Read 6 December 1961

On the A-numbers in the quadratic fields $\mathbf{K}(\sqrt{\pm 37})$

By Trygve Nagell

§ 1. Introduction

1. Every integer α $(\neq 0)$ in the algebraic field $\mathbf{\Omega}$ is said to be an *A-number* in $\mathbf{\Omega}$ if it is representable as the sum of two integral squares in $\mathbf{\Omega}$. In a previous paper [1] we have determined the A-numbers in the quadratic fields $\mathbf{K}(\sqrt{D})$, where $D=-1$, ± 2, ± 3, ± 7, ± 11, ± 19, ± 43, ± 67 and ± 163. In another paper [2] we determined the A-numbers when $D=\pm 5$ and ± 13. In the present paper we shall treat the cases $D=\pm 37$. The fields $\mathbf{K}(\sqrt{\pm 37})$ have in the main the same properties as the fields $\mathbf{K}(\sqrt{\pm 5})$ and $\mathbf{K}(\sqrt{\pm 13})$ treated in paper [2]. There is, however, an essential difference: The fundamental unit has the form $6+\sqrt{37}$. Thus the equations $x^2-37y^2=\pm 4$ have no solutions in odd (rational) integers. This fact necessitates a modification of the methods used in paper [2]. The following developments are in general analogous to those occurring in [1] and [2].

The number of ideal classes in the field $\mathbf{K}(\sqrt{37})$ is $=1$ and in the field $\mathbf{K}(\sqrt{-37})=2$. In the Dirichlet field $\mathbf{K}(\sqrt{37}, \sqrt{-37})$ the number of ideal classes is $=1$. If $x+y\sqrt{-37}$ is an A-number in $\mathbf{K}(\sqrt{-37})$, x and y rational integers, then y is even. If α is an integer in $\mathbf{K}(\sqrt{37}, \sqrt{-37})$, the number 2α belongs to the ring $\mathbf{R}(1, \sqrt{-1}, \sqrt{37}, \sqrt{-37})$. For the proofs see [1], p. 8–9.

In the sequel we shall write θ instead of $\sqrt{37}$ and consequently $i\theta$ instead of $\sqrt{-37}$.

§ 2. The real field $\mathbf{K}(\theta)$

2. *Units and divisors of the rational primes* 2 *and* 37. Every A-number in this field must be positive and have a positive norm. The fundamental unit ε is $6+\theta$. Since $N(\varepsilon)=-1$, ε is not an A-number. The nth power of ε is an A-number if and only if n is even. The number 2 is a prime in the field and, of course, an A-number.

Since the prime θ has the negative norm -37, it cannot be an A-number. The number -1 is a quadratic residue modulo θ. From the relation

$$(6+\theta)\,\theta=\tfrac{1}{4}(5+\theta)^2+\tfrac{1}{4}(7+\theta)^2$$

it follows that the product $\varepsilon\theta$ is an A-number. Hence the number $\varepsilon^m\theta^n$, where m and n are rational integers, $n\geqslant 0$, is an A-number if and only if $m+n$ is even.

3. *The rational primes for which 37 is a quadratic non-residue.* Let p be an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = +1 \quad \text{and} \quad \left(\frac{37}{p}\right) = -1.$$

Then p is a prime in the field and since

$$p = u^2 + v^2,$$

where u and v are rational integers, p is an A-prime.

Suppose next that p is an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = -1 \quad \text{and} \quad \left(\frac{37}{p}\right) = -1.$$

Then p is a prime in $\mathbf{K}(\theta)$. Since $\left(\frac{-37}{p}\right) = +1$ we have, in $\mathbf{K}(i\theta)$,

$$(p) = \mathfrak{p}\mathfrak{p}',$$

where $\mathfrak{p}$ and $\mathfrak{p}'$ are different prime ideals. In this field we further have

$$\left(\frac{-1}{\mathfrak{p}}\right) = (-1)^{\frac{1}{2}(N\mathfrak{p}-1)} = -1.$$

The ideal $\mathfrak{p}$ *can never be principal.* In fact, if we had $\mathfrak{p} = (x + yi\theta)$ with rational integers x and y, we should have

$$p = x^2 + 37y^2.$$

But this equation clearly implies $p \equiv +1 \pmod 4$. In $\mathbf{K}(i\theta)$ we further have $(2) = \mathfrak{q}^2$, where $\mathfrak{q}$ is a prime ideal that is not principal. Since the number of ideal classes in $\mathbf{K}(i\theta)$ is $=2$, the product $\mathfrak{p}\mathfrak{q}$ is a principal ideal. Hence

$$2p = x^2 + 37y^2,$$

where x and y are rational odd integers. Since this relation may be written

$$p = \tfrac{1}{4}(x + y\theta)^2 + \tfrac{1}{4}(x - y\theta)^2,$$

the number p is an A-prime in $\mathbf{K}(\theta)$. Thus the number -1 is a quadratic residue modulo p in this field.

