ARKIV FÖR MATEMATIK Band 2 nr 4

Communicated 12 September 1951 by F. CARLSON and T. NAGELL

On the solvability of the Diophantine equation $ax^2+by^2+cz^2=0$ in imaginary Euclidean quadratic fields

By OVE HEMER

§ 1. Introduction

LEGENDRE [1][1] has given the first proof of the following theorem:

Let a, b and c be three rational integers such that abc is square-free. Then the equation

$$ax^2+by^2+cz^2=0 \tag{1}$$

is solvable in rational integers x, y, z not all zero if and only if $-bc$, $-ca$, and $-ab$ are quadratic residues of a, b and c respectively, and a, b and c are not all of the same sign.

In DIRICHLET, Zahlentheorie [2], and in most other text-books of number theory, this theorem is proved by means of a method which we call the *index method*. See also T. NAGELL, Introduction to Number Theory [3].

Then the following question arises: In which algebraic fields is it possible to determine the necessary and sufficient conditions for the solvability of (1) by the index method?

An algebraic field is called *simple* when the number of ideal classes is $=1$. A simple field is said to be Euclidean when there is a Euclidean algorithm between every two integers α and β in the field, $\beta \neq 0$. See HARDY-WRIGHT: The Theory of Numbers [4].

The index method can only be applied to Euclidean fields, because it is based on an algorithm. In this paper we shall only consider the case of an imaginary Euclidean quadratic field. There are five such fields, namely $K(\sqrt{-1})$, $K(\sqrt{-2})$, $K(\sqrt{-3})$, $K(\sqrt{-7})$ and $K(\sqrt{-11})$.

In an imaginary field the condition "a, b and c not all of the same sign" has no meaning. We shall examine whether the other conditions are sufficient or not in these fields. TH. SKOLEM [5] has shown that they are in $K(\sqrt{-1})$ and $K(\sqrt{-3})$ but his method is rather different and we shall treat these fields too by means of the index method.

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

§ 2. Lemma from the theory of quadratic fields

We need some elementary results from the theory of quadratic fields. Let $K(\sqrt{m})$ be a quadratic field, m being a square-free rational integer. If ξ is a number in $K(\sqrt{m})$, we denote by ξ' its conjugate and by $N(\xi)=\xi\xi'$ its norm. In an imaginary field the norm is always positive (provided that $\xi \neq 0$) since $\xi\xi' = |\xi|^2$. If ξ is any integer in $K(\sqrt{m})$ the number of residue classes modulo ξ is $=|N(\xi)|$.

In the following we suppose that the field is a Euclidean imaginary field. Since these fields are simple, their arithmetic is analogous to that of the rational field. A prime π is of degree 1 if $N(\pi)=p$ and of degree 2 if $N(\pi)=p^2$, where p is associated with a rational prime. Hence primes of degree 2 are rational.

Let α and ξ be two relatively prime integers in $K(\sqrt{m})$. Then α is called a quadratic residue of the integer ξ if the congruence

$$x^2 \equiv \alpha \pmod{\xi}$$

is solvable in $K(\sqrt{m})$. Otherwise α is a quadratic non-residue of ξ.

If π is a prime in $K(\sqrt{m})$ which does not divide 2, α is a quadratic residue or a quadratic non-residue of π according as

$$\alpha^{\frac{1}{2}(N(\pi)-1)} \equiv 1 \pmod{\pi}$$

or

$$\alpha^{\frac{1}{2}(N(\pi)-1)} \equiv -1 \pmod{\pi}.$$

There are $\frac{1}{2}(N(\pi)-1)$ incongruent residues and as many incongruent non-residues modulo π. Further, if π is a divisor of 2, all integers prime to π are quadratic residues of π. See SOMMER: Vorlesungen über Zahlentheorie [6].

The integer ξ in $K(\sqrt{m})$ is said to be square-free if it is not divisible by the square of any prime in $K(\sqrt{m})$. If ξ is a square-free integer in $K(\sqrt{m})$, we conclude, exactly in the same manner as in the rational field, that α is a residue of ξ if and only if α is a residue of all the prime factors of ξ.

We prove the following

Lemma. *Let ξ be a square-free integer in $K(\sqrt{m})$ and let D be a rational integer which is prime to ξ. Then D is a quadratic non-residue of ξ if and only if ξ contains a prime factor π of degree 1 such that D is a quadratic non-residue of $N(\pi)$ in the rational field.*

Proof. Let π be a prime divisor of ξ such that D is a non-residue of π. Then, according to a remark above, π cannot be a divisor of 2. π can neither be a rational prime, for in this case $\pi > 2$ gives

$$D^{\frac{1}{2}(N(\pi)-1)} = D^{\frac{1}{2}(\pi^2-1)} = (D^{\pi-1})^{\frac{1}{2}(\pi+1)} \equiv 1 \pmod{\pi}.$$

If π is of degree 1, and if $N(\pi)=p$ is a rational prime >2, we have

$$D^{\frac{1}{2}(N(\pi)-1)} = D^{\frac{1}{2}(p-1)} \equiv -1 \pmod{\pi}.$$

Since D is rational, this implies

$$D^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}.$$

Hence D is a non-residue of p in the rational field. Inversely the last congruence immediately shows that if D is a non-residue of p in the rational field, it must also be a non-residue of π in $K(\sqrt{m})$. This proves the lemma.

Hence every rational integer is a quadratic residue of each square-free integer which contains no prime factors of degree 1 except divisors of 2.

It can be decided by the lemma, whether an arbitrary integer α is a residue or not of a prime π of degree 1, since there is always a rational integer D such that $\alpha \equiv D \pmod{\pi}$.

Example:

$$1 + \sqrt{-2} \equiv 1 - 16\sqrt{-2} \equiv 25 \equiv 8 \pmod{3 + 2\sqrt{-2}}.$$

Hence $1 + \sqrt{-2}$ is a residue of $3 + 2\sqrt{-2}$ in the field $K(\sqrt{-2})$.

For the investigation in this paper we only need this lemma.

If the integer α is not rational and p is an odd prime of degree 2, the lemma is not applicable to decide, whether α is a residue or not of p, for then we have no complete system of incongruent residues modulo p containing only rational integers. However, it is always easy to determine a complete system of residues and then examine, whether α is a residue or not of p.

Example:

$$2 + 5\sqrt{-7} \equiv -1 - \sqrt{-7} \equiv \frac{1 + \sqrt{-7}}{2} \pmod{3}.$$

A complete system of incongruent residues modulo 3 in $K(\sqrt{-7})$ is

$$0, \ \pm 1, \ \pm\frac{1 + \varepsilon\sqrt{-7}}{2}, \ \frac{3 + \varepsilon\sqrt{-7}}{2}, \ \varepsilon = 1 \text{ or } -1.$$

None of these integers is a solution of the congruence

$$x^2 \equiv \frac{1 + \sqrt{-7}}{2} \pmod{3}$$

and hence $2 + 5\sqrt{-7}$ is a non-residue of 3 in the field $K(\sqrt{-7})$.

The field $K(\sqrt{m})$ is Euclidean when the following proposition is true: If α and β are given integers in $K(\sqrt{m})$, $\beta \neq 0$, then there is an integer $\varkappa$ in $K(\sqrt{m})$ such that

$$\alpha = \varkappa \cdot \beta + \gamma$$

and

$$|N(\gamma)| < |N(\beta)|.$$

We shall now try to sharpen this inequality in imaginary fields.

If x_1 is a solution of the congruence

$$x^2 \equiv a \pmod{\xi}, \tag{2}$$

then every integer $x = x_1 + \varkappa \cdot \xi$, where $\varkappa$ is an arbitrary integer in $K(\sqrt{m})$, is a solution of (2). To find an upper bound of the norm of the least solution x_0 of (2) we distinguish the cases $m \not\equiv 1 \pmod 4$ and $m \equiv 1 \pmod 4$.

