

On a Diophantine equation of the second degree

By BENGT STOLT

§ 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. 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]–[5]) how it is possible to determine all the solutions of the Diophantine equation

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

where D and N are integers and D is not a perfect square, by quite elementary methods. The author ([6]–[8]) used these methods to the equation

$$x^2 - Dy^2 = \pm 4N. \tag{2}$$

Consider the Diophantine equation

$$Au^2 + Buv + Cv^2 = \pm N, \tag{3}$$

where A , B , C and N are integers and $B^2 - 4AC = D$ is a positive integer which is not a perfect square. It is obvious that (3) can be transformed into (1) by means of linear transformations with integral coefficients. The problem of determining all the solutions of (3) in integers u and v then reduces to the problem of finding all the integral solutions x and y of (1) which satisfy certain linear congruences; see Nagell [4], pp. 214–215. However, in this way we get no general view of the solutions of (3), and it will be rather laborious to discuss the different cases which may occur.

The purpose of this paper is to show how it is possible to avoid the linear transformations and congruences. In fact, for equation (3), we shall deduce inequalities analogous to those determined by Nagell for equation (1). We shall use the notions proposed by Nagell or notions analogous to them.

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

Consider the Diophantine equation

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

where D is a positive integer which is not a perfect square. When x and y are integers satisfying this equation, the number $\frac{1}{2}(x + y\sqrt{D})$ is said to be an *integral solution* of this equation. Two solutions $\frac{1}{2}(x + y\sqrt{D})$ and $\frac{1}{2}(x' + y'\sqrt{D})$ are equal, if $x = x'$ and $y = y'$. Among all the integral solutions of the equation there is a solution

$$\frac{1}{2}(x_1 + y_1\sqrt{D})$$

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

A well-known result is the following

THEOREM. *When D is a natural number which is not a perfect square, the Diophantine equation*

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

has an infinity of integral solutions. If the fundamental solution is denoted by ε , every integral solution $\frac{1}{2}(x + y\sqrt{D})$ may be written in the form

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

If $D \equiv 5 \pmod{8}$, there only exist integral solutions with even x and y .

§ 3. The classes of solutions of the Diophantine equation $Au^2 + Buv + Cv^2 = \pm N$.

The fundamental solutions of the classes

Let A and N be positive integers and B and C be rational integers such that $B^2 - 4AC = D$ is a positive integer which is not a perfect square. Consider the Diophantine equation

$$Au^2 + Buv + Cv^2 = \pm N. \tag{3}$$

It is suitable to define a solution of (3) in the following way. If $u = t/A$ is a fractional number and v is an integer which satisfy (3), the number

$$\frac{(2Au + Bv) + v\sqrt{D}}{2} \tag{5}$$

is called a *solution* of (3). If $(x + y\sqrt{D})/2$ is an integral solution of the Diophantine equation

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

the number

$$\frac{(2Au + Bv) + v\sqrt{D}}{2} \cdot \frac{x + y\sqrt{D}}{2} = \frac{(2Aux + Bvx + Dvy) + (2Auy + Bvy + vx)\sqrt{D}}{4}$$

is also a solution of (3). This solution is said to be *associated* with the solution $[(2Au + Bv) + \sqrt{D}]/2$. The set of all solutions associated with each other forms a *class of solutions* of (3).

If u and v are two integers satisfying (3), the number $[(2Au + Bv) + v\sqrt{D}]/2$ is called an *integral solution* of (3).

It is possible to decide whether the two given solutions $[(2Au + Bv) + v\sqrt{D}]/2$ and $[(2Au' + Bv') + v'\sqrt{D}]/2$ belong to the same class or not. In fact, it is easily seen that the necessary and sufficient condition for these two solutions to be associated with each other is that the two numbers $[2Auu' + B(uv' + u'v) + 2Cvv']/N$ and $(vu' - uv')/N$ be integers.

