Communicated 10 September 1952 by F. CARLSON and T. NAGELL

On a class of Diophantine equations of the second degree in imaginary quadratic fields

By LARS FJELLSTEDT

Introduction

The problem of solving the Diophantine equation

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

where D and N are rational integers and where D is not a perfect square, in rational integers has usually been treated by using either the theory of quadratic forms or the theory of quadratic fields. T. NAGELL [1], [2], [3], [4][1] has shown, however, how it is possible to determine all the solutions of (1) completely elementarily and without using either of the theories mentioned above.

The purpose of this paper is to show that NAGELL's method can also be used to determine the solutions in integers belonging to an imaginary quadratic number field, of equation (1), when D and N are integers in the field considered, and D is not a perfect square in that field.

I treat in § 1—§ 3 the equation

$$x^2 - \delta y^2 = \pm 1, \tag{2}$$

and in § 5 of this paper I will show how the theory developed here can be used for studying equation (1).

In § 4 we make a closer investigation of a special case of (2) and connect the equation with the units in certain quartic fields.

§ 1. A lemma and its application

The theory of the Diophantine equation $x^2 - \delta y^2 = 1$, can easily be developed starting from the following

Lemma 1: *Let α be any complex number which does not belong to the field $K(\sqrt{-m})$, where m is a squarefree natural number and where $\sqrt{-m}$ is taken to be $i\sqrt{m}$. Then the Diophantine inequality*

$$|x - \alpha y|^2 < \frac{(m+1)^2}{N(y)}, \tag{3}$$

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

where $N(y)$ denotes the norm in the field $\boldsymbol{K}(\sqrt{-m})$ with respect to the rational number field, has an infinitude of solutions in integers x and y belonging to the field $\boldsymbol{K}(\sqrt{-m})$.

In the Gaussian number field this Lemma has been proved by DIRICHLET [5].

Remark: Observe that if inequality (3) is satisfied by the system (x, y) it is also satisfied by the system $(\zeta x, \zeta y)$, where ζ denotes an arbitrary root of unity belonging to the field $\boldsymbol{K}(\sqrt{-m})$. In the following it will appear convenient not to regard any two such systems as being essentially different and for that reason we will agree to regard two systems (x, y) and (x', y') as different if and only if $|x-\alpha y| \neq |x'-\alpha y'|$, for it is obvious that the systems (x, y) and $(\zeta x, \zeta y)$ satisfy the equation

$$|x-\alpha y| = |\zeta x - \alpha \zeta y|.$$

Furthermore we exclude the case $x=0$, so that in the following lines $x-\alpha y$ is always an irrational number and consequently $\neq 0$.

Proof: We consider first the case $m \equiv 1, 2 \pmod{4}$. Let n be a natural number and let A satisfy the inequality $A > \frac{m+1}{4n^2}$. Furthermore let η be an integer in the field $\boldsymbol{K}(\sqrt{-m})$, for which the real part and the coefficient of $\sqrt{-m}$ is contained among the numbers

$$-n, -(n-1), -\cdots, -1, 0, +1, +\cdots, +(n-1), +n.$$

To each of the integers η, the number of which is $(2n+1)^2$, we determine such an integer ξ in $\boldsymbol{K}(\sqrt{-m})$ that in the number $\xi-\alpha\eta$ the real part and the coefficient of $\sqrt{-m}$ are positive and less than one. It is evident then that if $p\frac{1}{2n}$ and $q\frac{1}{2n}$ are the greatest multiples of $\frac{1}{2n}$ which are contained in the real part of $\xi-\alpha\eta$ and the coefficient of $\sqrt{-m}$ in the number $\xi-\alpha\eta$ respectively, the integers p and q are contained in the sequence

$$0, 1, 2, 3, \cdots, 2n-1.$$

The number of possible combinations of the integers p and q is $4n^2$, whereas the number of possibilities for the expression $\xi-\alpha\eta$ is $(2n+1)^2$ and consequently at least one of the combinations (p, q) has to appear twice. Let

$$\xi-\alpha\eta \quad \text{and} \quad \xi'-\alpha\eta'$$

be two expressions for which this is the case. If we put

$$\xi-\xi' = x \quad \text{and} \quad \eta-\eta' = y$$

we get a new expression $x-\alpha y$ in which y is obviously $\neq 0$, and in which the real part as well as the coefficient of $\sqrt{-m}$ are less than $\frac{1}{2n}$ as to their absolute values, and therefore it follows

$$|x-\alpha y|^2 < \frac{m+1}{4n^2} \tag{4}$$

and consequently $|x-\alpha y|^2 < A$.

If we now observe that in $y=\eta-\eta'$ the real part and the coefficient of $\sqrt{-m}$ are certainly both $\leqq 2n$ as to their absolute values, the inequality $N(y) < 4n^2(m+1)$ follows at once. This inequality combined with the inequality (4) immediately gives

$$|x-\alpha y|^2 < \frac{(m+1)^2}{N(y)}.$$

It remains now to consider the case $m \equiv 3 \pmod{4}$. The integers in $\boldsymbol{K}(\sqrt{-m})$ are here of the form $\frac{1}{2}(x+y\sqrt{-m})$, $x \equiv y \pmod{2}$. Let A obey the inequality $A > \frac{m+1}{4n^2}$, and let $\eta = \frac{1}{2}(a+b\sqrt{-m})$ be such an integer in $\boldsymbol{K}(\sqrt{-m})$ that a and b are contained among the numbers

$$-n,\ -(n-1),\ -\ \ldots,\ -1,\ 0,\ +1,\ +\ \ldots,\ +(n-1),\ +n.$$

To each of the integers η, the number of which is obviously $2n^2+2n+1$, we determine such a corresponding integer ξ in $\boldsymbol{K}(\sqrt{-m})$ that in the number $\xi-\alpha\eta$ the real part and the coefficient of $\sqrt{-m}$ are positive and less than $\frac{1}{2}$. It is then evident that if $p\frac{1}{2n}$ and $q\frac{1}{2n}$ are the greatest multiples of $\frac{1}{2n}$ which are contained in the real part of $\xi-\alpha\eta$ and the coefficient of $\sqrt{-m}$ in the number $\xi-\alpha\eta$, respectively, the integers p and q are contained in the sequence

$$0,\ 1,\ 2,\ 3,\ \ldots,\ n-1.$$

The number of possible combinations of the integers p and q is n^2, so that at least one of the combinations (p, q) has to appear twice. Let

$$\xi-\alpha\eta \quad \text{and} \quad \xi'-\alpha\eta'$$

be two expressions for which this is the case. If we put

$$\xi-\xi'=x \text{ and } \eta-\eta'=y$$

we get a new expression $x-\alpha y$ where y is $\neq 0$, and in which the real part as well as the coefficient of $\sqrt{-m}$ are less than $\frac{1}{2n}$ as to their absolute values, so that inequality (4) is still valid, and consequently $|x-\alpha y|^2 < A$.

If we now observe that in $y=\eta-\eta'$ the real part and the coefficient of $\sqrt{-m}$ are certainly both $\leqq n$, as to their absolute values, the inequality $N(y) < n^2(m+1)$ follows at once. On combining this inequality with (4) we get

$$|x-\alpha y|^2 < \frac{(m+1)^2}{4N(y)}$$

a result that is somewhat sharper than (3).

When we have now shown how it is possible to determine such pairs of integers x and y in $\boldsymbol{K}(\sqrt{-m})$ which obey (3) as well as (4), and this for A as small as we please, it is easy to prove that the inequality (3) has an infinitude of solutions. To that effect we consider a set of solutions of (3). Starting from this set we find a new set containing solutions different from the previous ones if we choose A to be the least of all the numbers $|x-\alpha y|^2$ belonging to the first set and, starting from this value of A, repeat the argument which has been described above.

In employing the results of Lemma 1 we are now able to prove

Lemma 2: *The Diophantine inequality*

$$(5) \qquad |x^2-\delta y^2| < (m+1)(m+1+2|\sqrt{\delta}|)$$

where δ is an integer in the field $\boldsymbol{K}(\sqrt{-m})$ which is not a perfect square, has an infinitude of solutions in integers x and y belonging to $\boldsymbol{K}(\sqrt{-m})$.

Proof. According to Lemma 1 the inequality $|x-\alpha y|^2 < \frac{(m+1)^2}{N(y)}$ has an infinity of solutions in integers x and y belonging to $\boldsymbol{K}(\sqrt{-m})$ and furthermore we have

$$|x+\alpha y| \leqq |x-\alpha y| + |2\alpha y|.$$

This gives us

$$|x+\alpha y| < (m+1)\frac{1}{|y|} + |2\alpha y|$$

and on multiplying with the inequality for $|x-\alpha y|$ we find

$$|x^2-\alpha^2 y^2| < \frac{(m-1)^2}{N(y)} + 2(m+1)|\alpha|.$$

Since y is an integer in $\boldsymbol{K}(\sqrt{-m})$ and consequently $N(y) \geqq 1$ this can be written

$$|x^2-\alpha^2 y^2| < (m+1)(m+1+2|\alpha|).$$

If we put $\alpha=\sqrt{\delta}$ here, where δ is an integer in $\boldsymbol{K}(\sqrt{-m})$ which is not a perfect square, our conditions in Lemma 1 are obviously fulfilled, and Lemma 2 is proved.