I. $m \not\equiv 1 \pmod 4$.

Then the integers are the numbers $u + v\sqrt{m}$, where u and v are arbitrary rational integers. The point-lattice corresponding to these integers shows easily that the lattice point of one integer x must fall inside of or on the boundary of a given rectangle for each ξ, whatever x_1 is. We get immediately that

$$|x_0| \leq \frac{|\xi|\sqrt{|m|}+1}{2}$$

i.e.

$$N(x_0) \leq \frac{|m|+1}{4} \cdot N(\xi) \tag{3}$$

II. $m \equiv 1 \pmod 4$.

Then we can write the integers $u + v\omega$, where $\omega = \frac{1+\sqrt{m}}{2}$, or what is the same thing $\frac{u+v\sqrt{m}}{2}$, $u \equiv v \pmod 2$. It is always possible to determine $\varkappa = u_1 + v_1\omega$ such that the lattice point of one integer x falls inside of or on the boundary of a given hexagon for each ξ, whatever x_1 is. This hexagon can be inscribed in a circle with its centre in the origin and we have

$$|x_0| \leq \frac{|\xi|}{4} \cdot \frac{|m|+1}{\sqrt{|m|}}$$

i.e.

$$N(x_0) \leq \frac{(|m|+1)^2}{16 \cdot |m|} \cdot N(\xi). \tag{4}$$

We can also easily see that the points in the plane which lie as far as possible from the nearest lattice point have the distance $\frac{\sqrt{|m|}+1}{2}$ and $\frac{|m|+1}{4\sqrt{|m|}}$ from this point in the cases I and II resp. This gives the same result.

§ 3. **Our problem and the index method.**

Let a, b and c be integers in the imaginary Euclidean quadratic field $K(\sqrt{m})$ such that

$$abc \text{ is square-free.} \tag{5}$$

Then it is necessary for the solvability of the equation

$$ax^2 + by^2 + cz^2 = 0 \tag{6}$$

in integers in $K(\sqrt{m})$, not all zero, that

(7) $-bc$, $-ca$ and $-ab$ are quadratic residues of a, b and c respectively.

A solution $[\xi, \eta, \zeta]$ of (6) is said to be *proper*, if $(\xi, \eta, \zeta) = 1$. It is clear that (6) either has proper solutions or has only the trivial solution [0, 0, 0]. If there are proper solutions of (6) we call the equation solvable.

It follows in exactly the same way as in the rational field that the postulate (5) is no limitation of the general case and that the conditions (7) are necessary.

Our problem is to decide, whether the conditions (7) are sufficient or not for the solvability of (6) in the imaginary Euclidean quadratic fields.

Range the terms in (6) so that

$$N(a) \leq N(b) \leq N(c).$$

Analogous to the proof of Legendre's theorem in the rational field we then define the index I of the equation (6) as

$$I = N(a)\,N(c) = N(ac).$$

We shall prove the following proposition.

Theorem. *If the index I of* (6) *is greater than a certain number and if the conditions* (7) *are satisfied, then it is always possible to derive a new equation*

$$AX^2 + BY^2 + CZ^2 = 0 \tag{8}$$

where, analogous to (5) *and* (7), *ABC is square-free and $-BC$, $-CA$ and $-AB$ are quadratic residues of A, B and C respectively, where the index is less than I and where* (6) *and* (8) *are solvable or not at the same time.*

The notions in the proof are the same as in [3]. The congruence

$$x^2 \equiv -ab \pmod{c}$$

has solutions by (7). Let x be a solution of this congruence. Since $(a, c) = 1$, we can always find an integer y such that $x \equiv ay \pmod{c}$. Hence we have

$$ay^2 \equiv -b \pmod{c}.$$

Thus we can always find integers r and Q such that

$$ar^2 + b = cQ. \tag{9}$$

Then

$$|Q| \leq \left|\frac{ar^2}{c}\right| + 1$$

and according to (3) and (4) we get in imaginary Euclidean quadratic fields

if $m \not\equiv 1 \pmod 4$

$$|Q| \leq |ac| \cdot \frac{|m|+1}{4} + 1 < |ac| = \sqrt{I}$$

(10)

$$\text{if } |ac| > \frac{4}{3-|m|}$$

and if $m \equiv 1 \pmod 4$

$$|Q| \leq |ac| \cdot \frac{(|m|+1)^2}{16 \cdot |m|} + 1 < |ac| = \sqrt{I}$$

(11)

$$\text{if } |ac| > \frac{16 \cdot |m|}{16|m| - (|m|+1)^2}.$$

Hence we can determine r so that $N(Q) < I$ if I is great enough. Of course it is not necessary that $N(r) < N(c)$, if we only get $N(Q) < I$.

$Q = 0$ gives $ar^2 + b = 0$ and (6) has the solution $[r, 1, 0]$.

According to (5) a, b and r are units.

If $Q \neq 0$ the derived equation (8) is determined by the following definitions.

$$A = (ar^2, b, cQ)$$

where by the postulate (5) A is square-free and r and Q are divisible by A. Put

$$r = A\alpha, \quad b = A\beta, \quad Q = AC\gamma^2,$$

where C is square-free. Substitution in (9) gives

$$aA\alpha^2 + \beta = cC\gamma^2 \tag{12}$$

where the three terms are relatively prime in pairs. Finally we put

$$a\beta = B$$

which gives $AB = ab$. Hence B is square-free and $(A, B) = 1$. According to (12) we have

$$(C, aA\beta) = (C, AB) = 1.$$

Thus ABC is square-free.

It follows from (12) that $-aA\beta = -AB$ is a quadratic residue of C and further that βcC is a residue of A. Since $-ac$ is a residue of b and therefore of A we have that

$$(-ac)(\beta cC) = -a\beta c^2 C = -BCc^2$$

is a residue of A. Hence $-BC$ is a residue of A. Further (12) gives that $aAcC$ is a residue of β and from $-ac$ a residue of β follows $-AC$ a residue of β. (12) also gives βcC a residue of a and, since $-bc$ is a residue of a,

$$(-bc)(\beta cC) = -b\beta c^2 C = -AC(\beta c)^2$$

is a residue of a. Thus $-AC$ is a residue of a and of β and, since $(a, \beta) = 1$, this gives that $-AC$ is a residue of $a\beta = B$.

Hitherto we have made almost no alterations of the proof in the rational field. It is, however, not immediately possible in $K(\sqrt{m})$ to infer that the index of (8) will be less than the index I of (6) if $N(Q) < I$. The analogous conclusion in the rational field is based upon the observation that

$$|b| < |c| \quad \text{if } I > 1$$

but in $K(\sqrt{m})$ we must take the eventuality

$$N(b) = N(c)$$

into consideration, because b and c may be conjugates. If $I > 1$ we can suppose

$$N(a) < N(c)$$

for if $N(a) = N(c)$ we have $c = \varepsilon a'$, where ε is a unit and a' is the conjugate of a. But then, against (5), we cannot have at the same time $(a, b) = 1$ and $(b, c) = 1$.

Suppose

$$N(a) < N(b) = N(c).$$

Then $N(AB) = I$ and $N(AC) \leq N(Q) < I$ give

$$N(C) < N(B).$$

Moreover $AB = ab$, $N(b) > 1$ and $c = \varepsilon b'$ imply $N(A) \neq N(B)$ and hence the two greatest norms of the coefficients in (8) are different.

If $N(A) > N(C)$ the index of (8) is less than I.

If $N(A) \leq N(C)$ we get the same index I in (8) but a repeated procedure by the same method on (8) gives certainly a new equation with less index, if I exceeds the given number.