If $u = t/A$ is a fractional number and v is an integer which satisfy (3), $-u$ and $-v$ also satisfy (3). It is apparent that the two solutions $\pm [(2Au + Bv) + v\sqrt{D}]/2$ belong to the same class.

Let u and v be two integers satisfying (3). Then there exists a fractional number $u' = -(Au + Bv)/A$ such that the numbers u' and v satisfy (3). So do the numbers $-u' = (Au + Bv)/A$ and $-v$. It is easily seen that the solutions

$$\pm \frac{(2Au' + Bv) + v\sqrt{D}}{2} = \mp \frac{(2Au + Bv) - v\sqrt{D}}{2}$$

belong to the same class.

Suppose that \mathbf{K} is the class consisting of the solutions $[(2Au_i + Bv_i) + v_i\sqrt{D}]/2$, $i = 1, 2, 3, \dots$. Then it is evident that the solutions $[(2Au_i + Bv_i) - v_i\sqrt{D}]/2$, $i = 1, 2, 3, \dots$, also constitute a class, which may be denoted by \mathbf{K}' . The classes \mathbf{K} and \mathbf{K}' are said to be *conjugates* of each other. Conjugate classes are in general distinct but may sometimes coincide.

Among all the solutions $[(2Au + Bv) + v\sqrt{D}]/2$ in a given class \mathbf{K} we now choose a solution $[(2Au_1 + Bv_1) + v_1\sqrt{D}]/2$ in the following way: Let v_1 be the least non-negative value of v which occurs in \mathbf{K} . If \mathbf{K} and \mathbf{K}' do not coincide, then the number u_1 is also uniquely determined; for the solution

$$\frac{(2Au'_1 + Bv_1) + v_1\sqrt{D}}{2} = \frac{-(2Au_1 + Bv_1) + v_1\sqrt{D}}{2}$$

belongs to the conjugate class \mathbf{K}' . If \mathbf{K} and \mathbf{K}' coincide, we get a uniquely determined u_1 by prescribing $u_1 \geq u'_1$. The solution $[(2Au_1 + Bv_1) + v_1\sqrt{D}]/2$ defined in this way is said to be the *fundamental solution of the class*.

The case $v_1 = 0$ can only occur when the classes coincide.

We prove

THEOREM 1. *Suppose that $[(2Au + Bv) + v\sqrt{D}]/2$ is the fundamental solution of the class \mathbf{K} of the Diophantine equation*

$$Au^2 + Buv + Cv^2 = N, \tag{7}$$

where A and N are positive integers and B and C rational integers, and further $D = B^2 -$

B. STOLT, *On a Diophantine equation of the second degree*

$4AC$ is a positive integer which is not a perfect square. If $(x_1 + y_1\sqrt{D})/2$ is the fundamental solution of equation (4), we have the inequality

$$0 \leq v \leq \sqrt{\frac{AN}{D}}(x_1 - 2). \quad (8)$$

Proof. If equality (8) is true for a class \mathbf{K} , it is also true for the conjugate class \mathbf{K}' . Thus we can suppose that $(2Au + Bv)$ is positive.

We easily get

$$\frac{Dvy_1}{4} = \sqrt{\frac{Dv^2}{4} \cdot \frac{Dy_1^2}{4}} = \sqrt{\left(\frac{x_1^2}{4} - 1\right) \left[\frac{(2Au + Bv)^2}{4} - AN\right]} > 0. \quad (9)$$

Consider the solution

$$\begin{aligned} & \frac{(2Au + Bv) + v\sqrt{D}}{2} \cdot \frac{x_1 - y_1\sqrt{D}}{2} \\ &= \frac{(2Au + Bv)x_1 - Dvy_1 + (vx_1 - (2Au + Bv)y_1)\sqrt{D}}{4} \end{aligned}$$

which belongs to the same class as $[(2Au + Bv) + v\sqrt{D}]/2$. Since $[(2Au + Bv) + v\sqrt{D}]/2$ is the fundamental solution, and since by (9) $[(2Au + Bv)x_1 - Dvy_1]/4$ is positive, we must have

$$\frac{(2Au + Bv)x_1 - Dvy_1}{4} \geq \frac{2Au + Bv}{2}. \quad (10)$$

From this inequality it follows that

$$(2Au + Bv)^2(x_1 - 2)^2 \geq Dv^2y_1^2$$

and finally

$$AN \geq \frac{Dv^2}{x_1 - 2}.$$

This proves inequality (8).

