Communicated 6 June 1951 by F. CARLSON and T. NAGELL

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

By BENGT STOLT

Part I

§ 1. Introduction

It is easy to solve the Diophantine equation

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$$

with integral coefficients, in integers x and y when the equation represents an ellipse or a parabola in the (x, y)-plane. If the equation represents a hyperbola, the problem is much more difficult. In this case the problem may be reduced to the solution of the equation

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

where D and N are integers. We exclude the case of D being a perfect square, which is without interest. For solving an equation of this type one may use either the theory of quadratic forms or the theory of quadratic fields.

T. NAGELL has shown[1] how it is possible to determine all the solutions of (1) independently of these theories.

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

$$x^2 - Dy^2 = 1, \tag{2}$$

the number

$$(u + v\sqrt{D})(x + y\sqrt{D}) = (u_1 + v_1\sqrt{D})$$

is also a solution of (1). This solution is said to be *associated* with the solution $u + v\sqrt{D}$. 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 $u + v\sqrt{D}$ and $u' + v'\sqrt{D}$ to belong to the same class is that the two expressions

$$\frac{uu' - vv'D}{N}, \quad \frac{vu' - uv'}{N} \tag{3}$$

be integers.

[1] See [1], [2], [3], [4]. In the following we use the notions proposed by NAGELL.

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

Among the solutions of K, a *fundamental solution of the class* is defined in the following way. $u^* + v^*\sqrt{D}$ is the fundamental solution of 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 $-u^* + v^*\sqrt{D}$ belongs to the conjugate class; if the class is ambiguous, u^* is uniquely determined by supposing $u^* \geq 0$. $u^* = 0$ or $v^* = 0$ only occurs when the class is ambiguous.[1]

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

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

Theorem. *If $u + v\sqrt{D}$ is the fundamental solution of the class* $\mathbf{K}$ *of the Diophantine equation*

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

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

$$0 \leq v \leq y_1 \sqrt{\frac{N}{2(x_1+1)}}, \tag{5}$$

$$0 < |u| \leq \sqrt{\tfrac{1}{2}(x_1+1)N}. \tag{6}$$

Theorem. *If $u + v\sqrt{D}$ is the fundamental solution of the class* $\mathbf{K}$ *of the Diophantine equation*

$$u^2 - Dv^2 = -N, \tag{7}$$

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

$$0 < v \leq y_1 \sqrt{\frac{N}{2(x_1-1)}}, \tag{8}$$

$$0 \leq |u| \leq \sqrt{\tfrac{1}{2}(x_1-1)N}. \tag{9}$$

Theorem. *The Diophantine equations* (4) *and* (7) *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.*

---

[1] In his first papers NAGELL defined the fundamental solution in a slightly different manner.

If $u^* + v^* \sqrt{D}$ *is the fundamental solution of the class* $\mathbf{K}$, *we obtain all the solutions* $u + v\sqrt{D}$ *of* $\mathbf{K}$ *by the formula*

$$u + v\sqrt{D} = (u^* + v^* \sqrt{D})\,(x + y\sqrt{D}),$$

when $x + y\sqrt{D}$ *runs through all the solutions of equation* (2), *including* ± 1. *The Diophantine equations* (4) *and* (7) *have no solutions when they have no solutions satisfying inequalities* (5) *and* (6), *or* (8) *and* (9) *respectively.*

NAGELL also proved the following theorem.

Theorem. 1) *If* p *is a prime, the Diophantine equation*

$$u^2 - Dv^2 = \pm p \tag{10}$$

has at most one solution $u + v\sqrt{D}$ *in which* u *and* v *satisfy inequalities* (5) *and* (6), *or* (8) *and* (9) *respectively, provided* $u \geq 0$.

2) *If solvable, equation* (10) *has one or two classes of solutions according as the prime* p *divides* $2D$ *or not.*

In this paper we shall extend the results of NAGELL to the more general equation

$$u^2 - Dv^2 = \pm 4N. \tag{11}$$

For this equation we deduce inequalities equivalent to those given by NAGELL. Furthermore, we shall treat the problem of the number of classes corresponding to a square-free N. An upper limit for the number of classes will be determined.

These investigations will be continued in a second part, in which the problem of determining an upper limit for the number of classes corresponding to an arbitrarily given N will be solved by elementary methods. Furthermore, we shall prove that there is at most one ambiguous class. In a third part, the same problems will be treated by means of the theory of algebraic numbers and ideals.

§ 2. The Diophantine equation $x^2 - Dy^2 = 4$

Consider the Diophantine equation

$$x^2 - Dy^2 = 4, \tag{12}$$

where D is a positive integer which is not a perfect square. When x and y are integers satisfying this equation, the number

$$\frac{x + y\sqrt{D}}{2}$$

is said to be a *solution* of this equation. Two solutions $\frac{x + y\sqrt{D}}{2}$ and $\frac{x' + y'\sqrt{D}}{2}$ are equal, if $x = x'$ and $y = y'$. Among all the solutions of the equation there is a solution

$$\frac{x_1 + y_1\sqrt{D}}{2}$$

in which x_1 and y_1 are the least positive integers satisfying the equation. This solution is called the *fundamental solution.*

A well-known result is the following

Theorem.[1] *When* D *is a natural number which is not a perfect square, the Diophantine equation*

$$x^2 - D y^2 = 4 \tag{12}$$

has an infinity of solutions. If the fundamental solution is denoted by ε, *every solution* $\frac{x + y\sqrt{D}}{2}$ *may be written in the form*

$$\frac{x + y\sqrt{D}}{2} = \pm \varepsilon^k, \qquad (k = 0, \pm 1, \pm 2, \pm 3, \ldots).$$

If the fundamental solution of the Diophantine equation

$$x^2 - D y^2 = 1 \tag{2}$$

is denoted by $x' + y'\sqrt{D}$, the following results are easily obtained.

If $D \equiv 1$ (*mod. 8*), $D \equiv 2$ (*mod. 4*), $D \equiv 3$ (*mod. 4*), *the fundamental solution of* (12) *is* $\frac{2x' + 2y'\sqrt{D}}{2}$.

If $D \equiv 5$ (*mod. 8*), *and if there exist odd solutions of* (12), *we have, for the fundamental solution, the relation*

$$\left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^3 = x' + y'\sqrt{D}. \tag{13}$$

If there only exist solutions with even x *and* y, *the fundamental solution of* (12) *is* $\frac{2x' + 2y'\sqrt{D}}{2} = x' + y'\sqrt{D}$.