To prove the last part of the theorem we make the same substitution in (6) as in the proof in the rational field.

$$\begin{aligned} x &= A\alpha X - \beta Y \\ y &= X + a\alpha Y \\ z &= C\gamma Z \end{aligned} \tag{13}$$

and this gives, according to (9) and (12),

$$ax^2 + by^2 + cz^2 = cC\gamma^2(AX^2 + BY^2 + CZ^2).$$

If $[X, Y, Z]$ is a proper solution of (8), then (6) has a proper solution, for otherwise

$$(\beta + A a \alpha^2)\, Y = c C \gamma^2\, Y = 0$$

as follows from (13) by elimination of X, and $c C \gamma^2 \neq 0$. Hence $x = y = z = 0$ implies $X = Y = Z = 0$.

If (8) has no proper solutions, i.e. $X = Y = Z = 0$, then the same applies to (6), for as

$$\begin{vmatrix} A\alpha & -\beta \\ 1 & a\alpha \end{vmatrix} = c C \gamma^2 \neq 0$$

we get from (13)

$$X = \frac{a\alpha x + \beta y}{c C \gamma^2} = 0$$

$$Y = \frac{-x + A\alpha y}{c C \gamma^2} = 0$$

$$Z = \frac{z}{C\gamma} = 0.$$

Hence, by elimination of x,

$$(\beta + a A \alpha^2)\, y = 0$$

and we can only have $x = y = z = 0$.

Then all parts of the theorem are proved.

According to (13) we can always find a solution of (6) if we know a solution of (8).

By this theorem all equations (6) in the rational field correspond to either the equation $x^2 + y^2 - z^2 = 0$ or to the equation $x^2 + y^2 + z^2 = 0$. The conditions (7) are not sufficient in the rational field, because no equations (6) corresponding to $x^2 + y^2 + z^2 = 0$ have proper solutions. It is easy to see that this restriction and the more practical "a, b and c not of the same sign" are equivalent.

In §§ 4–8 we shall decide if the conditions (7) are sufficient or not in the five imaginary Euclidean fields by examining the equations with less index than the number given by (10) or (11). Then it is clear that the two conjugated equations

$$a x^2 + b y^2 + c z^2 = 0$$

and

$$a' x^2 + b' y^2 + c' z^2 = 0$$

have or have not solutions at the same time, for if one of them has the solution $[\xi, \eta, \zeta]$, then the other one has the solution $[\xi', \eta', \zeta']$.

§ 4. The field $K(\sqrt{-1})$.

Since $m \not\equiv 1 \pmod 4$ the integers are the numbers $u + vi$. where u and v are rational integers.

The units are ± 1 and $\pm i$.

The integers εn, where ε is a unit, are associates.

The primes are $1+i$, all rational primes $\equiv -1 \pmod 4$ and the conjugated factors of all rational primes $\equiv 1 \pmod 4$ and the associates of all these integers.

From (10) follows that

$$N(Q) < I \quad \text{if} \quad I > 4.$$

Then, by the theorem, all equations (6) which satisfy (5) and (7) can be substituted by equations (8) with $I \leq 4$ and for the rest with the same properties. We then only have to examine the solvability of these equations.

It is enough to consider $I=1$ and 2, for $I=3$ is impossible, because I is the norm of the integer ac. Since $N(a) < N(c)$, $I=4$ implies $N(c)=4$ and $c=\varepsilon \cdot 2$, but $2=-i(1+i)^2$ is divisible by a square against the postulates in (5). Since -1 is a square, we have to find the solutions of a few number of equations.

$I=1$.

$$x^2 + y^2 + \varepsilon z^2 = 0. \tag{14}$$

has the solution $[1, i, 0]$.

$I=2$.

$$x^2 + y^2 + \varepsilon(1+i) z^2 = 0 \tag{15}$$

has the solution $[1, i, 0]$ and

$$x^2 + iy^2 + (1+i) z^2 = 0 \tag{16}$$

has the solution $[1, 1, i]$.

Hence the conditions (7) are sufficient in the field $K(\sqrt{-1})$.

§ 5. The field $K(\sqrt{-2})$.

The integers are the numbers $u + v\sqrt{-2}$, where u and v are rational integers.

The units are ± 1.

The primes are $\sqrt{-2}$, all rational primes $\equiv 5$ or $7 \pmod 8$ and the conjugated factors of all rational primes $\equiv 1$ or $3 \pmod 8$ and the associates of these integers.

(10) gives

$$N(Q) < I \quad \text{if} \quad I > 16.$$

Then we have to examine the equations (6) with $I \leq 16$, but for each I we can determine a number γ such that

$$N(Q) < I \quad \text{if} \quad N(b) < \gamma \cdot N(c).$$

From (9) we obtain the sharpened inequality

$$|Q| \leq \frac{|a| \cdot |r^2|}{|c|} + \frac{|b|}{|c|}.$$

and hence, according to (10), we get γ in $K(\sqrt{-2})$ from

$$\frac{3}{4}\sqrt{I} + \sqrt{\gamma} = \sqrt{I}$$

$$\text{i.e. } \gamma = \frac{I}{16}.$$

Thus we only need consider the equations where

$$N(b) \geq \frac{I}{16} N(c).$$

According to (5) and since I is a norm, we only have to examine $I = 1, 2, 3, 6, 9$ and 11.

$I = 1$.

(17) $x^2 + y^2 + z^2 = 0$. Solution $[1, 1, \sqrt{-2}]$.

(18) $x^2 - y^2 + z^2 = 0$. Solution $[1, 1, 0]$.

$I = 2$.

(19) $x^2 + y^2 + \varepsilon\sqrt{-2}\, z^2 = 0$. Solution $[1 + \varepsilon\sqrt{-2}, 1, \varepsilon\sqrt{-2}]$.

(20) $x^2 - y^2 + \varepsilon\sqrt{-2}\, z^2 = 0$. Solution $[1, 1, 0]$.

$I = 3$.

$$a = 1, \; c = \pm(1 + \varepsilon\sqrt{-2}). \quad N(b) = 1, 2 \text{ or } 3.$$

1) $N(b) = 1$. $b = \pm 1$.

-1 is a non-residue of $1 + \varepsilon\sqrt{-2}$ in $K(\sqrt{-2})$ by the lemma, since -1 is a non-residue of 3 in the rational field.

Then we only have

(21) $$x^2 - y^2 + cz^2 = 0$$

with the solution $[1, 1, 0]$.

2) $N(b) = 2$, $b = \pm\sqrt{-2}$.

$$\varepsilon\sqrt{-2} \equiv -1 \pmod{1 + \varepsilon\sqrt{-2}}$$ and hence a non-residue.

The remaining equations are

(22) $$x^2 + \varepsilon\sqrt{-2}\, y^2 + (1 + \varepsilon\sqrt{-2})\, z^2 = 0$$

with the solution $[1-\varepsilon\sqrt{-2}, 1, 1]$, and

$$x^2+\varepsilon\sqrt{-2}\,y^2-(1+\varepsilon\sqrt{-2})\,z^2=0 \tag{23}$$

with the solution $[1, 1, 1]$.

3) $N(b)=3$. $b=\pm(1-\sqrt{-2})$. $c=\pm(1+\sqrt{-2})$.

$1-\varepsilon\sqrt{-2}\equiv 2\equiv -1 \pmod{1+\varepsilon\sqrt{-2}}$ and hence a non-residue.

Then we only have

$$x^2+(1-\sqrt{-2})\,y^2+(1+\sqrt{-2})\,z^2=0 \tag{24}$$

with the solution $[\sqrt{-2}, 1, 1]$.

$I=6$.

1) $N(a)=1$. $N(c)=6$. $\gamma\cdot N(c)=\dfrac{6\cdot 6}{16}>2$.

