Communicated 14 October 1953 by T. Nagell and Otto Frostman

On the Diophantine equation $u^2 - D v^2 = \pm 4 N$

By Bengt Stolt

Part III

§ 1. Introduction

Consider the Diophantine equation

$$u^2 - D v^2 = \pm 4 N, \tag{1}$$

where D and N are integers and D is not a perfect square. In Part I of this investigation[1] it was shown that it is possible to determine all the solutions of (1) by elementary methods[2].

Suppose that (1) is solvable, and let u and v be two integers satisfying (1). Then $\frac{1}{2}(u + v\sqrt{D})$ is called a *solution* of (1). If $\frac{1}{2}(x + y\sqrt{D})$ is a solution of the Diophantine equation

$$x^2 - D y^2 = 4, \tag{2}$$

the number

$$\frac{u + v\sqrt{D}}{2} \cdot \frac{x + y\sqrt{D}}{2} = \frac{u_1 + v_1\sqrt{D}}{2}$$

is also a solution of (1). This solution is said to be *associated* with the solution $\frac{1}{2}(u + v\sqrt{D})$. The set of all solutions associated with each other forms a *class of solutions* of (1).

A necessary and sufficient condition for the two solutions $\frac{1}{2}(u + v\sqrt{D})$, $\frac{1}{2}(u' + v'\sqrt{D})$ to belong to the same class is that the number

$$\frac{v u' - u v'}{2 N}$$

be an integer.

[1] See [1].

[2] These methods were developed by T. Nagell, who used them for determining all the solutions of the Diophantine equation

$$u^2 - D v^2 = \pm N.$$

Nagell also proposed the notions used in this section. See [2], [3], [4], [5].

Let $\boldsymbol{K}$ be a class which consists of the numbers $\frac{1}{2}(u_i + v_i\sqrt{D})$, $i = 1, 2, 3, \cdots$. Then the numbers $\frac{1}{2}(u_i - v_i\sqrt{D})$, $i = 1, 2, 3, \ldots$ form another class, which is denoted by $\bar{\boldsymbol{K}}$. $\boldsymbol{K}$ and $\bar{\boldsymbol{K}}$ are said to be *conjugates* of one another. Conjugate classes are in general distinct but may sometimes coincide; in the latter case the class is called *ambiguous*.

Among the solutions of $\boldsymbol{K}$, a *fundamental solution of the class* is defined in the following way. $\frac{1}{2}(u^* + v^*\sqrt{D})$ is the fundamental solution of $\boldsymbol{K}$, if v^* is the smallest non-negative value of v of any solution belonging to the class. If the class is not ambiguous, u^* is also uniquely determined, because

$$\tfrac{1}{2}(-u^* + v^*\sqrt{D})$$

belongs to the conjugate class; if the class is ambiguous, u^* is uniquely determined by supposing $u^* \geqq 0$. $u^* = 0$ or $v^* = 0$ only occurs when the class is ambiguous.

If $N = 1$, there is only one class of solutions, and this class is ambiguous.

For the fundamental solution of a class the following theorems were deduced (D and N are natural numbers, and D is not a perfect square).

Theorem. *If* $\frac{1}{2}(u + v\sqrt{D})$ *is the fundamental solution of the class* $\boldsymbol{K}$ *of the Diophantine equation*

$$u^2 - Dv^2 = 4N, \tag{3}$$

and if $\frac{1}{2}(x_1 + y_1\sqrt{D})$ *is the fundamental solution of* (2), *we have the inequalities*

$$0 \leqq v \leqq \frac{y_1}{\sqrt{x_1 + 2}}\sqrt{N}, \tag{4}$$

$$0 < |u| \leqq \sqrt{(x_1 + 2)N}. \tag{5}$$

Theorem. *If* $\frac{1}{2}(u + v\sqrt{D})$ *is the fundamental solution of the class* $\boldsymbol{K}$ *of the Diophantine equation*

$$u^2 - Dv^2 = -4N, \tag{6}$$

and if $\frac{1}{2}(x_1 + y_1\sqrt{D})$ *is the fundamental solution of* (2), *we have the inequalities*

$$0 < v \leqq \frac{y_1}{\sqrt{x_1 - 2}}\sqrt{N}, \tag{7}$$

$$0 \leqq |u| \leqq \sqrt{(x_1 - 2)N}. \tag{8}$$

Theorem. *The Diophantine equations* (3) *and* (6) *have a finite number of classes of solutions. The fundamental solution of all the classes can be found after a finite number of trials by means of the inequalities in the preceding theorems.*

If $\frac{1}{2}(u_1+v_1\sqrt{D})$ *is the fundamental solution of the class* $\boldsymbol{K}$, *we obtain all the solutions* $\frac{1}{2}(u+v\sqrt{D})$ *of* $\boldsymbol{K}$ *by the formula*

$$\frac{u+v\sqrt{D}}{2}=\frac{u_1+v_1\sqrt{D}}{2}\cdot\frac{x+y\sqrt{D}}{2},$$

where $\frac{1}{2}(x+y\sqrt{D})$ *runs through all the solutions of* (2), *including* ± 1. *The Diophantine equations* (3) *and* (6) *have no solutions at all when they have no solutions satisfying inequalities* (4) *and* (5), *or* (7) *and* (8) *respectively.*

In Part II[1] it was shown that it is possible to determine the maximum number of classes corresponding to an arbitrarily given N by elementary methods. In this paper we shall determine the number of classes by means of the theory of algebraic numbers and ideals. The exact number of classes corresponding to square-free N will be determined. We shall also prove that the number n of classes corresponding to square-free N is a power of 2, incl. 1. Further, the number of classes corresponding to N which is the power of just one prime will be determined.