4. *The rational primes for which 37 is a quadratic residue.* Let p be an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = -1 \quad \text{and} \quad \left(\frac{37}{p}\right) = +1.$$

In this case we have

$$(p) = \omega\omega',$$

where ω and ω' are different primes. Since

$$\left(\frac{-1}{\omega}\right) = (-1)^{\frac{1}{2}(|N\omega|-1)} = -1,$$

the prime ω is not an A-number.

Finally, we consider an odd prime p such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = +1 \quad \text{and} \quad \left(\frac{37}{p}\right) = +1.$$

Since the field is simple, and since the norm of the fundamental unit ε is $= -1$, we have always

$$4p = u^2 - 37v^2,$$

where u and v are rational integers of the same parity. Then the numbers

$$\omega = \tfrac{1}{2}(u + v\theta) \quad \text{and} \quad \omega' = \tfrac{1}{2}(u - v\theta)$$

are conjugate prime factors of p in the field. If we suppose $u > 0$, the numbers ω and ω' are positive. Since the field $\mathbf{K}(\theta, i)$ is simple, we have

$$\omega = \pi_1 \pi_2 \eta,$$

where η is a unit and π_1 and π_2 are primes in that field. According to lemma 3 in [2], we may suppose that

$$\pi_1 = \tfrac{1}{2}(a + c\theta) + \tfrac{1}{2}i(b + d\theta)$$

and

$$\pi_2 = \tfrac{1}{2}(a + c\theta) - \tfrac{1}{2}i(b + d\theta),$$

a, b, c and d being rational integers. The unit η belongs to the field $\mathbf{K}(\theta)$ since the product $\pi_1\pi_2$ belongs to this field. Since ω is positive, η is so. The norm of ω is positive and the norm of $\pi_1\pi_2$ is also positive. Hence the norm of η is positive. Thus we have

$$\eta = \varepsilon^{2m}.$$

Putting

$$\psi_1 = \pi_1 \varepsilon^m \quad \text{and} \quad \psi_2 = \pi_2 \varepsilon^m,$$

we get

$$\omega = \psi_1 \psi_2,$$

where ψ_1 and ψ_2 are primes in $\mathbf{K}(\theta, i)$ such that ψ_1 is transformed into ψ_2 when i is substituted by $-i$ and vice versa. Consequently we may suppose that $\eta = 1$. Hence

$$\omega = \tfrac{1}{4}(a + c\theta)^2 + \tfrac{1}{4}(b + d\theta)^2, \tag{1}$$

which involves the relations

$$2u = a^2 + b^2 + 37(c^2 + d^2) \tag{2}$$

and

$$v = ac + bd. \tag{3}$$

If the numbers a, b, c, d are all odd or all even, it is clear that ω is an A-number. Suppose next that a and c are both even or both odd. Then it follows from (1) that $\frac{1}{2}(b+d\theta)$ is an integer and consequently ω is an A-number. Analogously when b and d are both even or both odd. Hence it remains to examine the following case: one of the numbers a and c is even and the other one odd, one of the numbers b and d is even and the other one odd. Then it follows from (3) that v is even. Hence u is also even, and we get from (2)

$$a^2+b^2+37(c^2+d^2) \equiv a^2+b^2+c^2+d^2 \equiv 0 \pmod 4.$$

But the sum of four squares is divisible by 4 only when the squares are all even or all odd. Thus we have proved that ω is always an A-number.

5. *Summary and proof of the main result.* As a consequence of the discussions in the preceding sections we may state the following result

Theorem 1. *The prime ω in* $\mathbf{K}(\theta)$ *is an A-number only in the following cases:* (i) $\omega=2\varepsilon^{2m}$; (ii) $\omega=\theta\varepsilon^{2m+1}$; (iii) $\omega=p\varepsilon^{2m}$, *when p is an odd rational prime such that* $\left(\frac{37}{p}\right)=-1$; (iv) *$\omega$ is of the form $\frac{1}{2}(u+v\theta)$, where u and v are rational integers such that $\frac{1}{4}(u^2-37v^2)$ is a rational prime $\equiv 1 \pmod 4$.*

We are now in a position to establish our main result.