After these preliminaries we are now in a position to prove

Theorem 1: *If δ is an integer in $\boldsymbol{K}(\sqrt{-m})$ which is not a perfect square there exists at least one pair of integers x and y in $\boldsymbol{K}(\sqrt{-m})$, $y \neq 0$, which satisfy the Diophantine equation*

$$(6) \qquad x^2-\delta y^2=1.$$

Proof. According to Lemma 2 the inequality (5) has an infinitude of solutions in integers x and y belonging to $\boldsymbol{K}(\sqrt{-m})$, and since, furthermore, $N(x^2-\delta y^2)$ is a natural number which is less than $(m+1)^2(m+1+2|\sqrt{\delta}|)^2$, there exists at least one integer λ in $\boldsymbol{K}(\sqrt{-m})$ such that $x^2-\delta y^2=\lambda$ for infinitely many integers x and y in $\boldsymbol{K}(\sqrt{-m})$. Among these infinitely many pairs there must be at least two, (x_1, y_1) and (x_2, y_2) which satisfy the congruences

$$x_1 \equiv x_2 \,(\text{mod. } \lambda),\ y_1 \equiv y_2 \ (\text{mod. } \lambda). \tag{7}$$

This depends on the fact that the remainders of the four integers x_1, x_2, y_1 and y_2 can only be combined in a finite number $(=N(\lambda)^4)$ of ways, and consequently we may assume

$$x_1^2-\delta y_1^2=x_2^2-\delta y_2^2=\lambda \tag{8}$$

where x_1, y_1, x_2 and y_2 satisfy the congruence conditions (7). We form the expression

$$(x_1-y_1\sqrt{\delta})\ (x_2+y_2\sqrt{\delta}) = x_1x_2-\delta y_1y_2+(x_1y_2-x_2y_1)\sqrt{\delta}.$$

From (7) and (8) it follows

$$x_1x_2-\delta y_1y_2 \equiv x_1^2-\delta y_1^2 \equiv 0 \ (\text{mod. } \lambda)$$

and

$$x_1y_2-x_2y_1 \equiv x_1y_1-x_1y_1 \equiv 0 \ (\text{mod. } \lambda)$$

and therefore

$$x_1x_2-\delta y_1y_2=\lambda u$$

and

$$x_1y_2-x_2y_1=\lambda v,$$

where u and v are integers in $\boldsymbol{K}(\sqrt{-m})$. It now follows

$$(x_1-y_1\sqrt{\delta})\ (x_2+y_2\sqrt{\delta})=\lambda\ (u+v\sqrt{\delta})$$

and

$$(x_1+y_1\sqrt{\delta})\ (x_2-y_2\sqrt{\delta})=\lambda\ (u-v\sqrt{\delta}).$$

On multiplying together member by member we have

$$(x_1^2-\delta y_1^2)\,(x_2^2-\delta y_2^2)=\lambda^2=\lambda^2\,(u^2-\delta v^2)$$

and we finally get

$$u^2-\delta v^2=1.$$

In this equation we have $v \neq 0$, because if we had $v=0$ we would get $x_1y_2=x_2y_1$ and $u=\pm 1$ and from this it would follow

$$(x_1-y_1\sqrt{\delta})\ (x_2+y_2\sqrt{\delta})\ (x_2-y_2\sqrt{\delta})=\pm\lambda\ (x_2-y_2\sqrt{\delta})$$

or when we divide by λ

$$x_1-y_1\sqrt{\delta}=\pm(x_2-y_2\sqrt{\delta})$$

which implies $x_1 = \pm x_2$ and $y_1 = \pm y_2$. According to our agreement in Lemma 1 this would mean that the systems (x_1, y_1) and (x_2, y_2) were not different. But we can choose $|x_1| \neq |x_2|$. Thus Theorem 1 is proved.

Remark 1. It is an incompleteness in the theory of equation (6) just developed, that from the reasoning which led to Theorem 1 we did not obtain an upper bound for the solution. It is easy, however, to modify the proof of the theorem in such a way that an upper limit may be determined.

We content ourselves with the case $m \equiv 1,\ 2 \pmod{4}$. Adopting the notations of Lemma 1 we consider the integers $x + y\sqrt{\delta}$ which obey inequality (4). Assuming $x_n + y_n\sqrt{\delta}$ to be one of these where n has the same meaning as in Lemma 1, we have assuming $n > \frac{1}{2}\sqrt{m+1}$

$$|x_n^2 - \delta y_n^2| = |x_n + y_n\sqrt{\delta}|\,|x_n + y_n\sqrt{\delta} - 2y_n\sqrt{\delta}| <$$

$$< \frac{m+1}{4n^2} + \frac{\sqrt{m+1}}{2n}\cdot 2n\sqrt{m+1}\,|\sqrt{\delta}| < 1 + (m+1)\,|\sqrt{\delta}|.$$

Given n_1 we determine n_2 so that

$$n_2\sqrt{m+1} \geqq |y_{n_2}| > n_1\sqrt{m+1} \geqq |y_{n_1}|.$$

Now

$$|x_{n_1} + y_{n_1}\sqrt{\delta}| = \frac{|x_{n_1}^2 - \delta y_{n_1}^2|}{|x_{n_1} + y_{n_1}\sqrt{\delta} - 2y_{n_1}\sqrt{\delta}|} > \frac{1}{1 + 2n_1\sqrt{m+1}\,|\sqrt{\delta}|}.$$

In order that

$$|x_{n_2} + y_{n_2}\sqrt{\delta}| < \frac{\sqrt{m+1}}{2n_2} < \frac{1}{1 + 2n_1\sqrt{m+1}\,|\sqrt{\delta}|}$$

it is obviously sufficient that

$$\frac{\sqrt{m+1}}{2n_2} < \frac{1}{1 + 2n_1\sqrt{m+1}\,|\sqrt{\delta}|}$$

or

$$n_2 > n_1[1 + (m+1)\,|\sqrt{\delta}|\,].$$

Generally we put

$$n_t = [1 + (m+1)\,|\sqrt{\delta}|\,]^t = \varphi^t$$

and consequently we have

$$|y_{n_{t+1}}| > |y_{n_t}|.$$

Putting $R = 4\varphi^6$, $\varphi^4 + 1$ at least among the R different integers

$$y_{n_1},\ y_{n_2},\ \ldots,\ y_{n_R}$$

give the same value for

$$x_{n_t}^2 - \delta y_{n_t}^2 = k_{n_t}.$$

Suppose that only φ^4 of the integers y_i, $(i = n_1, n_2, \ldots, n_R)$ gave the same value for k_{n_t}. The number of possibilities for k_{n_t} is $< 4\varphi^2$. Thus the total number of possibilities is $< 4\varphi^6 \leqq R - 1$.

Among the $\varphi^4 + 1$ different pairs of integers (x_n, y_n) such that

$$x_n^2 - \delta y_n^2 = k,$$

there are at least two pairs (x_i, y_i) and (x_r, y_r) which satisfy the congruence conditions

$$x_i \equiv x_r \text{ (mod. } k), \; y_i \equiv y_r \text{ (mod. } k).$$

We can now proceed as in the proof of Theorem 1. With

$$(x_i - y_i\sqrt{\delta})\,(x_r + y_r\sqrt{\delta}) = k\,(u + v\sqrt{\delta})$$

$$(x_i + y_i\sqrt{\delta})\,(x_r - y_r\sqrt{\delta}) = k\,(u - v\sqrt{\delta})$$

we have

$$u^2 - \delta v^2 = 1.$$

Putting

$$x_i = (x_i + y_i\sqrt{\delta}) - y_i\sqrt{\delta} = \varepsilon_i - y_i\sqrt{\delta}$$

$$x_r = (x_r + y_r\sqrt{\delta}) - y_r\sqrt{\delta} = \varepsilon_r - y_r\sqrt{\delta}$$

we find

$$k u = (\varepsilon_i - y_i\sqrt{\delta})\,(\varepsilon_r - y_r\sqrt{\delta}) - \delta y_i y_r = \varepsilon_i \varepsilon_r - \varepsilon_i y_r\sqrt{\delta} - \varepsilon_r y_i\sqrt{\delta}.$$

and

$$|u| < 1 + |\sqrt{\delta}|\,[\,|y_i| + |y_r|\,] \leqq 1 + 2\sqrt{m+1}\,|\sqrt{\delta}|\,n_R =$$

$$= 1 + 2\sqrt{m+1}\,|\sqrt{\delta}|\,(1 + (m+1)\,|\sqrt{\delta}|\,)^{4\,[1+(m+1)\,|\sqrt{\delta}|]^6}.$$

Further we have

$$k v = (\varepsilon_i - y_i\sqrt{\delta})\,y_r - (\varepsilon_r - y_r\sqrt{\delta})\,y_i = \varepsilon_i y_r - \varepsilon_r y_i.$$

$$|v| \leqq |y_r| + |y_i| \leqq 2\,n_R = 2\,(1 + (m+1)\,|\sqrt{\delta}|\,)^{4\,[1+(m+1)\,|\sqrt{\delta}|]^6}.$$

Thus we have found an upper limit for the integers u and v which satisfy the equation (6). Obviously we have not tried here to find a best upper limit, but merely shown the possibility of determining such a limit with aid of the DIRICHLET principle. REMAK [6] has given a similar limit for the fundamental solution of the ordinary Pell equation.