If $D = 4 D_1$, *we denote the fundamental solution of*

$$x^2 - D_1 y^2 = 1$$

[1] Se [5].

by $x^* + y^* \sqrt{D_1}$. *Then the fundamental solution of* (12) *is* $\dfrac{2x^* + y^* \sqrt{D}}{2}$. *If* y^* *is even, the fundamental solution of* (2) *is* $x^* + \dfrac{y^*}{2}\sqrt{D}$, *and the fundamental solution of* (12) *is* $x' + y'\sqrt{D}$, *as before. When* $y^* = y_1$ *is odd, we have the relation*

$$x' + y'\sqrt{D} = \frac{x_1^2 - 2 + x_1 y_1 \sqrt{D}}{2}. \tag{14}$$

The last formula is easily obtained by observing that

$$x' + y'\sqrt{D} = x^{*2} + D_1 y^{*2} + x^* y^* \sqrt{D}.$$

Finally, we give a table of the fundamental solutions of the equation $x^2 - Dy^2 = 4$ for $D \equiv 5 \pmod{8}$, $D < 100$.

D	Fundamental solution	D	Fundamental solution
5	$\frac{1}{2}(3 + \sqrt{5})$	53	$\frac{1}{2}(51 + 7\sqrt{53})$
13	$\frac{1}{2}(11 + 3\sqrt{13})$	61	$\frac{1}{2}(1523 + 195\sqrt{61})$
21	$\frac{1}{2}(5 + \sqrt{21})$	69	$\frac{1}{2}(25 + 3\sqrt{69})$
29	$\frac{1}{2}(27 + 5\sqrt{29})$	77	$\frac{1}{2}(9 + \sqrt{77})$
37	$\frac{1}{2}(146 + 24\sqrt{37})$	85	$\frac{1}{2}(83 + 9\sqrt{85})$
45	$\frac{1}{2}(7 + \sqrt{45})$	93	$\frac{1}{2}(29 + 3\sqrt{93})$

§ 3. The classes of solutions of the Diophantine equation $u^2 - Dv^2 = \pm 4N$. The fundamental solutions of the classes

Let D be a natural number which is not a perfect square, and consider the Diophantine equation

$$u^2 - Dv^2 = \pm 4N, \tag{11}$$

where N is a positive integer. Suppose that the equation is solvable, and that $\dfrac{u + v\sqrt{D}}{2}$ is a solution of it. If $\dfrac{x + y\sqrt{D}}{2}$ is any solution of

$$x^2 - Dy^2 = 4, \tag{12}$$

the number

$$\frac{u + v\sqrt{D}}{2} \cdot \frac{x + y\sqrt{D}}{2} = \frac{ux + vyD + (uy + vx)\sqrt{D}}{4}$$

is also a solution of (11). This solution is said to be *associated* with the solution $\frac{u+v\sqrt{D}}{2}$. The set of all solutions associated with each other forms *a class of solutions* of (11).

It is possible to decide whether the two given solutions $\frac{u+v\sqrt{D}}{2}$ and $\frac{u'+v'\sqrt{D}}{2}$ belong to the same class or not. In fact, it is easy to see that the necessary and sufficient condition for these two solutions to be associated with each other is that the two numbers

$$\frac{uu'-vv'D}{2N} \quad \text{and} \quad \frac{vu'-uv'}{2N}$$

be integers.

If K is the class consisting of the solutions $\frac{u_i+v_i\sqrt{D}}{2}$, $i=1, 2, 3, \ldots$, it is evident that the solutions $\frac{u_i-v_i\sqrt{D}}{2}$, $i=1, 2, 3, \ldots$, also constitute a class, which may be denoted by $\bar{K}$. The classes K and $\bar{K}$ are said to be *conjugates* of each other. Conjugate classes are in general distinct, but may sometimes coincide; in the latter case we speak of *ambiguous* classes.

Among all the solutions $\frac{u+v\sqrt{D}}{2}$ in a given class K we now choose a solution $\frac{u_1+v_1\sqrt{D}}{2}$ in the following way: Let v_1 be the least non-negative value of v which occurs in K. If K is not ambiguous, then the number u_1 is also uniquely determined; for the solution $\frac{-u_1+v_1\sqrt{D}}{2}$ belongs to the conjugate class $\bar{K}$. If K is ambiguous, we get a uniquely determined u_1 by prescribing that $u_1 \geqq 0$. The solution $\frac{u_1+v_1\sqrt{D}}{2}$ defined in this way is said to be the *fundamental solution of the class.*

In the fundamental solution the number $|u_1|$ has the least value which is possible for $|u|$, when $\frac{u+v\sqrt{D}}{2}$ belongs to K. The case $u_1=0$ can only occur when the class is ambiguous, and similarly for the case $v_1=0$.

If $N=1$, clearly there is only one class, and then it is ambiguous.

We prove

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

$$u^2 - Dv^2 = 4N, \tag{15}$$

where D and N are positive integers and D is not a perfect square, and if $\frac{x_1 + y_1\sqrt{D}}{2}$ is the fundamental solution of equation (12), *we have the inequalities*

$$0 \leqq v \leqq \frac{y_1}{\sqrt{x_1 + 2}}\sqrt{N}, \tag{16}$$

$$0 < |u| \leqq \sqrt{(x_1 + 2)N}. \tag{17}$$

Proof. If inequalities (16) and (17) are true for a class K, they are also true for the conjugate class $\bar{K}$. Thus we can suppose that u is positive.

It is plain that

$$\frac{u x_1 - D v y_1}{4} = \frac{u x_1}{4} - \sqrt{\left(\frac{u^2}{4} - N\right)\left(\frac{x_1^2}{4} - 1\right)} > 0. \tag{18}$$

Consider the solution

$$\frac{u + v\sqrt{D}}{2} \cdot \frac{x_1 - y_1\sqrt{D}}{2} = \frac{u x_1 - D v y_1 + (x_1 v - y_1 u)\sqrt{D}}{4}$$

which belongs to the same class as $\frac{u + v\sqrt{D}}{2}$. Since $\frac{u + v\sqrt{D}}{2}$ is the fundamental solution of the class, and since by (18) $\frac{u x_1 - D v y_1}{4}$ is positive, we must have

$$\frac{u x_1 - D v y_1}{4} \geqq \frac{u}{2}. \tag{19}$$

From this inequality it follows that

$$u^2 (x_1 - 2)^2 \geqq D v^2 y_1^2 = (u^2 - 4N)(x_1^2 - 4)$$

or

$$u^2 \frac{x_1 - 2}{x_1 + 2} \geqq u^2 - 4N$$

and finally

$$u^2 \leqq (x_1 + 2) N.$$

This proves inequality (17), and it is easily seen that (17) implies (16).