Thus we need consider $N(b)\geq 3$ and then only

$N(b)=3$ is possible, i.e. $a=1$, $b=\pm(1+\varepsilon\sqrt{-2})$ and
$c=\pm\sqrt{-2}\,(1-\varepsilon\sqrt{-2})=\pm(2+\varepsilon\sqrt{-2})$.
$1+\varepsilon\sqrt{-2}$ is a non-residue of $1-\varepsilon\sqrt{-2}$ and hence of $2+\varepsilon\sqrt{-2}$.
$-(2+\varepsilon\sqrt{-2})\equiv -1 \pmod{1+\varepsilon\sqrt{-2}}$ and thus a non-residue.

Then we only have

$$x^2+(1+\varepsilon\sqrt{-2})\,y^2-(2+\varepsilon\sqrt{-2})\,z^2=0. \tag{25}$$

with the solution $[1, 1, 1]$.

2) $N(a)=2$, $N(c)=3$ and hence $N(b)=3$.

$$a=\sqrt{-2},\ b=\pm(1-\sqrt{-2}),\ c=\pm(1+\sqrt{-2}).$$

As $-(2+\varepsilon\sqrt{-2})$ is a non-residue of $1+\varepsilon\sqrt{-2}$, we only have

$$\sqrt{-2}\,x^2-(1-\sqrt{-2})\,y^2+(1+\sqrt{-2})\,z^2=0 \tag{26}$$

with the solution $[\sqrt{-2}, 1, 1]$.

$I = 9.$

$N(a) < N(c)$, hence $N(a) = 1$, $N(c) = 9$.

$\gamma \cdot N(c) = \frac{9 \cdot 9}{16} > 5$. Thus, $N(b) = 6$ or 9, but both these values contradict the postulate (5).

$I = 11.$

$N(a) = 1$, $N(c) = 11$, $\gamma \cdot N(c) = \frac{11 \cdot 11}{16} > 7$. $N(b) = 9$ or 11.

1) $N(b) = 9$. $b = \pm 3$. $c = \pm (3 + \varepsilon\sqrt{-2})$.

$\pm (3 \pm \sqrt{-2}) \equiv \varepsilon\sqrt{-2} \equiv -1 \pmod{1 + \varepsilon\sqrt{-2}}$ and then a non-residue of 3 in $K(\sqrt{-2})$ by the lemma.

Hence no equations satisfy the conditions (7).

2) $N(b) = 11$. $b = \pm (3 - \sqrt{-2})$, $c = \pm (3 + \sqrt{-2})$.

$3 - \varepsilon\sqrt{-2} \equiv 6 \pmod{3 + \varepsilon\sqrt{-2}}$ are non-residues by the lemma. Then only one equation remains.

$$x^2 + (3 - \sqrt{-2})\, y^2 + (3 + \sqrt{-2})\, z^2 = 0 \tag{27}$$

has the solution $[\sqrt{-2},\ 1 + \sqrt{-2},\ 1 - \sqrt{-2}]$.

Hence the conditions (7) are sufficient in the field $K(\sqrt{-2})$.

§ 6. The field $K(\sqrt{-3})$.

The integers are all the numbers $\frac{u + v\sqrt{-3}}{2}$, where $u \equiv v \pmod 2$ and u and v are rational integers.

The units are ± 1, $\pm \varrho$ and $\pm \varrho^2$, where $\varrho = \frac{-1 + \sqrt{-3}}{2}$.

The primes are $\sqrt{-3}$, all rational primes $\equiv 2 \pmod 3$ and the conjugated factors of all rational primes $\equiv 1 \pmod 3$ and the associates of these integers.

(11) gives

$$N(Q) < I \quad \text{if} \quad I > 2.$$

Since 2 is a prime in $K(\sqrt{-3})$, we only need consider $I = 1$.

$I=1$.

Since ϱ^2 and $\varrho=(\varrho^2)^2$ are squares, we only have

(28) $x^2-y^2+z^2=0$. Solution [1, 1, 0].

(29) $x^2+y^2+z^2=0$. Solution $[1, \varrho, \varrho^2]$.

Hence the conditions (7) are sufficient in the field $K(\sqrt{-3})$.

§ 7. The field $K(\sqrt{-7})$.

The integers are all the numbers $\frac{u+v\sqrt{-7}}{2}$, where $u\equiv v \pmod 2$ and u and v are rational integers.

The units are ± 1.

The primes are $\sqrt{-7}$, $\frac{1+\varepsilon\sqrt{-7}}{2}$, all rational primes $\equiv 3, 5, 13 \pmod{14}$ and the conjugated factors of all rational primes $\equiv 1, 9, 11 \pmod{14}$ and the associates of these integers.

We can also write the integers $u+v\omega$, where $\omega=\frac{-1+\sqrt{-7}}{2}$ or another of the four numbers with the norm 2.

(11) gives

$$N(Q)<I \quad \text{if} \quad I>5.$$

$\frac{4\sqrt{I}}{7}+\sqrt{\gamma}=\sqrt{I}$ gives $\gamma=\frac{9I}{49}$, analogous to the determination in § 5. As 3 and 5 are primes, we only need consider $I=1$, 2 and 4 and $N(b)\geq\frac{9I}{49}\cdot N(c)$.

$I=1$.

(30) $x^2-y^2+z^2=0$. Solution [1, 1, 0].

The remaining equation

(31) $$x^2+y^2+z^2=0$$

has no solutions but the trivial [0, 0, 0], for suppose that we have the proper solution $[u_1+v_1\omega,\ u_2+v_2\omega,\ u_3+v_3\omega]$, where $\omega=\frac{-1+\sqrt{-7}}{2}$.

Then substitution in (31) gives

(a) $$\sum_{i=1}^{3}u_i^2-\sum_{i=1}^{3}u_iv_i-\tfrac{3}{2}\sum_{i=1}^{3}v_i^2=0$$

(b) $$\sum_{i=1}^{3}u_iv_i-\tfrac{1}{2}\sum_{i=1}^{3}v_i^2=0.$$

We get $\sum_{i=1}^{3} v_i^2 \equiv 0 \pmod 2$ and hence

$$\sum_{i=1}^{3} u_i^2 = 2 \sum_{i=1}^{3} v_i^2 \equiv 0 \pmod 4.$$

This gives $u_1 \equiv u_2 \equiv u_3 \equiv 0 \pmod 2$.

But then, according to (b)

$$\sum_{i=1}^{3} v_i^2 \equiv 0 \pmod 4 \text{ and } v_1 \equiv v_2 \equiv v_3 \equiv 0 \pmod 2.$$

This contradicts the postulate that the solution is proper and hence (31) is insolvable.

$I = 2$.

$N(a) = 1$, $N(c) = 2$, $N(b) = 1$ or 2.

1) $N(b) = 1$.

(32) $$x^2 - y^2 + cz^2 = 0$$

has the solution [1, 1, 0].

(33) $$x^2 + y^2 + \frac{1 + \varepsilon\sqrt{-7}}{2} z^2 = 0$$

has the solution $\left[1, \frac{1 - \varepsilon\sqrt{-7}}{2}, 1\right]$.

The remaining equations

(34) $$x^2 + y^2 - \frac{1 + \varepsilon\sqrt{-7}}{2} z^2 = 0$$

correspond to (31) and hence they are insolvable by the theorem. This follows, if we don't take the least solution $r = 1$ but the greater $r = \frac{1 - \varepsilon\sqrt{-7}}{2}$, $Q = 1$ of (9). Then $A = (ar^2, b, cQ) = 1$, $B = 1$ and $C = 1$.

The insolvability of (34) can also easily be shown by congruences.

2) $N(b) = 2$.

