ARKIV FÖR MATEMATIK Band 2 nr 10

Communicated 24 October 1951 by F. CARLSON and T. NAGELL

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

By BENGT STOLT

Part II

§ 1. Introduction.

Consider the Diophantine equation

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

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 $\frac{u + v\sqrt{D}}{2}$ is called a *solution* of (1). If $\frac{x + y\sqrt{D}}{2}$ is a solution of the Diophantine equation

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

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 $\frac{u + v\sqrt{D}}{2}$. 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 $\frac{u + v\sqrt{D}}{2}, \frac{u' + v'\sqrt{D}}{2}$ to belong to the same class is that the number

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

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

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

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 $\frac{u_i + v_i\sqrt{D}}{2}$, $i = 1, 2, 3, \ldots$ Then the numbers $\frac{u_i - v_i\sqrt{D}}{2}$, $i = 1, 2, 3, \ldots$ 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 follwing way. $\frac{u^* + v^*\sqrt{D}}{2}$ 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 in not ambiguous, u^* is also uniquely determined, because $\frac{-u^* + v^*\sqrt{D}}{2}$ 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* $\frac{u + v\sqrt{D}}{2}$ *is the fundamental solution of the class* $\boldsymbol{K}$ *of the Diophantine equation*

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

and if $\frac{x_1 + y_1\sqrt{D}}{2}$ *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* $\frac{u + v\sqrt{D}}{2}$ *is the fundamental solution of the class* $\boldsymbol{K}$ *of the Diophantine equation*

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

and if $\frac{x_1 + y_1\sqrt{D}}{2}$ *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 $\frac{u_1 + v_1\sqrt{D}}{2}$ *is the fundamental solution of the class* $\mathbf{K}$, *we obtain all the solutions* $\frac{u + v\sqrt{D}}{2}$ *of* $\mathbf{K}$ *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 (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.*

For the Diophantine equation

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

corresponding theorems were deduced by NAGELL. In a review published in the 'Zentralblatt für Mathematik' *36*, (1951), p. 303, CASSELS declares that NAGELL's results were substantially known by TCHEBYCHEF (J. Math. *16*, (1851), pp. 257—282). This is not quite correct. In fact, TCHEBYCHEF showed that when the Diophantine equation

$$u^2 - Dv^2 = \pm \mathrm{N}$$

is solvable, there is at least one solution satisfying the inequalities, and two solutions when N is not a prime. Thus he obtained a criterion for the solvability of the equation; but he could not solve it completely in this way. To obtain the complete solution of the equation it is necessary to introduce the concept of *class of solutions*, as was done by NAGELL.

In part I the maximum number of classes corresponding to square-free N was determined. The main subject of this paper is the determination of the maximum number of classes corresponding to an arbitrarily given N. We shall also prove that a given equation has at most one ambiguous class.

§ 2. Generalities.

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

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

where u, u_1 and v, v_1 satisfy inequalities (4) and (5), or (7) and (8) respectively. Then, as easily seen,

$$0 \leqq |uv_1 \mp u_1 v| \leqq 2y_1 N, \tag{9}$$

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

Eliminating D from the expressions

$$u^2 - Dv^2 = \pm 4N, \quad u_1^2 - Dv_1^2 = \pm 4N \tag{10}$$

we obtain

$$(uv_1 + u_1v)(uv_1 - u_1v) = \pm 4\mathrm{N}(v_1^2 - v^2). \tag{11}$$

From (10) we also get

$$(uu_1 \mp Dvv_1)^2 - D(uv_1 \mp u_1v)^2 = 16\,\mathrm{N}^2, \tag{12}$$

or, dividing by $4\,\mathrm{N}^2$,

$$\left(\frac{uu_1 \mp Dvv_1}{2N}\right)^2 - D\left(\frac{uv_1 \mp u_1v}{2N}\right)^2 = 4. \tag{13}$$

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

$$\frac{uv_1 \mp u_1v}{2}$$

as is apparent from (11). If all the prime factors of N are divisors of the same expression, the squares of the left-hand side of (13) are integers. Then

$$uv_1 \mp u_1v = 0 \quad \text{or} \quad uv_1 \mp u_1v = 2y_1N.$$

But then $u = u_1$, $v = v_1$, and the two solutions coincide.

Let $\frac{u_h + v_h\sqrt{D}}{2}$, $\frac{u_i + v_i\sqrt{D}}{2}$, $\frac{u_j + v_j\sqrt{D}}{2}$, $\frac{u_k + v_k\sqrt{D}}{2}$, ... be a number of solutions of the Diophantine equation

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

in which every u and v satisfy inequalities (4) and (5), or (7) and (8) respectively, provided u is non-negative.

For the sake of brevity we introduce the notions

$$(i, j)^+ = \tfrac{1}{2}(u_iv_j + u_jv_i),$$

$$(i, j)^- = \tfrac{1}{2}(u_iv_j - u_jv_i),$$

$$(i, j)^\pm = \tfrac{1}{2}(u_iv_j \pm u_jv_i).$$

Suppose that

$$N = p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_n^{\gamma_n},$$

where γ_r are positive integers, $1 \leqq r \leqq n$. If $p_r^{\gamma_r}$ is one of the prime powers which divide N, it is apparent from (11) that $(i, j)^+$ is divisible by $p_r^{\alpha_r}$ and

that $(i, j)^-$ is divisible by $p_r^{\beta_r}$, where α_r and β_r are non-negative integers which satisfy the condition $\alpha_r + \beta_r \geqq \gamma_r$. Then we may suppose that $(i, j)^+$ is divisible by

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

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

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

where $p_r^{\alpha_r}$ is the greatest divisor of $p_r^{\gamma_r}$ which divides $(i, j)^+$ and $p_r^{\beta_r}$ is the greatest divisor of $p_r^{\gamma_r}$ which divides $(i, j)^-$, $1 \leqq r \leqq n$. From (11) it is apparent that

$$\alpha_r + \beta_r \geqq \gamma_r.$$

We express this fact by the symbol

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

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

If $\alpha_r = \gamma_r$ holds for every r, $1 \leqq r \leqq n$, or if $\beta_r = \gamma_r$ holds for every r, $1 \leqq r \leqq n$, it is apparent from (13) that the solutions $\frac{u_i + v_i\sqrt{D}}{2}$ and $\frac{u_j + v_j\sqrt{D}}{2}$ coincide.