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

$$u^2 - D v^2 = -4N, \tag{20}$$

where D *and* N *are positive integers and* D *is not a perfect square, and if* $\frac{x_1 + y_1\sqrt{D}}{2}$ *is the fundamental solution of equation* (12), *we have the inequalities*

$$0 < v \leqq \frac{y_1}{\sqrt{x_1 - 2}}\sqrt{N}, \tag{21}$$

$$0 \leqq |u| \leqq \sqrt{(x_1 - 2)N}. \tag{22}$$

Proof. If inequalities (21) and (22) are true for a class K, they are also true for the conjugate class $\bar{K}$. Thus we can suppose that $u \geqq 0$.

We clearly have

$$\frac{x_1^2 v^2}{4} = \left(\frac{y_1^2}{4} + \frac{1}{D}\right)(u^2 + 4N) > \frac{y_1^2 u^2}{4}$$

or

$$\frac{x_1 v - y_1 u}{4} > 0. \tag{23}$$

Consider the solution

$$\frac{u + v\sqrt{D}}{2} \cdot \frac{x_1 - y_1\sqrt{D}}{2} = \frac{u x_1 - D v y_1 + (x_1 v - y_1 u)\sqrt{D}}{4}$$

which belongs to the same class as $\frac{u + v\sqrt{D}}{2}$. Since $\frac{u + v\sqrt{D}}{2}$ is the fundamental solution of the class, and since by (23) $\frac{x_1 v - y_1 u}{4}$ is positive, we must have

$$\frac{x_1 v - y_1 u}{4} \geqq \frac{v}{2}. \tag{24}$$

From this inequality it follows that

$$D v^2 (x_1 - 2) \geqq D y_1^2 u^2 = u^2 (x_1^2 - 4)$$

or

$$u^2 \leqq (x_1 - 2) N.$$

This proves inequality (22), and it is easily seen that (22) implies (21).

From Theorems 1 and 2 we deduce at once

Theorem 3. *If* D *and* N *are positive integers, and if* D *is not a perfect square, the Diophantine equations* (15) *and* (20) *have a finite number of classes of solutions. The fundamental solutions of all the classes can be found after a finite number of trials by means of the inequalities in Theorems 1 and 2.*

If $\frac{u_1 + v_1\sqrt{D}}{2}$ *is the fundamental solution of the class* **K**, *we obtain all the solutions* $\frac{u + v\sqrt{D}}{2}$ *of* **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 $\frac{x + y\sqrt{D}}{2}$ *runs through all the solutions of* (12), *including* ± 1. *The Diophantine equations* (15) *and* (20) *have no solutions at all when they have no solutions satisfying inequalities* (16) *and* (17), *or* (21) *and* (22) *respectively.*

We next prove

Theorem 4. *The necessary and sufficient condition for the solutions* $\frac{u + v\sqrt{D}}{2}$, $\frac{u_1 + v_1\sqrt{D}}{2}$ *of the Diophantine equation*

$$u^2 - Dv^2 = \pm 4N$$

to belong to the same class is that

$$\frac{uv_1 - u_1 v}{2N}$$

be an integer.

Proof. We already know that a necessary and sufficient condition is that

$$\frac{uu_1 - vv_1 D}{2N}, \quad \frac{uv_1 - u_1 v}{2N}$$

be integers. Thus it is sufficient to show that $\frac{uu_1 - vv_1 D}{2N}$ is an integer when $\frac{uv_1 - u_1 v}{2N}$ is an integer, and that $\frac{uv_1 - u_1 v}{2N}$ is not an integer when $\frac{uu_1 - vv_1 D}{2N}$ is not an integer.

Multiplying the equations

$$u^2 - Dv^2 = \pm 4N, \quad u_1^2 - Dv_1^2 = \pm 4N \tag{24}$$

we get

$$(uu_1 - vv_1 D)^2 - D(uv_1 - u_1 v)^2 = 4(2N)^2. \tag{25}$$

It is apparent from (25) that $uu_1 - vv_1 D$ is divisible by $2N$ when $uv_1 - u_1 v$ is divisible by $2N$. Further, if $\frac{uu_1 - vv_1 D}{2N}$ is not an integer, there exists an integer d which is a divisor of $2N$ but is not a divisor of $uu_1 - vv_1 D$. d is not a divisor of D, for if it were, it is apparent from (24) that both u and u_1 would be divisible by d, and thus d would be a divisor of $u u_1 - v v_1 D$, which is contrary to hypothesis. From (25) it is seen that if d were a divisor of $u v_1 - u_1 v$, it would also be a divisor of $u u_1 - v v_1 D$, which is contrary to hypothesis. Hence the theorem is proved.

If $x^* + y^* \sqrt{D}$ is the fundamental solution of

$$x^2 - D y^2 = 1 \tag{2}$$

and $\dfrac{x_1 + y_1 \sqrt{4 D}}{2}$ is the fundamental solution of

$$x^2 - 4 D y^2 = 4,$$

we have shown in § 2 that

$$x_1 = 2 x, \quad y_1 = y.$$

If the fundamental solution of the class K^* of the Diophantine equation

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

is $u^* + v^* \sqrt{D}$, we get from inequalities (5) and (6), or (8) and (9) respectively:

$$0 < v^* \leq y^* \sqrt{\frac{N}{2 (x^* \pm 1)}},$$

$$0 < |u^*| \leq \sqrt{\tfrac{1}{2} (x^* \pm 1) N}.$$

For the fundamental solution of the class K of the Diophantine equation

$$u^2 - 4 D v^2 = \pm 4 N, \tag{26}$$

from inequalities (16) and (17), or (21) and (22) respectively, we get

$$0 < v \leq y_1 \sqrt{\frac{N}{x_1 \pm 2}},$$

$$0 < |u| \leq \sqrt{(x_1 \pm 2) N}.$$

Observing that $x_1 = 2 x^*$, $y_1 = y^*$, we get the inequalities

$$0 < v^* \leq y_1 \sqrt{\frac{N}{x_1 \pm 2}},$$

$$0 < |u^*| \leq \sqrt{(x_1 \pm 2) N}.$$

Thus u^* and v^* lie between the same limits as u and v respectively.

Theorem 5. *The Diophantine equation*

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

has the same number of classes as the Diophantine equation

$$u^2 - 4 D v^2 = \pm 4 N. \tag{26}$$

Proof. If $u + v\sqrt{D}$ is a solution of (1), it is easily seen that $\frac{2u + v\sqrt{4D}}{2}$ is a solution of (26). Conversely, since (26) is only solvable when u is even, every solution of (26) corresponds to a solution of (1).

Let $u + v\sqrt{D}$ and $u_1 + v_1\sqrt{D}$ be two solutions of (1) which belong to different classes. Then the corresponding solutions of (26) belong to different classes of (26). In fact, if the solutions belong to different classes of (1),

$$\frac{u v_1 - u_1 v}{N}$$

is not an integer. For the corresponding solutions of (26) we get the condition that

$$\frac{2 u v_1 - 2 u_1 v}{2 N}$$

is not an integer. Thus Theorem 4 is proved.

