ERASMUS

8014

~~Netherlands school of economics~~

ECONOMETRIC INSTITUTE

FACTORIZATION METHODS FOR SOLVING DIOPHANTINE EQUATIONS

R.J. STROEKER

REPORT 8014/M

ERASMUS UNIVERSITY ROTTERDAM, P.O. BOX 1738. 3000 DR. ROTTERDAM. THE NETHERLANDS.

FACTORIZATION METHODS FOR SOLVING DIOPHANTINE EQUATIONS

by

R.J. Stroeker

ABSTRACT

In this exposition we give an overview of the algebraic factorization methods, based upon Dedekind's Unique Factorization Theorem for ideals in Dedekind domains, which are frequently used to effectively solve Diophantine equations. Emphasis is put on the practical computation of solutions. This finds expression in the many examples which have been included.

CONTENTS

AMS (MOS) subject classification scheme (1980): 10-02, 10B05, 10B10, 12A25, 12A30

1. INTRODUCTION

A *diophantine equation* is usually defined as an equation in two or more variables

$$f(x_1,x_2,\ldots,x_n) = 0 \quad , \quad n \geqq 2$$

the solutions of which are required to be integers or sometimes rational numbers. The function f is often a polynomial function with integer coefficients. At present a more general definition of the notion of diophantine equation is sometimes adopted: on the one hand it is possible to admit solutions taken from fields other than the field of rational numbers $\mathbb{Q}$, like algebraic extensions of $\mathbb{Q}$ or finite fields, or one could even search for solutions in different algebraic structures like groups and rings, on the other hand the defining function f need not be a polynomial function. But, in whatever way or direction one wishes to extend the original definition of a diophantine equation, one should always restrict its solutions to those one could call rightfully *rational* or *integral* in some sense.

We like in this place to abide by the traditional conception, i.e. $f \in \mathbb{Z}[x_1,\ldots,x_n]$ and a solution $(x_1,\ldots,x_n)$ of $f = 0$ is required to be integral in the sense that $x_i \in \mathbb{Z}$ for all $i = 1,\ldots,n$.

Even then it is almost impossible to classify diophantine equations in some sensible way. The lack of results of a general nature is partly responsible; such results do exist, but rather sparingly. The ad hoc character of the subject, especially of the period before 1930, is shown very clearly in Dickson's famous history on the theory of numbers ([8]). Nevertheless, if one insists on dividing diophantine equations into different classes, a division which put the emphasis on methods and techniques which have proven useful in diophantine analysis, is preferable, rather than a classification merely based upon the external form, such as degree, number of variables etc. This means that some equations belong to more than one class.

Roughly speaking, diophantine analysis borrows mainly from the following fields:
(1) *Elementary Number Theory*, (2) *Algebraic Number Theory*, (3) *Algebraic Geometry*, (4) *p-Adic Analysis*, (5) *Diophantine Approximation Theory and* (6) *Miscelleneous Theories* (*like Logic*, *Combinatorial Theory*, *Geometry of Numbers etc.*).

With even less sophistication one might maintain each and every diophantine equation to belong to at least one of the following categories:

(I) *Algebraic Methods*: (2), (1), (3) *and* (4).
(II) *Approximation Methods*: (5), (1) *and* (4).

Here we shall exclusively discuss equations related to the first category. This choice is not founded in the belief that the second category is the lesser important one. On the contrary, the last decade has seen a great many applications of approximation methods to the theory of diophantine equations, especially of the so-called Gel'fond - Baker method. For the interested reader, we have selected the following references: Baker [2], [3], Shorey et al [20], Tijdeman [30], [31].

A natural consequence of our choice of subject is that we shall illustrate the most important constructive techniques of category (I) by means of specific equations. The set of equations from which we shall draw our examples is the class of *binary polynomial equations* (a binary equation has two variables). This class has been investigated extensively and the results obtained give a clear picture of the algebraic possibilities. The restriction implied by our choice also means that the most famous diophantine equation of all, *Fermat's Last Theorem*, shall not be included in our discussion. Much information on this equation, i.e. $x^n + y^n = z^n$ ($n \geqq 3$), can be found in Edwards [9] and the recently published work of Ribenboim [18].

In the closing lines of this introduction, we like to draw attention to the books written by Bašmakova [4], Mordell [16] and Skolem [21], in which one may find a real treasure of information, also of a historical nature, on diophantine equations in general.

2. SOME RESULTS FROM ALGEBRAIC NUMBER THEORY

The purpose of the next example is to suggest that often the relation between the variables occurring in a diophantine equation can be made transparant by simple factorization. By this we mean application of the Fundamental Theorem of Arithmetic: *any positive integer may be written in one way only as a product of primes, except for the order in which the primes occur in the product.*

2.1 EXAMPLE

For given $k \in \mathbb{Z}$, $k \neq 0$ consider the equation $x^4 = y^2 + k$. If $x,y \in \mathbb{Z}$ gives a solution of this equation, then $(x^2 - y)(x^2 + y) = k$ and a divisor d of k exists such that

$$x^2 - y = d \quad \text{and} \quad x^2 + y = \frac{k}{d}\,.$$

Here we may assume that $\frac{k}{d} \geqq d$ and $\frac{k}{d} > 0$, because there is no loss of generality in taking $y \geqq 0$. Thus

$$x^2 = \tfrac{1}{2}(d + \frac{k}{d}) \quad \text{and} \quad y = \tfrac{1}{2}(\frac{k}{d} - d).$$

The number of divisors of k is finite and so it should be immediately clear from the above whether solutions do exist and if so how they can be computed.

If in addition one requires k to be prime ($k = p$), then d can have no value other than 1 and consequently

$$x^2 = \tfrac{1}{2}(p + 1) \quad \text{and} \quad y = \tfrac{1}{2}(p - 1).$$

This shows that at most one solution in positive integers x and y can exist. The prime numbers $p < 100$ for which the equation is soluble are $p = 7, 17, 31, 71$ and 97.

□

Another example of an equation which can be solved completely by elementary factorization is given in Stroeker [29].

Well then, most constructive methods used in diophantine problems apply at some stage factorization in certain algebraic number fields. Therefore, we intend to formulate a few theorems from the realm of Algebraic Number Theory, which in our view are of fundamental importance in the process of solving diophantine equations. We shall give no proofs, but confine ourselves to indicating the relevant places in the literature.

Let K be a number field (a number field is an algebraic - and thus finite - extension of the field $\mathbb{Q}$) with ring of algebraic integers $\mathcal{O}_K$. An ideal of $\mathcal{O}_K$ has a finite basis. A *fractional* ideal of $\mathcal{O}_K$ is a finitely generated $\mathcal{O}_K$-module $\mathfrak{a} \neq 0$, contained in K. Hence, each ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$ is also a fractional ideal of $\mathcal{O}_K$; in this context ideals of $\mathcal{O}_K$ are sometimes called *integral* ideals. In the set of fractional ideals of $\mathcal{O}_K$ we define multiplication as follows: let the fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ begenerated by $\alpha_1,\ldots,\alpha_n$ and $\beta_1,\ldots,\beta_m$ respectively; then the *product* $\mathfrak{a}\cdot\mathfrak{b}$ is the fractional ideal generated by all ring products $\alpha_i\cdot\beta_j$. This way, the set of fractional ideals of O_K becomes a group, the so-called *ideal group* of K. This group is denoted by I_K.

