ARKIV FÖR MATEMATIK Band 3 nr 2

Read 14 October 1953

On a special class of Diophantine equations of the second degree

By TRYGVE NAGELL

§ 1. Ambiguous ideals in real quadratic fields and Diophantine equations

Given the square-free integer $D>1$, the determination of the ambiguous ideal classes in the real quadratic field $\boldsymbol{K}(\sqrt{D})$ depends essentially on the following fact:

Theorem 1. *Let ε be the fundamental unit in $\boldsymbol{K}(\sqrt{D})$, and let*

$$\mathfrak{a}_1,\ \mathfrak{a}_2,\ \ldots,\ \mathfrak{a}_s$$

be all possible products of different ambiguous prime ideals in $\boldsymbol{K}(\sqrt{D})$.

If $N(\varepsilon)=-1$, none of the ideals $\mathfrak{a}_i$ is principal, apart from $(\sqrt{D})$.

If $N(\varepsilon)=+1$, exactly two of the ideals $\mathfrak{a}_i$ are principal, apart from $(\sqrt{D})$. The product of these principal ideals is $=(2\sqrt{D})$ when D is odd and the norms of the ideals are even; in all other cases the product is $=(\sqrt{D})$.

See f. ex. HILBERT [1], § 75 and HECKE [2], § 45.[1]

This theorem may also be formulated as follows:

Theorem 2. *Let D be a given square-free integer >1, and let C be any square-free divisor of $2D$, such that $C\neq 1$ and $\neq \pm D$. When $D\equiv 1 \pmod 4$, C shall be odd.*

Part 1. If the Diophantine equation

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

is solvable in integers u and v for $C=-1$, it is not solvable for any other value of C.

If it is not solvable for $C=-1$, it is solvable for exactly two different values of C. The product of these two values of C is $=-4D$ when D is odd and C is even; in all other cases the product is $=-D$.

[1] Figures in [ ] refer to the Bibliography at the end of this paper.

Part 2. Suppose that the Diophantine equation

$$u^2 - D v^2 = 4C \tag{2}$$

is solvable in odd integers u and v for $C = +1$.

If it is solvable for $C = -1$ in odd integers, it is not solvable for any other value of C in odd integers.

If it is not solvable for $C = -1$ in odd integers, it is solvable for exactly two different values of C in odd integers. The product of these two values of C is $= -D$.

A supplement to this result is

Theorem 2 a. *If $u = u_1$ and $v = v_1$ are the least positive solutions of* (1) *in integers, the number*

$$\frac{(u_1 + v_1\sqrt{D})^2}{|C|} = \frac{u_1^2 + D v_1^2}{|C|} + \frac{2 u_1 v_1}{|C|}\sqrt{D} = X_1 + Y_1\sqrt{D} \tag{3}$$

is the fundamental solution of the equation

$$X^2 - D Y^2 = 1. \tag{4}$$

If $u = u_1$ and $v = v_1$ are the least positive solutions of (2) *in odd integers, the number*

$$\frac{(u_1 + v_1\sqrt{D})^2}{4|C|} = \frac{u_1^2 + D v_1^2}{4|C|} + \frac{u_1 v_1}{2|C|}\sqrt{D} = \tfrac{1}{2}(U_1 + V_1\sqrt{D}) \tag{5}$$

is the fundamental solution of the equation

$$U^2 - D V^2 = 4. \tag{6}$$

Remark. When $X = X_1$ and $Y = Y_1$ are the least positive integers satisfying (4) we call the number

$$X_1 + Y_1\sqrt{D}$$

the fundamental solution of (4).

When $U = U_1$ and $V = V_1$ are the least positive integers satisfying (6) we call the number

$$\tfrac{1}{2}(U_1 + V_1\sqrt{D})$$

the fundamental solution of (6).

It is easy to see that Theorems 2 and 2 a may be replaced by the following results:

Theorem 3. *Part 1. Let D be a given square-free integer > 1, and let E be one of the four numbers ± 1 or ± 2. Further, let A and B be variable positive integers, satisfying the following conditions:*

$$AB=D, \tag{7}$$

$$1<A<B \quad \text{for } E=+1, \tag{8}$$

and

$$1\leqq A<B \quad \text{for } E=\pm 2 \text{ or } =-1. \tag{9}$$

When $E=\pm 2$, $AB=D$ *shall be odd.*

Under these conditions exactly one of the Diophantine equations

$$Ax^2-By^2=E \tag{10}$$

is solvable in integers x *and* y.