§ 4. The number of classes for square-free N

Suppose that $\frac{u + v\sqrt{D}}{2}$ and $\frac{u_1 + v_1\sqrt{D}}{2}$ are two solutions of the Diophantine equation

$$u^2 - D v^2 = \pm 4 N, \tag{11}$$

where u, u_1 and v, v_1 satisfy the inequalities (16) and (17), or (21) and (22) respectively. Then, as is easily seen,

$$0 \leq |u v_1 \mp u_1 v| \leq 2 y_1 N, \tag{27}$$

where the equality signs only hold if $u = u_1$, $v = v_1$.

Eliminating D from the expressions

$$u^2 - D v^2 = \pm 4 N, \quad u_1^2 - D v_1^2 = \pm 4 N, \tag{28}$$

we obtain

$$(u v_1 + u_1 v)(u v_1 - u_1 v) = \pm 4 N (v_1^2 - v^2). \tag{29}$$

From (28) we also get

$$(u u_1 \mp D v v_1)^2 - D (u v_1 \mp u_1 v)^2 = 16 N^2, \tag{30}$$

or, dividing by $4N^2$,

$$\left(\frac{uu_1 \mp Dvv_1}{2N}\right)^2 - D\left(\frac{uv_1 \mp u_1 v}{2N}\right)^2 = 4. \tag{31}$$

Thus all the prime factors of $2N$ are divisors of either of the expressions

$$\frac{uv_1 \mp u_1 v}{2},$$

as is apparent from (29). If all the prime factors of N are divisors of the same expression, the squares of the left-hand side of (31) are integers. Then $uv_1 \mp u_1 v = 0$ or $uv_1 \mp u_1 v = 2y_1 N$. But then $u = u_1$, $v = v_1$, and the two solutions coincide.

Theorem 6. 1) *Suppose that* $N = p$, *where* p *is a prime. The Diophantine equation*

$$u^2 - Dv^2 = \pm 4p \tag{32}$$

has at most one solution $\frac{u + v\sqrt{D}}{2}$ *in which* u *and* v *satisfy inequalities* (16) *and* (17), *or* (21) *and* (22) *respectively, provided* u *is non-negative.*

2) *Suppose that* p *is an odd prime. If solvable, the equation has one or two classes according as the prime* p *divides* D *or not.*

Suppose that $p = 2$. *If solvable, the equation has two classes when* $D \equiv 1$ (*mod.* 4), *and one class when* $D \not\equiv 1$ (*mod.* 4).

Proof. Suppose that there existed two solutions $\frac{u + v\sqrt{D}}{2}$, $\frac{u_1 + v_1\sqrt{D}}{2}$ in which u and v would satisfy the conditions of the first part of the theorem. Then it would be possible to obtain (31). For one of the signs, the squares of the left-hand side of (31) would be integers. Thus $u = u_1$, $v = v_1$. Hence the first part of the theorem is proved.

Thus there are no more than two classes. If the two solutions $\frac{u + v\sqrt{D}}{2}$, $\frac{-u + v\sqrt{D}}{2}$ are associated, $\frac{2uv}{2p}$ is an integer. But if D is divisible by p, u is divisible by p. Thus the necessary and sufficient condition for the two solutions to belong to the same class is that p be a divisor of D.

If $p = 2$, it is easily seen that (32) is only solvable in odd u and v when $D \equiv 1$ (mod. 4). In that case there are two classes at most. If $D \not\equiv 1$ (mod. 4), (32) is only solvable when u is even. Thus $\frac{2uv}{4}$ is an integer, and there is one single class. Hence the theorem is proved.

Theorem 7. 1) *Suppose that* $N = pq$, *where* p *and* q *are primes,* $p \neq q$. *The Diophantine equation*

$$u^2 - Dv^2 = \pm 4pq \tag{33}$$

has at most two solutions $\frac{u_i + v_i\sqrt{D}}{2}$ *in which* u_i *and* v_i *satisfy inequalities* (16) *and* (17), or (21) *and* (22) *respectively, provided* u_i *is non-negative.*

2) *Suppose that* p *and* q *are odd primes. If solvable, the equation has at most*
four classes when N *and* D *are relatively prime;*
two classes when either p *or* q *is a divisor of* D;
one class when N *is a divisor of* D.

Suppose that $q = 2$. *If solvable, the equation has at most*
four classes when N *and* D *are relatively prime,* $D \equiv 1$ (*mod. 4*);
two classes when N *and* D *are relatively prime,* $D \equiv 3$ (*mod. 4*);
when 2 *is a divisor of* D *and* p *is not a divisor of* D;
when p *is a divisor of* D, $D \equiv 1$ (*mod.* 4);
one class when p *is a divisor of* D, $D \equiv 3$ (*mod. 4*);
when N *is a divisor of* D.

Proof. Suppose that p and q are odd primes and that N and D are relatively prime. Then for every solution $\frac{u + v\sqrt{D}}{2}$, u and v are prime to pq.

Suppose that theorem were incorrect. Then there would exist three solutions $\frac{u_1 + v_1\sqrt{D}}{2}$, $\frac{u_2 + v_2\sqrt{D}}{2}$, $\frac{u_3 + v_3\sqrt{D}}{2}$ in which u_i and v_i would satisfy the conditions of the first part of the theorem. Treating them two by two, we would obtain three pairs of solutions from which three series of expressions analogous to (27)–(31) would be obtained.

If bot p and q were divisors of

$$\frac{u_i v_j \mp u_j v_i}{2} \tag{34}$$

when the same sign is chosen, we would have $u_i = u_j$, $v_i = v_j$. Thus two of the solutions would be identical. We therefore suppose that p and q would not be divisors of [34) for the same sign.

Consider the expressions

$$\tfrac{1}{2}(u_i v_j + u_j v_i) \equiv 0 \ (\text{mod. } p), \quad \tfrac{1}{2}(u_j v_k + u_k v_j) \equiv 0 \ (\text{mod. } p). \tag{35}$$

From these congruences we get

$$\tfrac{1}{2}(u_i u_j v_j v_k + u_j^2 v_i v_k) \equiv 0 \ (\text{mod. } p),$$

$$\tfrac{1}{2}(u_i u_j v_j v_k + u_i u_k v_j^2) \equiv 0 \ (\text{mod. } p).$$

Thus

$$\tfrac{1}{2}(u_j^2 v_i v_k - u_i u_k v_j^2) \equiv 0 \ (\text{mod. } p).$$

In this congruence, u_j^2 may be substituted by $D v_j^2$. Then

$$\tfrac{1}{2} v_j^2 (u_i u_k - D v_i v_k) \equiv 0 \ (\text{mod. } p).$$

From (30) we also get

$$\tfrac{1}{2}(u_i v_k - u_k v_i) \equiv 0 \pmod{p}. \tag{36}$$

Consider the expressions

$$\tfrac{1}{2}(u_i v_j + u_j v_i) \equiv 0 \pmod{p}, \quad \tfrac{1}{2}(u_j v_k - u_k v_j) \equiv 0 \pmod{p}. \tag{37}$$