(35) $$x^2 - \frac{1 - \sqrt{-7}}{2} y^2 - \frac{1 + \sqrt{-7}}{2} z^2 = 0$$

has the solution [1, 1, 1].

The three remaining equations are all insolvable in $K(\sqrt{-7})$, because they correspond to (31).

(36) $$x^2 + \frac{1 - \sqrt{-7}}{2} y^2 + \frac{1 + \sqrt{-7}}{2} z^2 = 0$$

gives the derived equation $X^2 + \frac{1-\sqrt{-7}}{2} Y^2 - \frac{1+\sqrt{-7}}{2} Z^2 = 0$, one of the equations (37), if we take the solution $r=1$, $Q=-\frac{1+\sqrt{-7}}{2}$ of (9).

$$x^2 - \frac{1+\varepsilon\sqrt{-7}}{2} y^2 + \frac{1-\varepsilon\sqrt{-7}}{2} z^2 = 0 \tag{37}$$

can be substituted by (34), if we take the solution $r=1$, $Q=1$ of (9), and (34) are insolvable.

$I=4$.

$N(a)=1$, $N(c)=4$, $\gamma \cdot N(c)=\frac{9\cdot 4\cdot 4}{49} > 2$.

$N(b)=3$ is impossible and $N(b)=4$ is against the postulate (5).

The conditions (7) are not sufficient in the field $K(\sqrt{-7})$. As in $K(1)$ we must make the restriction that all the equations corresponding to $x^2+y^2+z^2=0$ are insolvable.

The following 28 equations with $I<22$ satisfy the conditions in the problem but are insolvable, because they correspond to $x^2+y^2+z^2=0$.

$$x^2 + y^2 + z^2 = 0$$

$$x^2 + y^2 - \frac{1+\varepsilon\sqrt{-7}}{2} z^2 = 0$$

$$x^2 + \frac{1-\varepsilon\sqrt{-7}}{2} y^2 - \frac{1+\varepsilon\sqrt{-7}}{2} z^2 = 0$$

$$x^2 + \frac{1-\sqrt{-7}}{2} y^2 + \frac{1+\sqrt{-7}}{2} z^2 = 0$$

$$x^2 + y^2 + 2z^2 = 0$$

$$x^2 - \frac{1+\varepsilon\sqrt{-7}}{2} y^2 + \varepsilon\sqrt{-7}\, z^2 = 0$$

$$x^2 - 2y^2 + \varepsilon\sqrt{-7}\, z^2 = 0$$

$$x^2 - 2y^2 + 3z^2 = 0$$

$$x^2 - 2y^2 - 3z^2 = 0$$

$$x^2 + 2y^2 + 3z^2 = 0$$

$$x^2 + y^2 - 3z^2 = 0$$

$$x^2 - \frac{1+\varepsilon\sqrt{-7}}{2} y^2 - (2+\varepsilon\sqrt{-7})\, z^2 = 0$$

$$x^2 + 2y^2 - (2 + \varepsilon\sqrt{-7})\,z^2 = 0$$

$$x^2 - \frac{1 + \varepsilon\sqrt{-7}}{2}\,y^2 + \frac{7 + \varepsilon\sqrt{-7}}{2}\,z^2 = 0$$

$$x^2 - (2 + \varepsilon\sqrt{-7})\,y^2 + \frac{7 - \varepsilon\sqrt{-7}}{2}\,z^2 = 0$$

$$x^2 + y^2 + \frac{3(1 + \varepsilon\sqrt{-7})}{2}\,z^2 = 0$$

$$x^2 + \varepsilon\sqrt{-7}\,y^2 + \frac{3(1 + \varepsilon\sqrt{-7})}{2}\,z^2 = 0$$

$$\frac{1 - \sqrt{-7}}{2}\,x^2 + \frac{1 + \sqrt{-7}}{2}\,y^2 + 3z^2 = 0$$

$\varepsilon = 1$ or -1.

Then each equation (6) which by reduction with the index method to $I < 22$ gives one of these 28 equations, is insolvable. This we also can say immediately about every equation with rational coefficients all of the same sign which satisfies the conditions (7) in the rational field, for $K(\sqrt{-7})$ contains $K(1)$ and hence such an equation corresponds to $x^2 + y^2 + z^2 = 0$. However, all equations with rational coefficients of the same sign are not insolvable. For instance, $x^2 + y^2 + 3z^2 = 0$ has the solution $\left[\frac{1 - \sqrt{-7}}{2}, \frac{1 + \sqrt{-7}}{2}, 1\right]$, but then the conditions (7) are not satisfied in the rational field.

§ 8. The field $K(\sqrt{-11})$.

The integers are all the numbers $\frac{u + v\sqrt{-11}}{2}$, where $u \equiv v \pmod 2$ and u and v are rational integers.

The units are ± 1.

The primes are $\sqrt{-11}$, 2, all the rational primes $\equiv 7, 13, 17, 19, 21 \pmod{22}$ and the conjugated factors of all the rational primes $\equiv 1, 3, 5, 9, 15 \pmod{22}$ and the associates of these integers.

(11) gives

$$N(Q) < I \quad \text{if} \quad I > 30.^1$$

As in $K(\sqrt{-2})$ and $K(\sqrt{-7})$ we get

$$\frac{9}{11}\sqrt{I} + \sqrt{\gamma} = \sqrt{I} \quad \text{and} \quad \gamma = \frac{4I}{121}.$$

[1] The inequalities in [4] § 14.7 give only $N(Q) < I$ if $I > 256$.

According to the postulate (5) we then have to examine

$$I = 1,\ 3,\ 4,\ 5,\ 9,\ 11,\ 12,\ 15,\ 20,\ 23 \text{ and } 25 \text{ and } N(b) \geq \frac{4I}{121} \cdot N(c).$$

$I = 1$.

(38) $\quad x^2 - y^2 + z^2 = 0$. Solution [1, 1, 0].

(39) $\quad x^2 + y^2 + z^2 = 0$. Solution $\left[1,\ \frac{3 - \sqrt{-11}}{2},\ \frac{3 + \sqrt{-11}}{2}\right]$.

$I = 3$.

$N(a) = 1,\ N(c) = 3,\ N(b) = 1$ or 3.

1) $N(b) = 1,\ b = \pm 1,\ c = \pm \frac{1 + \varepsilon\sqrt{-11}}{2}$.

-1 is a non-residue of $\frac{1 + \varepsilon\sqrt{-11}}{2}$ by the lemma. Then we only have

(40) $$x^2 - y^2 + cz^2 = 0$$

with the solution [1, 1, 0].

2) $N(b) = 3,\ b = \pm \frac{1 - \sqrt{-11}}{2},\ c = \pm \frac{1 + \sqrt{-11}}{2}$.

$-\frac{1 - \varepsilon\sqrt{-11}}{2} \equiv -1 \left(\text{mod } \frac{1 + \varepsilon\sqrt{-11}}{2}\right)$ and hence non-residues.

(41) $$x^2 - \frac{1 - \sqrt{-11}}{2} y^2 - \frac{1 + \sqrt{-11}}{2} z^2 = 0$$

has the solution [1, 1, 1].

$I = 4$.

$N(a) = 1,\ N(c) = 4,\ N(b) = 1$ or 3.

1) $N(b) = 1,\ b = \pm 1,\ c = \pm 2$.

(42) $\quad x^2 - y^2 \pm 2z^2 = 0$. $\quad$ Solution [1, 1, 0].

(43) $\quad x^2 + y^2 - 2z^2 = 0$. $\quad$ Solution [1, 1, 1].

(44) $\quad x^2 + y^2 + 2z^2 = 0$. $\quad$ Solution [3, $\sqrt{-11}$, 1].