A direct generalization of the fundamental theorem of arithmetic is given in Dedekind's theorem:

2.2 THEOREM (see Janusz [12], theorem I.4.2)

Each fractional ideal a of O_K can be written in one way only as the product of prime ideals of O_K, except for the order in which the prime ideals occur in the product: $a = \wp_1^{a_1} \cdots \wp_n^{a_n}$ with distinct prime ideals $\wp_i$ and $a_i \in \mathbb{Z}$. □

From this theorem it easily follows that the ideal group I_K is a free abelian group generated by the prime ideals of O_K. An important subgroup of I_K is the group of all fractional ideals generated by one prime ideal only. This is the subgroup H_K of fractional *principal* ideals. The factor group $I_K/H_K =: Cl_K$, the so-called *class group* of K, has the following important property, discovered by Dirichlet:

2.3 THEOREM (see Janusz [12], theorem I.11.10)

The class group Cl_K is finite. □

The order of Cl_K is known as the *class number* of K, notation: $h = h_K$.

2.4 COROLLARY

Let a be a fractional ideal. Then a^h is principal. Moreover, if k and h are relatively prime then a is principal whenever a^k is principal. □

A very important theorem is Dirichlet's *unit* theorem:

2.5 <u>THEOREM</u> (see Janusz [12], theorem I.11.19)

The unit group in the ring O_K *is the direct product of a finite cyclic group of roots of unity and a free abelian group of rank* $r+s-1$. *Here* r *is the number of real conjugate fields of* K *and* s *is the number of pairs of complex conjugate fields of* K; *then* $r + 2s = [K:\mathbb{Q}]$ *the extension degree of* K *over* $\mathbb{Q}$. □

The meaning of the theorem is the following: in O_K a set of units $\{\varepsilon_1,\dots,\varepsilon_{r+s-1}\}$ may be found, so-called *fundamental units*, with the property that for any unit $\eta \in O_K$ rational integers a_i exist such that the quotient of η and the product $\varepsilon_1^{a_1}\dots\dots\varepsilon_{r+s-1}^{a_{r+s-1}}$ is one of a finite number of roots of unity contained in O_K:

$$\eta = \zeta\cdot \prod_{i=1}^{r+s-1} \varepsilon_i^{a_i} , \ \zeta^m = 1 .$$

The next theorem may be considered the most fundamental tool in the process of solving diophantine equations, at least from an algebraic point of view.

2.6 <u>THEOREM</u> (see also London & Finkelstein [15], theorem 25 p. 70)

Let O_K *be the ring of integers of the number field* K. *Further,* a_o *is a fixed ideal of* O_K *and* m *is a fixed positive rational integer. If* $x, y, z \in O_K$ *satisfy the requirements:*

(i) $x\cdot y = z^m$ *and* (ii) *the ideal generated by* x *and* y *divides* a_o , *then* $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in O_K$ *may be found belonging to a finite set of units, and elements* α, β, γ *of* K *belonging to a finite subset of* K *and also* $a, b \in O_K$ *such that*

$$x = \varepsilon_1\alpha a^m , \ y = \varepsilon_2\beta b^m , \ z = \varepsilon_3\gamma ab \text{ and } \varepsilon_1\varepsilon_2\alpha\beta = \varepsilon_3^m\gamma^m .$$

<u>Proof</u> From the assumption, together with theorem 2.2 we deduce that

the principal ideals generated by x and y may be written as

$$(x) = \mathfrak{a}_1 A^m \quad \text{and} \quad (y) = \mathfrak{a}_2 B^m ,$$

where $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are elements of a fixed finite set of integral ideals with the property that any common ideal divisor of $\mathfrak{a}_1$ and $\mathfrak{a}_2$ also divides $\mathfrak{a}_o$; the ideals A and B are arbitrary ideals of O_K. Now, the number of ideal classes is finite. So, if A belongs to class C, then a (fractional) ideal A' exists belonging to the inverse class C^{-1} such that $A \cdot A' = (a)$ for some $a \in O_K$. Thus

$$(A')^m(x) = \mathfrak{a}_1(a)^m,$$

which shows that $(A')^m$ and $\mathfrak{a}_1$ belong to the same ideal class. Consequently, $\mathfrak{a}_1/(A')^m$ is a (fractional) principal ideal, generated by $\alpha \in K$, say. Then $(x) = (\alpha)(a)^m$ and hence

$$x = \varepsilon_1 \alpha a^m ,$$

where ε_1 is a unit. Now ε_1 may be written as $\varepsilon_1 = \eta_1 \cdot \eta_2^m$, where the unit η_1 can assume only finitely many different values. Now let η_2^m be absorbed by a^m. Also α may be chosen from a finite subset of K, because Cl_K is finite. The remainder of the proof now follows easily. □

2.7 REMARK

If $\mathfrak{a}_o = (1)$ and m and h_K are relatively prime, then

$$x = \varepsilon_1 a^m , \; y = \varepsilon_2 b^m , \; z = \varepsilon_3 ab$$

with $a,b \in O_K$ and finitely many possible values for the units ε_1, ε_2 and ε_3. This follows immediately from corollary 2.4. □

2.8 EXAMPLE

We return to example 2.1, but now we take $k = p^2$, where p is a given prime number. The positive divisors of k are 1, p and p^2. For d = 1 we find $x^2 = \frac{1}{2}(p^2 + 1)$ and $y = \frac{1}{2}(p^2 - 1)$. This is the only possible value for d, since $d = p$ yields $x^2 = p$. Hence

$$p^2 - 2x^2 = -1 ,$$

which may also be written as

$$\mathrm{Norm}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(p + x\sqrt{2}) = -1 .$$

This expression means that $p + x\sqrt{2}$ is a unit of $\mathcal{O}_K$ with norm -1; here $K = \mathbb{Q}(\sqrt{2})$. The group of units of $\mathcal{O}_K$ is a simple one: 1 and -1 are the only roots of unity and $\varepsilon = 1 + \sqrt{2}$ is a fundamental unit (i.e. ε generates the free abelian unit group; $r + s - 1 = 1$). Since we may assume x and p to be positive, we find that

$$p + x\sqrt{2} = (1 + \sqrt{2})^{2k+1}$$

for some non-negative rational integer k. This means also that the prime p can be written as

$$p = \sum_{j=0}^{k} \binom{2k+1}{2j} 2^j \quad (k \in \mathbb{Z},\ k \geqq 0).$$

A different formulation of the problem may be given as follows. Let the sequences $\{a_k\}$ and $\{b_k\}$ bedefined by

$$a_k + b_k\sqrt{2} = (1 + \sqrt{2})^{2k+1} , \quad k \in \mathbb{Z}.$$

The sequence $\{a_k\}$ complies with the recurrence relation

$$a_{k+1} = 6a_k - a_{k-1} , \ k \in \mathbb{Z}$$

with initial conditions $a_0 = 1$, $a_1 = 7$. (The sequence $\{b_k\}$ satisfies the same recurrence relation, however with a different set of initial values.) Because the sequence $\{a_k\}_{k \geqq 0}$ is increasing, we claim that the original diophantine equation is soluble (with a single solution only) if and only if the prime p appears in the sequence $\{a_k\}_{k \geqq 0}$. The prime numbers $p < 1000$ for which a solution exists are $p = 7$, 41 and 239.