Theorem 2. *The integer α in the field* $\mathbf{K}(\theta)$ *is an A-number if and only if*

$$\alpha=\beta\gamma^2\theta^m\varepsilon^n,$$

where β and γ are integers in the field with the following properties: β and γ are prime to θ; β is either $=1$ or $=$ a product of A-primes, different or not; γ is either a unit or $=$ a product of primes π such that, in $\mathbf{K}(\theta)$,

$$\left(\frac{-1}{\pi}\right)=-1. \tag{4}$$

m and n are rational integers, $m>0$, such that $m+n$ is even. ε is the fundamental unit, chosen >1.

Proof. It is evident that the conditions are sufficient. Suppose that α is an A-number and that

$$\alpha=\xi\eta\theta^m,$$

where ξ and η are integers in the field with the following properties: they are prime to θ; η is either $=1$ or $=$ a product of primes π satisfying the relation (4) in $\mathbf{K}(\theta)$; ξ is either $=1$ or $=$ a product of A-primes; m is a rational integer $\geqslant 0$. Then we must have $\eta=\varrho\gamma^2$, where γ is an integer in the field and ϱ a unit. Thus the number α/γ^2 is an A-number. Now applying lemma 4 in [2] a certain number of times to the prime factors π of ξ, we find that the number

$$\frac{\alpha}{\gamma^2\xi}=\varrho\theta^m$$

must be an A-number. Finally, applying a result in section 2 we achieve the proof.

§ 3. The imaginary field $\mathbf{K}(i\theta)$

6. *Units and divisors of the rational primes 2 and 37.* The number -1 is an A-number in the field since

$$-1 = 6^2 + (i\theta)^2.$$

Thus the numbers α and $-\alpha$ are simultaneously A-numbers or not.

The prime $i\theta$ is clearly not an A-number, and $(i\theta)^m$ is an A-number only when m is even. The number -1 is a quadratic residue modulo $i\theta$. The number $u+vi\theta$, where u and v are rational integers, is never an A-number when v is odd. In virtue of the relation

$$2i\theta = 6^2 + (1+i\theta)^2$$

we state: *the number $2i\theta$ is an A-number.* We have

$$(2) = \mathfrak{q}^2 = (1^2+1^2),$$

where the prime ideal $\mathfrak{q}$ is not principal. The number -1 is a quadratic residue modulo $\mathfrak{q}$.

7. *The rational primes for which -37 is a quadratic non-residue.* Let p be an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = +1 \quad \text{and} \quad \left(\frac{-37}{p}\right) = -1.$$

Then (p) is a prime ideal in the field and since

$$p = u^2 + v^2,$$

where u and v are rational integers, p is an A-prime.

Suppose next that p is an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = -1 \quad \text{and} \quad \left(\frac{-37}{p}\right) = -1.$$

Then (p) is a prime ideal in the field $\mathbf{K}(i\theta)$. Since 37 is a quadratic residue of p, and since the field $\mathbf{K}(\theta)$ is simple, the equation

$$4p = x^2 - 37y^2$$

is solvable in rational integers x and y.

If x and y are both even, we get

$$p = x_1^2 - 37y_1^2 = x_1^2 + (i\theta y_1)^2,$$

where $x_1 = \frac{1}{2}x$ and $y_1 = \frac{1}{2}y$. *Hence p is an A-prime.*

If x and y are both odd, we shall show that p is not an A-number. In fact we have, for every rational integer m,

$$\tfrac{1}{2}(x+y\theta)(6+\theta)^m = \tfrac{1}{2}(u+v\theta),$$

where the rational integers u and v are clearly odd when x and y are odd. Hence, in this case, the equation

$$p = u^2 - 37v^2$$

is not possible in rational integers u and v. Suppose next that

$$p = (a + ci\theta)^2 + (b + di\theta)^2,$$

where a, b, c and d are rational integers. This relation implies

$$p = a^2 + b^2 - 37(c^2 + d^2),\ ac = -bd.$$

If $d = 0$ we must have $a = 0$. Hence we should have $p = b^2 - 37c^2$ which is impossible as was shown above. If $d \neq 0$ we get $b = -acd^{-1}$ and by elimination of b