2) $N(b) = 3,\ b = \pm \frac{1 + \varepsilon\sqrt{-11}}{2},\ c = \pm 2$.

$2 \equiv -1 \left(\text{mod } \frac{1 + \varepsilon\sqrt{-11}}{2}\right)$ is a non-residue.

(45) $$x^2 + \frac{1+\varepsilon\sqrt{-11}}{2} y^2 + 2z^2 = 0.$$

has the solution $\left[\frac{1-\varepsilon\sqrt{-11}}{2}, 1, 1\right]$.

(46) $$x^2 - \frac{1+\varepsilon\sqrt{-11}}{2} y^2 + 2z^2 = 0$$

has the solution $\left[1, \frac{1+\varepsilon\sqrt{-11}}{2}, \frac{1-\varepsilon\sqrt{-11}}{2}\right]$

$I = 5$.

$N(a) = 1$, $N(c) = 5$. $N(b) = 1, 3, 4$ or 5.

1) $N(b) = 1$. $b = \pm 1$. $c = \pm \frac{3+\varepsilon\sqrt{-11}}{2}$

(47) $$x^2 - y^2 + cz^2 = 0$$

has the solution $[1, 1, 0]$.

(48) $$x^2 + y^2 + \frac{3+\varepsilon\sqrt{-11}}{2} z^2 = 0$$

has the solution $\left[1, \frac{1-\varepsilon\sqrt{-11}}{2}, 1\right]$.

(49) $$x^2 + y^2 - \frac{3+\varepsilon\sqrt{-11}}{2} z^2 = 0$$

has the solution $\left[2, \frac{1+\varepsilon\sqrt{-11}}{2}, 1\right]$

2) $N(b) = 3$. $b = \pm \frac{1+\varepsilon\sqrt{-11}}{2}$

$$-\frac{3+\varepsilon\sqrt{-11}}{2} \equiv -1 \left(\mathrm{mod}\ \frac{1+\varepsilon\sqrt{-11}}{2}\right)$$

$$\frac{3-\varepsilon\sqrt{-11}}{2} \equiv 2 \equiv -1 \left(\mathrm{mod}\ \frac{1+\varepsilon\sqrt{-11}}{2}\right)$$

$$\frac{1+\varepsilon\sqrt{-11}}{2} \equiv 2 \left(\mathrm{mod}\ \frac{3-\varepsilon\sqrt{-11}}{2}\right)$$

and $$-\frac{1+\varepsilon\sqrt{-11}}{2} \equiv -2 \left(\mathrm{mod}\ \frac{3-\varepsilon\sqrt{-11}}{2}\right)$$

are all non-residues by the lemma. Then only two types remain

$$x^2 + \frac{1+\varepsilon\sqrt{-11}}{2}y^2 - \frac{3+\varepsilon\sqrt{-11}}{2}z^2 = 0 \tag{50}$$

with the solution [1, 1, 1].

$$x^2 - \frac{1+\varepsilon\sqrt{-11}}{2}y^2 - \frac{3+\varepsilon\sqrt{-11}}{2}z^2 = 0 \tag{51}$$

with the solution $\left[\frac{3-\varepsilon\sqrt{-11}}{2}, 1, \frac{1-\varepsilon\sqrt{-11}}{2}\right]$.

3) $N(b)=4$. $b=\pm 2$.

± 2 are non-residues of $\frac{3+\varepsilon\sqrt{-11}}{2}$ by the lemma, and hence no equations satisfy the conditions (7).

4) $N(b)=5$. $b=\pm\frac{3-\sqrt{-11}}{2}$, $c=\pm\frac{3+\sqrt{-11}}{2}$.

$\pm\frac{3-\sqrt{-11}}{2}\equiv\pm 3 \left(\mathrm{mod}\ \frac{3+\sqrt{-11}}{2}\right)$ are non-residues by the lemma, and no equations satisfy the conditions (7).

$I=9$.

$N(a)=1$, $N(c)=9$, $\gamma\cdot N(c)=\frac{4\cdot 81}{121}>2$.

We only have to determine $N(b)=4$ and 5.

1) $N(b)=4$. $b=\pm 2$, $c=\pm 3$.

2 is a non-residue of 3.

Further we have

$$x^2 + 2y^2 - 3z^2 = 0. \qquad \text{Solution } [1, 1, 1]. \tag{52}$$

$$x^2 + 2y^2 + 3z^2 = 0. \qquad \text{Solution } [5, 2, \sqrt{-11}]. \tag{53}$$

2) $N(b)=5$. $b=\pm\frac{3+\varepsilon\sqrt{-11}}{2}$.

± 3 are non-residues of $\frac{3+\varepsilon\sqrt{-11}}{2}$ and no equations satisfy the conditions (7).

$I=11.$

$N(a)=1,\ N(c)=11,\ \gamma\cdot N(c)=4.$

$N(b)=4,\ 5$ and 9 must be examined.

1) $N(b)=4,\ b=\pm 2,\ c=\pm\sqrt{-11}.$

2 is a non-residue of $\sqrt{-11}$ by the lemma.

(54) $$x^2+2y^2+\varepsilon\sqrt{-11}z^2=0$$

has the solution $\left[\frac{5+\varepsilon\sqrt{-11}}{2},\ 1,\ \frac{1+\varepsilon\sqrt{-11}}{2}\right].$

2) $N(b)=5.\ \ b=\pm\frac{3+\varepsilon\sqrt{-11}}{2}.\ \ c=\pm\sqrt{-11}.$

$$\varepsilon\sqrt{-11}\equiv -3\ \left(\mathrm{mod}\ \frac{3+\varepsilon\sqrt{-11}}{2}\right)$$

and $\varepsilon\sqrt{-11}\equiv 3\ \left(\mathrm{mod}\ \frac{3-\varepsilon\sqrt{-11}}{2}\right).$

They are all non-residues by the lemma and no equations satisfy the conditions (7).

3) $N(b)=9.\ \ b=\pm 3,\ c=\pm\sqrt{-11}.$

$\varepsilon\sqrt{-11}\equiv -1\ \left(\mathrm{mod}\ \frac{1+\varepsilon\sqrt{-11}}{2}\right)$, and hence non-residues of 3 by the lemma. No equations satisfy the conditions (7).

$I=12.$

I. $N(a)=1,\ N(c)=12,\ \gamma\cdot N(c)=\frac{4\cdot 144}{121}>4.$

$N(b)=5$ and 11 must be examined.

1) $N(b)=5.\ \ b=\pm\frac{3\pm\sqrt{-11}}{2},\ \ c=\pm(1\pm\sqrt{-11}).$

$\pm(1+\varepsilon\sqrt{-11})\equiv\mp 2\ \left(\mathrm{mod}\ \frac{3+\varepsilon\sqrt{-11}}{2}\right)$ and hence non-residues by the lemma.

$\frac{3-\varepsilon\sqrt{-11}}{2}\equiv 2\ \left(\mathrm{mod}\ \frac{1+\varepsilon\sqrt{-11}}{2}\right)$ and then a non-residue of $1+\varepsilon\sqrt{-11}$ by the lemma.

Thus we only have

$$x^2 + \frac{3+\varepsilon\sqrt{-11}}{2}y^2 + (1-\varepsilon\sqrt{-11})z^2 = 0 \tag{55}$$

with the solution $\left[\frac{1+\varepsilon\sqrt{-11}}{2}, 1, 1\right]$.

$$x^2 + \frac{3+\varepsilon\sqrt{-11}}{2}y^2 - (1-\varepsilon\sqrt{-11})z^2 = 0 \tag{56}$$

with the solution $\left[\frac{3-\varepsilon\sqrt{-11}}{2}, 1, 1\right]$.

2) $N(b)=11$. $b=\pm\sqrt{-11}$, $c=\pm(1\pm\sqrt{-11})$.