If $x=\xi$ *and* $y=\eta$ *are the least positive solutions of* (10) *in integers, the number*

$$\frac{1}{|E|}(\xi\sqrt{A}+\eta\sqrt{B})^2=\frac{A\xi^2+B\eta^2}{|E|}+\frac{2\xi\eta}{|E|}\sqrt{D} \tag{11}$$

is the fundamental solution of (4).

Part 2. Let D *be a given square-free integer* >1, *such that equation* (6) *is solvable in odd integers* U *and* V. *Further, let* A *and* B *be variable positive integers, satisfying the following conditions:*

$$AB=D$$

and

$$1\leqq A<B.$$

Under these conditions exactly one of the Diophantine equations

$$Ax^2-By^2=\pm 4 \tag{12}$$

is solvable in odd integers x *and* y, *apart from the equation*

$$x^2-Dy^2=4. \tag{13}$$

If $x=\xi$ *and* $y=\eta$ *are the least positive solutions of* (12) *in odd integers, the number*

$$\tfrac{1}{4}(\xi\sqrt{A}+\eta\sqrt{B})^2=\tfrac{1}{4}(A\xi^2+B\eta^2)+\tfrac{1}{2}\xi\eta\sqrt{D} \tag{14}$$

is the fundamental solution of (13).

Remarks. Denote by τ the number of positive divisors of D. Then the number of pairs A, B satisfying (7) and (8) is $=\frac{1}{2}\tau-1$. The number of pairs A, B satisfying (7) and (9) is $=\frac{3}{2}\tau$ if D is odd and $=\frac{1}{2}\tau$ if D is even. Hence the number of different equations (10) is $2\tau-1$ or $\tau-1$ according as D is odd or even.

It is evident that, in Part 2 of Theorem 3, we must have $D\equiv 5 \pmod 8$. Equation (12) is, however, not solvable in odd integers for all $D\equiv 5 \pmod 8$. For example, when $D=37$, the solutions x and y are all even.

If τ is the number of positive divisors of D, the number of different equations (12) is clearly $=\tau-1$.

The purpose of this paper is to show that Theorem 3 may be proved by means of elementary methods without using ideal theory.

§ 2. Lemmata

We need the following lemmata:

Lemma 1. Let x, y, x_1, y_1, a, b and a_1 be rational numbers $\neq 0$, such that $\sqrt{a}$, $\sqrt{b}$ and $\sqrt{a_1}$ are irrational. Then we can never have a relation of the form

$$x\sqrt{a}+y\sqrt{b}=x_1\sqrt{a_1}+y_1. \tag{15}$$

Lemma 2. Let x, y, x_1, y_1, a, b, a_1 and b_1 be rational numbers $\neq 0$, such that $\sqrt{a}$, $\sqrt{b}$, $\sqrt{a_1}$, $\sqrt{b_1}$, $\sqrt{ab}$ and $\sqrt{a_1 b_1}$ are irrational. Then the relation

$$x\sqrt{a}+y\sqrt{b}=x_1\sqrt{a_1}+y_1\sqrt{b_1} \tag{16}$$

holds only in the following cases: It is either $x\sqrt{a}=x_1\sqrt{a_1}$ or $x\sqrt{a}=y_1\sqrt{b_1}$.

Proof of Lemma 1. Squaring both sides of (15) we get

$$ax^2+by^2+2xy\sqrt{ab}=a_1x_1^2+2x_1y_1\sqrt{a_1}+y_1^2.$$

Hence

$$u\sqrt{ab}-v\sqrt{a_1}=w,$$

where u, v and w are rational numbers, $uv\neq 0$. Squaring once more we get

$$\sqrt{aba_1}=\frac{abu^2+a_1v^2-w^2}{2uv}.$$

Hence $\sqrt{aba_1}$ is rational. Then equation (15) may be written

$$x\sqrt{a}+y\sqrt{b}=z\sqrt{ab}+y_1,$$

where z is rational and $\neq 0$. Thus

$$\sqrt{a}=u_1+v_1\sqrt{b},$$

where u_1 and v_1 are rational, $v_1\neq 0$. Here the square of the right-hand side is rational. Hence $u_1=0$. Thus $\sqrt{ab}$ is rational. Since $\sqrt{aba_1}$ is rational, this implies that $\sqrt{a_1}$ is rational. But by hypothesis $\sqrt{a_1}$ is irrational.