THEOREM 2. *Suppose that $[(2Au + Bv) + v\sqrt{D}]/2$ is the fundamental solution of the class \mathbf{K} of the Diophantine equation*

$$Au^2 + Buv + Cv^2 = -N, \quad (11)$$

where A and N are positive integers and B and C rational integers, and further $D = B^2 - 4AC$ is a positive integer which is not a perfect square. If $(x_1 + y_1\sqrt{D})/2$ is the fundamental solution of equation (4), we have the inequality

$$0 < v \leq \sqrt{\frac{AN}{D}}(x_1 + 2). \quad (12)$$

Proof. If equality (12) is true for a class \mathbf{K} , it is also true for the conjugate class \mathbf{K}' . Thus we can suppose $(2Au + Bv) \geq 0$.

We clearly have

$$\frac{x_1^2 v^2}{4} = \frac{y_1^2}{4} + \frac{1}{D} [(2Au + Bv)^2 + 4AN] > \frac{y_1^2 (2Au + Bv)^2}{4}.$$

Thus
$$\frac{x_1 v - y_1 (2Au + Bv)}{4} > 0. \tag{13}$$

Consider the solution

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

which belongs to the same class as $[(2Au + Bv) + v\sqrt{D}]/2$. Since $[(2Au + Bv) + v\sqrt{D}]/2$ is the fundamental solution of the class, and since, by (13), $[x_1 v - y_1 (2Au + Bv)]/4$ is positive, we must have

$$\frac{x_1 v - y_1 (2Au + Bv)}{4} \geq \frac{v}{2}. \tag{14}$$

From this inequality it follows that

$$(x_1 - 2)^2 v^2 \geq y_1^2 (2Au + Bv)^2 = y_1^2 (Dv^2 - 4AN)$$

or
$$v^2 \leq \frac{4N}{D} (x_1 + 2).$$

This proves inequality (12).

As only integral solutions are of interest, we prove

THEOREM 3. *If one of the solutions of the class \mathbf{K} is an integral solution, every solution of \mathbf{K} is integral.*

Proof. Let \mathbf{K} be a class and $[(2Au + Bv) + v\sqrt{D}]/2$ be an integral solution of it. If there existed a solution $[(2Au_1 + Bv_1) + v_1\sqrt{D}]/2$ belonging to \mathbf{K} , where $u_1 = t/A$ were no integer, we would have an integral solution $(x + y\sqrt{D})/2$ of (4) such that

$$\frac{(2Au + Bv) + v\sqrt{D}}{2} \cdot \frac{x + y\sqrt{D}}{2} = \frac{(2Au_1 + Bv_1) + v_1\sqrt{D}}{2}$$

would hold.

Hence
$$u_1 = \frac{u(x - By)}{2} - Cvy, \quad v_1 = \frac{v(x + By)}{2} + Auy.$$

Both u_1 and v_1 are integers, for if B is even, D is divisible by 4 and x is divisible by 2. If B is odd, D is odd. In that case both x and y are either even or odd. This proves the theorem.

B. STOLT, On a Diophantine equation of the second degree

If the solutions of a class \mathbf{K} are integral, \mathbf{K} is called a *class of integral solutions*. If the classes K and K' are conjugates of each other, it may happen that \mathbf{K} but not \mathbf{K}' is a class of integral solutions.