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

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

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

Suppose that a and b be two non-negative integers, and let *min* (a, b) be the least one of the two numbers a and b. If

$$\min(\alpha_r, \alpha_r') + \min(\beta_r, \beta_r') \geqq \gamma_r$$

holds for every r, $1 \leqq r \leqq n$, the distributions corresponding to $(i, j)^{\pm}$ and $(h, k)^{\pm}$ are said to be *positive-equivalent* to each other. If

$$\min(\alpha_r, \beta_r') + \min(\beta_r, \alpha_r') \geqq \gamma_r$$

holds for every r, $1 \leqq r \leqq n$, the distributions corresponding to $(i, j)^{\pm}$ and $(h, k)^{\pm}$ are said to be *negative-equivalent* to each other.

The definitions of *distribution corresponding to the solutions* $\frac{u_i + v_i\sqrt{D}}{2}, \frac{u_j + v_j\sqrt{D}}{2}$,

positive-equivalent distributions and *negative-equivalent distributions* given above include the definitions given in Part I, which hold for $\gamma_1 = \gamma_2 = \cdots = \gamma_n = 1$.

When proving Theorem 7 in Part I we proved the following results.

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 to each other, it is apparent that

$$\min(\alpha_r, \alpha_r') + \min(\beta_r, \beta_r') \geqq \gamma_r$$

holds for every r, $1 \leqq r \leqq n$. Thus

$$\beta_r'' = \gamma_r$$

holds for every r, $1 \leqq r \leqq n$. In the same way, if the distributions corresponding to $(i,j)^{\pm}$ and $(i,k)^{\pm}$ are negative-equivalent, it is apparent that

$$\alpha_r'' = \gamma_r$$

holds for every r, $1 \leqq r \leqq n$. 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 (1) in which u and v satisfy inequalities (4) and (5), or (7) and (8) respectively, provided u is non-negative.

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

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

If $\alpha_r = \gamma_r$, $r = 1, 2, 3, \ldots, n$, or if $\beta_r = \gamma_r$, $r = 1, 2, 3, \ldots, n$, it is apparent that 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 inequalities (4) and (5), or (7) and (8) respectively, and where u is non-negative, depends on the number of distributions corresponding to $(1, 2)^{\pm}$, $(1, 3)^{\pm}, \ldots, (1, i)^{\pm}, \ldots$ any two of which are neither positive-equivalent nor negative-equivalent.

Let

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

be a distribution in which

$$\alpha_r + \beta_r > \gamma_r$$

holds for one or more r, $1 \leqq r \leqq n$. If

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

is a distribution in which

$$\alpha_r \geqq \alpha_r', \beta_r \geqq \beta_r', \alpha_r' + \beta_r' = \gamma_r$$

holds for every r, $1 \leqq r \leqq n$, the distributions corresponding to $(1, i)^{\pm}$ and $(1, j)^{\pm}$ are positive-equivalent.

§ 3. The number of classes for an arbitrarily given N.

Theorem 9. 1) *Suppose that*

$$N = p_1^{2a_1} p_2^{2a_2} \ldots p_m^{2a_m} q_1^{2b_1+1} q_2^{2b_2+1} \ldots q_n^{2b_n+1},$$

where a_i are positive integers and b_j are non-negative integers and p_i and q_j are primes all of which are different.

Suppose that $n > 0$. Then the Diophantine equation

$$u^2 - Dv^2 = \pm 4 p_1^{2a_1} p_2^{2a_2} \ldots p_m^{2a_m} q_1^{2b_1+1} q_2^{2b_2+1} \ldots q_n^{2b_n+1} \tag{14}$$

has at most $2^{n-1}(2a_1 + 1)(2a_2 + 1) \ldots (2a_m + 1)(b_1 + 1)(b_2 + 1) \ldots (b_n + 1)$ solutions $\frac{u_i + v_i\sqrt{D}}{2}$ in which u_i and v_i satisfy inequalities (4) and (5), or (7) and (8) respectively, provided u_i is non-negative.