Lemma 1 may be proved somewhat shorter by means of algebraic number theory. In fact, the right-hand side of (15) is an algebraic number of the second degree, while the left-hand is of the fourth degree, except when $\sqrt{ab}$ is rational.

Proof of Lemma 2. Multiplying both sides of (16) by $\sqrt{a}$ we get

$$ax+y\sqrt{ab}=x_1\sqrt{aa_1}+y_1\sqrt{ab_1}.$$

But, by Lemma 1, this relation is possible only when either of the numbers $\sqrt{aa_1}$ or $\sqrt{ab_1}$ is rational. If $\sqrt{aa_1}$ is rational, it follows from (16) that $\sqrt{bb_1}$ is also rational. Hence we must have $x\sqrt{a}=x_1\sqrt{a_1}$ and $y\sqrt{b}=y_1\sqrt{b_1}$. Similarly if $\sqrt{ab_1}$ is rational.

§ 3. Further lemmata

We shall establish the following result:

Lemma 3. Under the conditions of Theorem 3, Part 1, at most one of the Diophantine equations

$$Ax^2-By^2=E \tag{17}$$

is solvable in integers x and y.

Proof. Suppose that A, B, E and A_1, B_1, E_1 are two different triplets of integers satisfying the conditions of Theorem 3, Part 1. Suppose further that the Diophantine equations

$$Ax^2-By^2=E \tag{18}$$

and

$$A_1x^2-B_1y^2=E_1 \tag{19}$$

are both solvable in integers x and y. Let $x=\xi$, $y=\eta$ be the least positive solutions of (18) and let $x=\xi_1$, $y=\eta_1$ be the least positive solutions of (19).

Consider first the case $A_1=1$, $B_1=D$, $E=-1$. Then we get from (18)

$$\frac{1}{|E|}(\xi\sqrt{A}+\eta\sqrt{B})^2=U+V\sqrt{D}$$

and from (19)

$$(\xi_1+\eta_1\sqrt{D})^2=X_1+Y_1\sqrt{D},$$

where U and V are positive integers satisfying the equation

$$U^2-DV^2=1.$$

Thus we have

$$U+V\sqrt{D}=(X_1+Y_1\sqrt{D})^m$$

where m is a positive integer. Hence we get

$$\frac{1}{|E|}(\xi\sqrt{A}+\eta\sqrt{B})^2=(\xi_1+\eta_1\sqrt{D})^{2m}$$

and so

$$\xi\sqrt{\frac{A}{|E|}}+\eta\sqrt{\frac{B}{|E|}}=(\xi_1+\eta_1\sqrt{D})^m. \tag{20}$$

But here the right-hand side is of the form

$$c_m+d_m\sqrt{D},$$

where c_m and d_m are positive integers. The numbers $\sqrt{\frac{A}{|E|}}$, $\sqrt{\frac{B}{|E|}}$ and $\sqrt{D}$ are irrational. Hence, by Lemma 1, the relation (20) is impossible. Thus we conclude: When the equation

$$x^2-Dy^2=-1 \tag{21}$$

is solvable in integers x, y, no other of the equations (17) is solvable.

Suppose next that equation (21) is not solvable. Then we get from (18)

$$\frac{1}{|E|}(\xi\sqrt{A}+\eta\sqrt{B})^2=U+V\sqrt{D}$$

and from (19)

$$\frac{1}{|E_1|}(\xi_1\sqrt{A_1}+\eta_1\sqrt{B_1})^2=U_1+V_1\sqrt{D},$$

where U, V, U_1 and V_1 are positive integers such that

$$U^2-DV^2=1$$

and

$$U_1^2-DV_1^2=1.$$

Thus we have

$$U+V\sqrt{D}=(X_1+Y_1\sqrt{D})^m$$

and

$$U_1+V_1\sqrt{D}=(X_1+Y_1\sqrt{D})^n,$$

where m and n are positive integers. Hence

$$\left[\xi\sqrt{\frac{A}{|E|}}+\eta\sqrt{\frac{B}{|E|}}\right]^n=\left[\xi_1\sqrt{\frac{A_1}{|E_1|}}+\eta_1\sqrt{\frac{B_1}{|E_1|}}\right]^m. \tag{22}$$

If m and n are both even, we can take the square root on both sides. Consequently we may suppose either that both m and n are odd ($\geqq 1$) or that m is odd ($\geqq 1$) and n even ($\geqq 2$).