We could also treat the equation

$$x^4 = y^2 + p^2 \quad , \text{p priem}$$

in a different way. If x,y gives a solution, we write

$$x^4 = (y + pi)(y - pi).$$

Thus we factorize the right hand side in $\mathcal{O}_L$ with $L = \mathbb{Q}(i)$. Here $h_L = 1$, the cyclic group of roots of unity is $\{1,-1,i,-i\}$ and the free abelian unit group is trivial, because $r + s - 1 = 0$. It is not difficult to prove that p cannot possibly divide both x and y. This implies that the only possible common prime ideal divisors of $(y + pi)$ and $(y - pi)$ are $(1 + i)$, (π) and $(\overline{\pi})$, where $p = \pi\cdot\overline{\pi}$ in case $p \equiv 1 \pmod 4$. Now by 2.6 we see that

$$y + pi = \varepsilon(1 + i)^a(\pi)^b(\overline{\pi})^c A^4$$

with $\varepsilon \in \{1,-1,i,-i\}$; $a,b,c \in \{0,1,2,3\}$ and $A \in \mathcal{O}_L$. From $\mathrm{Norm}_{L/\mathbb{Q}}(y + pi) = x^4$ it then follows that $a = b = c = 0$. Thus

$$y + pi = \varepsilon(u + iv)^4 = \varepsilon\{u^4 - 6u^2v^2 + v^4 + i(4u^3v - 4uv^3)\}$$

for certain $u,v \in \mathbb{Z}$. Because of the primality of p, we must have $\varepsilon = \pm i$. Then equating coefficients of 1 and i gives

$$\pm p = u^4 - 6u^2v^2 + v^4 \ , \ \mp y = 4uv(u^2 - v^2) \ , \ x = u^2 + v^2$$

where the ± signs correspond as indicated. This gives rise to the generally very difficult representation problem of type $(F = \mathbb{Q}(\theta))$

$$\mathrm{Norm}_{F/\mathbb{Q}}(u - v\theta) = m \ , \quad 0 \neq m \in \mathbb{Z}$$

with $[F:\mathbb{Q}] = 4$. We shall discuss such problems in section 4.

The positive values of u and v corresponding with the solutions (x,y) of the original equation with p = 7, 41 and 239 are (u,v) = (1,2), (2,5) and (5,12) repectively.

□

3. INHOMOGENEOUS CUBIC EQUATIONS

A fundamental problem when studying diophantine equations is the question of solvability. And further, assuming a given equation is solvable, how many solutions are there? A very important problem, closely related to the previous one, is the question of the actual (and practical!) computation of the existing solutions, or in case infinitely many solutions exist, can they be characterized in a simple way (such as parametrization)?

Very little is known about solvability criteria: on the one hand it is quite often easy to show the insolubility of a given equation by means of impossible congruences (see: Nagell [17], Chapter VII and Mordell [16], Chapters 2, 26; see also: Borevich [6] problem 4 on page 3), and, on the other hand is the proof of the existence of solutions nearly always constructive.

One of the most widely applied results obtained in diophantine analysis is A. Thue's famous theorem on the approximation of irrational numbers by rationals, dating from 1909. A direct consequence of Thue's result is the following theorem:

3.1 THEOREM (see Mordell [16], Chapter 22)

Let f *be a binary form (i.e. a homogeneous polynomial in two variables) with coefficients in* $\mathbb{Z}$ *and of degree at least 3. If* f *is irreducible over* $\mathbb{Q}$ *, then for any* $m \in \mathbb{Z}$ *(*$m \neq 0$*) the equation* $f(x,y) = m$ *has at most a finite number of solutions in integers* x *and* y*.*

□

3.2 REMARK

The condition "f is irreducible over $\mathbb{Q}$" can be replaced by "the discriminant of f (see section 4) does not vanish". Thue's proof is ineffective. This means that it does not supply an algorithm for constructing possible solutions, neither does it give a solvability criterium.

□

The equation $f(x,y) = m$ may be viewed as a so-called *norm equation*. Indeed, let ξ be a root of $f(t,1) = 0$ and let K be the number field generated by ξ over $\mathbb{Q}$. Then $f(x,y) = \mathrm{Norm}_{K/\mathbb{Q}}(x - y\xi)$. A great deal of information is available on this type of equation. We refer to Mordell [16], Chapters 18, 24 and 25. In the next section we shall give some attention to this kind of diophantine equation.

Moreover, an important class of (inhomogeneous) equations exist the solutions of which may be obtained from finite systems of binary norm equations. A well-known example is the equation

$$y^2 = x^3 + ax + b \qquad , \quad 4a^3 + 27b^2 \neq 0 \quad (a,b \in \mathbb{Z}).$$

This is a Weierstrass equation for an elliptic curve defined over the rationals; any elliptic curve defined over $\mathbb{Q}$ can be represented by such an equation. A wealth of information on this topic may be found in Cassels' survey article [7]; see also Zimmer [32].

An important special case is the so-called *Mordell equation*, which is obtained by setting $a = 0$ in the Weierstrass equation above. For a proof of the next theorem, see Mordell [16], Chapters 24, 25 and 26, or London & Finkelstein [15].

3.4. THEOREM

Solving the equation $x^3 = y^2 + k$ $(k \in \mathbb{Z},\ k \neq 0)$ *in rational integers* x *and* y *is equivalent to one of the following*:

(i) *solving finitely many equations of type* $f_3(u,v) = 1$ *in rational integers* u *and* v, *where* f_3 *is a binary cubic form of negative or positive discriminant as* k *is negative or positive respectively.*

(ii) *solving finitely many equations of type* $f_4(u,v) = 1$ *in rational integers* u *and* v, *where* f_4 *is a binary quartic form of negative discriminant.*

(The terminology used is explained in section 4.) □

From Thue's theorem 3.1 it follows immediately that Mordell's equation $x^3 = y^2 + k$ ($k \in \mathbb{Z}$, $k \neq 0$) admits of at most finitely many solutions. Although we shall not attempt to prove theorem 3.4, it may help to know that equations of type $f_3(u,v) = 1$ are obtained by the factorization of $y^2 + k$ in prime ideals of a quadratic number field, whereas the factorization of $x^3 - k$ in prime ideals of a cubic extension of $\mathbb{Q}$ yields equations of type $f_4(u,v) = 1$.

Finally we allude to the exemplary character of theorem 3.4; the assertion, or part of it, is true for a larger class of equations than just those mentioned. This becomes evident in the next example.