From the preceding theorems we deduce at once

THEOREM 4. *If A and N are positive integers and B and C rational integers, and further $D = B^2 - 4AC$ is a positive integer which is not a perfect square, the Diophantine equations (7) and (11) have a finite number of classes of integral 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.*

$[(2Au_1 + Bv_1) + v_1\sqrt{D}]/2$ is the fundamental solution of the class \mathbf{K} , we obtain all the solutions $[(2Au + Bv) + v\sqrt{D}]/2$ by the formula

$$\frac{(2Au + Bv) + v\sqrt{D}}{2} = \frac{(2Au_1 + Bv_1) + v_1\sqrt{D}}{2} \cdot \frac{x + y\sqrt{D}}{2},$$

where $(x + y\sqrt{D})/2$ runs through all the solutions of (4), including ± 1 . The Diophantine equations (7) and (11) have no integral solutions at all when they have no integral solutions satisfying inequality (8), or (12) respectively.

We next prove

THEOREM 5. *The necessary and sufficient condition for the solutions*

$$\frac{(2Au + Bv) + v\sqrt{D}}{2}, \quad \frac{(2Au_1 + Bv_1) + v_1\sqrt{D}}{2}$$

of the Diophantine equation

$$Au^2 + Buv + Cv^2 = \pm N \tag{3}$$

to belong to the same class is that

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

be an integer.

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

$$\frac{2Auu_1 + B(uv_1 + u_1v) + 2Cvv_1}{N}, \quad \frac{uv_1 - u_1v}{N}$$

be integers. Thus it is sufficient to show that

$$\frac{2Auu_1 + B(uv_1 + u_1v) + 2Cvv_1}{N}$$

is an integer when $(uv_1 - u_1v)/N$ is an integer.

Multiplying the equations

$$Au^2 + Buv + Cv^2 = \pm N, Au_1^2 + Bu_1v_1 + Cv_1^2 = \pm N \tag{14}$$

we get $(2Au_1u_1 + B(uv_1 + u_1v) + 2Cvv_1)^2 - D(uv_1 - u_1v)^2 = 4N^2.$ (15)

It is apparent from (15) that $2Au_1u_1 + B(uv_1 + u_1v) + 2Cvv_1$ is divisible by N when $uv_1 - u_1v$ is divisible by N .

§ 4. Quasi-ambiguous classes

Let \mathbf{K} be a class of solutions of the Diophantine equation

$$Au^2 + Buv + Cv^2 = \pm N. \tag{3}$$

Further let $[(2Au + Bv) + v\sqrt{D}]/2$ be a solution of \mathbf{K} . If the number

$$\frac{(2Au + Bv)v}{N} \tag{16}$$

is an integer, \mathbf{K} is called a *quasi-ambiguous class*. If u and v are integers, \mathbf{K} is a *quasi-ambiguous class of integral solutions*.

We prove

THEOREM 6. *If the conjugate classes \mathbf{K} and \mathbf{K}' of (3) coincide, the resulting class is quasi-ambiguous.*

Proof. Let \mathbf{K} and \mathbf{K}' be a pair of conjugate classes of (3), and let $[(2Au + Bv) + \sqrt{D}]/2$ and $[(2Au' + Bv) + v\sqrt{D}]/2$ be one solution of every class. As the classes coincide, according to Theorem 5 the number $(u - u')v/N$ is an integer.

As $(2Au + Bv) = -(2Au' + Bv)$, we get $Bv = -A(u - u')$. Hence we get

$$\frac{(2Au + Bv)v}{N} = \frac{-(2Au' + Bv)v}{N} = \frac{A(u - u')v}{N}.$$

Clearly this number is an integer. This proves the theorem.

It is apparent from Example 4 that two conjugate classes \mathbf{K} and \mathbf{K}' may be quasi-ambiguous without coinciding.