Suppose that $n = 0$ or that $n > 0$ and the greatest power of q_j which divides D is $q_j^{2a_j}$ or $q_j^{2\beta_j+1}$, $a_j > b_j$, $\beta_j \geqq 0$, $j = 1, 2, \ldots, n$. If $q_{j'} = 2$ holds for $j = j'$, for j' it is sufficient that $D = 2^{2a_{j'}} D_1$ holds, $b_{j'} \geqq a_{j'} \geqq 0$, $D_1 \equiv 3 \pmod 4$. Then (14) has at most $\frac{1}{2}((2a_1 + 1)(2a_2 + 1) \ldots (2a_m + 1) + 1)$ solutions $\frac{u_i + v_i\sqrt{D}}{2}$ in

which u_i *and* v_i *satisfy inequalities (4) and (5), or (7) and (8) resqectively, provided* u_i *is non-negative.*

2) *Suppose that* $n > 0$ *and that all* p_i *and* q_j *are odd primes. If solvable, the equation has at most*

$2^n (2a_1 + 1)(2a_2 + 1) \ldots (2a_m + 1)(b_1 + 1)(b_2 + 1) \ldots (b_n + 1)$ *classes when* N *and* D *are relatively prime;*

$2^{n-n'}(2(a_{\gamma_1} - \alpha_{\gamma_1}) + 1)(2(a_{\gamma_2} - \alpha_{\gamma_2}) + 1) \ldots (2(a_{\gamma_{m-m'}} - \alpha_{\gamma_{m-m'}}) + 1)(b_{\gamma_1} - \beta_{\gamma_1} + 1) \cdot$
$\cdot (b_{\gamma_2} - \beta_{\gamma_2} + 1) \ldots (b_{\gamma_{n-n'}} - \beta_{\gamma_{n-n'}} + 1)$ *classes when* $p_i^{2a_i}$ *is the greatest power of* p_i *which divides* D, $a_i > \alpha_i \geqq 0$, $i = 1, 2, \ldots, m - m'$, *and when* $p_h^{2a_h}$ *or* $p_h^{2\beta_h+1}$ *is the greatest power of* p_h *which divides* D, $\alpha_h \geqq a_h$, $\beta_h \geqq 0$, $h = m - m' + 1$, $m - m' + 2, \ldots, m$, $0 \leqq m' \leqq m$, *and further, when* $q_j^{2\alpha_j}$ *is the greatest power of* q_j *which divides* D, $b_j \geqq \alpha_j \geqq 0$, $j = 1, 2, \ldots, n - n'$, *and when* $q_r^{2\alpha_r}$ or $q_r^{2\beta_r+1}$ *is the greatest power of* q_r *which divides* D, $\alpha_r > b_r$, $\beta_r \geqq 0$, $r = n - n' + 1, n - n' + 2, \ldots, n$, $0 \leqq n' \leqq n$;

one class when N *is a divisor of* D.

Suppose that $n > 0$ *and that* $p_m = 2$, *or* $q_n = 2$ *respectively. If solvable, the equation has at most*

the same number of classes as if all primes were odd, when $D = 2^{2\alpha} D_1$, $\alpha \geqq 0$, $D_1 \equiv 1 \pmod 4$;

the same number of classes as if there were only $m - 1$ *primes* p_i, *or* $n - 1$ *primes* q_j *respectively, and if all primes were odd,*

when $D = 2^{2\alpha} D_1$, $\alpha \geqq 0$, $D_1 \equiv 3 \pmod 4$;
when $D = 2^{2\beta+1} D_1$, $\beta \geqq 0$.

Suppose that $n = 0$ *or that* $n > 0$ *and the greatest power of* q_j *which divides* D *is* $q_j^{2\alpha_j}$ *or* $q_j^{2\beta_j+1}$, $\alpha_j > b_j$, $\beta_j \geqq 0$, $j = 1, 2, \ldots, n$. *If* $q_{j'} = 2$ *holds for* $j = j'$, *for* j' *it is sufficient that* $D = 2^{2\alpha_{j'}} D_1$ *holds,* $b_{j'} \geqq \alpha_{j'} \geqq 0$, $D_1 \equiv 3 \pmod 4$. *If solvable, the equation has at most*

$(2a_1 + 1)(2a_2 + 1) \ldots (2a_m + 1)$ *classes when all* p_i *are odd primes which are prime to* D;

$(2(a_{\gamma_1} - \alpha_{\gamma_1}) + 1)(2(a_{\gamma_2} - \alpha_{\gamma_2}) + 1) \ldots (2(a_{\gamma_{m-m'}} - \alpha_{\gamma_{m-m'}}) + 1)$ *classes when* $p_i^{2a_i}$ *is the greatest power of* p_i *which divides* D, $a_i > \alpha_i \geqq 0$, $i = 1, 2, \ldots, m - m'$, *and when* $p_h^{2a_h}$ *or* $p_h^{2\beta_h+1}$ *is the greatest power of* p_h *which divides* D, $\alpha_h \geqq a_h$, $\beta_h \geqq 0$, $h = m - m' + 1$, $m - m' + 2, \ldots, m$, $0 \leqq m' \leqq m$;

the same number of classes as if all p_i *were odd, when* $p_m = 2$ *and when* $D = 2^{2\alpha} D_1$, $\alpha \geqq 0$, $D_1 \equiv 1 \pmod 4$;

the same number of classes as if there were only $m - 1$ *primes* p_i *all of which were odd, when* $p_m = 2$ *and*

when $D = 2^{2\alpha} D_1$, $\alpha \geqq 0$, $D_1 \equiv 3 \pmod 4$;
when $D = 2^{2\beta+1} D_1$, $\beta \geqq 0$.

Proof: Suppose that all primes are odd and that N and D are relatively prime, and consider the solutions $\frac{u_1 + v_1\sqrt{D}}{2}, \frac{u_2 + v_2\sqrt{D}}{2}, \ldots, \frac{u_t + v_t\sqrt{D}}{2}, \ldots$ in

which u and v satisfy the conditions of the first part of the theorem. It is apparent from Section 2 that the number of distinct solutions satisfying these conditions depends on the number of distributions corresponding to $(1, 2)^{\pm}$, $(1, 3)^{\pm}, \ldots, (1, t)^{\pm}, \ldots$ any two of which are neither positive-equivalent nor negative-equivalent.