$$pd^2 = (c^2 + d^2)(a^2 - 37d^2).$$

Put $c = fc_1$ and $d = fd_1$ where $(c_1, d_1) = 1$. Then we get

$$p = (c_1^2 + d_1^2)(a^2 d_1^{-2} - 37f^2).$$

Hence a is divisible by d_1. Putting $a = gd_1$ we must have either

$$p = c_1^2 + d_1^2$$

or

$$p = g^2 - 37f^2.$$

But these equations are both impossible. *Hence p is not an A-number.* We say that the rational prime p is a *B-prime* when p has the following properties: $p \equiv -1 \pmod 4$, 37 is a quadratic residue modulo p; the equation $p = x^2 - 37y^2$ has no solutions in rational integers x and y. Hence we have proved that a B-prime is not an A-number. By the same method we may show that the equation

$$2p = (a + ci\theta)^2 + (b + di\theta)^2,$$

where p is a B-prime, is not possible in rational integers a, b, c and d. In fact, if $d = 0$ we get $2p = b^2 - 37c^2$, which is impossible modulo 4. If $d \neq 0$ we get in the same way as above

$$2p = (c_1^2 + d_1^2)(g^2 - 37f^2).$$

Hence $c_1^2 = d_1^2 = 1$ and $p = g^2 - 37f^2$. Since p is a B-prime the latter equation is impossible. Thus we have proved

Lemma 1. *When p is a B-prime none of the numbers p or $2p$ is an A-number.*

We further prove

Lemma 2. *The product of two B-primes is an A-number.*
Proof. Let p and p_1 be two B-primes

$$p = \tfrac{1}{4}[x^2 + (yi\theta)^2] \quad \text{and} \quad p_1 = \tfrac{1}{4}[x_1^2 + (y_1 i\theta)^2],$$

where x, y, x_1 and y_1 are odd rational integers. Then

$$16pp_1 = [xx_1 \pm 37yy_1]^2 + [(xy_1 \pm x_1y)i\theta]^2.$$

Here the sign may be chosen such that the number $xx_1 \pm 37yy_1$ is divisible by 4. Then $xy_1 \pm x_1y$ is also divisible by 4. This proves the lemma.

8. *The rational primes $p \equiv -1$ (mod 4) for which -37 is a quadratic residue.* Let p be an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = -1 \quad \text{and} \quad \left(\frac{-37}{p}\right) = +1.$$

Then we have

$$(p) = \mathfrak{p}\mathfrak{p}',$$

where $\mathfrak{p}$ and $\mathfrak{p}'$ are different prime ideals in the field $\mathbf{K}(i\theta)$. In this field we further have

$$\left(\frac{-1}{\mathfrak{p}}\right) = (-1)^{\frac{1}{2}(N\mathfrak{p}-1)} = -1. \tag{5}$$

The ideal $\mathfrak{p}$ can never be principal. In fact, if we had $\mathfrak{p} = (x + yi\theta)$ with rational integers x and y, we should have

$$p = x^2 + 37y^2.$$

But this equation clearly implies $p \equiv +1$ (mod 4).

Lemma 3. *Let α and β be integers in $\mathbf{K}(i\theta)$, not both equal to zero. Further, let $\mathfrak{p}$ be a prime ideal in the field satisfying relation* (5). *If the sum $\alpha^2 + \beta^2$ is divisible by the power $\mathfrak{p}^m$, we must have*

$$\alpha \equiv \beta \equiv 0 \pmod{\mathfrak{p}^\nu},$$

where $\nu = [\frac{1}{2}(m+1)]$.

The proof is the same as that of lemma 6 in paper [2].

The following results may be obtained in the same manner as the lemmata 7–10 in paper [2].

Lemma 4. *Let $\mathfrak{p}$ be a prime ideal in the field satisfying relation* (5). *Then $\mathfrak{p}^2$ is a principal ideal $= (u + vi\theta)$, u and v being rational integers, u even and v odd. Further, the numbers $2(u + vi\theta)$ and $i\theta(u + vi\theta)$ are A-numbers.*

Let $\mathfrak{p}_1$ be another prime ideal satisfying relation (5). *Then $\mathfrak{p}\mathfrak{p}_1$ is a principal ideal $=(\alpha)$, where the integer α is not an A-number.*