3.5 <u>EXAMPLE</u> (see Stroeker [28])

In this example we consider the equation

$$(2y^2 - 3)^2 = x^2(3x^2 - 2).$$

We shall show, at least in outline, that solutions of this equation in integers x and y are determined by those of the equation

$$u^4 - 24uv^3 + 24v^4 = 1$$

in integers u and v. To be precise, the connection is given by:
$|x| = u^2 - 2uv + 4v^2$ and $|y| = u^2 + 2uv - 6v^2$.

Well then, suppose $x,y \in \mathbb{N}$ solve the original equation. Then a positive integer z exists such that

$$3x^2 - 2 = z^2 \quad \text{and} \quad 2y^2 - 3 = xz .$$

It is easy to see that both x and z must be odd and $1 \leqq x \leqq z$. On setting $u = \frac{1}{2}(z + x)$ and $v = \frac{1}{2}(z - x)$, one finds the relations

$$u^2 - 4uv + v^2 = 1 \quad \text{and} \quad u^2 - v^2 + 3 = 2y^2.$$

Hence, also $2u^2 - 6uv + v^2 = y^2$ and this equation may be written as

$$\left(\frac{v-3u-y}{2}\right)\left(\frac{v-3u+y}{2}\right) = 7\left(\frac{u}{2}\right)^2,$$

where u is even, v is odd and the factors of the left hand side are relatively prime. Moreover, these factors both have negative sign. Thus

$$v - 3u = \tfrac{1}{2}(v - 3u - y) + \tfrac{1}{2}(v - 3u + y) = -a^2 - 7b^2$$

and $$u = 2ab$$

for certain co-prime integers a and b. On substituting of $u = 2ab$, $v = -a^2 + 6ab - 7b^2$ into $u^2 - 4uv + v^2 = 1$, the equation

$$(a - b)^4 - 24(a - b)b^3 + 24b^4 = 1$$

is obtained, from which the required result follows.

Finally, we note that the original equation in x and y, representing equation is for an elliptic curve defined over $\mathbb{Q}$. The group of rational points on this curve is generated by the point $(x,y) = (3,3)$. There is only one other solution in positive integers, namely $(x,y) = (1,1)$. □

3.6 EXAMPLE (see Stroeker [24])

In this example we intend to give a rather sketchy proof of the assertion (note that we follow theorem 3.4 to the letter): the solutions in integers x and y of the equation

$$x^3 - 7y^2 = 1$$

are determined by, either the solutions in integers u and v of

(i) $u^3 - 21uv^2 = 1$ and

$u^3 - 42uv^2 + 98v^3 = 1$,

or those of the equations

(ii) $u^4 - 84u^2v^2 - 392uv^3 - 588v^4 = 1$,

$u^4 - 168u^2v^2 - 1{,}176uv^3 - 2{,}352v^4 = 1$ and

$u^4 - 924u^2v^2 - 15{,}288uv^3 - 71{,}148v^4 = 1$.

Firstly, we factorize $7y^2 + 1$ in prime ideals of $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{-7})$. Thus

$$(1 + y\sqrt{-7})(1 - y\sqrt{-7}) = x^3 .$$

The number field K has the following fundamental properties: the class number $h_K = 1$, $\{1,\omega\}$ with $\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-7}$ is a basis for $\mathcal{O}_K$ and $2 = \omega\cdot\bar{\omega}$.

Common prime ideal divisors of $(1 + y\sqrt{-7})$ and $(1 - y\sqrt{-7})$ are possibly (ω) or $(\bar{\omega})$ and no others. Hence

$$1 - y + 2y\omega = 1 + y\sqrt{-7} = (\omega)^{\alpha}(\bar{\omega})^{\beta}(a + b\omega)^3$$

with $\alpha,\beta \in \{0,1,2\}$ and $a,b \in \mathbb{Z}$. Taking also the conjugate equation into consideration, we see immediately that $\alpha + \beta = 0$ or 3. If $\alpha = \beta = 0$, then comparison of coefficients of 1 and ω left and right, and subsequently elimination of y from the resulting equations, yields

$$u^3 - 21uv^2 = 1.$$

Here u and v are defined by $2u = 2a + b$, $2v = b$.

If $\alpha = 1$ and $\beta = 2$, then similarly we obtain the equation

$$u^3 - 42uv^2 + 98v^3 = 1 ,$$

where $u = a + 4b$, $v = b$. Analogously, the assumption $\alpha = 2$, $\beta = 1$ leads to the same equation in $u = a - 3b$ and $v = -b$. This proves the first part of our assertion.

Secondly, factorization in $\mathbb{Z}$ of $x^3 - 1$ yields

$$(x - 1)(x^2 + x + 1) = 7y^2 .$$

This furnishes the three possibilities:

$$\left.\begin{aligned} x - 1 &= \lambda a^2 \\ x^2 + x + 1 &= \mu b^2 \end{aligned}\right\} \text{ with } (\lambda,\mu) = (1,7), (3,21) \text{ or } (21,3).$$

Note that $\mathrm{hcf}(x - 1, x^2 + x + 1) = 1$ or 3.

Now the particulars of the number field $L = \mathbb{Q}(\rho)$, where ρ is the third root of unity $\rho = \frac{1}{2} + \frac{1}{2}\sqrt{-3}$, are: $h_L = 1$, $\{1,\rho\}$ is a basis for O_L, the cyclic group of roots of unity is generated by ρ and the free abelian group of units is trivial, because $r + s - 1 = 0$.

For $\lambda = 1$, $\mu = 7$ we write

$$x - 1 = a^2 \quad , \quad (x + \rho)(x - \rho^2) = 7b^2 .$$

From theorem 2.6 we deduce

$$x + \rho = \pm\alpha(1 - 2\rho)^s(c + d\rho)^2 ,$$

where $\alpha \in \{2 + \rho, 3 - \rho\}$, $s \in \{0,1\}$ and $(c,d) \in \mathbb{Z}$. Note that units may be absorbed in the square $(c + d\rho)^2$.

From $\mathrm{Norm}_{L/\mathbb{Q}}(x + \rho) = 7 \cdot 3^s(c^2 + cd + d^2)^2$ and also $\mathrm{Norm}_{L/\mathbb{Q}}(x + \rho) = 7b^2$, one deduces immediately $s = 0$.

The choice $\alpha = 3 - \rho$ leads to a contradiction when considering congruences mod 4 and mod 3 successively. On the other hand, if $\alpha = 2 + \rho$ then equating coefficients yields

$$x = 2c^2 - 2cd - 3d^2 \quad \text{and} \quad 1 = c^2 + 6cd + 2d^2 .$$

Because of $a^2 = x - 1 = c^2 - 8cd - 5d^2 = (c - 4d)^2 - 21d^2$, we may write

$$21d^2 = (c - 4d - a)(c - 4d + a).$$

Further, from $\mathrm{hcf}(c - 4d - a, c - 4d + a) = 2$, we deduce the existence of co-prime integers u and v such that

$$c - 4d + a = 2u^2 \ , \ c - 4d - a = 42v^2 \ , \ d = 2uv \ .$$

The second possibility, namely $c - 4d + a = 6u^2$, $c - 4d - a = 14v^2$ and $d = 2uv$, gives rise to an impossible congruence mod 5.