In order to determine the fundamental solutions we may also use inequalities derived by means of algebraic number theory. It will be shown that inequalities derived by elementary methods give better results.

§ 2. Generalities

In this section we define some notions of the theory of algebraic numbers. For the details of this theory see for example Landau, Zahlentheorie.[2]

Let D be a rational integer which is square-free. An algebraic integer of the field $\boldsymbol{K}(\sqrt{D})$ is denoted by α and its conjugate integer by α'. An ideal of the field is denoted by one of the letters $A, B, \ldots$ and its conjugate ideal by A', or $B'\ldots$ respectively. An ideal which is generated by α is denoted by (α).

Let p be a rational prime. If $\Delta=D$, when $D\equiv 1 \pmod{4}$, and $\Delta=4D$ in other cases, the ideal (p) is the product of two conjugate prime ideals, or is the square of a prime ideal, or is itself a prime ideal, according as Kronecker's symbol $\left(\frac{\Delta}{p}\right)$ has the value $+1$, or 0, or -1 respectively. When (p) is not a prime ideal we write $(p)=\mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}'=\mathfrak{p}$ if $\left(\frac{\Delta}{p}\right)=0$.

Consider the Diophantine equation

$$u^2-Dv^2=\pm 4N, \tag{1}$$

where D and N are integers and D is square-free. If (1) is solvable, every solution of (1) is an algebraic integer α of the field $\boldsymbol{K}(\sqrt{D})$. Thus the ideal (N) is the product of two conjugate principal ideals, $(N)=(\alpha)(\alpha')$. Then it is

[1] See [6].
[2] See [7].

apparent that every one of the ideals (α), (α') corresponds to just one class of solutions as defined above. If $(\alpha) = (\alpha')$, (α) corresponds to an ambiguous class.

Now suppose that D contains quadratic factors. Then $D = r^2 D_1$, where D_1 is square-free. In that case every solution of (1) is an algebraic integer of the ring $\boldsymbol{R}(r\sqrt{D_1})$. Thus we have to consider integers and ideals of this ring.

In the following sections we shall determine the number of classes of the Diophantine equation

$$(1) \qquad u^2 - Dv^2 = \pm 4N$$

for certain values of N. In all the cases D and N are rational integers and D is not a perfect square. The theorems are proved for the case when D is square-free. If D contains quadratic factors, $D = r^2 D_1$, D_1 square-free, in all the theorems we have to substitute the field $\boldsymbol{K}(\sqrt{D})$ by the ring $\boldsymbol{R}(r\sqrt{D_1})$.

§ 3. *N* is square-free

Theorem 11. *Suppose that* $N = p_1 p_2 \dots p_n$, *where* $p_1, p_2, \dots, p_n$ *are primes,* $p_i \neq p_j$, *and suppose that the Diophantine equation*

$$(10) \qquad u^2 - Dv^2 = \pm 4 p_1 p_2 \dots p_n$$

is solvable. Further suppose that $\left(\frac{\Delta}{p_i}\right) = +1$ *holds for* m *of the primes* p_i, $n \geqq m \geqq 1$, *and that* $\left(\frac{\Delta}{p_j}\right) = 0$ *holds for the remaining primes* p_j, $m \geqq i \geqq 1$, $n \geqq j \geqq m+1$. *If* $(p_i) = \mathfrak{p}_i \mathfrak{p}_i'$, $(p_j) = \mathfrak{p}_j^2$, *as* (10) *is solvable there exists the equivalence*

$$\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m \mathfrak{p}_{m+1} \dots \mathfrak{p}_n \sim (1).$$

Suppose that

$$\mathfrak{p}_i \sim \mathfrak{p}_i'$$

holds for k_1 *of the prime ideals,* $m \geqq i \geqq 1$,

$$\mathfrak{p}_i \mathfrak{p}_j \sim \mathfrak{p}_i' \mathfrak{p}_j'$$

holds for k_2 *pairs of the remaining prime ideals,* $k_1 + k_2 \geqq i \geqq k_1 + 1$, $k_1 + 2k_2 \geqq j \geqq k_1 + k_2 + 1$,

$$\mathfrak{p}_i \mathfrak{p}_j \mathfrak{p}_k \sim \mathfrak{p}_i' \mathfrak{p}_j' \mathfrak{p}_k'$$

holds for k_3 *triples of the remaining prime ideals,*

$$k_1 + 2k_2 + k_3 \geqq i \geqq k_1 + 2k_2 + 1, \quad k_1 + 2k_2 + 2k_3 \geqq j \geqq k_1 + 2k_2 + k_3 + 1,$$

$k_1 + 2k_2 + 3k_3 \geqq k \geqq k_1 + 2k_2 + 2k_3 + 1$, *and so on, every* $\mathfrak{p}_i$ *belonging to just one* *of the equivalences,* $\left[\frac{m}{h}\right]\geqq k_h\geqq 0$. *If* $k=\sum k_h$ *the Diophantine equation has* 2^k *classes,* $m\geqq k\geqq 1$.

If N *divides* D, (10) *has one class.*

Proof. Suppose that (10) is solvable. If N divides D, it was shown by elementary methods that (10) has only one class.

Suppose that (10) is solvable. Further suppose that $\left(\frac{\Delta}{p_i}\right)=+1$ holds for m of the primes p_i, $m\geqq i\geqq 1$, $n\geqq m\geqq 1$, and suppose that $\left(\frac{\Delta}{p_j}\right)=0$ holds for the remaining primes p_j, $n\geqq j\geqq m+1$. Then $(p_i)=\mathfrak{p}_i\mathfrak{p}_i'$, $(p_j)=\mathfrak{p}_j^2$.