THEOREM 7. *Let \mathbf{K} and \mathbf{K}' be two conjugate classes of integral solutions. If their fundamental solutions are $[(2Au + Bv) + v\sqrt{D}]/2$ and $[(2Au' + Bv) + v\sqrt{D}]/2$, respectively, and if we have $v = 0$, the classes \mathbf{K} and \mathbf{K}' coincide.*

Let \mathbf{K} be a class of integral solutions. If it has a solution $[(2Au + Bv) + v\sqrt{D}]/2$, where $u = 0$, and if C divides B , the class is quasi-ambiguous.

Proof. Let \mathbf{K} and \mathbf{K}' be two conjugate classes of integral solutions, and let $[(2Au + Bv) + v\sqrt{D}]/2$ and $[(2Au' + Bv) + v\sqrt{D}]/2$ be their fundamental solutions. The necessary and sufficient condition for the two classes to coincide is that the number

B. STOLT, On a Diophantine equation of the second degree

$$\frac{(u - u')v}{N}$$

be an integer. If we have $v = 0$, the condition is clearly fulfilled.

Let \mathbf{K} be a class of integral solutions, and let $[(2Au + Bv) + v\sqrt{D}]/2$ be a solution of it, where $u = 0$. If we put the values 0 and v into the Diophantine equation

$$Au^2 + Buv + Cv^2 = \pm N, \quad (3)$$

we get

$$\pm N = Cv^2.$$

The condition for the class \mathbf{K} to be quasi-ambiguous is that the number

$$\frac{(2Au + Bv)v}{N} \quad (16)$$

be an integer.

Putting $u = 0$ and $\pm N = Cv^2$ into (16) we get

$$\frac{(2Au + Bv)v}{N} = \frac{B}{|C|}.$$

This proves the theorem.

THEOREM 8. *A necessary condition for the Diophantine equation*

$$Au^2 + Buv + Cv^2 = \pm N \quad (3)$$

to have quasi-ambiguous classes is $N = st^2$, where s is a square-free integer that divides $4AD$.

Proof. Let

$$Au^2 + Buv = Cv^2 = \pm N \quad (3)$$

be a Diophantine equation, and suppose that $u = w/A$ is a fractional number and v an integer which satisfy (3). Then the Diophantine equation

$$(2Au + Bv)^2 - Dv^2 = \pm 4AN \quad (18)$$

is solvable in integers $(2Au + Bv)$ and v .

Suppose that we have $N = st^2$, where s is square-free. Further suppose that (3) has a quasi-ambiguous class, and let the number $[(2Au + Bv) + v\sqrt{D}]/2$ be a solution of it. Then the number

$$\frac{(2Au + Bv)v}{st^2} \quad (19)$$

is an integer.

Let p be a prime that divides t . If p divides v , it follows from (18) that it also divides $(2Au + Bv)$. If p and v are coprime, p^2 divides $(2Au + Bv)$ as is easily seen from (19). But then it follows from (18) that p^2 divides D .

Now let p be a prime that divides s . If p divides v , it also divides $(2Au + Bv)$. But then p^2 divides $4AN$ and thus p divides $4A$. If p and v are coprime, p divides $(2Au + Bv)$ and thus p divides D . This proves the theorem.

§ 5. Numerical examples

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

Example 1. $209u^2 + 29uv + v^2 = 31, D = 5$.

The fundamental solution of the equation $x^2 - 5y^2 = 4$ is $(3 + \sqrt{5})/2$. For the fundamental solutions, according to inequality (8), we get $0 \leq v \leq 35$.

We find the fundamental solutions $[(2Au_i + Bv_i) + v_i\sqrt{D}]/2, i = 1, 2, \dots, 8$, where $v_{1,2} = 1, u_1 = 6/19, u_2 = -5/11; v_{3,4} = 14, u_3 = -11/19, u_4 = -15/11; v_{5,6} = 23, u_5 = -249/209, u_6 = -2; v_{7,8} = 35, u_7 = -2, u_8 = -597/209$. Thus the equation has only two classes of integral solutions.

Example 2. $u^2 + 3uv + v^2 = -5, D = 5$.

For the fundamental solutions, according to inequality (12), we get $0 \leq v \leq 1$.