Now, on substitution of $c = u^2 + 8uv + 21v^2$ and $d = 2uv$ into $c^2 + 6cd + 2d^2 = 1$, we find

$$u^4 + 28u^3v + 210u^2v^2 + 588uv^3 + 441v^4 = 1.$$

The unimodular transformation given by the matrix $\begin{pmatrix} 1 & 7 \\ 0 & -1 \end{pmatrix}$ carries this equation to the equation

$$u^4 - 84u^2v^2 - 392uv^3 - 588v^4 = 1.$$

Similar arguments are used to obtain the other two norm equations. □

4. NORM EQUATIONS

A *binary* n*-ic form* is a homogeneous polynomial of degree n in two unknowns, with coefficients in $\mathbb{Z}$. If $f_n(x,y) = \sum_{i=0}^{n} a_i x^i y^{n-i}$ is such a form, we always assume the leading coefficient a_n to be non-zero. The *discriminant* of f_n is the number $D = D(f_n) = a_n^{2n-2} \cdot \prod_{i<j} (\theta_i - \theta_j)^2$, where

$\theta_1, \theta_2, \ldots, \theta_n$ are the roots of the equation $f_n(t,1) = 0$. Clearly, $D \neq 0$ if and only if the roots of $f_n(t,1) = 0$ are distinct. Now, *norm equations* are equations of type

$$f_n(x,y) = m \qquad (m \in \mathbb{Z},\ m \neq 0),$$

where f_n is an irreducible (over $\mathbb{Q}$) binary n-ic form.

A root θ of $f_n(t,1) = 0$ gives the extension $K = \mathbb{Q}(\theta)$ of $\mathbb{Q}$ of degree n. The other roots of $f_n(t,1) = 0$ are the field conjugates of θ and

$$f_n(x,y) = \mathrm{Norm}_{K/\mathbb{Q}}(x - y\theta).$$

Solving an equation of type $\mathrm{Norm}_{K/\mathbb{Q}}(x - y\theta) = m$ ($m \in \mathbb{Z}$, $m \neq 0$) in rational integers x and y always boils down to solving a finite number of equations of the form

$$x - y\theta = \varepsilon \cdot \alpha \tag{*}$$

where α takes only finitely many different values in $\mathcal{O}_K$ (this number depends on the factorization of (m) into prime ideals of $\mathcal{O}_K$), and ε runs through the unit group of $\mathcal{O}_K$. What makes equation (*) so special is the fact that the left hand side does not contain the basis elements $\theta^2, \ldots, \theta^{n-1}$. Hence, for each value of α, the expression (*) asks for units ε of a very special type. Consequently, each equation (*) is equivalent to finitely many sets (depending on the number of roots of unity contained in $\mathcal{O}_K$) of $n - 2$ equations in the exponents of fundamental units. In case the number of fundamental units (which is the rank of the free abelian unit group: $r + s - 1$), agrees with the number of exponential equations mentioned above (this number is $n - 2 = r + 2s - 2$), then Skolem's p-adic method [22] is applicable; see also Lewis [13]. In example 4.3 we shall give a brief application of this method.

All these contemplations are illustrated by some examples.

4.1 EXAMPLE (see Nagell [17], Chapter VI)

Suppose $(x,y) \in \mathbb{Z}^2$ gives a solution of the quadratic equation

$$15x^2 + 20xy + 6y^2 = 1.$$

On setting $u = 10x + 6y$, $v = x$ this equation becomes

$$u^2 - 10v^2 = 6.$$

If $K = \mathbb{Q}(\sqrt{10})$ then $h_K = 2$, $\{1,\omega\}$ with $\omega = \sqrt{10}$ is a basis for $\mathcal{O}_K$ and $\varepsilon = 3 + \omega$ is a fundamental unit of norm -1 (see the tables of quadratic number fields in Borevich [6]). Further, 2 and 3 factor into prime ideals of $\mathcal{O}_K$ as follows: $(2) = \mathfrak{p}^2$ and $(3) = \mathfrak{q}\cdot\mathfrak{q}'$ where $\mathfrak{p} = (2,\omega)$, $\mathfrak{q} = (3,1 + \omega)$ and $\mathfrak{q}' = (3,1 - \omega)$. Hence

$$u^2 - 10v^2 = \mathrm{Norm}_{K/\mathbb{Q}}(u + v\omega) = 6$$

and this gives in terms of ideals of $\mathcal{O}_K$

$$(u + v\omega) = \mathfrak{p}\cdot\mathfrak{q} \text{ or } \mathfrak{p}\cdot\mathfrak{q}' .$$

It is not difficult to prove that $\mathfrak{p}\cdot\mathfrak{q} = (4 + \omega)$ and $\mathfrak{p}\cdot\mathfrak{q}' = (4 - \omega)$ and consequently

$$u + v\omega = \pm(4 \pm \omega)(3 + \omega)^{2k}$$

with $k \in \mathbb{Z}$ and independent ± signs. If we assume both u and v to be possitive (this is no loss of generality) then we may drop the first ± sign. As in example 2.8 the solutions can be determined by means of recurrences of order two.

The first few values of u and v are: $(u,v) = (4,1)$, $(16,5)$, $(136,43)$, $(604,191)$ etc., and the corresponding values of x (> 0) and y are: $(x,y) = (1,-1)$, $(5,11)$, $(43,-49)$, $(191,419)$ etc.

Continued fractions are also used quite frequently when dealing with quadratic equations.

□

4.2 EXAMPLE

We return to example 3.6 (i). The equation $u^3 - 21uv^2 = 1$ is trivially solvable: the only solution is $u = 1$, $v = 0$. The cubic equation

$$f_3(u,v) = u^3 - 42uv^2 + 98v^3 = 1$$

is anything but trivial. The discriminant D of f_3 is positive, to be precise $D = 2^3 3^3 7^3$ and this means that the equation $f_3(t,1) = 0$ has three real roots θ_1, θ_2 and θ_3 say. For each $i = 1,2,3$ the number field $K_i = \mathbb{Q}(\theta_i)$ has a free abelian unit group of rank 2. Hence

$$u^3 - 42uv^2 + 98v^3 = 1$$

or

$$\mathrm{Norm}_{K_i/\mathbb{Q}}(u - v\theta_i) = 1$$

is equivalent with

$$u - v\theta_i = \pm\varepsilon_1^{m_1}\cdot\varepsilon_2^{m_2} \quad ,$$

where $\{\varepsilon_1,\varepsilon_2\}$ is a set of fundamental units of $\mathcal{O}_{K_i}$. This gives rise to only *one* equation in the *two* unknown exponents m_1 and m_2; Skolem's method, referred to above, is not applicable in this case. Considering also the conjugate equations, one may try factorization in an extension of K_i. That this could get very complicated is apparent from Ljunggren [14], where the similar equation $x^3 - 3xy^2 - y^3 = 1$ is treated.