If m and n are both odd, we obtain from (22) the relation

$$u\sqrt{\frac{A}{|E|}}+v\sqrt{\frac{B}{|E|}}=u_1\sqrt{\frac{A_1}{|E_1|}}+v_1\sqrt{\frac{B_1}{|E_1|}},$$

where u, v, u_1 and v_1 are positive rational numbers. But since the numbers

$$\sqrt{\frac{A}{|E|}},\ \sqrt{\frac{B}{|E|}},\ \sqrt{\frac{A_1}{|E_1|}},\ \sqrt{\frac{B_1}{|E_1|}} \quad \text{and} \quad \sqrt{D}$$

are irrational, it follows, in virtue of Lemma 2, that either

$$\frac{A}{|E|} = \frac{B_1}{|E_1|} \quad \text{and} \quad \frac{B}{|E|} = \frac{A_1}{|E_1|}$$

or

$$\frac{A}{|E|} = \frac{A_1}{|E_1|} \quad \text{and} \quad \frac{B}{|E|} = \frac{B_1}{|E_1|}.$$

In both cases we get, since $AB = A_1B_1 = D$, $|E| = |E_1|$. Then, since $A < B$ and $A_1 < B_1$, we see that the first case is impossible. Hence we must have

$$A = A_1,\ B = B_1,\ E = -E_1.$$

Then, from the equations

$$A\xi^2 - B\eta^2 = E$$

and

$$A\xi_1^2 - B\eta_1^2 = -E$$

we get by multiplication

$$\left[\frac{A\xi\xi_1 + B\eta\eta_1}{E}\right]^2 - D\left[\frac{\xi\eta_1 + \xi_1\eta}{E}\right]^2 = -1,$$

where the numbers $\frac{1}{E}(A\xi\xi_1 + B\eta\eta_1)$ and $\frac{1}{E}(\xi\eta_1 + \xi_1\eta)$ are integers. But this is contrary to our hypothesis that equation (21) is not solvable.

If m is odd and n even, we obtain from (22) the relation

$$u + v\sqrt{D} = u_1\sqrt{\frac{A_1}{|E_1|}} + v_1\sqrt{\frac{B_1}{|E_1|}},$$

where u, v, u_1 and v_1 are positive numbers. But this relation is impossible in virtue of Lemma 1, since the numbers

$$\sqrt{D},\ \sqrt{\frac{A_1}{|E_1|}} \quad \text{and} \quad \sqrt{\frac{B_1}{|E_1|}}$$

are irrational. Thus the proof of Lemma 3 is complete.

In a similiar way we can prove

Lemma 4. Under the conditions of Theorem 3, Part 2, at most one of the Diophantine equations

(23) $$Ax^2 - By^2 = \pm 4$$

is solvable in odd integers x and y, apart from the equation

$$x^2 - Dy^2 = 4. \tag{24}$$

In fact, we have only to replace, in the above proof of Lemma 3, E and E_1 by ± 4 and further $X_1 + Y_1\sqrt{D}$ by the fundamental solution $\frac{1}{2}(x_1 + y_1\sqrt{D})$ of (24).

§ 4. Proof of Theorem 3

Let $X = X_1$ and $Y = Y_1$ be the least positive solutions of equation

$$X^2 - DY^2 = 1 \tag{25}$$

in integers. If X_1 is even, the numbers $X_1 + 1$ and $X_1 - 1$ are coprime and it follows from

$$X_1^2 - 1 = DY_1^2 \tag{26}$$

that

$$X_1 \pm 1 = A\xi^2, \quad X_1 \mp 1 = B\eta^2,$$

where A, B, ξ and η are positive integers, such that $AB = D$ and $\xi\eta = Y_1$. Hence by subtraction

$$A\xi^2 - B\eta^2 = \pm 2. \tag{27}$$

If X_1 is odd, the numbers $\frac{1}{2}(X_1 + 1)$ and $\frac{1}{2}(X_1 - 1)$ are coprime and it follows from (26) that

$$X_1 \pm 1 = 2A\xi^2, \quad X_1 \mp 1 = 2B\eta^2,$$

where A, B, ξ and η are positive integers, such that $AB = D$ and $2\xi\eta = Y_1$. Hence by subtraction

$$A\xi^2 - B\eta^2 = \pm 1. \tag{27'}$$

Thus at least one of the equations (10) in Theorem 3, Part 1, is solvable. In fact, since X_1 and Y_1 are the least positive solutions of equation (4), the equation (27') can neither have the form $\xi^2 - D\eta^2 = +1$ nor the form $D\xi^2 - \eta^2 = -1$.