Remark 2. Theorem 1 states obviously that as soon as $N(\delta) > 1$, equation (6) has at least one solution $x + y\sqrt{\delta}$ in which x and y are both different from zero (about the definition of the concept of solution see § 2). When $N(\delta) = 1$, we may have, as will be shown in § 2, improper solutions $x + y\sqrt{\delta}$ of (6) where

$x=0$. In this case Theorem 1 gives no information about the existence of proper solutions of (6).

We shall now make a complementary investigation and show that the equation (6) always has at least one proper solution. For this purpose we have to study the following equations:

a) $x^2+y^2=1$. We leave the field $\boldsymbol{K}(i)$ out of consideration since -1 is a perfect square in that case. The equation a) has always a proper solution in $\boldsymbol{K}(\sqrt{-m})$, $m>1$, of the form $u+v\sqrt{-m}\sqrt{-1}$, where u and v are natural numbers, which satisfy the equation $u^2-mv^2=1$. It is wellknown that this equation has proper solutions.

b) $x^2+\varrho y^2=1$, where $\varrho=\frac{1}{2}(-1+\sqrt{-3})$. This equation has for instance the solution $2+\frac{1}{2}(3+\sqrt{-3})\sqrt{-\varrho}$.

c) $x^2+\varrho^2 y^2=1$, where $\varrho^2=\frac{1}{2}(-1-\sqrt{-3})$. This equation has for example the solution $2+\frac{1}{2}(-3+\sqrt{-3})\sqrt{-\varrho^2}$.

We treat here for later purposes also the equation

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

although δ is a perfect square in this case. If $m\equiv 1$, 2 (mod. 4) we put $x=a+b\sqrt{-m}$ and $y=c+d\sqrt{-m}$, where a, b, c and d are rational integers. This gives us

$$a^2-mb^2-(c^2-md^2)=1$$

$$ab=cd$$

or if we eliminate a^2 between these two equations

$$(d^2-b^2)(c^2+mb^2)=b^2,$$

which is obviously impossible if $b\neq 0$. If we assume $b=0$, we must also have $c=0$ and we get $a^2+md^2=1$ which has only the following solutions: $a=\pm 1$, $d=0$.

If $m\equiv 3$ (mod. 4) we put $x=\frac{1}{2}(a+b\sqrt{-m})$ and $y=\frac{1}{2}(c+d\sqrt{-m})$ and find analogously the equation

$$(d^2-b^2)(c^2+mb^2)=4b^2.$$

Here we cannot have $d^2-b^2>1$ because $m\geqq 3$. From $d^2-b^2=1$ it follows $b=c=0$, and we get the equation $a^2+md^2=4$. In this equation we must have $a\equiv d\equiv 0$ (mod. 2) since we have assumed x and y to be integers in $\boldsymbol{K}(\sqrt{-m})$. If we put $a=2a_1$ and $d=2d_1$, we get $a_1^2+md_1^2=1$, so that we must have $d_1=0$ and $a_1=\pm 1$. Thus our result is that the equation $x^2-y^2=1$ only has improper solutions in $\boldsymbol{K}(\sqrt{-m})$.

§ 2. The Diophantine equation $x^2 - \delta y^2 = 1$

In paragraph 1 we showed that the Diophantine equation (6) is always solvable in integers x and y of the field $K(\sqrt{-m})$. If equation (6) is satisfied by the integers x and y we say that the number $x + y\sqrt{\delta}$ is a *solution* of the equation. To get the value of $\sqrt{\delta}$ uniquely determined we prescribe the imaginary part of $\sqrt{\delta}$ to be positive. Solutions $x + y\sqrt{\delta}$ of (6) in which either x or y is zero are called *improper*. When we speak of solutions in the following lines we shall always mean *proper* solutions, i. e. solutions in which both x and y are different from zero.

In this paragraph we shall study a little closer the properties of the solutions and begin with a few remarks.

The only improper solutions of (6) are the following

1) $x = \pm 1$, $y = 0$.

2) $x = 0$, $x = \pm \varrho$ for $\delta = -\varrho$ where $\varrho = \frac{1}{2}(-1 + \sqrt{-3})$.

3) $x = 0$, $y = \pm \varrho^2$ for $\delta = -\varrho^2$, where $\varrho^2 = -\frac{1}{2}(1 + \sqrt{-3})$.

4) $x = 0$, $y = \pm 1$, for $\delta = -1$ and $K(\sqrt{-m}) \neq K(i)$.

The improper solutions enumerated above obviously satisfy the equation

$$|x + y\sqrt{\delta}| = 1, \tag{9}$$

and we further assert that there are no proper solutions of (6) satisfying (9).

Our assertion is obviously equivalent to the following proposition: The equation

$$|x + y\sqrt{\delta}|^2 + |x - y\sqrt{\delta}|^2 = 2, \tag{10}$$

has only the solutions enumerated above.

If we observe that for any two complex numbers r and s we have the identity

$$|r + s|^2 + |r - s|^2 = 2(|r|^2 + |s|^2)$$

equation (10) may be written

$$|x|^2 + |y|^2 |\delta| = 1.$$

Since the absolute values of x, y and δ are $\geqq 1$ if they are different from zero it follows that we can have no proper solution of (6) satisfying (9). Thus we have only the following possibilities: $x = \pm 1$, $y = 0$ or if $N(\delta) = 1$

a) $\delta = -1$. In every imaginary quadratic field the equation $x^2 + y^2 = 1$ has solutions with $x = 0$, $y = \pm 1$ and $x = \pm 1$, $y = 0$, but in $K(i)$ -1 is a perfect square.

b) $\delta = \pm i$. As is seen at once the equations $x^2 \pm i y^2 = 1$, have no improper solutions in $K(i)$ except $x = \pm 1$, $\mathrm{y} = 0$.

c) $\delta = \varrho$ or ϱ^2, where $\varrho = \frac{1}{2}(-1 + \sqrt{-3})$. In these cases δ is a perfect square.

d) $\delta = -\varrho$ or $-\varrho^2$. The Diophantine equations $x^2 + \varrho y^2 = 1$ and $x^2 + \varrho^2 y^2 = 1$, have only the solutions $\varrho \sqrt{-\varrho}$ and $\varrho^2 \sqrt{-\varrho^2}$ respectively, apart from $x = \pm 1$, $y = 0$.

We now assert that two solutions $x + y\sqrt{\delta}$ and $x' + y'\sqrt{\delta}$ of (6) satisfy the condition $|x + y\sqrt{\delta}| = |x' + y'\sqrt{\delta}|$ if and only if $x' = \pm x$ and $y' = \pm y$, where the upper signs correspond. It is evident that to the two solutions $x + y\sqrt{\delta}$ and $x' + y'\sqrt{\delta}$ there exists a new one $\xi + \eta\sqrt{\delta}$ of (6) which satisfies the equation

$$\xi + \eta\sqrt{\delta} = \frac{x' + y'\sqrt{\delta}}{x + y\sqrt{\delta}}.$$

If we identify here the rational parts and the coefficients of $\sqrt{\delta}$ we get

$$\xi = xx' - \delta yy', \ \eta = xy' - yx'.$$

But for the solution $\xi + \eta\sqrt{\delta}$ we have

$$|\xi + \eta\sqrt{\delta}| = \frac{|x' + y'\sqrt{\delta}|}{|x + y\sqrt{\delta}|} = 1,$$

and if $N(\delta) = 1$ we have to consider the following cases:

a) $\delta = -1$. Here we have either $\xi = xx' + yy' = 0$ which implies $x' = \pm y$ and $y' = \pm x$, or $\eta = 0$ which implies $x' = \pm x$ and $y' = \pm y$. Because of the symmetry of $x^2 + y^2 = 1$ our proposition is true.

b) $\delta = \pm i$. Here we have $\eta = 0$ which implies $x' = \pm x$ and $y' = \pm y$.

c) $\delta = -\varrho$, where $\varrho = \frac{1}{2}(-1 + \sqrt{-3})$. Suppose that we have $\xi = xx' + \varrho yy' = 0$ and $\eta = xy' - yx' = \pm \varrho$. $\xi = 0$ implies either $x = \pm \varrho y'$, $y = \mp x'$ leading to $\eta = \pm (x'^2 + \varrho y'^2) = \pm \varrho$ which is impossible, or $x = \pm y'$, $y = \mp \varrho x'$ and here we get $\eta = \pm (\varrho x'^2 + y'^2) = \pm \varrho$. On multiplication with ϱ^2 we find $x'^2 + \varrho^2 y'^2 = \pm 1$, where we must have the minus sign. If we combine the equations $x'^2 + \varrho y'^2 = 1$ and $x'^2 + \varrho^2 y'^2 = -1$ we get

$$x'^2 (\varrho - 1) = 1 + \varrho = -\varrho^2,$$

which is again impossible. Thus we must have $\eta = 0$ and it follows $x' = \pm x$ and $y' = \pm y$.

d) $\delta = -\varrho^2$, where $\varrho^2 = -\frac{1}{2}(1 + \sqrt{-3})$. Suppose that we have $\xi = xx' + \varrho^2 yy' = 0$ and $\eta = xy' - yx' = \pm \varrho^2$. There are now three possibilities:

1) $x = \pm \varrho^2 y'$, $y = \mp x'$, which implies $\eta = \pm (\varrho^2 y'^2 + x'^2) = \pm \varrho^2$, or $x'^2 + \varrho^2 y'^2 = \pm \varrho^2$, but this is impossible.