We first suppose that $m = 0$, $n = 1$. Consider the following distributions.

$$(1, 2) \oplus q_1^{2b_1+1},$$
$$(1, 3) \oplus q_1^{2b_1}, \ominus q_1,$$
$$(1, 4) \oplus q_1^{2b_1-1}, \ominus q_1^2,$$
$$\ldots$$
$$(1, 2b_1 + 3) \ominus q_1^{2b_1+1}.$$

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. Moreover, 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 $b_1 + 1$. If we exclude the distribution

$$(1, 2) \oplus q_1^{2b_1+1} \quad \text{or} \quad (1, 2b_1 + 3) \ominus q_1^{2b_1+1}$$

there remains b_1 distributions. Then it is apparent that there are at most $b_1 + 1$ solutions satisfying the conditions of the first part of the theorem.

We now suppose that $m = 0$, $n = 2$. From the preceding case it is apparent that there are the following number of distributions any two of which are neither positive-equivalent nor negative-equivalent.

$$(1, 2) \oplus q_1^{2b_1+1} q_2^{2b_2+1},$$
$$(1, 3) \oplus q_1^{2b_1+1} q_2^{2b_2}, \ominus q_2,$$
$$\ldots$$
$$(1, 2[b_2 + 1] + 1) \oplus q_1^{2b_1+1}, \ominus q_2^{2b_2+1},$$
$$(1, 2[b_2 + 1] + 2) \oplus q_1^{2b_1} q_2^{2b_2+1}, \ominus q_1,$$
$$\ldots$$
$$(1, 4[b_2 + 1] + 1) \oplus q_1^{2b_1}, \ominus q_1 q_2^{2b_2+1},$$
$$\ldots$$
$$(1, 2[b_1 + 1][b_2 + 1] + 1) \oplus q_1^{b_1+1}, \ominus q_1^{b_1} q_2^{2b_2+1}.$$

It is easily seen that any two of these distributions are neither positive-equivalent nor negative-equivalent and that every other distribution is positive-equivalent or negative-equivalent to one of these distributions at least. If we exclude the distribution

$$(1, 2) \oplus q_1^{2b_1+1} q_2^{2b_2+1}$$

there remains $2(b_1 + 1)(b_2 + 1) - 1$ distributions. Then it is apparent that there are at most $2(b_1 + 1)(b_2 + 1)$ solutions satisfying the conditions of the first part of the theorem.

We now consider the case when $m = 0$. From the preceding case it is apparent how to determine a set of distributions any two of which are neither positive-equivalent nor negative-equivalent. In fact there are

$$2^{n-1}(b_1 + 1)(b_2 + 1) \ldots (b_n + 1)$$

such distributions. If we exclude the distribution

$$(1, 2) \oplus q_1^{2b_1+1} q_2^{2b_2+1} \ldots q_n^{2b_n+1}$$

there remains $2^{n-1}(b_1 + 1)(b_2 + 1) \ldots (b_n + 1) - 1$ distributions. Then it is apparent that there are at most $2^{n-1}(b_1 + 1)(b_2 + 1) \ldots (b_n + 1)$ solutions satisfying the conditions of the first part of the theorem.

We now suppose that $m = 1$, $n = 0$. Then we have to consider the following distributions.

$$(1, 2) \oplus p_1^{2a_1},$$
$$(1, 3) \oplus p_1^{2a_1-1}, \quad \ominus p_1,$$
$$\ldots$$
$$(1, 2a_1 + 2) \ominus p_1^{2a_1}.$$

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. Moreover, it is apparent that all distributions except

$$(1, a_1 + 2) \oplus p_1^{a_1}, \ \ominus p_1^{a_1}$$

are negative-equivalent in pairs and that two distributions of different pairs are not negative-equivalent. Nor is

$$(1, a_1 + 2) \oplus p_1^{a_1}, \ \ominus p_1^{a_1}$$

negative-equivalent to any other distribution. Thus the maximum number of distributions any two of which are neither positive-equivalent nor negative-equivalent is $a_1 + 1$. If we exclude the distribution

$$(1, 2) \oplus p_1^{2a_1} \text{ or } (1, 2a_1 + 2) \ominus p_1^{2a_1}$$

there remains a_1 distributions. Then it is apparent that there are at most

$$a_1 + 1 = \tfrac{1}{2}((2a_1 + 1) + 1)$$

solutions satisfying the conditions of the first part of the theorem.

We next consider the case when $m = 2$, $n = 0$. Then it is apparent that there are the following distributions any two of which are neither positive-equivalent nor negative-equivalent.

$$(1, 2) \oplus p_1^{2a_1}\ p_2^{2a_2},$$

$$(1, 3) \oplus p_1^{2a_1}\ p_2^{2a_2-1},\ \ominus p_2,$$

$$\ldots$$

$$(1, a_2 + 1) \oplus p_1^{2a_1}\ p_2^{a_2+1},\ \ominus p_2^{a_2-1},$$

$$(1, a_2 + 2) \oplus p_1^{2a_1-1}\ p_2^{2a_2},\ \ominus p_1,$$

$$\ldots$$

$$(1, a_1 a_2 + 1) \oplus p_1^{a_1+1}\ p_2^{a_2+1},\ \ominus p_1^{a_1-1}\ p_2^{a_2-1},$$

$$(1, a_1 a_2 + 2) \oplus p_1^{2a_1},\ \ominus p_2^{2a_2},$$

$$\ldots$$

$$(1, 2a_1 a_2 + 1) \oplus p_1^{a_1+1}\ p_2^{a_2-1},\ \ominus p_1^{a_1-1}\ p_2^{a_2+1}$$