We find the fundamental solution $[(2Au + Bv) + v\sqrt{D}]/2$, where $v = 1, u = 1$. The equation is also satisfied by the numbers $v = 1, u = -4$. However, according to Theorem 5 there is only one class, and this class is quasi-ambiguous, according to Theorem 6.

Example 3. $3u^2 + 7uv + 3v^2 = -13, D = 13$.

The fundamental solution of the equation $x^2 - 13y^2 = 4$ is $(11 + 3\sqrt{13})/2$. For the fundamental solutions, according to inequality (12), we get $0 \leq v \leq 6$.

We find the fundamental solutions $[(2Au_i + Bv_i) + v_i\sqrt{D}]/2, i = 1, 2$, where $v_{1,2} = 5, u_1 = 11/3, u_2 = -8$. Thus the equation has only one class of integral solutions, and this class is quasi-ambiguous.

Example 4. $2u^2 + 5uv + v^2 = 16 = 2^4, D = 17$.

The fundamental solution of the equation $x^2 - 17y^2 = 4$ is $(66 + 16\sqrt{17})/2$.

For the fundamental solutions, according to inequality (8), we get $0 \leq v \leq 10$.

We find the fundamental solutions $[(2Au_i + Bv_i) + v_i\sqrt{D}]/2, i = 1, 2, \dots, 6$, where $v_{1,2} = 2, u_1 = 2, u_2 = -6; v_{3,4} = 4, u_3 = 0, u_4 = -10; v_{5,6} = 7, u_5 = -1, u_6 = -33/2$. According to Theorem 7 the solutions $[(2Au_j + Bv_j) + v_j\sqrt{D}]/2$, where $j = 3$ or 4 , belong to quasi-ambiguous classes.

Example 5. $u^2 + 5uv + 2v^2 = 32 = 2^5, D = 17$.

For the fundamental solutions, according to inequality (8), we get $0 \leq v \leq 10$.

We find the fundamental solutions $[(2Au_i + Bv_i) + v_i\sqrt{D}]/2, i = 1, 2, \dots, 6$, where $v_{1,2} = 2, u_1 = 2, u_2 = -12; v_{3,4} = 4, u_3 = 0, u_4 = -20; v_{5,6} = 7, u_5 = -2, u_6 = -33$. According to Theorem 7 the solution $[(2Au_3 + Bv_3) + v_3\sqrt{D}]/2$, where $u_3 = 0$, belongs to a class which is not quasi-ambiguous.

Example 6. $3u^2 + 14uv + 4v^2 = 259 = 7 \cdot 37, D = 148$.

The fundamental solution of the equation $x^2 - 148y^2 = 4$ is $(146 + 12\sqrt{148})/2$.

For the fundamental solutions, according to inequality (8), we get $0 \leq v \leq 27$.

We find the fundamental solutions $[(2Au_i + Bv_i) + v_i\sqrt{D}]/2, i = 1, 2$, where $v_{1,2} = 4, u_1 = 3, u_2 = -65/3$. According to Theorem 8 the only class of integral solutions is not quasi-ambiguous.

B. STOLT, *On a Diophantine equation of the second degree*

REFERENCES

1. T. NAGELL, En elementær metode til å bestemme gitterpunktene på en hyperbel. Norsk Matem. Tidsskr. 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. ——— Introduction to Number Theory. Uppsala 1951, 204–210.
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 $u^2 - Dv^2 = \pm 4N$. Arkiv för matematik 2 (1951), 1–23.
7. ——— On the Diophantine equation $u^2 - Dv^2 = \pm 4N$, Part II. Arkiv för matematik 2 (1952), 251–268.
8. ——— On the Diophantine equation $u^2 - Dv^2 = \pm 4N$, Part III. Arkiv för matematik 3 (1954), 117–132.

Tryckt den 18 januari 1957

Uppsala 1957. Almqvist & Wiksells Boktryckeri AB