2) $x = \pm \varrho y'$, $y = \pm \varrho x'$, which implies $\eta = \pm \varrho (x'^2 + y'^2) = \pm \varrho^2$ or $(\varrho x')^2 + \varrho^2 y'^2 = \pm 1$. Here we must have the minus sign. Now from

$$\begin{cases} x'^2+y'^2=-\varrho \\ x'^2+\varrho^2 y'^2=1 \end{cases}$$

it follows

$$y'^2(\varrho^2-1)=1+\varrho=-\varrho^2,$$

which is impossible.

3) $x=\pm y'$, $y=\mp\varrho^2 x'$. It follows $\eta=\pm(y'^2+\varrho^2 x'^2)=\pm\varrho^2$, and we must have $x'^2+\varrho y'^2=-1$, which combined with $x'^2+\varrho^2 y'^2=1$, leads to

$$x'^2(1-\varrho)=1+\varrho=-\varrho^2.$$

This equation, however, is impossible.

The (proper) solutions of (6) always occur in groups of four. In the following we shall call such a group a *set* of solutions. It is obvious that in a given set the expression $x+y\sqrt{\delta}$ assumes four different values which can be expressed by $\pm\zeta$ and $\pm\frac{1}{\zeta}$, where ζ is an arbitrary of these values, while $|x+y\sqrt{\delta}|$ only assumes two different values $|\zeta|$ and $\left|\frac{1}{\zeta}\right|$ reciprocal to each other. Since $|x+y\sqrt{\delta}|$ assumes only one value >1 in each set this value may be used for the purpose of characterizing the set, because the equation $|x+y\sqrt{\delta}|=|x'+y'\sqrt{\delta}|$ implies that $x+y\sqrt{\delta}$ and $x'+y'\sqrt{\delta}$ belongs to the same set. We now call the set for which $|x+y\sqrt{\delta}|$ assumes its least value greater than one the *fundamental set* of the equation (6).

Let ϱ be a positive real number. When ϱ increases from 1, $\varrho+\frac{1}{\varrho}$ increases from 2. From this it follows that for the fundamental set the expression

$$|x+y\sqrt{\delta}|^2+\frac{1}{|x+y\sqrt{\delta}|^2}=|x+y\sqrt{\delta}|^2+|x-y\sqrt{\delta}|^2=2(|x|^2+|y|^2)$$

assumes its least value greater than 2. This may be used as a definition of the fundamental set and although it is essentially equal to the previous definition it has the advantage of being independent of the condition $|x+y\sqrt{\delta}|>1$, since the expression above assumes the same value for every solution $x+y\sqrt{\delta}$ belonging to a given set.

If we have found a solution $x_1+y_1\sqrt{\delta}$ of equation (6) it is easy to determine the fundamental set. All we have to do is to calculate $|x_1+y_1\sqrt{\delta}|^2$ which, for the sake of brevity, we denote by b, for the given solution, to determine the solutions which satisfy the inequalities

$$1<|x|^2+|y|^2|\delta|<\tfrac{1}{2}\left(b+\frac{1}{b}\right)$$

and finally to decide for which one of these solutions the expression $|x+y\sqrt{\delta}|$ assumes its least value >1.

We will now show how it is possible to determine all the solutions of (6) starting from the fundamental set. Although we may start from an arbitrary solution in the fundamental set for convenience we choose one of these, i.e. the one satisfying the following conditions: $|x+y\sqrt{\delta}|>1$ and $-\frac{\pi}{2}\leqq \arg.\ y<\frac{\pi}{2}$. We call this solution the *fundamental solution* of the equation (6). The fundamental solution will for the rest of this paragraph be denoted by $x_1+y_1\sqrt{\delta}$.

We put $|x_1+y_1\sqrt{\delta}|=\sigma$ and prove

Theorem 2. *If δ is an integer in $\boldsymbol{K}(\sqrt{-m})$ which is not a perfect square, the Diophantine equation (6) has an infinitude of solutions $x+y\sqrt{\delta}$. All the solutions (one representative from each set) are obtained by the formula*

$$x_n+y_n\sqrt{\delta}=(x_1+y_1\sqrt{\delta})^n, \qquad (n=1,\ 2,\ 3,\ \ldots) \tag{11}$$

where $x_1+y_1\sqrt{\delta}$ is the fundamental solution. On identifying the rational parts and the coefficients of $\sqrt{\delta}$ we get

$$\begin{cases} x_n=x_1^n+\sum\limits_{k=1}\binom{n}{2k}x_1^{n-2k}y_1^{2k}\delta^k \\ y_n=\sum\limits_{k=1}\binom{n}{2k-1}x_1^{n-2k+1}y_1^{2k-1}\delta^{k-1}. \end{cases} \tag{12}$$

Proof. Clearly it follows from (11) that

$$x_n-y_n\sqrt{\delta}=(x_1-y_1\sqrt{\delta})^n.$$

Then, on multiplying together the corresponding members of this equation and of equation (11) we have

$$(x_n^2-\delta y_n^2)=(x_1^2-\delta y_1^2)^n=1.$$

Hence $x_n+y_n\sqrt{\delta}$ is a solution of (6).

Suppose now that $\xi+\eta\sqrt{\delta}$ were a solution of (6) which could not be obtained by formula (11). Then, since $|x_1+y_1\sqrt{\delta}|^n$ is monotonously increasing with n, such a natural number t would exist that

$$|\xi+\eta\sqrt{\delta}|=\sigma^t \text{ or } \sigma^t<|\xi+\eta\sqrt{\delta}|<\sigma^{t+1}.$$

In the first case we have $|\xi+\eta\sqrt{\delta}|=|x_t+y_t\sqrt{\delta}|$, and according to a previous result this implies $\xi=\pm x_t$, $\eta=\pm y_t$, where the sign is uniquely determined. In the second case we get the double inequality

$$1<\frac{|\xi+\eta\sqrt{\delta}|}{|x_t+y_t\sqrt{\delta}|}<|x_1+y_1\sqrt{\delta}|$$

and consequently the solution $\xi'+\eta'\sqrt{\delta}$ of (6) defined by

$$\xi' + \eta' \sqrt{\delta} = \frac{\xi + \eta \sqrt{\delta}}{x_t + y_t \sqrt{\delta}}$$

satisfies the inequalities

$$1 < |\xi' + \eta' \sqrt{\delta}| < |x_1 + y_1 \sqrt{\delta}|.$$

This, however, is contrary to our definition of the fundamental solution $x_1 + y_1 \sqrt{\delta}$. Hence Theorem 2 is proved.

In special cases one can immediately find the fundamental solution of equation (6). To give an example the equation

$$x^2 - (u^2 - 1) y^2 = 1, \quad N(u) > 1,$$

where u denotes an arbitrary integer in $K(\sqrt{-m})$, has the fundamental solution $u + \sqrt{u^2 - 1}$.

More generally we have

Theorem 3. *Let δ be an integer in the field $K(\sqrt{-m})$ which is not a perfect square. If ξ and η are integers in $K(\sqrt{-m})$ which satisfy the inequalities*

$$(13) \qquad \begin{cases} N(\xi) > \dfrac{N(\eta^2)(m+5)^2}{4(m+1)^2} + \dfrac{1}{4}, & \text{for } m \equiv 3 \pmod{4} \\ N(\xi) > \dfrac{N(\eta^2)(m+1)^2}{4m^2} + \dfrac{1}{4}, & \text{for } m \equiv 1, 2, \pmod{4}, \end{cases}$$

and if $\alpha = \xi + \eta \sqrt{\delta}$ is a solution of the equation (6), then α is the fundamental solution of (6).

Proof. We prove first that if $x_1 + y_1 \sqrt{\delta}$ is the fundamental solution of (6) i.e. if $|x_1|^2 + |y_1|^2 |\delta|$ assumes its least value > 1, then so does $|y_1|$. According to (12) we have

$$y_n = \sum_{k=1} \binom{n}{2k-1} x_1^{n-2k+1} y_1^{2k-1} \delta^{k-1}$$

and hence

$$N(y_n) = N(y_1) N(u), \quad (n = 1, 2, 3, \ldots)$$

where u is an integer in $K(\sqrt{-m})$, so that $N(u) \geqq 1$. Here the equality sign is obviously possible only for $n = 1$.

