision processes*, 1976. ISBN 90 6196 129 7.

MCT 72 J.K.M. JANSEN, *Simple periodic and nonperiodic Lamé functions and their applications in the theory of conical waveguides*, 1977. ISBN 90 6196 130 0.

MCT 73 D.M.R. LEIVANT, *Absoluteness of intuitionistic logic*, 1979. ISBN 90 6196 122 X.

MCT 74 H.J.J. TE RIELE, *A theoretical and computational study of generalized aliquot sequences*, 1976. ISBN 90 6196 131 9.

MCT 75 A.E. BROUWER, *Treelike spaces and related connected topological spaces*, 1977. ISBN 90 6196 132 7.

MCT 76 M. REM, *Associations and the closure statement*, 1976. ISBN 90 6196 135 1.

MCT 77 W.C.M. KALLENBERG, *Asymptotic optimality of likelihood ratio tests in exponential families*, 1977. ISBN 90 6196 134 3.

MCT 78 E. DE JONGE & A.C.M. VAN ROOIJ, *Introduction to Riesz spaces*, 1977. ISBN 90 6196 133 5.

MCT 79 M.C.A. VAN ZUIJLEN, *Empirical distributions and rank statistics*, 1977. ISBN 90 6196 145 9.

MCT 80 P.W. HEMKER, *A numerical study of stiff two-point boundary problems*, 1977. ISBN 90 6196 146 7.

MCT 81 K.R. APT & J.W. DE BAKKER (eds), *Foundations of computer science II*, part 1, 1976. ISBN 90 6196 140 8.

MCT 82 K.R. APT & J.W. DE BAKKER (eds), *Foundations of computer science II*, part 2, 1976. ISBN 90 6196 141 6.

MCT 83 L.S. BENTHEM JUTTING, *Checking Landau's "Grundlagen" in the AUTOMATH system*, 1979. ISBN 90 6196 147 5.

MCT 84 H.L.L. BUSARD, *The translation of the elements of Euclid from the Arabic into Latin by Hermann of Carinthia (?) books vii-xii*, 1977. ISBN 90 6196 148 3.

MCT 85 J. VAN MILL, *Supercompactness and Wallman spaces*, 1977. ISBN 90 6196 151 3.

MCT 86 S.G. VAN DER MEULEN & M. VELDHORST, *Torrix I, A programming system for operations on vectors and matrices over arbitrary fields and of variable size*. 1978. ISBN 90 6196 152 1.

*MCT 87 S.G. VAN DER MEULEN & M. VELDHORST, *Torrix II*, ISBN 90 6196 153 X.

MCT 88 A. SCHRIJVER, *Matroids and linking systems*, 1977. ISBN 90 6196 154 8.

MCT 89 J.W. DE ROEVER, *Complex Fourier transformation and analytic functionals with unbounded carriers*, 1978. ISBN 90 6196 155 6.

MCT 90 L.P.J. GROENEWEGEN, *Characterization of optimal strategies in dynamic games*, 1981 . ISBN 90 6196 156 4.

MCT 91 J.M. GEYSEL, *Transcendence in fields of positive characteristic*, 1979. ISBN 90 6196 157 2.

MCT 92 P.J. WEEDA, *Finite generalized Markov programming*, 1979. ISBN 90 6196 158 0.

MCT 93 H.C. TIJMS & J. WESSELS (eds), *Markov decision theory*, 1977. ISBN 90 6196 160 2.

MCT 94 A. BIJLSMA, *Simultaneous approximations in transcendental number theory*, 1978. ISBN 90 6196 162 9.

MCT 95 K.M. VAN HEE, *Bayesian control of Markov chains*, 1978. ISBN 90 6196 163 7.

MCT 96 P.M.B. VITÁNYI, *Lindenmayer systems: Structure, languages, and growth functions*, 1980. ISBN 90 6196 164 5.

*MCT 97 A. FEDERGRUEN, *Markovian control problems; functional equations and algorithms*, . ISBN 90 6196 165 3.

MCT 98 R. GEEL, *Singular perturbations of hyperbolic type*, 1978. ISBN 90 6196 166 1.

MCT 99 J.K. LENSTRA, A.H.G. RINNOOY KAN & P. VAN EMDE BOAS, *Interfaces between computer science and operations research*, 1978. ISBN 90 6196 170 X.

MCT 100 P.C. BAAYEN, D. VAN DULST & J. OOSTERHOFF (eds), *Proceedings bicentennial congress of the Wiskundig Genootschap, part 1*, 1979. ISBN 90 6196 168 8.

MCT 101 P.C. BAAYEN, D. VAN DULST & J. OOSTERHOFF (eds), *Proceedings bicentennial congress of the Wiskundig Genootschap, part 2*, 1979. ISBN 90 6196 169 6.

MCT 102 D. VAN DULST, *Reflexive and superreflexive Banach spaces*, 1978. ISBN 90 6196 171 8.

MCT 103 K. VAN HARN, *Classifying infinitely divisible distributions by functional equations*, 1978. ISBN 90 6196 172 6.