From these congruences we get

$$\tfrac{1}{2}(u_i u_j v_j v_k + u_j^2 v_i v_k) \equiv 0 \pmod{p},$$

$$\tfrac{1}{2}(u_i u_j v_j v_k - u_i u_k v_j^2) \equiv 0 \pmod{p}.$$

Thus

$$\tfrac{1}{2}(u_j^2 v_i v_k + u_i u_k v_j^2 \equiv 0 \pmod{p}.$$

In the same way as before, we get the congruences

$$\tfrac{1}{2}(u_i u_k + D v_i v_k) \equiv 0 \pmod{p},$$

$$\tfrac{1}{2}(u_i v_k + u_k v_i) \equiv 0 \pmod{p}. \tag{38}$$

Now suppose that for every pair of solutions of (33) these expressions hold.

$$\tfrac{1}{2}(u_i v_j + u_j v_i) \equiv 0 \pmod{p}, \quad \not\equiv 0 \pmod{q},$$

$$\tfrac{1}{2}(u_i v_j - u_j v_i) \equiv 0 \pmod{q}, \quad \not\equiv 0 \pmod{p}.$$

From (35), however, it follows that

$$\tfrac{1}{2}(u_i v_k - u_k v_i) \equiv 0 \pmod{p}.$$

This is contrary to hypothesis. If there are three solutions satisfying the conditions of the first part of the theorem, the only possibility is that the following expressions hold.

$$\tfrac{1}{2}(u_1 v_2 + u_2 v_1) \equiv 0 \pmod{p}, \quad \not\equiv 0 \pmod{q},$$

$$\tfrac{1}{2}(u_2 v_3 + u_3 v_2) \equiv 0 \pmod{p}, \quad \not\equiv 0 \pmod{q},$$

$$\tfrac{1}{2}(u_3 v_1 + u_1 v_3) \equiv 0 \pmod{q}, \quad \not\equiv 0 \pmod{p},$$

$$\tfrac{1}{2}(u_1 v_2 - u_2 v_1) \equiv 0 \pmod{q}, \quad \not\equiv 0 \pmod{p},$$

$$\tfrac{1}{2}(u_2 v_3 - u_3 v_2) \equiv 0 \pmod{q}, \quad \not\equiv 0 \pmod{p},$$

$$\tfrac{1}{2}(u_3 v_1 - u_1 v_3) \equiv 0 \pmod{p}, \quad \not\equiv 0 \pmod{q}.$$

Then follows

$$\tfrac{1}{2}(u_2 v_3 + D v_2 v_3) \equiv 0 \pmod{p}, \quad \not\equiv 0 \pmod{q}. \tag{39}$$

According to (37), from the third and the fourth of the six congruences above we get

$$\tfrac{1}{2}(u_2 u_3 + D v_2 v_3) \equiv 0 \pmod{q}.$$

But this is contrary to (39). Hence the first part of the theorem is proved.

If N and D are relatively prime, there are no more than four classes since it is clear that every solutions satisfying the conditions of the first part of the theorem may correspond to two classes. If q is a divisor of D, every u is divisible by q. Thus it is apparent from (34) that there is only one solution $\frac{u + v\sqrt{D}}{2}$ in which u and v satisfy the conditions of the first part of the theorem. Then there are no more than two classes. If N is a divisor of D, every u is divisible by N. Thus there is one single class at most.

If $q = 2$, (33) is only solvable in odd u and v, when $D \equiv 1 \pmod{4}$. If N and D are relatively prime, there are four classes at most. If p is a divisor of D, it is apparent that there are no more than two classes. If $D \not\equiv 1 \pmod{4}$, every u is divisible by 2, and every Dv^2 is divisible by 4. Thus, if p is not a divisor of D, there are two classes at most, and if p is a divisor of D, there is no more than one class. This proves the second part of the theorem.

Theorem 8. 1) *Suppose that $N = p_1 p_2 \ldots p_n$, where $p_1, p_2, \ldots, p_n$ are primes, $p_i \neq p_j$. The Diophantine equation*

$$u^2 - Dv^2 = \pm 4 p_1 p_2 \ldots p_n \tag{40}$$

has 2^{n-1} solutions $\frac{u_i + v_i\sqrt{D}}{2}$ at most in which u_i and v_i satisfy inequalities (16) *and* (17), *or* (21) *and* (22) *respectively, provided u_i is non-negative.*

2) *Suppose that all p_i are odd primes. If solvable, the equation has at most*

2^n classes when N and D are relatively prime;

2^{n-m} classes when m of the prime divisors of N are divisors of D;

one class when N is a divisor of D.

Suppose that $p_n = 2$. If solvable, the equation has at most

2^n classes when N and D are relatively prime, $D \equiv 1 \pmod{4}$;

2^{n-m} classes when m of the odd prime divisors of N are divisors of D, $D \equiv 1 \pmod{4}$; when $m-1$ of the odd prime divisors of N are divisors of D, $D \equiv 3 \pmod{4}$; when the prime 2 and $m-1$ of the odd prime divisors of N are divisors of D.

Proof. Let $\frac{u_h + v_h\sqrt{D}}{2}, \frac{u_i + v_i\sqrt{D}}{2}, \frac{u_j + v_j\sqrt{D}}{2}, \frac{u_k + v_k\sqrt{D}}{2}, \ldots$ be a number of solutions of (40) in which u and v satisfy the conditions of the first part of the theorem.

For the sake of brevity we introduce the notions

$$(i, j)^+ = \tfrac{1}{2}(u_i v_j + u_j v_i),$$

$$(i, j)^- = \tfrac{1}{2}(u_i v_j - u_j v_i),$$

$$(i, j)^\pm = \tfrac{1}{2}(u_i v_j \pm u_j v_i).$$

If p_r is a prime divisor of N, it is apparent from (29) that p_r divides either $(i, j)^+$ or $(i, j)^-$, or perhaps both of them. Then we may suppose that $(i, j)^+$ is divisible by

$$p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

and that $(i, j)^-$ is divisible by

$$p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n},$$

where $\alpha_r = 1$ or 0 according as p_r divides $(i, j)^+$ or not, and $\beta_r = 1$ or 0 according as p_r divides $(i, j)^-$ or not. From (29) it is apparent that

$$\alpha_r + \beta_r \geqq 1.$$

We express this fact by the symbol

$$(i, j) \;\oplus p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}, \;\; \ominus p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}.$$

We call this symbol *the distribution corresponding to the solutions* $\dfrac{u_i + v_i \sqrt{D}}{2}$, $\dfrac{u_j + v_j \sqrt{D}}{2}$, or shorter *the distribution corresponding to* $(i, j)^{\pm}$.