The fact that $f_3(u,v) = 1$ can be solved after all, is a consequence of the relation which exists between the solutions of this equation and those of $x^3 - 7y^2 = 1$; the solutions of the latter equation are in turn related to those of the three norm equations of 3.6 (ii), which can be solved by Skolem's p-adic method. The equations $f_4(u,v) = 1$ are found to have the solution $(u,v) = (1,0)$ and only the third equation has the additional solution $(u,v) = (13,-1)$. Further, the only solutions of $x^3 - 7y^2 = 1$ are $(x,y) = (2,1)$, $(4,3)$ and $(22,39)$. For all this and the corresponding relations we refer to [24].

The implication of these results is that the equation

$$f_3(u,v) = u^3 - 42uv^2 + 98v^3 = 1$$

has no other than the following three solutions: $(u,v) = (1,0)$, $(-3,-1)$ and $(9,2)$.

□

4.3 EXAMPLE (see Stroeker [26])

Now we shall give an example of Skolem's p-adic method. We consider the quartic norm equation

$$f_4(u,v) = u^4 + 2u^2v^2 - 2v^4 = 1 .$$

The discriminant of f_4 equals $-2^9 3^3$ and thus $f_4(t,1) = 0$ has two real roots and one pair of complex conjugate roots; $r + 2s = 4$, $r = 2$ and $s = 1$. Let θ be a real root of $f_4(t,1) = 0$. Then the ring $\mathcal{O}_K$ of $K = \mathbb{Q}(\theta)$ has a free abelian unit group of rank 2. Since K is a quadratic extension of $\mathbb{Q}(\sqrt{3})$, it easily follows that $\{1,\theta,\theta^2,\theta^3\}$ is a basis for $\mathcal{O}_K$. It is also reasonably easy to establish that $\{1 + \theta, 1 - \theta\}$ is a fundamental set. (In section 5 methods will be given for constructing a basis and a set of fundamental units for $\mathcal{O}$.)

From

$$u^4 + 2u^2v^2 - 2v^4 = 1 \quad \text{or} \quad \mathrm{Norm}_{K/\mathbb{Q}}(u - v\theta) = 1$$

we deduce

$$u - v\theta = \pm(1 + \theta)^p(1 - \theta)^q$$

with $p,q \in \mathbb{Z}$. If we do not specify the sign of u and v, then the ± sign may be dropped. Further, it is no restriction to assume $p \geq q$. Thus

$$u - v\theta = (1 + \theta)^{p-q}(1 - \theta^2)^q.$$

Because of

$$u^2 - v^2\theta^2 = (1 - \theta^2)^{p+q} = 1 - \binom{p+q}{1}\theta^2 + 2(\ldots\ldots),$$

$p - q$ is apparently odd. Put $2n + 1 = p - q$. We intend to show that $n = 0$. Define a_i, b_i, c_i and d_i for each $i \in \mathbb{Z}$ by

$$(1 + \theta)^{2i+1} = a_i + b_i\theta + c_i\theta^2 + d_i\theta^3.$$

Then from

$$u - v\theta = (a_n + b_n\theta + c_n\theta^2 + d_n\theta^3)(1 - \theta^2)^q$$

we deduce

$$a_n d_n = b_n c_n .$$

Further, let α_i and β_i be given by

$$\theta^{2i} = \alpha_i + \beta_i\theta^2 \qquad (i \in \mathbb{Z}).$$

Now, after some calculations, we obtain the expressions

$$a_n = 2\sum_{j=0}^{n} \binom{2n+1}{2j}\beta_{j-1} \quad , \quad b_n = 2\sum_{j=0}^{n} \binom{2n+1}{2j+1}\beta_{j-1} \quad ,$$

$$c_n = \sum_{j=0}^{n} \binom{2n+1}{2j}\beta_j \quad \text{and} \quad d_n = \sum_{j=0}^{n} \binom{2n+1}{2j+1}\beta_j \quad .$$

Substituting these expressions for a_n, b_n, c_n and d_n into the relation $a_nd_n = b_nc_n$, yields, after dividing through by $4(n + 1)(2n + 1)^2$,

$$\sum_{i,j=0}^{n} r_{ij}(n)\binom{2n}{2i}\binom{2n}{2j}\beta_{i-1}\beta_j = 0,$$

where the rational numbers $r_{ij}(n)$, defined by

$$r_{ij}(n) := (j - i)/(2i + 1)(2j + 1)(2n - 2i + 1)(2n - 2j + 1)$$

are 2-adic integers, i.e. they have odd denominators.

Now suppose $n \geqq 1$ with 2-adic value m (this means that n contains precisely m factors 2 in its prime decomposition). Then it is easy to show that for any pair (i,j) with $i \geqq 0$ and $j \geqq 0$ ($i = j = 0$ is excluded) the (i,j)th term in the dubble sum above has 2-adic value at least $m + 1$, with the single exception of the $(0,1)$th term, which has 2-adic value m. This is a clear contradiction, because the total sum equals zero. Hence $n = 0$. Then

$$u - v\theta = (1 + \theta)(1 - \theta^2)^q,$$

and this is only possible when $q = 0$. Consequently, $(u,v) = (1,0)$ is the only solution of the original equation $f_4(u,v) = 1$.

For more examples on this type of equation, see Stroeker [24], [25], [27] and [28].

□

5. COMPUTATIONAL CONSIDERATIONS

From the previous sections it is clear that in the process of solving a diophantine equation one is often confronted with the necessity of computing:

(i) *The class number of a number field.*

There are computer programs for calculating the class number of quadratic number fields (tables can be found in Borevich [6]) and certain cubic number fields (cf. the tables by Selmer [19] and Angell [1]).

In case one is dealing with a norm equation of type $f(x,y) = 1$, one only needs to have information on units; knowledge of class numbers of number fields involved is of little importance here.

But when studying equations of type $f(x,y) = m \neq 1$, the prime ideal decomposition of (m) plays an important part; in particular, one needs information on the class group in such cases.

Most practical methods for calculating the class number of a number field $K = \mathbb{Q}(\theta)$ use the fact that each ideal class contains an integral ideal of bounded norm (this bound M_K only depends on K).

By inspection of principal ideals of small norm, generated by elements of type $u + v\theta$ $(u,v \in \mathbb{Z})$, it is often possible to select a maximal set of inequivalent ideals representing all classes, and such that each ideal is bounded by M_K. This way one may find the class number of K. For further information the reader should consult the relevant parts of Borevich [6] and Janusz [12].

(ii) *A basis for the ring O_K of a number field* K.

In general, this is not very hard. A well written description of the computation of a canonical basis is given in Holzer [11]. We shall give a brief summary in example 5.1.

(iii) *A set of generators of the free abelian group of units (a fundamental set) in the ring* O_K *of the number field* K.

This is a very important, and often difficult part of the methods described in this exposition. In example 5.2 we will discuss a method due to Berwick [5], which is applicable in case $r + s - 1 = 2$ (thus, if $n = r + 2s$, in the cases: $(n,r,s) = (3,3,0)$, $(4,2,1)$, $(5,1,2)$ and $(6,0,3)$).