MCT 104 J.M. VAN WOUWE, *Go-spaces and generalizations of metrizability*, 1979. ISBN 90 6196 173 4.

MCT 105 R. HELMERS, *Edgeworth expansions for linear combinations of order statistics*, 1982. ISBN 90 6196 174 2.

MCT 106 A. SCHRIJVER (ed.), *Packing and covering in combinatorics*, 1979. ISBN 90 6196 180 7.

MCT 107 C. DEN HEIJER, *The numerical solution of nonlinear operator equations by imbedding methods*, 1979. ISBN 90 6196 175 0.

MCT 108 J.W. DE BAKKER & J. VAN LEEUWEN (eds), *Foundations of computer science III*, part *1*, 1979. ISBN 90 6196 176 9.

MCT 109 J.W. DE BAKKER & J. VAN LEEUWEN (eds), *Foundations of computer science III*, part *2*, 1979. ISBN 90 6196 177 7.

MCT 110 J.C. VAN VLIET, *ALGOL 68 transput*, part *I*: *Historical review and discussion of the implementation model*, 1979. ISBN 90 6196 178 5.

MCT 111 J.C. VAN VLIET, *ALGOL 68 transput*, part *II*: *An implementation model*, 1979. ISBN 90 6196 179 3.

MCT 112 H.C.P. BERBEE, *Random walks with stationary increments and renewal theory*, 1979. ISBN 90 6196 182 3.

MCT 113 T.A.B. SNIJDERS, *Asymptotic optimality theory for testing problems with restricted alternatives*, 1979. ISBN 90 6196 183 1.

MCT 114 A.J.E.M. JANSSEN, *Application of the Wigner distribution to harmonic analysis of generalized stochastic processes*, 1979. ISBN 90 6196 184 X.

MCT 115 P.C. BAAYEN & J. VAN MILL (eds), *Topological Structures II*, part *1*, 1979. ISBN 90 6196 185 5.

MCT 116 P.C. BAAYEN & J. VAN MILL (eds), *Topological Structures II*, part *2*, 1979. ISBN 90 6196 186 6.

MCT 117 P.J.M. KALLENBERG, *Branching processes with continuous state space*, 1979. ISBN 90 6196 188 2.

MCT 118 P. GROENEBOOM, *Large deviations and asymptotic efficiencies*, 1980. ISBN 90 6196 190 4.

MCT 119 F. J. PETERS, *Sparse matrices and substructures, with a novel implementation of finite element algorithms*, 1980. ISBN 90 6196 192 0.

MCT 120 W.P.M. DE RUYTER, *On the asymptotic analysis of large-scale ocean circulation*, 1980. ISBN 90 6196 192 9.

MCT 121 W.H. HAEMERS, *Eigenvalue techniques in design and graph theory*, 1980. ISBN 90 6196 194 7.

MCT 122 J.C.P. BUS, *Numerical solution of systems of nonlinear equations*, 1980. ISBN 90 6196 195 5.

MCT 123 I. YUHÁSZ, *Cardinal functions in topology - ten years later*, 1980. ISBN 90 6196 196 3.

MCT 124 R.D. GILL, *Censoring and stochastic integrals*, 1980. ISBN 90 6196 197 1.

MCT 125 R. EISING, *2-D systems, an algebraic approach*, 1980. ISBN 90 6196 198 X.

MCT 126 G. VAN DER HOEK, *Reduction methods in nonlinear programming*, 1980. ISBN 90 6196 199 8.

MCT 127 J.W. KLOP, *Combinatory reduction systems*, 1980. ISBN 90 6196 200 5.

MCT 128 A.J.J. TALMAN, *Variable dimension fixed point algorithms and triangulations*, 1980. ISBN 90 6196 201 3.

MCT 129 G. VAN DER LAAN, *Simplicial fixed point algorithms*, 1980. ISBN 90 6196 202 1.

MCT 130 P.J.W. TEN HAGEN et al., *ILP Intermediate language for pictures*, 1980. ISBN 90 6196 204 8.

MCT 131 R.J.R. BACK, *Correctness preserving program refinements: Proof theory and applications*, 1980. ISBN 90 6196 207 2.

MCT 132 H.M. MULDER, *The interval function of a graph*, 1980. ISBN 90 6196 208 0.

MCT 133 C.A.J. KLAASSEN, *Statistical performance of location estimators*, 1981. ISBN 90 6196 209 9.

MCT 134 J.C. VAN VLIET & H. WUPPER (eds), *Proceedings international conference on ALGOL 68*, 1981. ISBN 90 6196 210 2.

MCT 135 J.A.G. GROENENDIJK, T.M.V. JANSSEN & M.J.B. STOKHOF (eds), *Formal methods in the study of language*, part *I*, 1981. ISBN 90 6196 211 0.

MCT 136 J.A.G. GROENENDIJK, T.M.V. JANSSEN & M.J.B. STOKHOF (eds), *Formal methods in the study of language*, part *II*, 1981. ISBN 90 6196 213 7.

MCT 137 J. TELGEN, *Redundancy and linear programs*, 1981. ISBN 90 6196 215 3.