According to Lemma 3 at most one of the equations (10) is solvable in integers. Thus we have proved the first part of Theorem 3, except the assertion on the number (11). To complete the proof we consider the solvable one among the equations (10), say

$$Ax^2 - By^2 = E.$$

Then this equation has the solution $x = \xi$, $y = \eta$, where ξ and η are the integers uniquely determined in the above part of this proof. ξ and η are connected with the numbers X_1 and Y_1 by the relations

$$X_1 = \frac{A\,\xi^2 + B\eta^2}{|E|} \quad \text{and} \quad Y_1 = \frac{2\,\xi\,\eta}{|E|}.$$

Now let $x = x_1$, $y = y_1$ be any solution of the same equation in positive integers. Then we must have

$$\frac{1}{|E|}(x_1\sqrt{A} + y_1\sqrt{B})^2 = (X_1 + Y_1\sqrt{D})^m = \left[\frac{A\,\xi^2 + B\,\eta^2}{|E|} + \frac{2\,\xi\,\eta}{|E|}\sqrt{D}\right]^m,$$

where m is an odd integer $\geqq 1$. In fact, if m were even and $= 2\,\mu$, we should have

$$x_1\sqrt{\frac{A}{|E|}} + y_1\sqrt{\frac{B}{|E|}} = (X_1 + Y_1\sqrt{D})^\mu = X_2 + Y_2\sqrt{D},$$

where X_2 and Y_2 are positive integers. But, by Lemma 1, this relation is impossible. Hence we get

$$2\,x_1\,y_1\,|\,E\,|^{m-1} = \sum_{k=0}^{\frac{1}{2}(m-1)} \binom{m}{2k+1} (A\,\xi^2 + B\,\eta^2)^{m-2k-1}\,(2\,\xi\,\eta)^{2k+1}$$

and

$$(A\,x_1^2 + B\,y_1^2)\,|\,E\,|^{m-1} = \sum_{k=0}^{\frac{1}{2}(m-1)} \binom{m}{2k} \binom{m}{2k} (A\,\xi^2 + B\,\eta^2)^{m-2k}\ (2\,\xi\,\eta)^{2k}.$$

When $m > 1$, it follows from these relations that

$$x_1\,y_1 = \xi\,\eta\,u \quad \text{and} \quad A\,x_1^2 + B\,y_1^2 = (A\,\xi^2 + B\,\eta^2)\,v,$$

where u and v are integers $\geqq 2$. Hence

$$x_1\,y_1 > \xi\,\eta \quad \text{and} \quad A\,x_1^2 + B\,y_1^2 > A\,\xi^2 + B\,\eta^2,$$

and since

$$A\,x_1^2 - B\,y_1^2 = A\,\xi^2 - B\,\eta^2 = E$$

we get

$$x_1 > \xi \text{ and } y_1 > \eta.$$

Thus we see that the least positive values of x_1 and y_1 are ξ and η respectively.

This proves our assertion on the number (11).

It remains to prove the second part of Theorem 3. Let $x = X_1$ and $y = Y_1$ be the least positive solutions of equation

$$x^2 - D\,y^2 = 4 \tag{28}$$

in odd integers. Since x_1 is odd, the numbers $X_1 + 2$ and $X_1 - 2$ are coprime and it follows from

$$X_1^2 - 4 = D\,Y_1^2 \tag{29}$$

that

$$X_1 \pm 2 = A\,\xi^2,\ X_1 \mp 2 = B\,\eta^2,$$

where A, B, ξ and η are positive integers, such that $AB=D$ and $\xi\eta=Y_1$. Hence by subtraction

$$A\xi^2-B\eta^2=\pm 4. \tag{30}$$

Thus at least one of the equations (12) in Theorem 3, Part 2, is solvable. In fact, since X_1 and Y_1 are the least positive solutions of equation (28), the equation (30) can neither have the form $\xi^2-D\eta^2=+4$ nor the form $D\xi^2-\eta^2=-4$.