$$(1, 2a_1 a_2 + 2) \oplus p_1^{a_1}\ p_2^{2a_2},\ \ominus p_1^{a_1},$$

$$\ldots$$

$$(1, 2a_1 a_2 + a_2 + 1) \oplus p_1^{a_1}\ p_2^{a_2+1},\ \ominus p_1^{a_1}\ p_2^{a_2-1},$$

$$\ldots$$

$$(1, 2a_1 a_2 + a_2 + 2) \oplus p_1^{2a_1}\ p_2^{a_2},\ \ominus p_2^{a_2},$$

$$\ldots$$

$$(1, 2a_1 a_2 + a_1 + a_2 + 1) \oplus p_1^{a_1+1}\ p_2^{a_2},\ \ominus p_1^{a_1-1}\ p_2^{a_2},$$

$$(1, 2a_1 a_2 + a_1 + a_2 + 2) \oplus p_1^{a_1}\ p_2^{a_2},\ \ominus p_1^{a_1}\ p_2^{a_2}.$$

It is apparent that any two of these distributions are neither positive-equivalent nor negative-equivalent and that every other distribution is positive-equivalent either to one of these distributions or to a distribution which is negative-equivalent to one of these distributions. If we exclude the distribution

$$(1, 2) \oplus p_1^{2a_1}\ p_2^{2a_2}$$

there remains $2a_1 a_2 + a_1 + a_2$ distributions. Then it is apparent that there are at most

$$2a_1 a_2 + a_1 + a_2 + 1 = \tfrac{1}{2}\left((2a_1 + 1)(2a_2 + 1) + 1\right)$$

solutions satisfying the conditions of the first part of the theorem.

We next consider the case when $m = 3$, $n = 0$. From the preceding case it is easily seen that we get $4a_1 a_2 a_3$ distributions in which $(1, t)^+$ and $(1, t)^-$ are not divisible by any $p_i^{a_i}$ on the same time, $2a_1 a_2$ distributions in which $(1, t)^+$ and $(1, t)^-$ are only divisible by $p_3^{a_3}$ by the same time, a_1 distributions in which $(1, t)^+$ and $(1, t)^-$ are divisible by $p_2^{a_2}\ p_3^{a_3}$ on the same time and one distribution in which both $(1, t)^+$ and $(1, t)^-$ are divisible by $p_1^{a_1}\ p_2^{a_2}\ p_3^{a_3}$. Then it is apparent that there are

$$4a_1a_2a_3 + 2a_1a_2 + 2a_2a_3 + 2a_3a_1 + a_1 + a_2 + a_3 + 1$$

distributions any two of which are neither positive-equivalent nor negative-equivalent. Then there are at most

$$\tfrac{1}{2}((2a_1 + 1)(2a_2 + 1)(2a_3 + 1) + 1)$$

solutions satisfying the conditions of the first part of the theorem.

We now consider the case when $n = 0$ and m is arbitrary. From the preceding cases it is apparent how to find the maximum number of distributions any two of which are neither positive-equivalent nor negative-equivalent.

If S_k is the *k-th* elementary symmetric function of the numbers $a_1, a_2, \ldots, a_m$, $1 \leqq k \leqq m$, we get

2^{m-1} S_m distributions in which $(1, t)^+$ and $(1, t)^-$ are not divisible by any $p_i^{a_i}$ on the same time,

2^{m-2} S_{m-1} distributions in which $(1, t)^+$ and $(1, t)^-$ are divisible by just one $p_i^{a_i}$ on the same time,

...

2^{k-1} S_k distributions in which $(1, t)^+$ and $(1, t)^-$ are divisible by $m - k$ of the powers $p_i^{a_i}$ on the same time,

...

S_1 distributions in which $(1, t)^+$ and $(1, t)^-$ are divisible by all the powers $p_i^{a_i}$ except one on the same time.

If we add the distribution

$$(1, 2) \oplus p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}, \ominus p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$$

and exclude the distribution in which any of $(1, t)^+$ and $(1, t)^-$ is divisible by $p_1^{2a_1} p_2^{2a_2} \ldots p_m^{2a_m}$ there remains

$$\tfrac{1}{2}((2a_1 + 1)(2a_2 + 1) \ldots (2a_m + 1) + 1) - 1$$

distributions any two of which are neither positive-equivalent nor negative-equivalent. It is easily seen that every other distribution is positive-equivalent either to one of these distributions or to a distribution which is negative-equivalent to one of them. Then it is apparent that there are at most

$$\tfrac{1}{2}((2a_1 + 1)(2a_2 + 1) \ldots (2a_m + 1) + 1)$$

solutions satisfying the conditions of the first part of the theorem.

We next consider the case when $m = 1$, $n = 1$. Then it is clear that any two of the following distributions are not positive-equivalent and that every other distribution is positive-equivalent to one of these distributions.

$$(1, 2) \oplus p_1^{2a_1} q_1^{2b_1+1},$$

$$(1, 3) \oplus p_1^{2a_1} q_1^{2b_1}, \ominus q_1,$$

...

$$(1, [2a_1 + 1][2b_1 + 2] + 1) \ominus p_1^{2a_1} q_1^{2b_1+1}.$$

It is apparent that these distributions are negative-equivalent in pairs and that two distributions of different pairs are not negative-equivalent. Thus there are

$$(2a_1 + 1)\ (b_1 + 1)$$

distributions any two of which are neither positive-equivalent nor negative-equivalent. If we exclude the distribution

$$(1, 2) \oplus p_1^{2a_1}\, q_1^{2b_1+1} \quad \text{or} \quad (1, [2a_1 + 1]\,[2b_1 + 2] + 1) \ominus p_1^{2a_1}\, q_1^{2b_1+1}$$

there remains $(2a_1 + 1)\ (b_1 + 1) - 1$ distributions. Then there are at most $(2a_1 + 1)\ (b_1 + 1)$ solutions satisfying the conditions of the first part of the theorem.