The theorem is true for $N(\eta) = 1$. We suppose therefore that $N(\eta) > 1$ and furthermore that $x_1 + y_1 \sqrt{\delta}$ is the fundamental solution of (6) and that $1 \leqq N(y_1) < N(\eta)$. However we have

$$\delta = \frac{x_1^2 - 1}{y_1^2} = \frac{\xi^2 - 1}{\eta^2},$$

which may be written

$$x_1^2\eta^2-y_1^2\xi^2=\eta^2-y_1^2=\beta,$$

or

$$x_1\eta+y_1\xi=\beta_1,\quad x_1\eta-y_1\xi=\beta_2,$$

where β_1, β_2 and $\beta\neq 0$ are integers in $K(\sqrt{-m})$. Now it follows

$$N(\xi)=\frac{N(\beta_1-\beta_2)}{4N(y_1)}\leqq\frac{N(\beta)+1}{4N(y_1)}=\frac{N(\eta^2-y_1^2)+1}{4N(y_1)}\leqq$$

$$\leqq\begin{cases}\dfrac{N(\eta^2)(m+5)^2}{4(m+1)^2}+\dfrac{1}{4}, & \text{for } m\equiv 3 \text{ (mod. 4).}\\[2ex] \dfrac{N(\eta^2)(m+1)^2}{4m^2}+\dfrac{1}{4}, & \text{for } m\equiv 1,\ 2 \text{ (mod. 4).}\end{cases}$$

By (12) we find $N(\eta)=N(y_1)N(y)$, where $N(y)\geqq 2$, so that if $m\equiv 3$ (mod. 4) we must have $N(y)\geqq\frac{m+1}{4}$ and if $m\equiv 1$, 2 (mod. 4) we must have $N(y)\geqq m$. Consequently the inequalities mentioned above for $N(\xi)$ are true. Thus our assumption that $N(\eta)>N(y_1)$ is false and Theorem 3 is proved.

We have the following corrolary to this theorem:

Let y_1 and u be integers in $K(\sqrt{-m})$ where $N(u)\geqq 5$. If we put

$$\delta=u(uy_1^2+2)$$

the number

$$1+uy_1^2+y_1\sqrt{\delta}$$

is the fundamental solution of equation (6).

By letting u vary, we obtain an infinity of values δ for which y_1 has the same value.

An important problem concerning the equation (6) is the following: Given an equation of the type (6). How can we determine the fundamental solution of that equation? If we write the equation on the form $x^2=\delta y^2+1$, and in the expression δy^2+1 let y successively run through the integers of $K(\sqrt{-m})$ for which $N(y)=1, 2, 3, \ldots$, we find after a finite number of trials an integer y_1 for which δy_1^2+1 is a perfect square. By our mode of construction the solution $x_1+y_1\sqrt{\delta}$ of (6) found in this way belongs to the fundamental set. In most cases it is, however, impossible to use this method of determination because of the laborious calculations it requires. In general, however, it is the only method available at present.

For the Euclidean fields $m=1$, 2, 3, 7 and 11, A. STEIN [7] and A. ARWIN [8] have shown how the fundamental solution of (6) may be determined by the expansion of $\sqrt{\delta}$ in a certain type of continued fraction. A STEIN who does not consider the equation (6) but the units in relative quadratic fields, treats the field $K(i)$ only but makes a more exhaustive investigation than does ARWIN.

§ 3. The Diophantine equation $x^2 - \delta y^2 = -1$

While equation (6) is solvable in integers belonging to $\boldsymbol{K}(\sqrt{-m})$ for every integer δ in $\boldsymbol{K}(\sqrt{-m})$ which is not a perfect square, the Diophantine equation

$$x^2 - \delta y^2 = -1, \tag{14}$$

is solvable only for certain values of δ. Let us consider as an example the equation

$$x^2 - (1 + \sqrt{-2})\, y^2 = -1 \tag{15}$$

in $\boldsymbol{K}(\sqrt{-2})$. The equation

$$x^2 - (1 + \sqrt{-2})\, y^2 = 1,$$

has the fundamental solution

$$(1 - \sqrt{-2}) + (\sqrt{-2})\sqrt{1 + \sqrt{+2}}.$$

Suppose that $\xi + \eta\sqrt{\delta}$ is the fundamental solution of (15). According to (17) we have $2\xi n = \pm\sqrt{-2}$, which is obviously impossible.

If x and y are integers in $\boldsymbol{K}(\sqrt{-m})$ which satisfy the equation (14), the number $x + y\sqrt{\delta}$ is called a *solution* of the equation. The solution is said to be *proper* if x and y are both different from zero, otherwise it is called *improper*. When we speak of solutions in the following lines we shall always mean proper solutions.

We assume in the following that equation (14) is solvable and shall investigate the properties of the solutions. It turns out that the field $\boldsymbol{K}(i)$ needs a special treatment.

Let $x + y\sqrt{\delta}$ be a solution of equation (6) which, as we have seen, is always solvable in $\boldsymbol{K}(i)$. Then $xi + yi\sqrt{\delta}$ is obviously a solution of equation (14). On the other hand, if $u + v\sqrt{\delta}$ is a solution of (14) then $ui + vi\sqrt{\delta}$ is a solution of (6). Hence the Diophantine equation (14) is always solvable in $\boldsymbol{K}(i)$ and its solutions are connected with the solutions of (6) in a very simple way. We have

Theorem 4. *The Diophantine equation (14) is always solvable in integers belonging to $\boldsymbol{K}(i)$ and we obtain all solutions $x_n + y_n\sqrt{\delta}$ of the equation (one representative from each set) by the formula*

$$x_n + y_n\sqrt{\delta} = i\,(x + y\sqrt{\delta})^n, \quad (n + 1, 2, 3, \cdots) \tag{16}$$

where $x + y\sqrt{\delta}$ denotes the fundamental solution of equation (6).

Because of Theorem 4 we leave the field $\boldsymbol{K}(i)$ out of consideration for the rest of this paragraph, i.e. we shall always assume $\boldsymbol{K}(\sqrt{-m}) \neq \boldsymbol{K}(i)$.

In analogy with our exposition in § 2 we shall now introduce the concepts of fundamental set and fundamental solution. First, however, we will have to make a few remarks.

Our first remark concerns the existence of improper solutions of equation (14). According to theorem 4 we do not take the field $\boldsymbol{K}(i)$ into consideration. Since the equation $x^2=-1$ is not solvable in $\boldsymbol{K}(\sqrt{-m})$, $m>1$, we cannot have $y=0$ in (14). Thus $N(\delta)=1$ is a necessary condition for the existence of improper solutions. This means that we will have to study the equation $-\delta y^2=-1$. Now the only possibilities for δ are $\delta=\varrho$ and $\delta=\varrho^2$, where $\varrho=\frac{1}{2}(-1+\sqrt{-3})$, but for these values δ is a perfect square. Hence equation (14) has no improper solutions in $\boldsymbol{K}(\sqrt{-m})$, $m>1$.

Let $x+y\sqrt{\delta}$ and $x'+x'\sqrt{\delta}$ be two solutions of (14) for which we have $|x+y\sqrt{\delta}|=|x'+y'\sqrt{\delta}|$. Then $x'=\pm x$ and $y'=\pm y$, where the upper signs correspond. It is evident that to the two solutions $x+y\sqrt{\delta}$ and $x'+y'\sqrt{\delta}$ of (14) there exists a solution $\xi+\eta\sqrt{\delta}$ of the equation (6) such that

$$\xi+\eta\sqrt{\delta}=\frac{x'+y'\sqrt{\delta}}{x+y\sqrt{\delta}}.$$

On identifying the rational parts and the coefficients of $\sqrt{\delta}$ we get

$$\xi=\delta y y'-x x', \quad \eta=x' y-y' x.$$

But for the solution $\xi+\eta\sqrt{\delta}$ of (6) we have

$$|\xi+\eta\sqrt{\delta}|=\frac{|x'+y'\sqrt{\delta}|}{|x+y\sqrt{\delta}|}=1,$$

and according to our result in § 2 it follows $\xi=\pm 1$, $\eta=0$ and consequently $x'=\pm x$, $y'=\pm y$.

The solutions of (14) always occur in groups of four. In the following we shall call such a group a *set* of solutions. In a given set the expression $\zeta=x+y\sqrt{\delta}$ obviously assumes four different values which may be expressed by $\pm\zeta$ and $\pm\frac{1}{\zeta}$, where ζ denotes an arbitrary of these values, while $|x+y\sqrt{\delta}|$ only assumes two different values $|\zeta|$ and $\left|\frac{1}{\zeta}\right|$. Since $|x+y\sqrt{\delta}|$ assumes only one value >1 in each set this value may be used for the purpose of characterizing the set, because the equation $|x+y\sqrt{\delta}|=|x'+y'\sqrt{\delta}|$ implies that $x+y\sqrt{\delta}$ and $x'+y'\sqrt{\delta}$ belongs to the same set. We now call the set for which $|x+y\sqrt{\delta}|$ assumes its least value >1 the *fundamental set* of equation (14).

For the fundamental set the expression

$$|x+y\sqrt{\delta}|^2+\frac{1}{|x+y\sqrt{\delta}|^2}=|x+y\sqrt{\delta}|^2+|x-y\sqrt{\delta}|^2=2\left(|x|^2+|y|^2\right)$$

assumes its least value >2, which may also be used as a definition of the fundamental set.

If we have found a solution $x_1+y_1\sqrt{\delta}$ of equation (14) it is easy to determine the fundamental set. All we have to do is to calculate $|x_1+y_1\sqrt{\delta}|^2$ which, for the sake of brevity, we denote by b, for the given solution, to determine the solutions which satisfy the inequalities

$$1<|x|^2+|y|^2|\delta|<\tfrac{1}{2}\left(b+\frac{1}{b}\right)$$

and finally to decide for which one of these, the expression $|x+y\sqrt{\delta}|$ assumes its least value >1.