As (10) is solvable there exists an equivalence

$$\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_m\mathfrak{p}_{m+1}\ldots\mathfrak{p}_n\sim(1) \tag{11}$$

which corresponds to a class of solutions of (10). Now suppose that $\mathfrak{p}_i\sim\mathfrak{p}_i'$ holds for $i=1, 2, \ldots, k_1$, $m\geqq k_1\geqq 0$. Changing $\mathfrak{p}_i$ and $\mathfrak{p}_i'$ in (11) we get another principal ideal which also corresponds to a class of (10). Since there are k_1 equivalences $\mathfrak{p}_i\sim\mathfrak{p}_i'$ it is apparent that the number of classes is a multiple of 2^{k_1}.

Now suppose that $\mathfrak{p}_i\mathfrak{p}_j\sim\mathfrak{p}_i'\mathfrak{p}_j'$ holds for k_2 pairs of the remaining prime ideals, $k_1+k_2\geqq i\geqq k_1+1$, $k_1+2k_2\geqq j\geqq k_1+k_2+1$, every prime ideal belonging to one pair at most. Then changing $\mathfrak{p}_i\mathfrak{p}_j$ and $\mathfrak{p}_i'\mathfrak{p}_j'$ in every one of the 2^{k_1} equivalences for which (11) holds we get 2^{k_1} new equivalences for which (11) holds. Since there are k_2 equivalent pairs of prime ideals we get $2^{k_1+k_2}$ classes.

If $\mathfrak{p}_i\mathfrak{p}_j\mathfrak{p}_k\sim\mathfrak{p}_i'\mathfrak{p}_j'\mathfrak{p}_k'$ holds for k_3 triples of the remaining $m-(k_1+2k_2)$ prime ideals,

$$k_1+2k_2+k_3\geqq i\geqq k_1+2k_2+1,\ k_1+2k_2+2k_3\geqq j\geqq k_1+2k_2+k_3+1,$$
$$k_1+2k_2+3k_3\geqq k\geqq k_1+2k_2+2k_3+1,$$

every prime ideal belonging to one triple at most, it is apparent that we get $2^{k_1+k_2+k_3}$ classes.

Considering the quadruples of prime ideals and so on it is apparent that every prime ideal $\mathfrak{p}_i$, $m\geqq i\geqq 1$, belongs to just one product of prime ideals which is equivalent to the product of its conjugate prime ideals. Thus if $k=k_1+$ $+k_2+\cdots+k_h$ the number of classes is 2^k. This proves the theorem.

From Theorem 11 we deduce at once

Theorem 12. *Suppose that* $N=p_1p_2\ldots p_n$, *where* $p_1, p_2, \ldots, p_n$ *are distinct primes. If the Diophantine equation*

$$u^2-Dv^2=\pm 4p_1p_2\ldots p_n \tag{10}$$

is solvable, the number of classes is a power of 2.

We also prove

Theorem 13. *Suppose that* $p_1, p_2, \ldots, p_n$ *are distinct primes. Then it is possible to determine an integer* D *which is not a perfect square in such way that*

$\left(\frac{\Delta}{p_i}\right) = +1$ *holds for* $i = 1, 2, \ldots; n$. *If the number of ideal classes in the field* $K(\sqrt{D})$ *is* $\leqq 2$, *the Diophantine equation*

$$u^2 - Dv^2 = \pm 4\, p_1 p_2 \ldots p_n \tag{10}$$

has 2^n *classes of solutions when solvable.*

Proof. Suppose that there is only one class of ideals of the field $K(\sqrt{D})$. Then every prime ideal of the field is a principal ideal. If there are two classes in the field, one of them contains all principal ideals. If A is an ideal of the other class, clearly $A^2 \sim (1)$. Thus $A \sim A'$. Hence the theorem is proved.

If $D = 2$ and $p_i \equiv \pm 1$ (mod. 8) holds for $i = 1, 2, \ldots, n$ the corresponding equation is always possible. In Part I this case was treated by elementary methods.

§ 4. N is a prime power

We next prove

Theorem 14. *Suppose that* $N = p^{2b+1}$, *where* b *is a positive integer and* p *is a prime. Further suppose that the Diophantine equation*

$$u^2 - Dv^2 = \pm 4\, p^{2b+1} \tag{12}$$

is solvable.

If the greatest power of p *which divides* D *is* $p^{2\alpha}$ *or* $p^{2\beta+1}$, $\alpha > b$, $\beta \geqq 0$, (12) *has only one class.*

Suppose that the greatest power of p *which divides* D *is* $p^{2\alpha}$, $b \geqq \alpha \geqq 0$, *and suppose that* $D = p^{2\alpha} D_1$ *and that* Δ_1 *refers to the field* $K(\sqrt{D_1})$. *If* $\left(\frac{\Delta_1}{p}\right) = 0$ *holds,* (12) *has only one class. If* $\left(\frac{\Delta_1}{p}\right) = +1$ *holds,* $(p) = \mathfrak{p}\mathfrak{p}'$. *Suppose that* $\mathfrak{p}^{2b'+1}$ *is the least odd power of* $\mathfrak{p}$ *for which*

$$\mathfrak{p}^{2b'+1} \sim (1)$$

holds, $b' \geqq 0$. *If* $\left[\frac{b - \alpha + b' + 1}{2b' + 1}\right]$ *denotes the greatest integer* $\leqq \frac{b - \alpha + b' + 1}{2b' + 1}$, (12) *has* $2\left[\frac{b - \alpha + b' + 1}{2b' + 1}\right]$ *classes.*

Proof. Suppose that (12) is solvable. In Part II the case when the greatest power of p which divides D is $p^{2\alpha}$ or $p^{2\beta+1}$, $\alpha > b$, $\beta \geqq 0$, was solved by elementary methods.