5.1 EXAMPLE (see Holzer [11], §29 pp.119 - 130)

Let θ be an algebraic integer of degree n, and put $K = \mathbb{Q}(\theta)$. A *canonical basis* for the ring O_K is a basis $\{\omega_1,\omega_2,\ldots,\omega_n\}$, where the ω_i have the following shape:

$$\begin{aligned}
\omega_1 &= 1\\
\omega_2 &= (a_{21} + \theta)/b_2\\
\omega_3 &= (a_{31} + a_{32}\theta + \theta^2)/b_3 \qquad\qquad a_{jk}, b_i \in \mathbb{Z}\\
&\vdots\\
\omega_n &= (a_{n1} + a_{n2}\theta + \ldots + a_{n,n-1}\theta^{n-2} + \theta^{n-1})/b_n
\end{aligned}$$

Moreover, $b_1 = 1$ and $b_j \geqq 1$ divides b_{j+1} for each $j = 1,\ldots,n-1$.

Such a basis always exists. In a canonical basis the a_{jk} can invariably be chosen such that

$$-\tfrac{1}{2}b_j < a_{jk} \leqq \tfrac{1}{2}b_j \quad , j = 2,\ldots,n; k = 1,\ldots,j-1$$

If $D(\theta)$ is the discriminant of the monic minimal polynomial of θ over $\mathbb{Q}$, then $\prod_{i=1}^{n} b_i^2$ divides $D(\theta)$. This puts a drastic restriction on the values of b_i.

The procedure for calculating a canonical basis runs along the following lines: suppose $\omega_1,\ldots,\omega_i$ have been determined ($\omega_1 = 1$). Then b_{i+1} must satisfy the requirements

$$b_{i+1} \geqq 1 \quad \text{and} \quad b_{i+1}^{2n-2i} \text{ divides the quotient } D(\theta)/\prod_{j=1}^{i} b_j^2 .$$

For each of the possible values for b_{i+1}, find $a_{i+1,k}$ such that

$$-\tfrac{1}{2}b_{i+1} < a_{i+1,k} \leqq \tfrac{1}{2}b_{i+1} \qquad k = 1,\ldots,i .$$

Finally, check whether ω_{i+1}, thus obtained, is an algebraic integer. The last part of this process may be accomplished as follows: For $\alpha = (a_1 + a_2\theta + \ldots + a_{n-1}\theta^{n-2} + \theta^{n-1})/b$ with $-\frac{1}{2}b < a_j \leqq \frac{1}{2}b$, we try to construct the monic defining polynomial of α over $\mathbb{Q}$. To this end we consider the $n\times n$ matrix R with rational entries, satisfying:

(1) bR has only integral entries, and

(2) $(\alpha I_n - R)v_\theta = 0$, where v_θ is the column vector with components $1,\theta,\ldots,\theta^{n-1}$. To calculate this expression, note that for each i the product $\alpha\theta^i$ can be written as a linear combination of $1,\theta,\ldots,\theta^{n-1}$ with coefficients in $\frac{1}{b}\mathbb{Z}$.

Since $v_\theta \neq 0$, we have $\det(\alpha I_n - R) = 0$. Now, $\det(tI_n - R) = t^n + A_1t^{n-1} + \ldots + A_n$ is the minimal defining polynomial of α over $\mathbb{Q}$. Hence α is an algebraic integer if and only if $A_i \in \mathbb{Z}$ for all i. Because $b^iA_i \in \mathbb{Z}$ and $-\frac{1}{2}b < a_i \leqq \frac{1}{2}b$, it is not difficult, using congruences, to decide whether α is integral or not.

A non-trivial example can be found in Stroeker [25], p.137. The discriminant of $f(t) = t^4 - 126t^2 - 756t - 1323$ equals $D(f) = -2^8 3^9 7^4$. If ξ is a real root of $f(t) = 0$, then a canonical basis for $\mathcal{O}_K$ with $K = \mathbb{Q}(\xi)$ is $\{\omega_1,\omega_2,\omega_3,\omega_4\}$ with $\omega_1 = 1$, $\omega_2 = \xi$, $\omega_3 = (3 + \xi^2)/6$ and $\omega_4 = (63 + \xi^3)/126$.

□

5.2 EXAMPLE

We continu the previous example, but this time we direct our attention to the units of $\mathcal{O}_K$. Here $K = \mathbb{Q}(\xi)$ and ξ is a real root of the polynomial $f(t) = t^4 - 126t^2 - 756t - 1323$. Because $4 = r + 2s$ and $r = 2$, $s = 1$ a fundamental set of units has $r + s - 1 = 2$ elements. According to Berwick [5], p. 367, the free abelian unit group of O_K is generated by each couple of units defined by:

(1) $\varepsilon > 1$ and minimal , $|\varepsilon'| < 1$, $\varepsilon''\bar{\varepsilon}'' < 1$

(2) $|\varepsilon| < 1$, $\varepsilon' > 1$ and minimal , $\varepsilon''\bar{\varepsilon}'' < 1$

(3) $|\varepsilon| < 1$, $|\varepsilon'| < 1$, $|\varepsilon''| = |\bar{\varepsilon}''| > 1$ and minimal .

In addition we have $\varepsilon_1\varepsilon_2\varepsilon_3 = 1$ as ε_j is determined by (j). Note that ε', ε'' and $\bar{\varepsilon}''$ are the field conjugates of ε.

An algorithm for computing the units ε_j is easily devised: let each of the restrictions from (1), (2) and (3) successively be imposed on

$$\varepsilon = a\omega_1 + b\omega_2 + c\omega_3 + d\omega_4 \ .$$

Since the ω_i have known values, we get conditions on the rational integers a, b, c and d. So this provides ε with something like an "ideal ratio" $a : b : c : d$ for the $\mathrm{Norm}_{K/\mathbb{Q}}(\varepsilon)$ to be small (this process also can be used when calculating class numbers; see under (i) at the beginning of this section). A very clear exposition, with many examples, is given in London & Finkelstein [15], p.81 etc.; here the algorithm in question is called the *scaling algorithm*.

Finally, we end this example by giving the values of ε_j in the field $K = \mathbb{Q}(\xi)$:

$$\varepsilon_1 = 151\omega_1 + 117\omega_2 + 29\omega_3 - 98\omega_4 \ ,$$
$$\varepsilon_2 = \omega_1 + \omega_2 - \omega_4 \text{ and}$$
$$\varepsilon_3 = 9\omega_1 - 4\omega_2 - 2\omega_3 + 4\omega_4 \ .$$

The canonical basis $\{\omega_1,\omega_2,\omega_3,\omega_4\}$ used is the one exhibited in example 5.1.

□

REFERENCES

[1] ANGELL, I.O. - A table of totally real cubic fields. Math. Comp. 30 (1976), no.133, 184 - 187

[2] BAKER, A. - Effective methods in Diophantine problems. Proc. Sympos. Pure Math., vol.20, Amer. Math. Soc., Providence R.I. (1971), 195 - 205

[3] BAKER, A. - Effective methods in Diophantine problems, II. Proc. Sympos. Pure Math., vol.24, Amer. Math. Soc., Providence R.I. (1973), 1 - 7

[4] BAŠMAKOVA, I.G. - Diophant und Diophantische Gleichungen. Uni-Taschenbücher 360, Birkhäuser Verlag, Basel und Stuttgart, 1974

[5] BERWICK, W.E.H. - Algebraic number fields with two independent units. Proc. London Math. Soc. 34 (1932), 360 - 378

[6] BOREVICH, Z.I. & I.R. SHAFAREVICH - Number theory. Pure and Appl. Math. Ser., vol.20, Acad. Press, London and New York, 1966

[7] CASSELS, J.W.S. - Diophantine equations with special reference to elliptic curves. J. Math. Soc. 41 (1966), 193 - 291

[8] DICKSON, L.E. - History of the theory of numbers, Vol.II: Diophantine analysis. Chelsea Publ., New York (1971), (repr. from orig. 1920 ed.)