MCT 138 H.A. LAUWERIER, *Mathematical models of epidemics*, 1981. ISBN 90 6196 216 1.

MCT 139 J. VAN DER WAL, *Stochastic dynamic programming, successive approximations and nearly optimal strategies for Markov decision processes and Markov games*, 1980. ISBN 90 6196 218 8.

MCT 140 J.H. VAN GELDROP, *A mathematical theory of pure exchange economies without the no-critical-point hypothesis*, 1981.
ISBN 90 6196 219 6.

MCT 141 G.E. WELTERS, *Abel-Jacobi isogenies for certain types of Fano three-folds*, 1981.
ISBN 90 6196 227 7.

MCT 142 H.R. BENNETT & D.J. LUTZER (eds), *Topology and order structures*, part 1, 1981.
ISBN 90 6196 228 5.

MCT 143 H. J.M. SCHUMACHER, *Dynamic feedback in finite- and infinite dimensional linear systems*, 1981.
ISBN 90 6196 229 3.

MCT 144 P. EIJGENRAAM, *The solution of initial value problems using interval arithmetic. Formulation and analysis of an algorithm*, 1981.
ISBN 90 6196 230 7.

MCT 145 A.J. BRENTJES, *Multi-dimensional continued fraction algorithms*, 1981. ISBN 90 6196 231 5.

MCT 146 C. VAN DER MEE, *Semigroup and factorization methods in transport theory*, 1982. ISBN 90 6196 233 1.

MCT 147 H.H. TIGELAAR, *Identification and informative sample size*, 1982.
ISBN 90 6196 235 8.

MCT 148 L.C.M. KALLENBERG, *Linear programming and finite Markovian control problems*, 1983. ISBN 90 6196 236 6.

MCT 149 C.B. HUIJSMANS, M.A. KAASHOEK, W.A.J. LUXEMBURG & W.K. VIETSCH, (eds), *From A to Z, proceeding of a symposium in honour of A.C. Zaanen*, 1982. ISBN 90 6196 241 2.

MCT 150 M. VELDHORST, *An analysis of sparse matrix storage schemes*, 1982.
ISBN 90 6196 242 0.

MCT 151 R.J.M.M. DOES, *Higher order asymptotics for simple linear Rank statistics*, 1982. ISBN 90 6196 243 9.

MCT 152 G.F. VAN DER HOEVEN, *Projections of Lawless sequences*, 1982.
ISBN 90 6196 244 7.

MCT 153 J.P.C. BLANC, *Application of the theory of boundary value problems in the analysis of a queueing model with paired services*, 1982.
ISBN 90 6196 247 1.

MCT 154 H.W. LENSTRA, JR. & R. TIJDEMAN (eds), *Computational methods in number theory, part I*, 1982.
ISBN 90 6196 248 X.

MCT 155 H.W. LENSTRA, JR. & R. TIJDEMAN (eds), *Computational methods in number theory, part II*, 1982.
ISBN 90 6196 249 8.

MCT 156 P.M.G. APERS, *Query processing and data allocation in distributed database systems*, 1983.
ISBN 90 6196 251 X.

MCT 157 H.A.W.M. KNEPPERS, *The covariant classification of two-dimensional smooth commutative formal groups over an algebraically closed field of positive characteristic*, 1983.
ISBN 90 6196 252 8.

MCT 158 J.W. DE BAKKER & J. VAN LEEUWEN (eds), *Foundations of computer science IV, Distributed systems*, part 1, 1983.
ISBN 90 6196 254 4.

MCT 159 J.W. DE BAKKER & J. VAN LEEUWEN (eds), *Foundations of computer science IV, Distributed systems*, part 2, 1983.
ISBN 90 6196 255 0.

MCT 160 A. REZUS, *Abstract automat*, 1983.
ISBN 90 6196 256 0.

MCT 161 G.F. HELMINCK, *Eisenstein series on the metaplectic group, An algebraic approach*, 1983.
ISBN 90 6196 257 9.

MCT 162 J.J. DIK, *Tests for preference*, 1983.
ISBN 90 6196 259 5

MCT 163 H. SCHIPPERS, *Multiple grid methods for equations of the second kind with applications in fluid mechanics*, 1983.
ISBN 90 6196 260 9.

MCT 164 F.A. VAN DER DUYN SCHOUTEN, *Markov decision processes with continuous time parameter*, 1983.
ISBN 90 6196 261 7.

MCT 165 P.C.T. VAN DER HOEVEN, *On point processes*, 1983.
ISBN 90 6196 262 5.

MCT 166 H.B.M. JONKERS, *Abstraction, specification and implementation techniques, with an application to garbage collection*, 1983.
ISBN 90 6196 263 3.

MCT 167 W.H.M. ZIJM, *Nonnegative matrices in dynamic programming*, 1983.
ISBN 90 6196 264 1

MCT 168 J.H. EVERTSE, *Upper bounds for the numbers of solutions of diophantine equations*, 1983.
ISBN 90 6196 265 X.

An asterisk before the number means "to appear"