Suppose that the greatest power of p which divides D is $p^{2\alpha}$, $b \geqq \alpha \geqq 0$. Then both sides of (12) are divisible by $p^{2\alpha}$. If $u = p^{\alpha} u'$, $D = p^{2\alpha} D_1$, dividing (12) by $p^{2\alpha}$ we get

$$u'^2 - D_1 v^2 = \pm 4\, p^{2(b-\alpha)+1}. \tag{13}$$

Suppose that Δ_1 refers to the field $\boldsymbol{K}(\sqrt{D_1})$. If $\left(\frac{\Delta_1}{p}\right)=0$ it is apparent that (12) has only one class.

Suppose that $\left(\frac{\Delta_1}{p}\right)=+1$ holds. Then $(p)=\mathfrak{p}\,\mathfrak{p}'$, where $\mathfrak{p}$ and $\mathfrak{p}'$ are prime ideals.

Consider

$$(p)^{2(b-\alpha)+1}=\mathfrak{p}^{2(b-\alpha)+1}\,\mathfrak{p}'^{\,2(b-\alpha)+1}. \tag{14}$$

It is apparent that the prime ideals of the right-hand side of (14) may be combined together in the following $b-\alpha+1$ different ways in order to form pairs of conjugate ideals.

$$\begin{aligned}
&\mathfrak{p}^{2(b-\alpha)+1},\ \mathfrak{p}'^{\,2(b-\alpha)+1},\\
&\mathfrak{p}^{2(b-\alpha)}\,\mathfrak{p}',\ \mathfrak{p}\,\mathfrak{p}'^{\,2(b-\alpha)},\\
&\cdots\cdots\cdots\cdots\\
&\mathfrak{p}^{b-\alpha+1}\,\mathfrak{p}'^{\,b-\alpha},\ \mathfrak{p}^{b-\alpha}\,\mathfrak{p}'^{\,b-\alpha+1}.
\end{aligned}$$

Observing that $(p)=\mathfrak{p}\,\mathfrak{p}'$ these ideals may be written

$$\begin{aligned}
&\mathfrak{p}^{2(b-\alpha)+1},\ \mathfrak{p}'^{\,2(b-\alpha)+1},\\
&\mathfrak{p}^{2(b-\alpha)-1}\,(p),\ \mathfrak{p}'^{\,2(b-\alpha)-1}\,(p),\\
&\mathfrak{p}^{2(b-\alpha)-3}\,(p)^2,\ \mathfrak{p}'^{\,2(b-\alpha)-3}\,(p)^2,\\
&\cdots\cdots\cdots\cdots\\
&\mathfrak{p}^{3}\,(p)^{b-\alpha-1},\ \mathfrak{p}'^{\,3}\,(p)^{b-\alpha-1},\\
&\mathfrak{p}\,(p)^{b-\alpha},\ \mathfrak{p}'\,(p)^{b-\alpha}.
\end{aligned}$$

If $\mathfrak{p}\sim(1)$ every one of these ideals is a principal ideal. In that case the number of classes is $2(b-\alpha+1)$.

Suppose that $\mathfrak{p}^{2b'+1}$ is the least odd power of $\mathfrak{p}$ for which

$$\mathfrak{p}^{2b'+1}\sim(1)$$

holds. In that case only the following ideals are principal ideals.

$$\begin{aligned}
&\mathfrak{p}^{2b'+1}\,(p)^{b-\alpha-b'},\ \mathfrak{p}'^{\,2b'+1}\,(p)^{b-\alpha-b'},\\
&\mathfrak{p}^{3(2b'+1)}\,(p)^{b-\alpha-3b'-1},\ \mathfrak{p}'^{\,3(2b'+1)}\,(p)^{b-\alpha-3b'-1},\\
&\mathfrak{p}^{5(2b'+1)}\,(p)^{b-\alpha-5b'-2},\ \mathfrak{p}'^{\,5(2b'+1)}\,(p)^{b-\alpha-3b'-1},\\
&\cdots\cdots\cdots\cdots\\
&\mathfrak{p}^{(2m+1)(2b'+1)}\,(p)^{b-\alpha-(2m+1)b'-m},\\
&\qquad\qquad\mathfrak{p}'^{\,(2m+1)(2b'+1)}\,(p)^{b-\alpha-(2m+1)b'-m},\\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

If $\left[\frac{b-\alpha+b'+1}{2b'+1}\right]$ denotes the greatest integer $\leqq \frac{b-\alpha+b'+1}{2b'+1}$, it is apparent that (12) has

$$2\left[\frac{b-\alpha+b'+1}{2b'+1}\right]$$

classes. Hence the theorem is proved.

We also prove

Theorem 15. *Suppose that* $N=p^{2a}$, *where* a *is a positive integer and* p *is a prime. Further suppose that the Diophantine equation*

$$u^2-Dv^2=\pm 4p^{2a} \tag{15}$$

is solvable.