We shall now show how it is possible to determine all solutions of equation (14) starting from the fundamental set. Although we may start from an arbitrary solution in the fundamental set we choose for convenience one of these, i.e. the one which satisfies the following conditions: $|x+y\sqrt{\delta}|>1$ and $-\frac{\pi}{2}\leqq$ $\leqq \arg.\ y<\frac{\pi}{2}$. We call this solution the *fundamental solution* of the equation (14). It will in the following be denoted by $x_1+y_1\sqrt{\delta}$.

The square of a solution of (14) is obviously a solution of equation (6). We prove the following

Theorem 5. *Let δ be an integer in $K(\sqrt{-m})$, $m>1$, which is not a perfect square, and suppose that the Diophantine equation (14) is solvable in $K(\sqrt{-m})$. Suppose furthermore that $x_1+y_1\sqrt{\delta}$ is the fundamental solutions of the equation. Then either the number*

$$x_2+y_2\sqrt{\delta}=(x_1+y_1\sqrt{\delta})^2=x_1^2+\delta y_1^2+2x_1y_1\sqrt{\delta} \tag{17}$$

or the number $-x_2-y_2\sqrt{\delta}$ is the fundamental solution of equation (6), according as $-\frac{\pi}{2}\leqq \arg.\ 2x_1y_1<\frac{\pi}{2}$ or not.

If, further, we put

$$x_n+y_n\sqrt{\delta}=(x_1+y_1\sqrt{\delta})^n, \quad (n=1,\ 2,\ 3\ \ldots) \tag{18}$$

where

$$\left\{\begin{aligned} x_n&=x_1^n+\sum_{k=1}\binom{n}{2k}x_1^{n-2k}y_1^{2k}\delta^k\\ y_n&=\sum_{k=1}\binom{n}{2k-1}x_1^{n-2k+1}y_1^{2k-1}\delta^{k-1}\end{aligned}\right. \tag{19}$$

we obtain by formula (18)

1. *All the solutions (one representative from each set) of equation (14) when n runs through all positive odd integers.*

2. *All the solutions* (*one representative from each set*) *of equation* (*6*), *when n runs through all positive even integers.*

Proof. Clearly it follows from (18) that

$$x_n - y_n\sqrt{\delta} = (x_1 - y_1\sqrt{\delta})^n.$$

Then, on multiplying together the corresponding members of this equation and of equation (18) we have

$$(x_n^2 - \delta y_n^2) = (x_1^2 - \delta y_1^2)^n = (-1)^n.$$

Hence $x_n + y_n\sqrt{\delta}$ is a solution of (14) or of (6) according as the exponent n is odd or even.

Suppose now that the fundamental solutions of equations (6) and (14) are not related by the formula (17). Then we must have

$$1 < |x + y\sqrt{\delta}| < |x_1 + y_1\sqrt{\delta}|^2$$

where $x + y\sqrt{\delta}$ denotes the fundamental solution of equation (6), and on multiplication with the number $|x_1 - y_1\sqrt{\delta}|$ it follows

$$|x_1 - y_1\sqrt{\delta}| < |x x_1 - \delta y y_1 + (y x_1 - x y_1)\sqrt{\delta}| < |x_1 + y_1\sqrt{\delta}|$$

where the integers

$$x_0 = x x_1 - \delta y y_1 \text{ and } y_0 = y x_1 - x y_1$$

satisfies equation (14). On the other hand it is obvious from the properties of the solutions $x_1 - y_1\sqrt{\delta}$ and $x_1 + y_1\sqrt{\delta}$ that we must have $x_0 = y_0 = 0$, since it does not exist any improper solutions of equation (14). From $x_0 = y_0 = 0$ it follows $x = \pm x_1$ and $y = \pm y_1$ which is obviously impossible. Thus (17) is true. As a consequence of this result and of Theorem 2 we obtain immediately the proof of the last part of Theorem 5.

It remains to prove the second part of our theorem. Suppose the $x + y\sqrt{\delta}$ were a solution of (14) which is not obtainable by formula (18) i.e. such a one that none of the solutions belonging to the same set as $x + y\sqrt{\delta}$ is obtainable by (18). Then such a natural number t would exist that either

$$|x + y\sqrt{\delta}| = |x_1 + y_1\sqrt{\delta}|^{2t-1}$$

or

$$|x_1 + y_1\sqrt{\delta}|^{2t-1} < |x + y\sqrt{\delta}| < |x_1 + y_1\sqrt{\delta}|^{2t+1}.$$

In the first case we have $|x + y\sqrt{\delta}| = |x_{2t-1} + y_{2t-1}\sqrt{\delta}|$ and according to a previous result, $x + y\sqrt{\delta}$ and $x_{2t-1} + y_{2t-1}\sqrt{\delta}$ belongs to the same set. In the second case we get after having divided by $|x_1 + y_1\sqrt{\delta}|^{2t-1}$

$$1<\frac{|x+y\sqrt{\delta}|}{|x_1+y_1\sqrt{\delta}|^{2t-1}}<|x_1+y_1\sqrt{\delta}|^2.$$

For the solution $\xi+\eta\sqrt{\delta}$ of (6) defined by

$$\xi+\eta\sqrt{\delta}=\frac{x+y\sqrt{\delta}}{(x_1+y_1\sqrt{\delta})^{2t-1}}$$

we have however

$$1<|\xi+\eta\sqrt{\delta}|<|x_1+y_1\sqrt{\delta}|^2$$

but this is impossible, since $(x_1+y_1\sqrt{\delta})^2$ belongs to the fundamental set of equation (6). Thus the proof of Theorem 5 is completed.

§ 4. The Diophantine equation $x^2-Dy^2=\pm 1$

In this section we study equation (2) for the special case of δ being a rational integer. We first put $\delta=D$ where D is a natural number which is not a perfect square in $K(\sqrt{-m})$. Furthermore we assume $\sqrt{D}$ to be positive and consider the equation

$$x^2-Dy^2=1. \tag{20}$$

It is seen at once that if $x+y\sqrt{D}$ is a solution of (20), where $x=\frac{1}{2}(a_1+b_1\sqrt{-m})$, $y=\frac{1}{2}(a_2+b_2\sqrt{-m})$, with $a_k\equiv b_k$ (mod. 2) for $m\equiv 3$ (mod. 4) and $a_k\equiv b_k\equiv 0$ (mod. 2) for $m\equiv 1, 2$ (mod. 4), then $\bar{x}+\bar{y}\sqrt{D}$, where, $\bar{x}=\frac{1}{2}(a_1-b_1\sqrt{-m})$ and $\bar{y}=\frac{1}{2}(a_2-b_2\sqrt{-m})$, is also a solution of (20), and for these two solutions we have $|x+y\sqrt{D}|=|\bar{x}+\bar{y}\sqrt{D}|$. According to our results in § 2, this implies $a_1-b_1\sqrt{-m}=\pm(a_1+b_1\sqrt{-m})$ and $a_2-b_2\sqrt{-m}=\pm(a_2+b_2\sqrt{-m})$, where the upper signs correspond, i.e. we have either $b_1=b_2=0$ or $a_1=a_2=0$.

Let us first consider the case $b_1=b_2=0$. In this case equation (20) may be written

$$a_1^2-Da_2^2=4$$

i.e. the equation coincides with Pell's equation.

Let us now assume that $a_1=a_2=0$. Then equation (20) is of the form

$$(b_1\sqrt{-m})^2-D(b_2\sqrt{-m})^2=4$$

or

$$-mb_1^2+Dmb_2^2=4,$$

which is possible only for $m=1$. Hence $K(i)$ is the only imaginary quadratic field in which equation (20) has non-real solutions. On observing that an imaginary solution of equation (20) in $K(i)$ may be regarded as a solution in rational integers of the equation

(21) $x^2-Dy^2=-1$, we can formulate

Theorem 6. *The Diophantine equation (20) has in the field $K(i)$ either alternately purely imaginary solutions and real solutions, or real solutions only, according as equation (21) is solvable in rational integers or not.*

For the other imaginary quadratic fields we have

Theorem 7. *The Diophantine equation (20) has in the field $K(\sqrt{-m})$, $m>1$, only real solutions $x+y\sqrt{D}$ i.e. x and y are rational integers.*

For the Diophantine equation (21) we have the same result i.e. if equation (21) is solvable, the solutions are real numbers.

We now turn our attention to the equation

$$x^2+Dy^2=1, \tag{22}$$

where D is a squarefree natural number such that $-D$ is not a perfect square in $K(\sqrt{-m})$. With $x=\frac{1}{2}(a_1+b_1\sqrt{-m})$, $y=\frac{1}{2}(a_2+b_2\sqrt{-m})$, where $a_k\equiv b_k$ (mod. 2) for $m\equiv 3$ (mod. 4) and $a_k\equiv b_k\equiv 0$ (mod. 2) for $m\equiv 1$, 2 (mod. 4), we get

$$\begin{cases} a_1^2-mb_1^2+D(a_2^2-mb_2^2)=4. \\ a_1b_1+Da_2b_2=0. \end{cases}$$

On eliminating a_2^2 between these two equations we find

$$(b_1^2+Db_2^2)(a_1^2-mDb_2^2)=4Db_2^2,$$

and there are the following possibilities to examine

1) $b_1=a_2=0$. Putting $a_1=2c_1$ and $b_2=2d_2$, equation (22) reduces to

$$c_1^2-mDd_1^2=1. \tag{23}$$

It cannot occur here that mD is the square of a natural number.