$\varepsilon\sqrt{-11} \equiv -1 \pmod{1+\varepsilon\sqrt{-11}}$

and $-(1+\varepsilon\sqrt{-11}) \equiv -1 \pmod{\sqrt{-11}}$

are non-residues by the lemma. Then we only have

$$x^2 + \varepsilon\sqrt{-11}\,y^2 - (1+\varepsilon\sqrt{-11})z^2 = 0 \tag{57}$$

with the solution [1, 1, 1].

II. $N(a)=3$, $N(c)=4$ and hence $N(b)=3$.

$$a=\pm\frac{1-\sqrt{-11}}{2},\quad b=\pm\frac{1+\sqrt{-11}}{2},\quad c=2.$$

$1+\varepsilon\sqrt{-11} \equiv 2 \left(\mathrm{mod}\ \frac{1-\varepsilon\sqrt{-11}}{2}\right)$ and hence a non-residue. Only one equation remains

$$\frac{1-\sqrt{-11}}{2}x^2 + \frac{1+\sqrt{-11}}{2}y^2 + 2z^2 = 0 \tag{58}$$

with the solution $\left[1, \frac{3+\sqrt{-11}}{2}, 2\right]$.

$I=15$.

I. $N(a)=1$, $N(c)=15$, $\gamma\cdot N(c)=\frac{4\cdot 225}{121}>7$.

$N(b)=11$, 12 or 15.

1) $N(b)=11$, $b=\pm\sqrt{-11}$, $c=\pm(2\pm\sqrt{-11})$ or $=\pm\frac{7\pm\sqrt{-11}}{2}$.

$$\varepsilon\sqrt{-11} \equiv -2 \pmod{2+\varepsilon\sqrt{-11}}$$

$$\varepsilon\sqrt{-11} \equiv 2 \pmod{2-\varepsilon\sqrt{-11}}$$

$$\varepsilon\sqrt{-11} \equiv -7 \left(\mathrm{mod}\ \frac{7+\varepsilon\sqrt{-11}}{2}\right)$$

$$\varepsilon\sqrt{-11} \equiv 7 \left(\mathrm{mod}\ \frac{7-\varepsilon\sqrt{-11}}{2}\right)$$

and hence a non-residue of all these numbers by the lemma, because ± 2 and ± 7 are non-residues of 5 in the rational field. Then no equations satisfy the conditions (7).

2) $N(b)=12$. $b=\pm(1\pm\sqrt{-11})$.

$$1+\varepsilon\sqrt{-11} \equiv -1 \pmod{2+\varepsilon\sqrt{-11}}$$

$$-(2+\varepsilon\sqrt{-11}) \equiv -1 \pmod{1+\varepsilon\sqrt{-11}}$$

$$\pm(1+\varepsilon\sqrt{-11}) \equiv \pm 8 \left(\mathrm{mod}\ \frac{7-\varepsilon\sqrt{-11}}{2}\right)$$

and they are all non-residues by the lemma.

$1+\varepsilon\sqrt{-11}$ and $2-\varepsilon\sqrt{-11}$ have a common divisor and so have $1+\varepsilon\sqrt{-11}$ and $\frac{7+\varepsilon\sqrt{-11}}{2}$. Then only the following pair remains

$$x^2+(1+\varepsilon\sqrt{-11})y^2-(2+\varepsilon\sqrt{-11})z^2=0 \tag{59}$$

with the solution [1, 1, 1].

3) $N(b)=15$. $b=\pm(2-\sqrt{-11})$, $c=\pm(2+\sqrt{-11})$

or $b=\pm\frac{7-\sqrt{-11}}{2}$ and $c=\pm\frac{7+\sqrt{-11}}{2}$.

$$-(2-\varepsilon\sqrt{-11}) \equiv -4 \pmod{2+\varepsilon\sqrt{-11}}$$

$$\pm\frac{7-\varepsilon\sqrt{-11}}{2} \equiv \pm 7 \left(\mathrm{mod}\ \frac{7+\varepsilon\sqrt{-11}}{2}\right)$$

are non-residues by the lemma.

$$x^2-(2-\sqrt{-11})y^2-(2+\sqrt{-11})z^2=0 \tag{60}$$

has the solution [2, 1, 1].

II. $N(a)=3$, $N(c)=5$, $N(b)=3$, 4 or 5.

1) $N(b)=3$.

Then $ab=\pm 3$ and $c=\pm\frac{3\pm\sqrt{-11}}{2}$, but ± 3 are non-residues of $\frac{3+\varepsilon\sqrt{-11}}{2}$ and hence no equations satisfy the conditions (7).

2) $N(b)=4$, $a=\frac{1\pm\sqrt{-11}}{2}$, $b=\pm 2$, $c=\pm\frac{3\pm\sqrt{-11}}{2}$.

$$\pm(1+\varepsilon\sqrt{-11})\equiv\mp 2 \left(\mathrm{mod}\ \frac{3+\varepsilon\sqrt{-11}}{2}\right)$$

$$-(3-\varepsilon\sqrt{-11})\equiv -4\equiv -1 \left(\mathrm{mod}\ \frac{1+\varepsilon\sqrt{-11}}{2}\right)$$

and hence non-residues. Two pairs of conjugated equations remain

$$\frac{1+\varepsilon\sqrt{-11}}{2}x^2-2y^2+\frac{3-\varepsilon\sqrt{-11}}{2}z^2=0 \tag{61}$$

with the solution [1, 1, 1] and

$$\frac{1+\varepsilon\sqrt{-11}}{2}x^2+2y^2-\frac{3-\varepsilon\sqrt{-11}}{2}z^2=0 \tag{62}$$

with the solution $\left[\frac{3+\varepsilon\sqrt{-11}}{2},\ 1,\ \frac{1-\varepsilon\sqrt{-11}}{2}\right]$.

3) $N(b)=5$, $a=\frac{1\pm\sqrt{-11}}{2}$, $b=\pm\frac{3-\sqrt{-11}}{2}$, $c=\pm\frac{3+\sqrt{-11}}{2}$;

$$\pm\frac{1+\varepsilon\sqrt{-11}}{2}\cdot\frac{3-\varepsilon\sqrt{-11}}{2}=\pm\frac{7+\varepsilon\sqrt{-11}}{2}\equiv\pm 2 \left(\mathrm{mod}\ \frac{3+\varepsilon\sqrt{-11}}{2}\right)$$

and hence non-residues by the lemma. No equations satisfy the conditions (7).

$I=20$.

I. $N(a)=1$, $N(c)=20$, $\gamma\cdot N(c)=\frac{4\cdot 400}{121}>13$.

It is only necessary to examine $N(b)=15$. Then, according to the postulate (5) we can suppose $a=1$, $b=\pm(2+\varepsilon\sqrt{-11})$ or $\pm\frac{7+\varepsilon\sqrt{-11}}{2}$ and $c=\pm(3+\varepsilon\sqrt{-11})$.

$$-(3+\varepsilon\sqrt{-11})\equiv -1 \pmod{2+\varepsilon\sqrt{-11}}$$

$$\pm\frac{7+\varepsilon\sqrt{-11}}{2}\equiv\pm 2 \left(\mathrm{mod}\ \frac{3+\varepsilon\sqrt{-11}}{2}\right)$$

are all non-residues by the lemma.

The following equations remain

$$x^2 + (2 + \varepsilon\sqrt{-11})\,y^2 - (3 + \varepsilon\sqrt{-11})\,z^2 = 0 \tag{63}$$

with the solution [1, 1, 1] and

$$x^2 - (2 + \varepsilon\sqrt{-11})\,y^2 - (3 + \varepsilon\sqrt{-11})\,z^2 = 0 \tag{64}$$

with the solution $\left[\sqrt{-11},\ 1,\ \frac{1 + \varepsilon\sqrt{-11}}{2}\right]$.