If the greatest power of p *which divides* D *is* $p^{2\alpha}$ *or* $p^{2\beta+1}$, $\alpha\geqq a$, $\beta\geqq 0$, (15) *has only one class.*

Suppose that the greatest power of p *which divides* D *is* $p^{2\alpha}$, $a>\alpha\geqq 0$. *Further suppose that* $D=p^{2\alpha}D_1$ *and that* Δ_1 *refers to the field* $\boldsymbol{K}(\sqrt{D_1})$. *If* $\left(\frac{\Delta_1}{p}\right)\neq +1$ *holds,* (15) *has only one class. If* $\left(\frac{\Delta_1}{p}\right)=+1$ *holds,* $(p)=\mathfrak{p}\mathfrak{p}'$. *Suppose that* $\mathfrak{p}^{2a'}$ *is the least even power of* $\mathfrak{p}$ *for which*

$$\mathfrak{p}^{2a'}\sim(1)$$

holds, and suppose that $\left[\frac{a-\alpha}{a'}\right]$ *denotes the greatest integer* $\leqq\frac{a-\alpha}{a'}$. *If the Diophantine equation*

$$x^2-D_1y^2=\pm 4 \tag{16}$$

is solvable, (15) *has* $2\left[\frac{a-\alpha}{a'}\right]+1$ *classes. If* (16) *is not solvable,* (15) *has* $2\left[\frac{a-\alpha}{a'}\right]$ *classes.*

Proof. Suppose that (15) is solvable. In Part II the case when the greatest power of p which divides D is $p^{2\alpha}$ or $p^{2\beta+1}$, $\alpha\geqq a$, $\beta\geqq 0$, was solved by elementary methods.

Suppose that the greatest power of p which divides D is $p^{2\alpha}$, $a>\alpha\geqq 0$. Then both sides of (15) are divisible by $p^{2\alpha}$. If $u=p^{\alpha}u'$, $D=p^{2\alpha}D_1$, dividing (15) by $p^{2\alpha}$ we get

$$u'^2-D_1v^2=\pm 4p^{2(a-\alpha)}. \tag{17}$$

Suppose that Δ_1 refers to the field $\boldsymbol{K}(\sqrt{D_1})$. If $\left(\frac{\Delta_1}{p}\right)\neq +1$ it is apparent that (15) has only one ambiguous class the solutions of which correspond to the solutions of the Diophantine equation

$$x^2-D_1y^2=\pm 4. \tag{16}$$

Suppose that $\left(\frac{\Delta_1}{p}\right) = +1$ holds. Then $(p) = \mathfrak{p}\,\mathfrak{p}'$, where $\mathfrak{p}$ and $\mathfrak{p}'$ are prime ideals.

Consider the product

$$(p)^{2(a-\alpha)} = \mathfrak{p}^{2(a-\alpha)}\,\mathfrak{p}'^{\,2(a-\alpha)}. \tag{18}$$

It is apparent that the prime ideals of the right-hand side of (18) may be combined in $a-\alpha+1$ different ways in order to form pairs of conjugate ideals. Observing $\mathfrak{p}\,\mathfrak{p}' = (p)$ these pairs of conjugate ideals may be written

$$\begin{gathered}\mathfrak{p}^{2(a-\alpha)},\ \mathfrak{p}'^{\,2(a-\alpha)},\\ \mathfrak{p}^{2(a-\alpha-1)}(p),\ \mathfrak{p}'^{\,2(a-\alpha-1)}(p),\\ \mathfrak{p}^{2(a-\alpha-2)}(p)^2,\ \mathfrak{p}'^{\,2(a-\alpha=2)}(p)^2,\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\\ (p)^{a-\alpha},\ (p)^{a-\alpha}.\end{gathered}$$

The ideals of the last pair coincide. As $(p)^{a-\alpha}$ is a principal ideal, it corresponds to the ambiguous class the solutions of which correspond to the solutions of (16). If (16) is not solvable, (15) has no ambiguous class.

Suppose that $\mathfrak{p}^{2a'}$ is the least even power of $\mathfrak{p}$ for which

$$\mathfrak{p}^{2a'} \sim (1)$$

holds. Then the following pairs of conjugate ideals are principal ideals.

$$\begin{gathered}\mathfrak{p}^{2a'}(p)^{a-\alpha-a'},\ \mathfrak{p}'^{\,2a'}(p)^{a-\alpha-a'},\\ \mathfrak{p}^{4a'}(p)^{a-\alpha-2a'},\ \mathfrak{p}'^{\,4a'}(p)^{a-\alpha-2a'},\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\\ \mathfrak{p}^{2ma'}(p)^{a-\alpha-ma'},\ \mathfrak{p}'^{\,2ma'}(p)^{a-\alpha-ma'},\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\end{gathered}$$

Suppose that $\left[\frac{a-\alpha}{a'}\right]$ denotes the greatest integer $\leqq \frac{a-\alpha}{a'}$. Then it is apparent that (15) has $2\left[\frac{a-\alpha}{a'}\right]+1$ classes when (16) is solvable and $2\left[\frac{a-\alpha}{a'}\right]$ classes when (16) is not solvable. This proves the theorem.

It is apparent that these investigations may be extended to an arbitrary N.

§ 5. Inequalities derived from algebraic number theory

Given an algebraic field $\boldsymbol{K}$ of the degree n, and given a ring $\boldsymbol{R}$ of integers in it, containing integers of the degree n and the natural number 1. Then it is well-known that the whole set of integers in $\boldsymbol{R}$ with a given norm N may be determined by means of the following theorem.[1]

Theorem. *Given a ring of integers* $\boldsymbol{R}$ *which contains integers of the degree* n *and the natural number* 1, *and let* N *be the norm of any integer in* $\boldsymbol{R}$. *Then there is in* $\boldsymbol{R}$ *a finite number of non-associate integers* $\beta_1, \beta_2, \ldots, \beta_m$ *with the norm* N, *such that all integers in* $\boldsymbol{R}$ *with the norm* N *are given by*

$$\varepsilon \beta_1, \varepsilon \beta_2, \ldots, \varepsilon \beta_m,$$

where ε *runs through all units in* $\boldsymbol{R}$ *having a positive norm. If* $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ *is a system of fundamental units in* $\boldsymbol{R}$, *it is possible to choose the integers* β *in such way that they satisfy inequalities*

$$\left|\log\left|\frac{\beta^{(i)}}{\sqrt[n]{N}}\right|\right| \leqq \tfrac{1}{2}\sum_{k=1}^{r}\left|\log\left|\varepsilon_k^{(i)}\right|\right| \quad (1 \leqq i \leqq n). \tag{19}$$

Let $\omega_1, \omega_2, \ldots, \omega_n$ be a base of $\boldsymbol{R}$, and let α be an integer of it. Then all integers

$$\alpha = x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n$$

with a given norm C are given by the Diophantine equation

$$N(x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n) = C. \tag{20}$$

Then by the theorem just mentioned it is possible to determine all the integers α satisfying (20).