According to Lemma 4 at most one of the equations (12) is solvable in odd integers x and y. Thus we have proved the second part of Theorem 3, except the assertion on the number (14). To complete the proof we consider the solvable one among the equations (12), say

$$Ax^2-By^2=\pm 4.$$

The proof proceeds exactly as in the previous case. We have only to replace E by ± 4 and $X_1+Y_1\sqrt{D}$ by $\frac{1}{2}(X_1+Y_1\sqrt{D})$.

Thus the proof of Theorem 3 is complete.

Remark. LEGENDRE found the following result: Given a positive integer D not square, it is always possible to decompose it into two factors A and B, such that at least one of the equations $Ax^2-By^2=\pm 1$ and $Ax^2-By^2=\pm 2$ is solvable in integers x and y when the signs are suitably chosen; see [3], p. 64–71.

§ 5. Proof of Theorem 2

Consider the equations

$$u^2-Dv^2=C, \tag{31}$$

where the numbers C and D satisfy the conditions in Theorem 2, Part 1. If $\frac{D}{|C|}=B$ is an integer, we put $A=|C|$. Then the number u in (31) is divisible by A. Putting $u=Au_1$ we get

$$Au_1^2-Bv^2=\pm 1. \tag{32}$$

If $\frac{D}{|C|}=\frac{1}{2}B$ is not an integer, B is an integer and so is $A=\frac{1}{2}|C|$. Then the number u in (31) is divisible by A, and putting $u=Au_1$ we get

$$Au_1^2-Bv^2=\pm 2. \tag{32'}$$

Hence, applying Theorem 3 to equations (32) and (32') we obtain Theorem 2, Part 1.

To prove Part 2 of Theorem 2 we consider the equations

$$u^2 - D v^2 = 4 C, \tag{33}$$

where the numbers C and D satisfy the conditions in Theorem 3, Part 2. The solutions u and v shall be odd integers. C cannot be even. Hence $\frac{D}{|C|} = B$ is an integer. If we put $A = |C|$, the number u in (33) is divisible by A. Putting $u = A u_1$ we get

$$A u_1^2 - B v^2 = \pm 4. \tag{34}$$

Thus applying Theorem 3 we obtain Theorem 2, Part 2.

To prove Theorem 2 a we have only to apply the results on the numbers (11) and (14) in Theorem 3.

§ 6. Numerical examples

We shall illustrate Theorem 3 by some numerical examples.

1. Consider first the case $D = 3 \cdot 5 \cdot 7 = 105$. The equations satisfying the conditions in Theorem 3, Part 1, are the following:

$$x^2 - 105 y^2 = -1, \tag{35}$$

$$x^2 - 105 y^2 = \pm 2, \tag{36}$$

$$3 x^2 - 35 y^2 = \pm 1, \tag{37}$$

$$3 x^2 - 35 y^2 = \pm 2, \tag{38}$$

$$5 x^2 - 21 y^2 = +1, \tag{39}$$

$$5 x^2 - 21 y^2 = -1, \tag{40}$$

$$5 x^2 - 21 y^2 = \pm 2, \tag{41}$$

$$7 x^2 - 15 y^2 = \pm 1, \tag{42}$$

$$7 x^2 - 15 y^2 = \pm 2. \tag{43}$$

Only equation (40) is solvable; its least positive solution is $x = 2$, $y = 1$. By Theorem 3 none of the other equations is solvable. Equation (35) is impossible when taken as a congruence modulo 3. Equations (36), (38), (41) and (43) are impossible modulo 8. Equations (37) and (42) are impossible modulo 5. Equation (39) is impossible modulo 7.

We see that, in this example, it is possible to determine the insolvable equations by considering the corresponding congruences for suitable moduli. This is, however, not always the case, as will be obvious from the following example.

2. Consider next the example $D = 2 \cdot 3 \cdot 73 = 438$. The equations satisfying the conditions in Theorem 3, Part 1, are the following:

$$x^2 - 438\,y^2 = -1, \tag{44}$$

$$2x^2 - 219\,y^2 = +1, \tag{45}$$

$$2x^2 - 219\,y^2 = -1, \tag{46}$$

$$3x^2 - 146\,y^2 = +1, \tag{47}$$

$$3x^2 - 146\,y^2 = -1, \tag{48}$$

$$6x^2 - 73\,y^2 = +1, \tag{49}$$

$$6x^2 - 73\,y^2 = -1. \tag{50}$$

Only equation (47) is solvable, its least positive solution is $x=7$, $y=1$. By Theorem 3 none of the other equations is solvable. Equations (44) (45), (48) and (49) are impossible modulo 8. Equations (46) and (50) are possible as congruences for an arbitrary modulus, as may easily be verified.