If $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 1$, or if $\beta_1 = \beta_2 = \cdots = \beta_n = 1$, it is apparent from (31) that the solutions $\dfrac{u_i + v_i \sqrt{D}}{2}$, $\dfrac{u_j + v_j \sqrt{D}}{2}$ coincide.

Let the distributions corresponding to $(i, j)^{\pm}$ and $(h, k)^{\pm}$ be

$$(i, j) \;\oplus p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}, \quad \ominus p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n},$$

$$(h, k) \;\oplus p_1^{\alpha_1'} p_2^{\alpha_2'} \ldots p_n^{\alpha_n'}, \quad \ominus p_1^{\beta_1'} p_2^{\beta_2'} \ldots p_n^{\beta_n'}.$$

Suppose that for every r, either $\alpha_r = \alpha_r' = 1$ or $\beta_r = \beta_r' = 1$ holds, $1 \leqq r \leqq n$. Then the distribution corresponding to $(i, j)^{\pm}$ and $(h, k)^{\pm}$ are said to be *positive-equivalent*. If for every r either $\alpha_r = \beta_r' = 1$ or $\beta_r = \alpha_r' = 1$ holds, $1 \leqq r \leqq n$, the distributions corresponding to $(i, j)^{\pm}$ and $(h, k)^{\pm}$ are said to be *negative-equivalent*.

When proving Theorem 7 we calculated (33)–(38). These results may be expressed as follows.

If p_r divides $(i, j)^+$ and $(i, k)^+$, it also divides $(j, k)^-$.

If p_r divides $(i, j)^+$ and $(i, k)^-$, it also divides $(j, k)^+$.

If p_r divides $(i, j)^-$ and $(i, k)^-$, it also divides $(j, k)^-$.

Let the distribution corresponding to $(j, k)^{\pm}$ be

$$(j, k) \;\oplus p_1^{\alpha_1''} p_2^{\alpha_2''} \ldots p_n^{\alpha_n''}, \;\; \ominus p_1^{\beta_1''} p_2^{\beta_2''} \ldots p_n^{\beta_n''}.$$

If the distributions corresponding to $(i, j)^{\pm}$ and $(i, k)^{\pm}$ are positive-equivalent, it is apparent that

$$\beta_1'' = \beta_2'' = \cdots = \beta_n'' = 1,$$

and if the distributions corresponding to $(i, j)^{\pm}$ and $(i, k)^{\pm}$ are negative-equivalent, it is apparent that

$$\alpha_1'' = \alpha_2'' = \cdots = \alpha_n'' = 1.$$

In both these cases the solutions $\frac{u_j + v_j \sqrt{D}}{2}$, $\frac{u_k + v_k \sqrt{D}}{2}$ coincide.

Let

$$\frac{u_1 + v_1 \sqrt{D}}{2}, \frac{u_2 + v_2 \sqrt{D}}{2}, \frac{u_3 + v_3 \sqrt{D}}{2}, \ldots,$$
$$\frac{u_i + v_i \sqrt{D}}{2}, \frac{u_j + v_j \sqrt{D}}{2}, \frac{u_k + v_k \sqrt{D}}{2}, \frac{u_m + v_m \sqrt{D}}{2}, \ldots$$

be the solutions of (40) in which u and v satisfy the conditions of the first part of Theorem 8.

If we know the distributions corresponding to $(1, 2)^{\pm}$ and $(1, 3)^{\pm}$, we may determine the distribution corresponding to $(2, 3)^{\pm}$. If we also know the distribution corresponding to $(1, 4)^{\pm}$, we may determine the distributions corresponding to $(2, 4)^{\pm}$ and $(3, 4)^{\pm}$, and so forth.

We now determine the conditions for all the solutions to be distinct.

Let the distribution corresponding to $(1, i)^{\pm}$ be

$$(1, i) \oplus p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}, \quad \ominus p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}.$$

If $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 1$, or if $\beta_1 = \beta_2 = \cdots = \beta_n = 1$, the solutions $\frac{u_1 + v_1 \sqrt{D}}{2}$, $\frac{u_i + v_i \sqrt{D}}{2}$ coincide. Thus these possibilities have to be excluded. Further, if the distributions corresponding to $(1, i)^{\pm}$ and $(1, j)^{\pm}$ are positive-equivalent or negative-equivalent, it is apparent that the solutions $\frac{u_i + v_i \sqrt{D}}{2}$, $\frac{u_j + v_j \sqrt{D}}{2}$ coincide. Thus the number of distinct solutions satisfying the conditions of the first part of Theorem 8 depends on the number of distributions corresponding to $(1, 2)^{\pm}$, $(1, 3)^{\pm}$, ..., $(1, i)^{\pm}$, ... any two of which are neither positive-equivalent nor negative-equivalent.

Let

$$(1, i) \oplus p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}, \quad \ominus p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$$

be a distibution in which $\alpha_r + \beta_r > 1$ holds for one or more r, $1 \leqq r \leqq n$. Then this distribution is positive-equivalent to the distribution

$$(1, j) \oplus p_1^{\alpha_1'} p_2^{\alpha_2'} \ldots p_n^{\alpha_n'}, \quad \ominus p_1^{\beta_1'} p_2^{\beta_2'} \ldots p_n^{\beta_n'}$$

in which $\alpha_r' + \beta_r' = 1$ holds for every r, $1 \leqq r \leqq n$.

Let us determine the maximum number of possibilities any two of which are not positive-equivalent. If we consider those distributions in which

$$\alpha_r + \beta_r = 1$$

holds for every r, $1 \leqq r \leqq n$, there are

$$\begin{array}{lll}
1 \text{ distribution} & (1, i) & \ominus p_1 p_2 \ldots p_n, \\
n \text{ distributions} & (1, j) & \oplus p_{\gamma_1}, \ \ominus p_{\gamma_2} p_{\gamma_3} \ldots p_{\gamma_n}, \\
\frac{n(n-1)}{2} \text{ distributions} & (1, k) & \oplus p_{\gamma_1} p_{\gamma_2}, \ \ominus p_{\gamma_3} p_{\gamma_4} \ldots p_{\gamma_n}, \\
\ldots\ldots & & \\
1 \text{ distribution} & (1, m) & \oplus p_1 p_2 \ldots p_n.
\end{array}$$

Here j runs through n values, k runs through $\frac{n(n-1)}{2}$ values, and so on.