The set of all integers with the norm C associated with each other are said to form a *class of solutions* of (20). If there are m non-associate integers with the norm C which satisfy (19), there are m classes of solutions of (20).

In this special case we consider the ring $\boldsymbol{R}$ consisting of all integers $\frac{1}{2}(u + v\sqrt{D})$ in the real quadratic field $\boldsymbol{K}(\sqrt{D})$. D is as above a positive integer which is not a square. It is not necessarily square-free.

Let $\alpha = \frac{1}{2}(u + v\sqrt{D})$ be an integer of $\boldsymbol{R}$ with norm $\pm N$. If ε is the fundamental unit of $\boldsymbol{R}$, $\varepsilon > 1$, there exists an integer β belonging to the same class $\boldsymbol{K}$ as α which satisfies (19). If $\beta = \frac{1}{2}(u^* + v^* \sqrt{D})$, where v^* is the smallest non-negative value of v of any integer belonging to the class, β is called the *fundamental solution of the class.*

Suppose that $\beta = \frac{1}{2}(u + v\sqrt{D})$, $\beta > 0$. If $N\beta = +N$ is positive, we get

$$u \leqq \sqrt{N}\,(1 + \sqrt{\varepsilon}). \tag{21}$$

It follows from Theorem 1 that, on the other side, we have

$$u \leqq \sqrt{N}\,\sqrt{x_1 + 2}. \tag{5}$$

[1] See NAGELL [8]. NAGELL pronounces this theorem only for the field, but the result may be extended to an arbitrary ring by a slight alteration of the arguments.

Suppose that $\beta=\frac{1}{2}(u+v\sqrt{D})$, $\beta>0$. If $N\beta=-N$ is negative, we get

$$v\sqrt{D}\leqq\sqrt{N}(1+\sqrt{\varepsilon}). \tag{22}$$

It follows from Theorem 2 that, on the other side, we have

$$v\sqrt{D}\leqq\frac{y_1\sqrt{D}}{\sqrt{x_1-2}}\sqrt{N}. \tag{7}$$

Nagell [2] assumes that inequalities (21) and (22) give a better result than inequalities (5) and (7) which are obtained by elementary methods. In this section we shall prove that the contrary is true. In fact, it follows from Theorem 16 that inequalities obtained by elementary methods give an upper limit which is lower than that obtained by means of algebraic number theory.

If $\beta=\frac{1}{2}(u+v\sqrt{D})$, $\beta>0$, by means of (19) it is also possible to obtain a lower limit for β. If $N\beta=+N$ is positive, we get

$$u\geqq\sqrt{N}\left(1+\frac{1}{\sqrt{\varepsilon}}\right). \tag{23}$$

On the other hand, from

$$u^2-Dv^2=+4N \tag{3}$$

we get the trivial result

$$u\geqq 2\sqrt{N}. \tag{24}$$

Since $\varepsilon>1$, clearly (24) is a better result than (23). In a similar way, if $N\beta=-N$ is negative, by (19) we get

$$v\sqrt{D}\geqq\sqrt{N}\left(1+\frac{1}{\sqrt{\varepsilon}}\right). \tag{25}$$

By

$$u^2-Dv^2=-4N \tag{6}$$

we get the trivial result

$$v\sqrt{D}\geqq 2\sqrt{N}. \tag{26}$$

Clearly (26) is a better result than (25).

We now prove

Theorem 16. *Part I. Suppose that $\frac{1}{2}(u+v\sqrt{D})$ is the fundamental solution of the class $\boldsymbol{K}$ of the Diophantine equation*

$$u^2-Dv^2=+4N, \tag{3}$$

and suppose that $\varepsilon = \frac{1}{2}(x_1 + y_1\sqrt{D})$ *is the fundamental solution of* (2). *Then*

$$u \leqq \sqrt{N}\sqrt{x_1+2} \tag{5}$$

gives an upper limit for u which is lower than that given by

$$u \leqq \sqrt{N}(1+\sqrt{\varepsilon}). \tag{21}$$

For the difference between the upper limits obtained by (21) *and* (5) *we have the following inequality.*

$$\sqrt{N}(1+\sqrt{\varepsilon}) - \sqrt{N}\sqrt{x_1+2} > 0.42\sqrt{N}.$$

Part II. Suppose that $\frac{1}{2}(u+v\sqrt{D})$ *is the fundamental solution of the class* $\boldsymbol{K}$ *of the Diophantine equation*

$$u^2 - Dv^2 = -4N, \tag{6}$$

and suppose that $\varepsilon = \frac{1}{2}(x_1 + y_1\sqrt{D})$ *is the fundamental solution of* (2). *Then*

$$v\sqrt{D} \leqq \sqrt{N}\frac{y_1\sqrt{D}}{\sqrt{x_1-2}} \tag{7}$$

gives an upper limit for v which is lower than that given by

$$\sqrt{D} \leqq \sqrt{N}(1+\sqrt{\varepsilon}). \tag{22}$$

For the difference between the upper limits obtained by (22) *and* (7) *we have the following inequality.*

$$\sqrt{N}(1+\sqrt{\varepsilon}) - \sqrt{N}\frac{y_1\sqrt{D}}{\sqrt{x_1-2}} > 0.42\sqrt{N}.$$

Proof. Let $\frac{1}{2}(u+v\sqrt{D})$ be the fundamental solution of the class $\boldsymbol{K}$ of the Diophantine equation

$$u^2 - Dv^2 = +4N, \tag{3}$$

and let $\varepsilon = \frac{1}{2}(x_1 + y_1\sqrt{D})$ be the fundamental solution of (2). It is apparent that (5) gives a lower limit than (21) if we may prove that

$$(1+\sqrt{\varepsilon}) - \sqrt{x_1+2} \tag{27}$$

is positive for every D and N.