3. Let us take the example $D=21$. In this case the equation

$$x^2 - 21\,y^2 = 4 \tag{51}$$

has the solution $x=5$, $y=1$. The equations satisfying the conditions in Theorem 3, Part 2, are the following:

$$x^2 - 21\,y^2 = -4, \tag{52}$$

$$3x^2 - 7\,y^2 = +4, \tag{53}$$

$$3x^2 - 7\,y^2 = -4. \tag{54}$$

Equations (52) and (53) are impossible modulo 3. Equation (54) has the solution $x=y=1$. The relation

$$\tfrac{1}{4}(\sqrt{3}+\sqrt{7})^2 = \tfrac{1}{2}(5+\sqrt{21})$$

gives the fundamental solution of (51).

4. When we take $D=5\cdot 41=205$, the equation

$$x^2 - 205\,y^2 = 4 \tag{55}$$

has the solution $x=43$, $y=3$. The equations satisfying the conditions in Theorem 3, Part 2, are the following:

$$x^2 - 205\,y^2 = -4, \tag{56}$$

$$5x^2 - 41\,y^2 = +4, \tag{57}$$

$$5x^2 - 41\,y^2 = -4. \tag{58}$$

Here equation (57) has the solution $x=3$, $y=1$. Thus equations (56) and (58) are insolvable in odd integers. The relation

$$\tfrac{1}{4}(3\sqrt{5}+\sqrt{41})^2=\tfrac{1}{2}(43+3\sqrt{205})$$

gives the fundamental solution of (55).

§ 7. The solvable equations and their solutions

It is obvious from the concluding proof of Theorem 3, Part 1, in § 4, how the solvable one among equations (10) may be determined when the fundamental solution $X=X_1$, $Y=Y_1$ of equation (25) is known. At the same time we find the least positive solutions $x=\xi$ and $y=\eta$ of that equation.

But even if X_1 and Y_1 are not known, we may obtain the same result by trial. In fact, when D is given, we may proceed in the following manner. We write down all the equations

$$Ax^2-By^2=E$$

satisfying the conditions in Theorem 3, Part 1. In every one of these equations we put successively $x=1$, 2, 3, 4 etc. and $y=1$, 2, 3, 4 etc., until one of them is satisfied.

Similarly we may determine the solvable one among equations (12) when the fundamental solution $\frac{1}{2}(X_1+Y_1\sqrt{D})$ of equation (28) is known. At the same time we get the least positive solution of that equation.

In this way we also obtain the two solvable equations among equations (1) in Theorem 2, Part 1, together with the corresponding least positive solutions, and similarly for equations (2) in Theorem 2, Part 2.

By means of the following result we may determine the whole set of solutions of these equations:

Theorem 4. *If D is a positive integer which is not a perfect square, and if C is a square-free integer which divides $2D$, the Diophantine equation*

$$u^2-Dv^2=C \tag{59}$$

has at most one class of solutions. If this class exists, it is ambiguous.

Remark. This result is contained in a more general result of STOLT; see [4], Theorem 8. For the definition of "class of solutions" see NAGELL [5], [6] and [7], section 58.

Proof. Let $u+v\sqrt{D}$ and $u'+v'\sqrt{D}$ be two different solutions of (59). Then the necessary and sufficient condition for these two solutions to be associated with each other is that the two numbers

$$\frac{uu'-vv'D}{C} \text{ and } \frac{vu'-uv'}{C} \tag{60}$$

be integers. If C is odd, it follows from (59) that the numbers u and u' must be divisible by C. This is also the case when C and D are both even. Hence the numbers (60) are integers in these cases. Suppose finally that C is even and D odd. Then the numbers u, u', v and v' are all odd; by (59) u and u' are divisible by $\frac{1}{2}C$. Hence the numbers $uu'-vv'D$ and $vu'-uv'$ are both even and divisible by C. Consequently, all the solutions of (59) belong to the same class. This class must be ambiguous. Hence all the solutions of (59) are given by the formula

$$u+v\sqrt{D}=\pm(u_1+v_1\sqrt{D})\,(X_1+Y_1\sqrt{D})^m,$$

where $u=u_1$ and $v=v_1$ are the least positive solutions of (59), where $X_1+Y_1\sqrt{D}$ is the fundamental solution of (25) and where m is an arbitrary integer.