Finally, we consider the case when both m and n are arbitrary. From the preceding case it is apparent that there are at most

$$2^{n-1}\,(2a_1 + 1)\ (2a_2 + 1) \ldots (2a_m + 1)\ (b_1 + 1)\ (b_2 + 1) \ldots (b_n + 1)$$

distributions any two of which are neither positive-equivalent nor negative-equivalent, and at most the same number of solutions satisfying the conditions of the first part of the theorem. Hence this part of the theorem is proved.

Suppose that $n > 0$ and that all p_i and q_j are odd primes. If N and D are relatively prime, there are at most

$$2^n (2a_1 + 1)\ (2a_2 + 1) \ldots (2a_m + 1)\ (b_1 + 1)\ (b_2 + 1) \ldots (b_n + 1)$$

classes, since it is apparent that every solution satisfying the conditions of the first part of the theorem may correspond to two classes. When $p_i^{2\alpha_i}$ is the greatest power of p_i which divides D, $a_i > \alpha_i \geqq 0$, every u is divisible by $p_i^{\alpha_i}$. If $\dfrac{u_1 + v_1\sqrt{D}}{2}$ and $\dfrac{u_t + v_t\sqrt{D}}{2}$ are two solutions satisfying the conditions of the first part of the theorem, $p_i^{\alpha_i}$ divides both $(1, t)^+$ and $(1, t)^-$. In order to get the maximum number of distributions any two of which are neither positive-equivalent nor negative-equivalent, it is clear that the factor $(2a_i + 1)$ of the expression deduced above must be substituted by the factor $(2(a_i - \alpha_i) + 1)$, and similarly in the number of classes. When $p_h^{2\alpha_h}$ is the greatest power of p_h which divides D, $\alpha_h \geqq a_h$, every u is divisible by $p_h^{a_h}$. When $p_h^{2\beta_h+1}$ is the greatest power of p_h which divides D, every u is also divisible by $p_h^{a_h}$. In fact, from (14) it is seen that if N is divisible by $p_h^{2a_h}$ and D is divisible by $p_h^{2\beta_h+1}$, u^2 is divisible by $p_h^{2\beta_h+1}$. Then u is divisible by $h_h^{\beta_h+1}$. But then Dv^2 is divisible by $p_h^{2\beta_h+2}$, and thus v^2 is divisible by p_h and v is divisible by p_h. But then Dv^2 is divisible by $p_h^{2\beta_h+3}$, and then u is divisible by $p_h^{\beta_h+2}$. It is apparent that we may continue, till u is divisible by $p_h^{a_h}$. In both these cases, the powers of $p_h^{2a_h}$ give no contribution to the number of distributions and the number of classes.

In the same way, when $q_j^{2a_j}$ is the greatest power of q_j which divides D, $b_j \geqq a_j \geqq 0$, the factor $(b_j + 1)$ may be substituted by $(b_j - a_j + 1)$, and when $q_r^{2a_r}$ or $q_r^{2\beta_r+1}$ is the greatest power of q_r which divides D, $a_r > b_r$, $\beta_r \geqq 0$, the powers of q_r give no contribution to the number of distributions and the number of classes. If $i = 1, 2, \ldots, m-m'$, $h = m - m' + 1$, $m - m' + 2, \ldots, m$, $0 \leqq \leqq m' \leqq m$, $j = 1, 2, \ldots, n-n'$, $r = n - n' + 1$, $n - n' + 2, \ldots, n$, $0 \leqq n' \leqq n$, the number of classes is at most

$$2^{n-n'} (2(a_{\gamma_1} - a_{\gamma_1}) + 1)(2(a_{\gamma_2} - a_{\gamma_2}) + 1) \ldots (2(a_{\gamma_{m-m'}} - a_{\gamma_{m-m'}}) + 1) \cdot$$

$$\cdot (b_{\gamma_1} - a_{\gamma_1} + 1)(b_{\gamma_2} - a_{\gamma_2} + 1) \ldots (b_{\gamma_{n-n'}} - a_{\gamma_{n-n'}} + 1).$$

If $n > 0$ and $p_m = 2$, or $q_n = 2$ respectively, (14) is only solvable in odd u and v when $D \equiv 1 \pmod 4$. If $D = 2^{2a} D_1$, $D_1 \equiv 1 \pmod 4$, every u is divisible by 2^a, $a \leqq a_m$, or $a \leqq b_n$ respectively, or by 2^{a_m}, or by 2^{b_n+1} respectively, when $a \geqq a_m$, or $a > b_n$ respectively. Thus the equation has the same number of classes as if all primes were odd. When $D = 2^{2a} D_1$, $a \geqq 0$, $D_1 \equiv 3 \pmod 4$, or when $D = 2^{2\beta+1} D_1$, $\beta \geqq 0$, every u is divisible by 2^{a_m}, or by 2^{b_n+1} respectively. In that case (14) has the same number of classes as if there were only $m - 1$ primes p_i, or $n - 1$ primes q_j respectively, and if all primes were odd.