It is apparent that any two of these distributions are not positive-equivalent and that every other distribution is positive-equivalent to at least one of these distributions. Thus the maximum number of distributions any two of which are not positive-equivalent, is

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = (1+1)^n = 2^n.$$

It is apparent that these distributions are negative-equivalent in pairs and that two distributions of different pairs are not negative-equivalent. Thus the maximum number of distributions any two of which are neither positive-equivalent nor negative-equivalent, is 2^{n-1}.

If we exclude the distribution

$$(1, m) \oplus p_1 p_2 \ldots p_n \quad \text{or} \quad (1, i) \ominus p_1 p_2 \ldots p_n$$

there remains $2^{n-1} - 1$ distributions corresponding to just one of $(1, 2)^{\pm}$, $(1, 3)^{\pm}$, $\ldots$, $(1, 2^{n-1})^{\pm}$. Then it is apparent that there are at most 2^{n-1} solutions satisfying the conditions of the first part of the theorem. Hence this part of the theorem is proved.

If N and D are relatively prime, it is apparent that there are 2^n classes at most. If the prime p_i divides D, it divides every u. Thus p_i is a divisor of $(i, j)^+$ as well as of $(i, j)^-$. If m of the primes p_i divide D, there are no more than $2^{n-m-1} - 1$ distributions and 2^{n-m} classes at most. If all the prime divisors of N except one divide D, there is no more than one solution satisfying the conditions of the first part of the theorem, and two classes at most. If N divides D, the equation has no more than one single class.

If $p_n = 2$, (40) is only solvable in odd u and v when $D \equiv 1 \pmod{4}$. If N and D are relatively prime, there are $2^{n-1} - 1$ distributions and 2^{n-1} solutions satisfying the conditions of the first part of the theorem. Thus there are 2^n classes at most. If $D \not\equiv 1 \pmod{4}$, every u is divisible by 2 and every Dv^2 is divisible by 4. Thus it is apparent that there are 2^{n-m} classes at most, when m of the odd prime divisors of N are divisors of D, $D \equiv 1 \pmod{4}$, or when $m - 1$ of the odd prime divisors of N are divisors of D, $D \not\equiv 1 \pmod{4}$. Hence the theorem is proved.

Theorem 9. *Suppose that* $N = p_1 p_2 \ldots p_n$, *where* $p_1, p_2, \ldots, p_n$ *are distinct primes* $\equiv \pm 1 \pmod{8}$. *The Diophantine equation*

$$u^2 - 2v^2 = p_1 p_2 \ldots p_n \tag{41}$$

has 2^n *classes.*

Proof. It is a well-known fact that the Diophantine equation

$$u_i^2 - 2v_i^2 = p_i \qquad (i = 1, 2, \ldots, n)$$

is always solvable in integers u_i and v_i, and according to Theorem 6 it has two classes. If the fundamental solutions are denoted by $u_i \pm v_i \sqrt{2}$,

$$u + v\sqrt{2} = \prod_{i=1}^{n} (u_i \pm v_i \sqrt{2}) \tag{42}$$

clearly is a solution of (41). From (42) we get 2^n solutions $u + v\sqrt{2}$ of (41). Thus Theorem 9 is proved, if all the solutions belong to different classes. We prove the theorem by induction.

Suppose that Theorem 9 holds for n primes, and consider the Diophantine equation

$$U^2 - 2V^2 = p_1 p_2 \ldots p_n p_{n+1},$$

where $p_{n+1} \equiv \pm 1 \pmod{8}$. If $u + v\sqrt{2}$ and $u_1 + v_1\sqrt{2}$ are two solutions of (41) belonging to different classes, and if $u_{n+1} \pm v_{n+1}\sqrt{2}$ are the fundamental solutions of the equation

$$u_{n+1}^2 - 2v_{n+1}^2 = p_{n+1},$$

clearly the solutions

$$U + V\sqrt{2} = (u + v\sqrt{2})(u_{n+1} + v_{n+1}\sqrt{2}),$$

$$U_1 + V_1\sqrt{2} = (u + v\sqrt{2})(u_{n+1} - v_{n+1}\sqrt{2})$$

belong to different classes. So do the solutions

$$U + V\sqrt{2} = (u + v\sqrt{2})(u_{n+1} + v_{n+1}\sqrt{2}),$$

$$U_1 + V_1\sqrt{2} = (u_1 + v_1\sqrt{2})(u_{n+1} + v_{n+1}\sqrt{2}).$$

If the solutions

$$U + V\sqrt{2} = (u + v\sqrt{2})(u_{n+1} + v_{n+1}\sqrt{2}),$$

$$U_1 + V_1\sqrt{2} = (u_1 + v_1\sqrt{2})(u_{n+1} - v_{n+1}\sqrt{2})$$

belong to the same class,

$$(u + v\sqrt{2})(u_{n+1} + v_{n+1}\sqrt{2})^2 = \varepsilon(u_1 + v_1\sqrt{2}) \cdot p_{n+1} = p_{n+1}(A + B\sqrt{2}),$$

holds. In this expression ε is a solution of (2), and $A + B\sqrt{2}$ is a solution of (41). Multiplying by $A - B\sqrt{2}$ we get

$$(u + v\sqrt{2})(A - B\sqrt{2})(u_{n+1} + v_{n+1}\sqrt{2})^2 = p_{n+1} \cdot p_1 p_2 \ldots p_n.$$

The left-hand side may be written

$$(A_1 + B_1\sqrt{2})(u_{n+1} + v_{n+1}\sqrt{2})^2 =$$
$$= A_1(u_{n+1}^2 + 2v_{n+1}^2) + 4B_1 u_{n+1} v_{n+1} + \sqrt{2}(B_1(u_{n+1}^2 + 2v_{n+1}^2) + 2A_1 u_{n+1} v_{n+1}).$$

From this we get the congruences

$$A_1(u_{n+1}^2 + 2v_{n+1}^2) + 4B_1 u_{n+1} v_{n+1} \equiv 0 \pmod{p_{n+1}},$$
$$B_1(u_{n+1}^2 + 2v_{n+1}^2) + 2A_1 u_{n+1} v_{n+1} \equiv 0 \pmod{p_{n+1}}.$$

From these congruences we get

$$2A_1^2 u_{n+1} v_{n+1} - 4B_1^2 u_{n+1} v_{n+1} \equiv 0 \pmod{p_{n+1}},$$

or, since neither v_{n+1} nor u_{n+1} is divisible by p_{n+1},

$$A_1^2 - 2B_1^2 \equiv 0 \pmod{p_{n+1}}.$$

This proves the theorem.

§ 5. Numerical examples

Finally, we give some examples which illustrate the preceding theorems.

Example 1. $u^2 - 5v^2 = 44 = 4.11$ (Theorem 6).