[9] EDWARDS, H.M. - Fermat's last theorem. A genetic introduction to algebraic number theory. Graduate texts in Maths, vol.50, Springer Verlag, New York, Heidelberg, Berlin, 1977

[10] FINKELSTEIN, R. & H. LONDON - On Mordell's equation $y^2 - k = x^3$: an interesting case of Sierpinski. J. Number Theory 2 (1970), 310 - 321

[11] HOLZER, L. - Zahlentheorie, Teil I. Math. Naturw. Bibl. 13, B.G. Teubner Verlag, Leipzig, 1958

[12] JANUSZ, G.J. - Algebraic number fields. Pure and Appl. Math. Ser. Vol. 55, Acad. Press, New York and London, 1973

[13] LEWIS, D.J. - Diophantine equations: p-adic methods. In: W.J. Leveque (ed.), Studies in number theory, Math. Ass. Amer., (1969), 25 - 75

[14] LJUNGGREN, W. - Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiven Diskriminante. Acta Math. 75 (1942), 1 - 21

[15] LONDON, H. & R. FINKELSTEIN - On Mordell's equation $y^2 - k = x^3$. Bowling Green State Un. Press, Bowling Green Ohio, 1973

[16] MORDELL, L.J. - Diophantine equations. Pure and Appl. Math. Ser. Vol. 30, Acad. Press, New York and London, 1969

[17] NAGELL, T. - Introduction to number theory. Chelsea Publ., New York, 1964 (repr. of 2nd ed. 1951)

[18] RIBENBOIM, P. - 13 Lectures on Fermat's last theorem. Springer Verlag, New York-Heidelberg-Berlin, 1979

[19] SELMER, E.S. - Tables for the purely cubic field $K(\sqrt[3]{m})$. Avh. Norske Vid. Akad. Oslo, I. Mat. Naturv., Klasse 1955, no. 5

[20] SHOREY, T.N., A.J. VAN DER POORTEN, R. TIJDEMAN & A. SCHINZEL - Applications of the Gel'fond - Baker method to Diophantine equations. In: A. Baker & D.W. Masser (eds.), Transcendence Theory: Advances and applications. Acad. Press, London, New York, San Francisco (1977),59 - 77

[21] SKOLEM, T. - Diophantische Gleichungen. Erg. Math. Grenzgeb. Bd. 5, Heft 4, Springer, Berlin 1938 (repr. by Chelsea N.Y., 1950)

[22] SKOLEM, T. - The use of p-adic methods in the theory of diophantine equations. Bull. Soc. Math. Belg. 7 (1955), 83 - 95

[23] STROEKER, R.J. - Pythagoras met een nevenvoorwaarde. Euclides 47 (6), (1971/72), 217 - 220

[24] STROEKER, R.J. - On the Diophantine equation $x^3 - Dy^2 = 1$. Nieuw Arch. v. Wisk. (3) XXIV (1976), 231 - 255

[25] STROEKER, R.J. - On a diophantine equation of E. Bombieri. Proc. Kon. Ned. Akad. v. Wetensch. (= Indag. Math.) Ser. A, 80 (2), (1977), 131 - 139

[26] STROEKER, R.J. - Triangular-square-pentagonal numbers. Report 7701/M, Econometric Inst., Erasmus Un. Rotterdam, 1977

[27] STROEKER, R.J. - A class of diophantine equations connected with certain elliptic curves over $\mathbb{Q}(\sqrt{-13})$. Comp. Math. 38 (3), (1979), 329 - 346

[28] STROEKER, R.J. - On the diophantine equation $(2y^2-3)^2 = x^2(3x^2-2)$ in connection with the existence of non-trivial tight 4-designs. Reports 7930/M and 7934/M, Econometric Inst., Erasmus Un. Rotterdam, 1979

[29] STROEKER, R.J. - The diophantine equation $(x^2+y)(x+y^2) = N(x-y)^3$. To appear in Simon Stevin

[30] TIJDEMAN, R. - Exponential diophantine equations. Proc. Intern. Congress Math., Helsinki 1978, 381 - 387

[31] TIJDEMAN, R. - Applications of the Gel'fond - Baker method to rational number theory. In: P. Turán (ed.), Topics in number theory. Colloq. Math. Soc. János Bolyai, 13. North-Holland Publ. Co., Amsterdam-Oxford-New York, 1976, 399 - 416

[32] ZIMMER, H.G. - Computational problems, methods, and results in algebraic number theory. Lect. Notes in Math. 262, Springer Verlag, Berlin-Heidelberg-New York, 1972

LIST OF REPORTS 1980

8000 "List of Reprints, nos 241-260, Abstracts of Reports Second Half 1979".

8001/O "A Stochastic Method for Global Optimization", by C.G.E. Boender, A.H.G. Rinnooy Kan, L. Stougie and G.T. Timmer.

8002/M "The General Linear Group of Polynomial Rings over Regular Rings", by A.C.F. Vorst.

8003/O "A Recursive Approach to the Implementation of Enumerative Methods", by J.K. Lenstra and A.H.G. Rinnooy Kan.

8004/E "Linearization and Estimation of the Add -Log Budget Allocation Model", by P.M.C. de Boer and J. van Daal.

8005/O "The Complexity of the Constrained Gradient Method for Linear Programming", by J. Telgen.

8006/S "On Functions with Small Differences", by J.L. Geluk and L. de Haan.

8007/O "Analytical Evaluation of Hierarchical Planning Systems", by M.A.H. Dempster, M.L. Fisher, L. Jansen, B.J. Lageweg, J.K. Lenstra and A.H.G. Rinnooy Kan.

8008/S "Looking at Multiway Tables (continued)", by A.P.J. Abrahamse and W.M. Lammerts van Bueren.

8009/O "An Introduction to Multiprocessor Scheduling", by J.K. Lenstra and A.H.G. Rinnooy Kan.

8010/M "On Families of Systems: Pointwise-Local-Global Isomorphism Problems, by M. Hazewinkel and A.M. Perdon.

8011/M "Proceedings Filter-Day Rotterdam 1980 (New Trends in Filtering and Identification of Stochastic Systems, 23 jan. 1980), by M. Hazewinkel (ed).

8012/E "Further Experience in Bayesian Analysis Using Monte Carlo Integration" by H.K. van Dijk and T. Kloek.

8013/M "Note on the Eigenvalues of the Covariance Matrix of Disturbances in the General Linear Model, II", by R.J. Stroeker.

8014/M "Factorization Methods for Solving Diophantine Equations", by R.J. Stroeker.