We next suppose that $n = 0$ or that $n > 0$ and the greatest power of q_j which divides D is $q_j^{2a_j}$ or $q_j^{2\beta_j+1}$, $a_j > b_j$, $\beta_j \geqq 0$, $j = 1, 2, \ldots, n$. If $q_{j'} = 2$ holds for $j = j'$, for j' it is sufficient that $D = 2^{2a_{j'}} D_1$ holds, $b_{j'} \geqq a_{j'} \geqq 0$, $D_1 \equiv 3 \pmod 4$. Then it is apparent that every u is divisible by $q_1^{b_1} q_2^{b_2} \ldots q_n^{b_n}$. In that case (14) has at most

$$\tfrac{1}{2}(2a_1 + 1)(2a_2 + 1) \ldots (2a_m + 1) + 1)$$

solutions in which u and v satisfy inequalities (4) and (5), or (7) and (8) respectively, provided u is non-negative. When all p_i are odd primes which do not divide D, there are at most

$$\tfrac{1}{2}(2a_1 + 1)(2a_2 + 1) \ldots (2a_m + 1)$$

classes because one of the solutions corresponds to only one class, and this class is ambiguous. In fact, suppose that

$$D = q_1^{2b_1'} q_2^{2b_2'} \ldots q_n^{2b_n'} D_1$$

holds, $b_j \geqq b_j' \geqq 0$. As D is divisible by $q_j^{2a_j}$ or by $q_j^{2\beta_j+1}$, $a_j > b_j$, $\beta_j \geqq 0$, it is apparent that every q_j divides D_1. Suppose that $\dfrac{u + v\sqrt{D}}{2}$ is a solution of (14) in which

$$u = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m} q_1^{b_1} q_2^{b_2} \ldots q_n^{b_n} u',$$

$$v = q_1^{2(b_1 - b_1')} q_2^{2(b_2 - b_2')} \ldots q_n^{2(b_n - b_n')} v'$$

holds. Then (14) may be written

$$p_1^{2a_1} p_2^{2a_2} \dots p_m^{2a_m} q_1^{2b_1} q_2^{2b_2} \dots q_n^{2b_n} (u'^2 - D_1 v'^2 = \pm 4 q_1 q_2 \dots q_n).$$

As D_1 is divisible by $q_1 q_2 \dots q_n$, it is apparent from Theorem 8 in Part I that

$$u'^2 - D_1 v'^2 = \pm 4 q_1 q_2 \dots q_n$$

has one ambiguous class, if it is solvable. It is apparent that this class corresponds to an ambiguous class of (14). If $p_i^{2a_i}$ is the greatest power p_i which divides D, $a_i > a_i \geqq 0$, $i = 1, 2, \dots, m-m'$, and when $p_h^{2a_h}$ or $p_h^{2\beta_h+1}$ is the greatest power of p_h which divides D, $a_h \geqq a_h$, $\beta_h \geqq 0$, $h = m - m' + 1, m - m' + 2, \dots, m$, $0 \leqq m' \leqq m$, it is apparent there are at most

$$(2(a_{\gamma_1} - a_{\gamma_1}) + 1)\,(2(a_{\gamma_2} - a_{\gamma_2}) + 1) \dots (2(a_{\gamma_{m-m'}} - a_{\gamma_{m-m'}}) + 1)$$

classes. When $p_m = 2$ and when $D = 2^{2a} D_1$, $a \geqq 0$, $D_1 \equiv 1 \pmod 4$, it is apparent from the preceding cases that there is the same number of classes as if all p_i were odd. When $p_m = 2$, $D = 2^{2a} D_1$, $a \geqq 0$, $D_1 \equiv 3 \pmod 4$, or when $p_m = 2$, $D = 2^{2\beta+1} D_1$, $\beta \geqq 0$, there is the same number of classes as if there were only $m - 1$ primes p_i. Hence the theorem is proved.

§ 4. The number of ambiguous classes.

We shall prove

Theorem 10. *The Diophantine equation*

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

has at most one ambiguous class.

Proof: Suppose that

$$N = p_1^{2a_1} p_2^{2a_2} \dots p_m^{2a_m} q_1^{2b_1+1} q_2^{2b_2+1} \dots q_n^{2b_n+1},$$

where a_i are positive integers and b_j are non-negative integers and p_i and q_j are primes all of which are different. Further suppose that $p_i^{2a_i}$ is the greatest power of p_i which divides D, $a_i > a_i \geqq 0$, $i = 1, 2, \dots, m'$, that $p_h^{2a_h}$ or $p_h^{2\beta_h+1j}$ is the greatest power of p_h which divides D, $a_h \geqq a_h$, $\beta_h \geqq 0$, $h = m' + 1$, $m' + 2, \dots, m$, that $q_j^{2a_j}$ is the greatest power of q_j which divides D, $b_j \geqq a_j \geqq 0$, $j = 1, 2, \dots, n'$, and that $q_r^{2a_r}$ or $q_r^{2\beta_r+1}$ is the greatest power of q_r which divides D, $a_r > b_r$, $\beta_r \geqq 0$, $r = n' + 1, n' + 2, \dots, n$. Then (1) may be divided by

$$p_1^{2a_1} p_2^{2a_2} \dots p_{m'}^{2a_{m'}} p_{m'+1}^{2a_{m'+1}} \dots p_m^{2a_m} q_1^{2a_1} q_2^{2a_2} \dots q_{n'}^{2a_{n'}} q_{n'+1}^{2b_{n'+1}} q_n^{2b_n},$$

and we get the Diophantine equation

$$u'^2 - q_{n'+1} q_{n'+2} \dots q_n D_1 v'^2 = \pm 4\, p_1^{2(a_1-a_1)} p_2^{2(a_2-a_2)} \dots p_{m'}^{2(a_{m'}-a_{m'})} \cdot q_1^{2(b_1-a_1)+1} \dots q_{n'}^{2(b_{n'}-a_{n'}+1)} q_{n'+1} \dots q_n$$

This equation may be written

$$u'^2 - rD_1v'^2 = \pm rst^2, \tag{15}$$

where st^2 and D_1 are relatively prime.