2) $a_1=b_2=0$. Putting $a_2=2c_2$ and $b_1=2d_1$, this implies

$$-md_1^2+Dc_2^2=1. \tag{24}$$

While (23) is always solvable, (24) is solvable only for certain values of D. If equation (24) is solvable and has the solution $d_1\sqrt{-m}+c_2\sqrt{-D}$, then

$$(d_1\sqrt{-m}+c_2\sqrt{-D})^2=-md_1^2-Dc_2^2+2c_2d_1\sqrt{mD}$$

is a solution of (23).

3) $b_1^2=3Db_2^2$, i.e. $D=3$. In this case (22) reduces to an equation of type (23).

4) Finally we may have $b_1^2=Db_2^2$, i.e. $D=1$. Here (22) is of the form

$$\left(\frac{a_1+b_1\sqrt{-m}}{2}\right)^2+\left(\frac{a_1-b_1\sqrt{-m}}{2}\right)^2=1, \tag{25}$$

and this equation is solvable if m does not contain any prime $p\equiv 3$, 5 (mod. 8), as is seen at once.

By Theorem 2 we have

Theorem 8. *If $D>1$ and equation (24) is solvable with the fundamental solution $x+y\sqrt{-D}$ this solution is also the fundamental solution of equation (22). Furthermore the solution $(x+y\sqrt{-D})^2$ belongs to the fundamental set of equation (23), which may be regarded as an ordinary Pell's equation. If (24) is not solvable the fundamental solution of (22) is equal to the fundamental solution of (23).*

If $D=1$ and (25) is solvable with the fundamental solution

$$\frac{a_1+b_1\sqrt{-m}}{2}+\frac{a_1-b_1\sqrt{-m}}{2}\sqrt{-1}$$

this solution is the fundamental solution of equation (22). If (25) is not solvable the fundamental solution of (22) is equal to the fundamental solution of equation (24).

For the equation

$$x^2+Dy^2=-1, \tag{26}$$

we have apart from trivial differences, the same results as for equation (22).

Our results in Theorems 6, 7 and 8 may be regarded as theorems concerning the units $x+y\sqrt{D}$ and $x+y\sqrt{-D}$ with integral coefficients x and y in the fields $K(\sqrt{-m};\ \sqrt{D})$ and $K(\sqrt{-m};\ \sqrt{-D})$ respectively. Leaving the roots of unity belonging to $K(\sqrt{-m};\ \sqrt{D})$ and $K(\sqrt{-m};\ \sqrt{-D})$ out of consideration we have

Theorem 9. *The cyclic group G of units $x+y\sqrt{D}$, with integral coefficients x and y belonging to $K(\sqrt{-m})$, in the field $K(\sqrt{-m};\ \sqrt{D})$, $m>1$, is generated by the fundamental unit of the subfield $K(\sqrt{D})$.*

In the field $K(\sqrt{-1};\ \sqrt{D})$ the group G is generated by $\sqrt{x+y\sqrt{D}}$ or $x+y\sqrt{D}$, where $x+y\sqrt{D}$ denotes the fundamental unit of $K(\sqrt{D})$ according as the Diophantine equation (21) is solvable in rational integers or not.

As to the fields $K\sqrt{-m};\ \sqrt{-D})$ we have

Theorem 10. *For $D>1$, the group G of units $\xi+\eta\sqrt{-D}$ with integral coefficients ξ and η in $K(\sqrt{-m})$ is generated by $\sqrt{u+v\sqrt{mD}}$ or $u+v\sqrt{mD}$, where $u+v\sqrt{mD}$, where $u+v\sqrt{mD}$ is the fundamental unit in the field $K(\sqrt{mD})$, according as either of the equations*

$$(-mx^2-Dy^2)^2=1, \tag{27}$$

and

$$x^2-my^2=-1, \tag{28}$$

are solvable in rational integers or not.

In the field $K(\sqrt{-m};\ \sqrt{-1})$ the group G is generated by $\sqrt{u+v\sqrt{m}}$ or $u+v\sqrt{m}$, where $u+v\sqrt{m}$ is the fundamental unit in the field $K(\sqrt{m})$, according as either of the equations

$$x^2 - my^2 = -1, \tag{29}$$

and

$$x^2 - my^2 = \pm 2, \tag{30}$$

are solvable in rational integers or not.

§ 5. The Diophantine equation $x^2 - \delta y^2 = \sigma$

Let $f(x, y)$ be a binary quadratic form with coefficients belonging to an algebraic number field Ω. If then σ is an integer in the field considered, the question arises whether or not σ can be represented by the form $f(x, y)$, or expressed in a different way, whether or not the Diophantine equation

$$f(x,y) = \sigma \tag{31}$$

is solvable in integers belonging to Ω. In investigating this problem one may use either the theory of quadratic forms or the theory of relative quadratic fields.

When Ω is the rational number field T. NAGELL [1] [2] [3] [4] has shown, as is previously mentioned, how the solutions of (31) can be determined very easily and with quite elementary methods.

Using the theory developed in §§ 1–3, we will show in this paragraph that the method employed by NAGELL can also be used when Ω is an imaginary quadratic field.

Obviously it is sufficient to study the equation

$$x^2 - \delta y^2 = \sigma \tag{32}$$

where δ is an integer in $K(\sqrt{-m})$ which is not a perfect square, instead of the more general equation (31).

If $x = u$ and $y = v$ are integers in $K(\sqrt{-m})$ which satisfy the equation (32) we say that the number

$$u + v\sqrt{\delta}$$

is a *solution* of that equation.

Two solutions $u + v\sqrt{\delta}$ and $u' + v'\sqrt{\delta}$ of (32) are said to be equal if and only if $u = u'$ and $v = v'$.

A solution $u + v\sqrt{\delta}$ of (32) is said to be greater than another solution $u' + v'\sqrt{\delta}$ of (32) if $|u + v\sqrt{\delta}| > |u' + v'\sqrt{\delta}|$.

In § 1 we have studied the equation

$$x^2 - \delta y^2 = 1. \tag{33}$$

We showed that (33) is always solvable in $\boldsymbol{K}(\sqrt{-m})$ and defined the fundamental solution of that equation to be the solution which satisfies the conditions $|v+y\sqrt{\delta}|>1$ and least, and $-\frac{\pi}{2}\leqq \text{arg. } y<\frac{\pi}{2}$.

Assume now that equation (32) is solvable and has the solution $u+v\sqrt{\delta}$. If $x+y\sqrt{\delta}$ is a solution of (33), then the number

$$(u+v\sqrt{\delta})(v+y\sqrt{\delta})=ux+\delta vy+(uy+vx)\sqrt{\delta}$$

is also a solution of (32). This solution is said to be *associated* with the solution $u+v\sqrt{\delta}$. The set of all solutions associated with each other forms a *class of solutions* of (32). By Theorem 2 every class contains an infinity of solutions.

It is possible to decide whether the two given solutions $u+v\sqrt{\delta}$ and $u'+v'\sqrt{\delta}$ 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

$$\frac{uu'-\delta vv'}{\sigma} \quad \text{and} \quad \frac{vu'-uv'}{\sigma}$$

be integers in $\boldsymbol{K}(\sqrt{-m})$.

Let $\boldsymbol{K}$ be the class consisting of the solutions $u_i+v_i\sqrt{\delta}$, $i=1, 2, 3, \ldots$, it is then evident that the solutions $u_i-v_i\sqrt{\delta}$, $i=1, 2, 3, \ldots$, also constitute a class, which may be denoted by $\overline{\boldsymbol{K}}$. The classes $\boldsymbol{K}$ and $\overline{\boldsymbol{K}}$ 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 $u+v\sqrt{\delta}$ in a given class $\boldsymbol{K}$ we now choose a solution $u^*+v^*\sqrt{\delta}$ in the following way: Let $N(u^*)$ be the least value of $N(u)$ which occurs in $\boldsymbol{K}$, and furthermore let u^* satisfy the inequalities $-\frac{\pi}{2}\leqq \text{arg. } u^*<\frac{\pi}{2}$. If $\boldsymbol{K}$ is not ambiguous, then the solution $u^*+v^*\sqrt{\delta}$ is uniquely determined. If $\boldsymbol{K}$ is ambiguous, we get a uniquely determined solution $u^*+v^*\sqrt{\delta}$ by prescribing also that $-\frac{\pi}{2}\leqq \text{arg. } v^*<\frac{\pi}{2}$. The solution defined in this way is said to be the *fundamental solution of the class.*

The case $N(u^*)=0$ can occur only when the class is ambiguous, and similarly for the case $N(v^*)=0$.