II. $N(a) = 4,\ N(c) = 5,\ N(b) = 5.$

$$a = 2,\ b = \pm\frac{3 - \sqrt{-11}}{2},\ c = \pm\frac{3 + \sqrt{-11}}{2}.$$

$$2x^2 + \frac{3 - \sqrt{-11}}{2}y^2 + \frac{3 + \sqrt{-11}}{2}z^2 = 0 \tag{65}$$

has the solution $\left[1,\ \frac{1 + \sqrt{-11}}{2},\ \frac{1 - \sqrt{-11}}{2}\right]$.

$$2x^2 - \frac{3 - \sqrt{-11}}{2}y^2 - \frac{3 + \sqrt{-11}}{2}z^2 = 0 \tag{66}$$

has the solution $\left[\frac{1 - \sqrt{-11}}{2},\ 1,\ \frac{1 + \sqrt{-11}}{2}\right]$.

$$2x^2 - \frac{3 - \varepsilon\sqrt{-11}}{2}y^2 + \frac{3 + \varepsilon\sqrt{-11}}{2}z^2 = 0 \tag{67}$$

has the solution $\left[2,\ \frac{1 + \varepsilon\sqrt{-11}}{2},\ \frac{3 + \varepsilon\sqrt{-11}}{2}\right]$.

$I = 23.$

$N(a) = 1,\ N(c) = 23,\ \gamma \cdot N(c) = \frac{4 \cdot 529}{121} > 16.$

1) $N(b) = 20,\quad b = \pm(3 \pm \sqrt{-11}),\quad c = \pm\frac{9 \pm \sqrt{-11}}{2}.$

$$\pm\frac{9 + \varepsilon\sqrt{-11}}{2} \equiv \pm 3 \left(\mathrm{mod}\ \frac{3 + \varepsilon\sqrt{-11}}{2}\right)$$

$$-(3 + \varepsilon\sqrt{-11}) \equiv -12 \left(\mathrm{mod}\ \frac{9 - \varepsilon\sqrt{-11}}{2}\right)$$

and hence they are non-residues by the lemma. Two pairs of equations remain

(68) $$x^2 - (3 + \varepsilon\sqrt{-11})\,y^2 - \frac{9 - \varepsilon\sqrt{-11}}{2}\,z^2 = 0$$

with the solution $\left[\sqrt{-11},\ 1,\ \frac{1 - \varepsilon\sqrt{-11}}{2}\right]$ and

(69) $$x^2 - (3 + \varepsilon\sqrt{-11})\,y^2 + \frac{9 - \varepsilon\sqrt{-11}}{2}\,z^2 = 0$$

with the solution $\left[\frac{9 + 11\varepsilon\sqrt{-11}}{2},\ 11 + 2\varepsilon\sqrt{-11},\ \frac{13 + 5\varepsilon\sqrt{-11}}{2}\right]$.

2) $N(b) = 23,\ b = \pm\frac{9 - \sqrt{-11}}{2},\ c = \pm\frac{9 + \sqrt{-11}}{2}$.

$$-\frac{9 - \varepsilon\sqrt{-11}}{2} \equiv -9 \left(\mathrm{mod}\ \frac{9 + \varepsilon\sqrt{-11}}{2}\right)$$

and hence a non-residue by the lemma. Only one equation remains.

(70) $$x^2 - \frac{9 - \sqrt{-11}}{2}\,y^2 - \frac{9 + \sqrt{-11}}{2}\,z^2 = 0$$

has the solution [3, 1, 1].

$I = 25$.

$N(a) = 1.\quad N(c) = 25.\quad \gamma \cdot N(c) = \frac{4 \cdot 625}{121} > 20.$

Then we only need consider $N(b) = 23,\ b = \pm\frac{9 \pm \sqrt{-11}}{2},\ c = \pm 5$.

$$\pm\frac{9 + \varepsilon\sqrt{-11}}{2} \equiv \pm 3 \left(\mathrm{mod}\ \frac{3 + \varepsilon\sqrt{-11}}{2}\right)$$

and hence non-residues of 5 by the lemma.

Then the conditions (7) are sufficient in the field $K(\sqrt{-11})$.

SUMMARY

In four of the five imaginary Euclidean quadratic fields, $K(\sqrt{-1})$, $K(\sqrt{-2})$, $K(\sqrt{-3})$ and $K(\sqrt{-11})$, this paper gives the following result:

If a, b and c are square-free integers, relatively prime in pairs and not zero or, simpler expressed, if abc is square-free, then the equation

$$ax^2 + by^2 + cz^2 = 0$$

has proper integral solutions if and only if $-bc$, $-ca$ and $-ab$ are quadratic residues of a, b and c respectively.

In the remaining field $K(\sqrt{-7})$ we must, as in the rational field, make the restriction that all the equations which by the index method correspond to the equation $x^2 + y^2 + z^2 = 0$ are insolvable. All the equations of this type with I less than 22 are given in § 7.

Remark 1. It is possible to replace this restriction by a congruence condition. In fact, the necessary and sufficient conditions for the solvability of the equation $ax^2 + by^2 + cz^2 = 0$ in a quadratic field $K(\sqrt{m})$ is that the congruence

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{N}$$

is solvable for every integral ideal modulus N in $K(\sqrt{m})$ in integers x, y, z such that $(x, y, z, N) = 1$.

In the rational field the completing condition can be written

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{8}$$

and in the field $K(\sqrt{-7})$ we have the condition

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{\pi^3}$$

where π is one of the prime divisors of 2, for instance $\frac{1+\sqrt{-7}}{2}$. This follows quite analogously to [3] pp. 222—225, because $\alpha^2 \equiv 1 \pmod{\pi^3}$ and $\alpha + \beta \equiv 0 \pmod{\pi}$, if α and β are integers not divisible by π.

Remark 2. It is possible to reduce all the equations (14)–(70) with $I > 1$ to equations with less index by the index method, even if we in some cases must take great solutions of the corresponding equation (9), for instance $r = \frac{5 + 3\varepsilon\sqrt{-11}}{2}$, $Q = -\left(\frac{7 - \varepsilon\sqrt{-11}}{2}\right)^2$ to reduce (46) to (40). Hence every equation (6), which satisfies the conditions (7), corresponds to an equation with $I = 1$.

By examination of only few equations more we can further prove that if $N(a) \leq N(b) \leq N(c)$ and $N(c) > 1$ and if $-ab$ is a quadratic residue of c, then we can find $N(AC) < N(ac)$ except in (36), and hence otherwise, according to (9), at least one of the Diophantine equations

$$a\xi^2 + k \cdot c \cdot \eta^2 = -b$$

where k is an integer and $N(k) < N(ac)$, is solvable.

BIBLIOGRAPHY. 1) **A. M. Legendre:** Mém. Acad. Sc. Paris (1785) pp. 507—513; see also Théorie des Nombres (1798) pp. 43—50. — 2) **Dirichlet-Dedekind:** Zahlentheorie §§ 156—157. — 3) **T. Nagell:** Introduction to Number Theory (Uppsala 1951), § 61. — 4) **Hardy-Wright:** The Theory of Numbers. Ch. XIV. — 5) **T. Skolem:** Über die Lösung der unbestimmten Gleichung $ax^2 + by^2 + cz^2 = 0$ in einigen einfachen Rationalitätsbereichen, Norsk Matematisk Tidskrift X (1928) pp. 50—54. — 6) **Sommer:** Vorlesungen über Zahlentheorie § 21.

Tryckt den 9 januari 1952

Uppsala 1952. Almqvist & Wiksells Boktryckeri AB