$\sqrt{\varepsilon}$ and $\sqrt{x_1+2}$ may be written

$$\sqrt{\varepsilon} = \sqrt{\tfrac{1}{2}x_1}\cdot\sqrt{1+\sqrt{1-4x_1^{-2}}}, \quad \sqrt{x_1+2} = \sqrt{x_1}\cdot\sqrt{1+2x_1^{-1}}.$$

Since $x_1 > 2$, it follows that

$$\left|\frac{4}{x_1^2}\right| < 1, \quad \left|\frac{2}{x_1}\right| < 1.$$

Then $\sqrt{\varepsilon}$ and $\sqrt{x_1+2}$ may be developed in binomial series which are absolutely convergent. Thus we get

$$1+\sqrt{\varepsilon} = 1 + x_1^{\frac{1}{2}} - \tfrac{1}{2} x_1^{-\frac{3}{2}} - \tfrac{5}{8} x_1^{-\frac{7}{2}} + R_m,$$

$$\sqrt{x_1+2} = x_1^{\frac{1}{2}} + x_1^{-\frac{1}{2}} - \tfrac{1}{2} x_1^{-\frac{3}{2}} + \tfrac{1}{2} x_1^{-\frac{5}{2}} + R_\mu,$$

where R_m and R_μ are remainders. Hence

$$(1+\sqrt{\varepsilon}) - \sqrt{x_1+2} = 1 - \frac{1}{\sqrt{x_1}} + R_n. \tag{28}$$

To calculate the remainder R_n we use the Lagrange form, and since $x_1 > 2$, it follows that $|R_n| < 0{,}0052$. It is apparent that (28) is positive for every D and N. Since $x_1 > 2$, it follows that

$$\sqrt{N}\,(1+\sqrt{\varepsilon}) - \sqrt{N}\sqrt{x_1+2} > 0.42\sqrt{N}. \tag{29}$$

Hence the first part of the theorem is proved.

We now prove the second part of the theorem.

Let $\frac{1}{2}(u+v\sqrt{D})$ be the fundamental solution of the class $\boldsymbol{K}$ of the Diophantine equation

$$u^2 - Dv^2 = -4N, \tag{6}$$

and let ε, as before, be the fundamental solution of (2). It is apparent that (7) gives a lower limit than (22) if we may prove that

$$\sqrt{N}\,(1+\sqrt{\varepsilon}) - \sqrt{N}\,\frac{y_1\sqrt{D}}{\sqrt{x_1-2}} \tag{30}$$

is positive for every D and N.

By means of (2) we obtain

$$\frac{y_1\sqrt{D}}{\sqrt{x_1-2}} = \sqrt{x_1+2}.$$

Hence (30) may be written

$$\sqrt{N}\,[(1+\sqrt{\varepsilon}) - \sqrt{x_1+2}]. \tag{30'}$$

But we have shown in Part I that $(1+\sqrt{\varepsilon}) - \sqrt{x_1+2}$ is always positive. Since $x_1 > 2$, it follows that

$$\sqrt{N}(1+\sqrt{\varepsilon}) - \sqrt{N}\sqrt{x_1+2} > 0.42\sqrt{N}.$$

This proves the theorem.

§ 6. Numerical examples

Finally we give some examples which illustrate the preceding theorems.

Example 1. $u^2 - 15v^2 = -476 = -4 \cdot 7 \cdot 17$ (Theorem 11).

As $\Delta = 4 \cdot 15 = 60$, we find $\left(\frac{\Delta}{7}\right) = \left(\frac{\Delta}{17}\right) = +1$. Then we get the following products of prime ideals.

$$(7) = (7,\ 1+\sqrt{15})(7,\ 1-\sqrt{15}),$$
$$(17) = (17,\ 7+\sqrt{15})(17,\ 7-\sqrt{15}).$$

$\mathfrak{p} \sim \mathfrak{p}'$ holds for every pair of prime ideals, as is apparent from

$$(7,\ 1+\sqrt{15})^2 = (8+\sqrt{15}),\ (17,\ 7+\sqrt{15})^2 = (23-4\sqrt{15}).$$

The equation is solvable, and thus it has 4 classes. Calculating the corresponding ideals we get

$$(7,\ 1+\sqrt{15})(17,\ 7+\sqrt{15}) = (11+4\sqrt{15}).$$
$$(7,\ 1+\sqrt{15})(17,\ 7-\sqrt{15}) = (4-3\sqrt{15}),$$
$$(7,\ 1-\sqrt{15})(17,\ 7+\sqrt{15}) = (4+3\sqrt{15}),$$
$$(7,\ 1-\sqrt{15})(17,\ 7-\sqrt{15}) = (11-4\sqrt{15}).$$

Example 2. $u^2 - 37v^2 = 231 = 3 \cdot 7 \cdot 11$ (Theorem 11, cf. Example 13 in Part I).