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

After these preliminaries we are now in a position to prove

Theorem 11. *Let $u+v\sqrt{\delta}$ be the fundamental solution in the class $\boldsymbol{K}$ of the Diophantine equation*

$$u^2-\delta v^2=\sigma \tag{32}$$

and let $v_1 + y_1 \sqrt{\delta}$ be the fundamental solution of the equation (33). Furthermore let us assume that δ takes none of the values $\pm\sqrt{-1}$, ± 2, $\pm\frac{1}{2}(3-\sqrt{-3})\pm\frac{1}{2}(3+\sqrt{-3})$ and $\pm\sqrt{-3}$. Under these conditions u and v obey the following inequalities

$$0 < |u^2| < \frac{|x_1^2 - 1|}{|x_1| - 1} |\sigma| \tag{34}$$

and

$$0 \leqq |v^2| < \left(\frac{|y_1^2|}{|x_1| - 1} + \frac{1}{|\delta|}\right) |\sigma| . \tag{35}$$

If σ is a perfect square in $\boldsymbol{K}(\sqrt{-m})$, $\sigma = \eta^2$, and η belongs to the class $\boldsymbol{K}$ we have the following inequalities as well, which have the advantage of being also valid for the exceptional values of δ enumerated above.

$$0 < |u| \leqq |x_1| |\sqrt{\sigma}| \tag{36}$$

$$0 \leqq |v| \leqq |y_1| |\sqrt{\sigma}| . \tag{37}$$

Proof. It is evident, that the inequalities (36) and (37) are valid when σ is a perfect square $\sigma = \eta^2$ and η belongs to the class $\boldsymbol{K}$, since in this case equation (32) has the solution $x_1 \eta + y_1 \eta \sqrt{\delta}$.

Let us then turn to the other inequalities. If (34) and (35) are valid for the class $\boldsymbol{K}$ they are aslo valid for the conjugate class $\bar{\boldsymbol{K}}$. We form

$$(u + v\sqrt{\delta})(x_1 + y_1\sqrt{\delta}) = u x_1 + \delta v y_1 + (v x_1 + u y_1)\sqrt{\delta}$$

and

$$(u + v\sqrt{\delta})(x_1 - y_1\sqrt{\delta}) = u x_1 - \delta v y_1 + (v x_1 - u y_1)\sqrt{\delta}$$

Let us consider

$$u x_1 + \delta v y_1 \quad \text{and} \quad u x_1 - \delta v y_1 .$$

According to the definition of fundamental solution these numbers both obey the inequalities

$$|u x_1 + \delta v y_1| \geqq |u| \quad \text{and} \quad |u x_1 - \delta v y_1| \geqq |u| .$$

But it is evident that at least one of these inequalities, let us assume that it is the first one, may be sharpened to

$$|u x_1 + \delta v y_1| \geqq |u x_1| ,$$

and here the equality sign holds only if $v = 0$ so that we can assume the inequality to be strict,

$$|u x_1 + \delta v y_1| > |u x_1| ,$$

since if $v=0$, $|u^2|$ satisfies the inequality $|u^2|\leqq|\sigma|$, which is obviously better than (34). It now follows

$$|u^2 x_1^2-\delta^2 v^2 y_1^2|>|u^2||x_1|$$

or

$$|u^2 x_1^2-(u^2-\sigma)(x_1^2-1)|>|u^2||x_1|$$

which can be written

$$|u^2+\sigma(x_1^2-1)|>|u^2||x_1|.$$

Hence

$$\frac{|\sigma|}{|u^2|}|x_1^2-1|>|x_1|-1,$$

and we get

$$|u^2|<\frac{|x_1^2-1|}{|x_1|-1}|\sigma|$$

under the condition $|x_1|\neq 1$. This condition is always fulfilled except for the values of δ enumerated in the theorem. Thus the inequalities (34) are true.

From (32) we deduce

$$|\delta||v^2|\leqq|u^2|+|\sigma|$$

and it follows

$$|v^2|<\frac{1}{|\delta|}\left(\frac{|x_1^2-1|}{|x_1|-1}+1\right)|\sigma|$$

which is in fact the right hand inequality in (35).

For those values of δ which are excepted in Theorem 11 we have

Theorem 11 a. *Let δ be one of the integers $\pm\sqrt{-1}$, ± 2, $\pm\frac{1}{2}(3-\sqrt{-3})$, $\pm\frac{1}{2}(3+\sqrt{-3})$, or $\pm\sqrt{-3}$. Furthermore let $u+v\sqrt{\delta}$ be the fundamental solution of the class K of the Diophantine equation*

$$u^2-\delta v^2=\sigma, \tag{32}$$

and let $x_2+y_2\sqrt{\delta}$ be the square of the fundamental solution of equation (33). Under these conditions u and v obey the following inequalities

$$0<|u^2|<\frac{|x_2^2-1|}{|x_2|-1}|\sigma| \tag{38}$$

and

$$0\leqq|v^2|<\left(\frac{|y_2^2|}{|x_2|-1}+\frac{1}{|\delta|}\right)|\sigma|. \tag{39}$$

Proof. The proof is exactly that of Theorem 11. We have only to prove that $|x_2|\neq 1$ is always true, which can be done by a simple calculation.

From Theorems 11 and 11 a we deduce immediately

Theorem 12. *Let δ and σ be integers in $K(\sqrt{-m})$, where δ is assumed not* *to be a perfect square. Then the Diophantine equation (32) has only a finite number of classes of solutions. The fundamental solution in each class can be determined by a finite number of trials using the inequalities in Theorems 11 and 11 a.*

If $u^* + v^* \sqrt{\delta}$ *is the fundamental solution in the class* $\boldsymbol{K}$*, we find all the solutions* $u + v\sqrt{\delta}$ *in* $\boldsymbol{K}$ *by the formula*

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

where $x + y\sqrt{\delta}$ *runs through all the solutions of equation (33).*

A supplement to Theorems 11 and 11 a is given by

Theorem 13. *If* π *is a prime in the field* $\boldsymbol{K}(\sqrt{-m})$*, the Diophantine equation*

$$u^2 - \delta v^2 = \pi, \tag{40}$$

where δ *is an integer in* $\boldsymbol{K}(\sqrt{-m})$*, which is not a perfect square and such that* $|\delta| \geqq 6$*, has at most one solution* $u + v\sqrt{\delta}$ *in which* u *and* v *satisfy the inequalities (34) and (35).*

If equation (40) is solvable, it has one or two classes of solutions according as the prime π *divides* 2δ *or not.*

Proof. Suppose that $u + v\sqrt{\delta}$ and $u_1 + v_1\sqrt{\delta}$ are two solutions of (40) which satisfy the conditions in the first part of Theorem 13.

Eliminating δ between the equations

$$u^2 - \delta v^2 = \pi \quad \text{and} \quad u_1^2 - \delta v_1^2 = \pi, \tag{41}$$

we get

$$u^2 v_1^2 - u_1^2 v^2 = \pi (v_1^2 - v^2).$$

Thus

$$u v_1 \equiv \pm u_1 v \pmod{\pi} \tag{42}$$

for the upper or for the lower sign.

Further, on multiplying together equations (41) member by member we have

$$(u u_1 \mp \delta v v_1)^2 - \delta (u v_1 \mp u_1 v)^2 = \pi^2.$$

In the equation

$$\left(\frac{u u_1 \mp \delta v v_1}{\pi}\right)^2 - \delta \left(\frac{u v_1 \mp u_1 v}{\pi}\right)^2 = 1 \tag{43}$$

let us choose the sign so that the congruence (42) is satisfied. Then the two squares on the left-hand side in (43) are integers. If $u v_1 \mp u_1 v \neq 0$, we conclude from (43) that

$$|u v_1 \mp u_1 v| \geqq |y_1|\,|\pi|. \tag{44}$$

On the other hand, applying inequalities (34) and (35) we obtain, under the condition $|\delta| \geqq 6$,

$$|u v_1 \mp u_1 v| < |y_1|\,|\pi|,$$

which is contrary to (44). The remaining case is that $u v_1 \mp u_1 v = 0$, which is obviously possible only for $u = u_1$ and $v = v_1$. Thus the first part of Theorem 13 is proved.

Consequently, there are at most two classes of solution. Suppose that $u + v\sqrt{\delta}$ and $u - v\sqrt{\delta}$ are two solutions which satisfy inequalities (34) and (35). These solutions are associated if and only if π divides the two numbers $2uv$ and $u^2 + \delta v^2 = 2\delta v^2 - \pi$. Since v cannot be divisible by π, the numbers $2u$ and 2δ are divisible by π. But, if 2δ is divisible by π, so is $2u$. Thus, the necessary and sufficient condition for $u + v\sqrt{\delta}$ and $u - v\sqrt{\delta}$ to belong to the same class is that 2δ be a multiple of π. This proves the second part of the theorem.

BIBLIOGRAPHY

[1] T. Nagell, En elementær metode til å bestemme gitterpunktene på en hyperbel. Norsk Matematisk Tidskrift 26 (1944), 60—65.

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

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

[4] —— Introduction to Number Theory. Stockholm 1951, 195—204.

[5] L. Dirichlet, Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. Journal für Math. 19 and 21. Werke I, 578—588.

[6] R. Remak, Abschätzung der Lösung der Pellschen Gleichung im Anschluss an den Dirichletschen Existenzbeweis. Journal für Math. 143 (1913), 250—254.

[7] A. Stein, Die Gewinnung der Einheiten in gewissen relativquadratischen Zahlkörpern durch das J. Hurwitsche Kettenbruchvervahren. Journal für Math. 156 (1927), 69—92.

[8] A. Arwin, Einige periodische Kettenbruchentwicklungen. Journal für Math. 155 (1926), 111—128.

Tryckt den 11 april 1953

Uppsala 1953. Almqvist & Wiksells Boktryckeri AB