The fundamental solution of the equation $u^2 - 5v^2 = 4$ is $\frac{3 + \sqrt{5}}{2}$. For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 1, \quad 0 < u \leqq 7.$$

We find the fundamental solutions $\frac{\pm 7 + \sqrt{5}}{2}$.

Example 2. $u^2 - 5v^2 = -20 = -4.5$ (Theorem 6).

For the fundamental solutions in which u and v are non-negative, according to inequalities (21) and (22) we get

$$0 < v \leqq 2, \quad 0 \leqq u \leqq 2.$$

We find the fundamental solution $\frac{2\sqrt{5}}{2}$. Thus the equation has only one class, and this class is ambiguous.

Example 3. $u^2 - 17v^2 = 8 = 4.2$ (Theorem 6).

The fundamental solution of the equation $u^2 - 17v^2 = 4$ is $\dfrac{66 + 16\sqrt{17}}{2}$. For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 5, \quad 0 < u \leqq 17.$$

We find the fundamental solutions $\dfrac{\pm 5 + \sqrt{17}}{2}$. As $D \equiv 1$ (mod. 4), the equation has the maximum number of classes.

Example 4. $u^2 - 5v^2 = 836 = 4.11.19$ (Theorem 7).

For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 6, \quad 0 < u \leqq 32.$$

We find the fundamental solutions $\dfrac{\pm 29 + \sqrt{5}}{2}$, $\dfrac{\pm 31 + 5\sqrt{5}}{2}$.

Example 5. $u^2 - 17v^2 = 104 = 4.2.13$ (Theorem 7).

For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 9, \quad 0 < u \leqq 17.$$

We find the fundamental solutions $\dfrac{\pm 11 + \sqrt{17}}{2}$, $\dfrac{\pm 23 + 5\sqrt{17}}{2}$.

Example 6. $u^2 - 33v^2 = 88 = 4.2.11$ (Theorem 7).

The fundamental solution of the equation $u^2 - 33v^2 = 4$ is $\dfrac{46 + 8\sqrt{33}}{2}$. For the fundamental solutions in which u and v are negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 5, \quad 0 < u \leqq 14.$$

We find the fundamental solutions $\dfrac{\pm 11 + \sqrt{33}}{2}$.

Example 7. $u^2 - 21v^2 = 84 = 4.3.7$ (Theorem 7).

The fundamental solution of the equation $u^2 - 21v^2 = 4$ is $\dfrac{5 + \sqrt{21}}{2}$. For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 1, \quad 0 < u \leqq 12.$$

We find no fundamental solutions. Thus the equation is not solvable.

Example 8. $u^2 - 21v^2 = -84 = -4.3.7$ (Theorem 7).

For the fundamental solutions in which u and v are non-negative, according to inequalities (21) and (22) we get

$$0 < v \leqq 2, \quad 0 \leqq u \leqq 10.$$

We find the fundamental solution $\frac{2\sqrt{21}}{2}$.

Example 9. $u^2 - 5v^2 = 751564 = 4.11.19.29.31$ (Theorem 8).

For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 193, \quad 0 < u \leqq 969.$$

We find the fundamental solutions

$$\frac{\pm 867 + 5\sqrt{5}}{2}, \quad \frac{\pm 872 + 40\sqrt{5}}{2}, \quad \frac{\pm 883 + 75\sqrt{5}}{2}, \quad \frac{\pm 888 + 86\sqrt{5}}{2},$$

$$\frac{\pm 897 + 103\sqrt{5}}{2}, \quad \frac{\pm 903 + 113\sqrt{5}}{2}, \quad \frac{\pm 937 + 159\sqrt{5}}{2}, \quad \frac{\pm 953 + 177\sqrt{5}}{2}.$$

Example 10. $u^2 - 148v^2 = 3108 = 4.777 = 4.3.7.37$ (Theorem 8).

The fundamental solution of the equation $u^2 - 148v^2 = 4$ is $\frac{146 + 12\sqrt{148}}{2}$. For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 27, \quad 0 < u \leqq 338.$$

We find the fundamental solutions $\frac{\pm 74 + 4\sqrt{148}}{2}$. Thus the equation has half the maximum number of classes.

Example 11. $u^2 - 37v^2 = 777 = 3.7.37$ (Theorem 8).

The fundamental solution of the equation $u^2 - 37v^2 = 1$ is $73 + 12\sqrt{37}$. For the fundamental solutions in which u and v are non-negative, according to inequalities (5) and (6) we get

$$0 \leqq v \leqq 18, \quad 0 < u \leqq 169.$$

We find the fundamental solutions $\pm 37 + 4\sqrt{37}$. According to Theorem 5, the given equation will have the same number of classes as the preceding equation.

Example 12. $u^2 - 148\,v^2 = 924 = 4.231 = 4.3.7.11$ (Theorem 8).

For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 14, \quad 0 < u \leqq 184.$$

We find the fundamental solutions $\dfrac{\pm 68 + 5\sqrt{148}}{2}$.

Example 13. $u^2 - 37\,v^2 = 231 = 3.7.11$ (Theorem 8).

According to Theorem 5, the equation has the same number of classes as the preceding equation. Then the fundamental solutions are $\pm 34 + 5\sqrt{37}$.

Example 14. $u^2 - 148\,v^2 = 5628 = 4.1407 = 4.3.7.67$ (Theorem 8).

For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 36, \quad 0 < u \leqq 456.$$

We find the fundamental solutions $\dfrac{\pm 76 + \sqrt{148}}{2}$, $\dfrac{\pm 220 + 17\sqrt{148}}{2}$.

Example 15. $u^2 - 148\,v^2 = 61908 = 4.15477 = 4.3.7.11.67$ (Theorem 8).

For the fundamental solutions in which u and v are non-negative, according to inequalities (16) and (17) we get

$$0 \leqq v \leqq 122, \quad 0 < u \leqq 1512.$$

We find the fundamental solutions $\dfrac{\pm 250 + 2\sqrt{148}}{2}$, $\dfrac{\pm 934 + 74\sqrt{148}}{2}$.

BIBLIOGRAPHY. [1] **T. Nagell,** En elementær metode til å bestemme gitterpunktene på en hyperbel, Norsk Matem. Tidskrift *26* (1944), 60—65. — [2]. ——, Elementär talteori, Uppsala 1950, 199—206. — [3]. ——, Über die Darstellung ganzer Zahlen durch eine indefinite binäre quadratische Form, Archiv der Mathematik *2* (1950), 161—165. — [4]. ——, Bemerkung über die diophantische Gleichung $u^2 - Dv^2 = C$, Archiv der Mathematik *3* (1951). — [5]. **E. Landau,** Vorlesungen über Zahlentheorie, Lpz. 1927, Bd. I, 63.

Tryckt den 25 oktober 1951

Uppsala 1951. Almqvist & Wiksells Boktryckeri AB