Remark. A result equivalent to Theorem 4 was found by SCHEPEL, see [9]; in his paper SCHEPEL also gives a proof of the first part of Theorem 2 a.

§ 8. Analogous results on equations of higher degree

In a previous paper I have established a result on cubic equations which is analogous to our Theorem 3 on quadratic equations; see NAGELL [8].

The Diophantine equation of the form

$$Ax^3+By^3=C, \tag{61}$$

where A, B and C are integers $\neq 0$, such that $\sqrt[3]{\frac{A}{B}}$ is irrational, is said to belong to the class of the (real) cubic field

$$\boldsymbol{K}\left(\sqrt[3]{\frac{A}{B}}\right).$$

There are always several equations belonging to the same class for a given C. For instance, if we replace A by A^2 and B by B^2, or A by 1 and B by A^2B, we get equations belonging to the same class as (61).

Theorem 5. *Consider all the Diophantine equations* (61), *where the coefficients A, B and C satisfy the following conditions: C is one of the numbers* 1 *or* 3; *A and B are coprime integers, such that $1\leqq A<B$; AB is not divisible by* 3 *when $C=3$; AB is not divisible by the cube of any prime.*

Among all the equations belonging to the same class there is at most one equation which is solvable in integers x and y, with $xy\neq 0$, except in the following cases.

In the class of the field $\boldsymbol{K}(\sqrt[3]{2})$ the existing equations are:

$$x^3+2y^3=1,\ x^3+2y^3=3,\ x^3+4y^3=3,\ x^3+4y^3=1.$$

The first three equations are solvable; the last one is not solvable for $y\neq 0$.

In the class of the field $\boldsymbol{K}(\sqrt[3]{20})$ *the existing equations are:*

$$x^3+20y^3=1,\ 2x^3+5y^3=3,\ x^3+20y^3=3,\ 2x^3+5y^3=1,$$

$$x^3+50y^3=1,\ 4x^3+25y^3=1,\ x^3+50y^3=3,\ 4x^3+25y^3=3.$$

Only the first two equations are solvable; the others are not solvable for $y\neq 0$.

In a following paper I shall establish analogous results on Diophantine equations of the type

$$Ax^3+By^3+Cz^3-3\sqrt[3]{ABC}\,xyz=E,$$

where E is $=1$ or $=3$, and where A, B and C are positive integers satisfying the following conditions: The number $\sqrt[3]{ABC}$ is rational. Every one of the numbers

$$\sqrt[3]{\frac{A}{B}},\ \sqrt[3]{\frac{A}{C}},\ \sqrt[3]{\frac{B}{C}}$$

generates the same (real) cubic field.

BIBLIOGRAPHY

[1]. D. HILBERT, Die Theorie der algebraischen Zahlkörper, Jahresbericht d. Deutschen Math. Ver. 1894–95, Bd. IV.

[2]. E. HECKE, Theorie der algebraischen Zahlen, Leipzig 1923.

[3]. A. M. LEGENDRE, Théorie des nombres, Paris 1830.

[4]. B. STOLT, On the Diophantine equation $u^2-Dv^2=\pm 4N$, Part I, Arkiv f. Matematik, Bd. 2, nr. 1, Stockholm 1951.

[5]. T. NAGELL, Über die Darstellung ganzer Zahlen durch eine indefinite binäre quadratische Form, Archiv d. Mathematik, Bd. 2 (1950).

[6]. ——, Bemerkung über die diophantische Gleichung $u^2-Dv^2=C$, Archiv d. Mathematik, Bd. 3 (1951).

[7]. ——, Introduction to Number Theory, New York & Stockholm 1951, p. 204–208.

[8]. ——, Solution complète de quelques équations cubiques à deux indéterminées, Journal de Mathématiques, 9^e sér., tome 4, Paris 1925, p. 209.

[9]. D. SCHEPEL, Over de Vergelijking van Pell, Nieuw Archief voor Wiskunde, Amsterdam 1935.

Tryckt den 16 januari 1954

Uppsala 1954. Almqvist & Wiksells Boktryckeri AB