According to Theorem 4 in Part I, the necessary and sufficient condition for the solutions $\frac{u + v\sqrt{D}}{2}$ and $\frac{u_1 + v_1\sqrt{D}}{2}$ of the Diophantine equation

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

to belong to the same class is that

$$\frac{uv_1 - u_1v}{2N}$$

be an integer.

Suppose that (15) is solvable and has an ambiguous class the fundamental solution of which is $\frac{u' + v'\sqrt{rD_1}}{2}$. As the class is ambiguous,

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

must be an integer. As st^2 and D_1 are relatively prime, st must divide v'. But then s also divides u' which is impossible. Thus a necessary condition for (15) to possess an ambiguous class is that $s = 1$ holds.

Suppose that there is another ambiguous class the fundamental solution of which is $\frac{u'_1 + v'_1\sqrt{rD_1}}{2}$. As the class is ambiguous,

$$\frac{u'_1v'_1}{2N}$$

is an integer. But then t divides v'_1. The necessary and sufficient condition for the two ambiguous classes to coincide is that

$$\frac{u'v'_1 - u'_1v'}{2rt^2}$$

be an integer. It is apparent that r divides u' as well as u'_1 and that t divides u', u'_1, v' and v'_1. Hence the theorem is proved.

§ 5. Numerical examples.

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

Example 1. $u^2 - 17v^2 = 128 = 4.2^5$.

The fundamental solution of the equation $u^2 - 17v^2 = 4$ is $\frac{1}{2}(66 + 16\sqrt{17})$. For the fundamental solutions in which u and v are non-negative, according to inequalities (4) and (5) we get

$$0 \leqq v \leqq \sqrt{\frac{64N}{17}},\ 0 < u \leqq \sqrt{68N}.$$

We find the fundamental solutions

$$\tfrac{1}{2}(\pm 14 + 2\sqrt{17}),\ \tfrac{1}{2}(\pm 20 + 4\sqrt{17}),\ \tfrac{1}{2}(\pm 31 + 7\sqrt{17}).$$

Example 2. $u^2 - 17v^2 = 256 = 4.2^6$.

We find the fundamental solutions $\tfrac{1}{2}\cdot 16$, $\tfrac{1}{2}(\pm 18 + 2\sqrt{17})$, $\tfrac{1}{2}(\pm 33 + 7\sqrt{17})$, $\tfrac{1}{2}(\pm 52 + 12\sqrt{17})$.

Example 3. $u^2 - 7v^2 = 128 = 4.2^5$.

The fundamental solution of the equation $u^2 - 7v^2 = 4$ is $\tfrac{1}{2}(16 + 6\sqrt{7})$. For the fundamental solutions in which u and v are non-negative, according to inequalities (4) and (5) we get

$$0 \leqq v \leqq \sqrt{2N},\ 0 < u \leqq \sqrt{18N}.$$

We find the fundamental solution $\tfrac{1}{2}(24 + 8\sqrt{7})$. As $D \equiv 3 \pmod 4$, the equation has only one class.

Example 4. $u^2 - 148v^2 = 78\,732 = 4.3^9$.

The fundamental solution of the equation $u^2 - 148v^2 = 4$ is $\tfrac{1}{2}(146 + 12\sqrt{148})$. For the fundamental solutions in which u and v are non-negative, according to inequalities (4) and (5) we get

$$0 \leqq v \leqq \sqrt{\frac{36N}{37}},\ 0 < u \leqq \sqrt{37N}.$$

We find the fundamental solutions $\tfrac{1}{2}(\pm 432 + 27\sqrt{148})$, $\tfrac{1}{2}(\pm 1048 + 83\sqrt{148})$. Thus the number of classes is less than the maximum number.

Example 5. $u^2 - 6v^2 = -180 = -4.45 = -4.5.3^2$.

The fundamental solution of the equation $u^2 - 6v^2 = 4$ is $\tfrac{1}{2}(10 + 4\sqrt{6})$. For the fundamental solutions in which u and v are non-negative, according to inequalities (7) and (8) we get

$$0 < v \leqq 7,\ 0 \leqq u \leqq 18.$$

We find the fundamental solutions $\tfrac{1}{2}(\pm 6 + 6\sqrt{6})$. As 3 divides 180 there are only two classes.

Example 6. $u^2 - 17v^2 = 70\,304 = 4.2^3.13^3$.

We find the fundamental solutions

$$\tfrac{1}{2}(\pm 269 + 11\sqrt{17}),\ \tfrac{1}{2}(\pm 286 + 26\sqrt{17}),\ \tfrac{1}{2}(\pm 326 + 46\sqrt{17}),\ \tfrac{1}{2}(\pm 377 + 65\sqrt{17}),$$
$$\tfrac{1}{2}(\pm 473 + 95\sqrt{17}),\ \tfrac{1}{2}(\pm 598 + 130\sqrt{17}),\ \tfrac{1}{2}(\pm 734 + 166\sqrt{17}),$$
$$\tfrac{1}{2}(\pm 949 + 221\sqrt{17}).$$

Thus the equation has the maximum number of classes.

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 elementaer 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).

Tryckt den 3 juni 1952

Uppsala 1952. Almqvist & Wiksells Boktryckeri AB