According to Theorem 5 in Part I this equation has the same number of classes as the Diophantine equation

$$u^2 - 148v^2 = 924 = 4.231.$$

Thus we have to consider the ring $\boldsymbol{R}(2\sqrt{37})$. In that ring we get the following products of prime ideals.

$$(3) = (3,\ 1+2\sqrt{37})(3,\ 1-2\sqrt{37}),$$
$$(7) = (7,\ 1+2\sqrt{37})(7,\ 1-2\sqrt{37}),$$
$$(11) = (11,\ 4+2\sqrt{37})(11,\ 4-2\sqrt{37}).$$

$\mathfrak{p} \neq \mathfrak{p}'$ holds for every pair of prime ideals, as is apparent from

$$(3,\ 1+2\sqrt{37})^2=(9,\ 2+2\sqrt{37}),\ (7,\ 1+2\sqrt{37})^2=(49,\ 28+2\sqrt{37}),$$
$$(11,\ 4+2\sqrt{37})^2=(121,\ 40+2\sqrt{37}).$$

On the other hand we get

$$(3,\ 1+2\sqrt{37})\,(7,\ 1+2\sqrt{37})\,(11,\ 4+2\sqrt{37})=(19+4\sqrt{37}).$$

Then $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \sim \mathfrak{p}_1'\mathfrak{p}_2'\mathfrak{p}_3'$ holds. As the equation is solvable, it has two classes.

Example 3. $u^2-37v^2=\pm 924=\pm 4\cdot 3\cdot 7\cdot 11.$ (Theorem 11.)

As $\Delta=37$ we find $\left(\frac{\Delta}{3}\right)=\left(\frac{\Delta}{7}\right)=\left(\frac{\Delta}{11}\right)=+1$. Then we get the following products of prime ideals.

$$(3)=\left(\frac{5+\sqrt{37}}{2}\right)\left(\frac{5-\sqrt{37}}{2}\right),$$
$$(7)=\left(\frac{3+\sqrt{37}}{2}\right)\left(\frac{3-\sqrt{37}}{2}\right),$$
$$(11)=\left(\frac{9+\sqrt{37}}{2}\right)\left(\frac{9-\sqrt{37}}{2}\right).$$

The equation is solvable, and as all the prime ideals are principal ideals, it has $2^3=8$ classes.

Example 4. $u^2-148v^2=78\,734=4\cdot 3^9$ (Theorem 14, cf. Example 4 in Part II). In the ring $\boldsymbol{R}(2\sqrt{37})$ we get

$$(3)=(3,\ 1+2\sqrt{37})\,(3,\ 1-2\sqrt{37}).$$

The last odd power which is a principal ideal is $(3,\ 1+2\sqrt{37})^3=(16-2\sqrt{37})$. As the equation is solvable, according to Theorem 14 it has $2\frac{4+1+1}{2\cdot 1+1}=4$ classes. Calculating the corresponding ideals we get

$$(3,\ 1+2\sqrt{37})^9=(11\,200-1\,832\sqrt{37}),$$
$$(3,\ 1+2\sqrt{37})^6\,(3,\ 1-2\sqrt{37})^3=(432-54\sqrt{37}),$$
$$(3,\ 1+2\sqrt{37})^3\,(3,\ 1-2\sqrt{37})^6=(432+54\sqrt{37}),$$
$$(3,\ 1+2\sqrt{37})^9=(11\,200+1\,832\sqrt{37}).$$

Example 5. $u^2 - 34v^2 = -100 = -4 \cdot 5^2$ (Theorem 15).

As $\Delta = 4 \cdot 34$ we find $\left(\frac{\Delta}{5}\right) = +1$. Then we get

$$(5) = (5,\ 1 + 2\sqrt{34})\,(5,\ 1 - 2\sqrt{34}).$$

We find $(5,\ 1 + 2\sqrt{34})^2 = (3 + \sqrt{34})$. The Diophantine equation

$$x^2 - 34y^2 = -4$$

is not solvable. The given equation is solvable, and thus it has 2 classes.

Example 6. $u^2 - 5v^2 = 836 = 4 \cdot 11 \cdot 19$ (Theorem 16, cf. Example 4 in Part I).

For the fundamental solutions in which u is positive, according to inequalities (5) and (21) we get

$$u \leqq 32, \quad u \leqq 38.$$

Example 7. $u^2 - 2v^2 = -2\,884 = -4 \cdot 7 \cdot 103$ (Theorem 16).

For the fundamental solutions in which v is positive, according to inequalities (7) and (22) we get

$$v \leqq 53, \quad v \leqq 63.$$

BIBLIOGRAPHY

[1] B. Stolt, On the Diophantine equation $u^2 - Dv^2 = \pm 4N$, Part I, Arkiv för Matematik *2* Nr 1 (1951), 1–23.

[2] T. Nagell, En elementær metode til å bestemme gitterpunktene på en hyperbel, Norsk Matem. Tidskrift *26* (1944), 60–65.

[3] ——, Elementär talteori, Uppsala 1950, 199–206.

[4] ——, Über die Darstellung ganzer Zahlen durch eine indefinite binäre quadratische Form, Archiv der Mathematik *2* (1950), 161–165.

[5] ——, Bemerkung über die diophantische Gleichung $u^2 - Dv^2 = C$, Archiv der Mathematik *3* (1952), 8–10.

[6] B. Stolt, On the Diophantine equation $u^2 - Dv^2 = \pm 4N$, Part II, Arkiv för Matematik *2* Nr 10 (1952), 251–268.

[7] E. Landau, Vorlesungen über Zahlentheorie, Lpz 1927, Bd. 3.

[8] T. Nagell, Zur algebraischen Zahlentheorie, Math. Zeitschrift *34* (1932), 183–193.

Tryckt den 13 april 1954

Uppsala 1954. Almqvist & Wiksells Boktryckeri AB