9. *The rational primes $p \equiv +1$ (mod 4) for which -37 is a quadratic residue.* Consider finally the case

$$\left(\frac{-1}{p}\right) = +1 \quad \text{and} \quad \left(\frac{-37}{p}\right) = +1,$$

where p is an odd rational prime. Here we have

$$(p) = \mathfrak{p}\mathfrak{p}',$$

where $\mathfrak{p}$ and $\mathfrak{p}'$ are different prime ideals in the field. Exactly as in paper [2], p. 272, it may be shown that these ideals are principal. Hence

$$p = u^2 + 37v^2,$$

where u and v are rational integers. Then the numbers

$$\omega = u + vi\theta \quad \text{and} \quad \omega' = u - vi\theta$$

are conjugate prime factors of p in $\mathbf{K}(i\theta)$. Since the field $\mathbf{K}(\theta, i\theta)$ is simple, we have

$$\omega = \pi_1 \pi_2,$$

where π_1 and π_2 are primes in the latter field. Since $2\pi_1$ and $2\pi_2$ belong to the ring $\mathbf{R}(1, i, \theta, i\theta)$ (cf. the introduction), we may suppose that

$$\pi_1 = \tfrac{1}{2}(a + ci\theta) + i\tfrac{1}{2}(b + di\theta)$$

and

$$\pi_2 = \tfrac{1}{2}(a + ci\theta) - i\tfrac{1}{2}(b + di\theta),$$

a, b, c and d being rational integers. Hence

$$\omega = \tfrac{1}{4}(a + ci\theta)^2 + \tfrac{1}{4}(b + di\theta)^2, \tag{6}$$

which involves the equations

$$4u = a^2 + b^2 - 37(c^2 + d^2) \tag{7}$$

and

$$2v = ac + bd. \tag{8}$$

If u is even and v odd the prime ω can never be an A-number. In this case we call ω a *C-prime*.

Suppose next that u is odd and v even. If the numbers a, b, c and d are all even, ω is an A-number. If they are all odd, we get from (7) $4u \equiv 0 \pmod 8$, thus u is even and ω is a C-prime. Exactly as in paper [2], p. 273, it may be shown that the only remaining possibility is that a and d are both even and b and c are both odd. (It is, of course, unnecessary to treat the case with b and c even and a and d odd). In this case we get from (7)

$$a^2 + d^2 \equiv 0 \pmod 8.$$

It follows from this congruence that $\tfrac{1}{2}a$ and $\tfrac{1}{2}d$ are either both odd or both even. If ω were an A-number, it is evident that it should exist a unit E in $\mathbf{K}(\theta, i\theta)$ such that

$$E\pi_1 = a_1 + c_1 i\theta + i(b_1 + d_1 i\theta), \tag{9}$$

a_1, b_1, c_1 and d_1 being rational integers. It suffices to consider the case that E is the fundamental unit in $\mathbf{K}(\theta, i\theta)$. In this field one may choose the fundamental unit $= 6 + \theta$, cf. paper [3], p. 11–15. Hence

$$E\pi_1 = \tfrac{1}{2}(6 + \theta)\,[a + ci\theta + i(b + di\theta)] =$$
$$= \tfrac{1}{2}[6a - 37d + (6c + b)\,i\theta + (6b + 37c)\,i + (a - 6d)\,\theta].$$

Since the number $6c+b$ is odd we see that $E\pi_1$ is not of the form (9) with rational integers a_1, b_1, c_1, d_1. Thus we conclude that ω is not an A-number in this case. We say that the prime ω is an *F-prime*, when ω is of the form (6), where a, b, c and d are rational integers, such that one of the numbers a^2+d^2 and b^2+c^2 is divisible by 8 and the other one only by 2.

In the above proof the numbers $6a-37d$ and $a-6d$ are even, and the numbers $6c+b$ and $6b+37c$ are odd. Hence we may state

Lemma 5. *In all the representations of an F-prime ω,*

$$\omega = \tfrac{1}{4}(a+ci\theta)^2 + \tfrac{1}{4}(b+di\theta)^2,$$

with rational integers a, b, c and d, one of the numbers a^2+d^2 and b^2+c^2 is divisible by 8 and the other one only by 2.

Lemma 6. *The product of two F-primes is an A-number.*

Proof. Let ω and ω_1 be two F-primes,

$$\omega = \tfrac{1}{4}(a+ci\theta)^2 + \tfrac{1}{4}(b+di\theta)^2,$$

$$\omega_1 = \tfrac{1}{4}(a_1+c_1i\theta)^2 + \tfrac{1}{4}(b_1+d_1i\theta)^2,$$

where a, b, c, d, a_1, b_1, c_1 and d_1 are rational integers, such that a, d, a_1 and d_1 are even and b, c, b_1 and c_1 are odd. Then we get

$$16\omega\omega_1 = [aa_1 - 37cc_1 \pm bb_1 \mp 37dd_1 + (ac_1 + a_1c \pm bd_1 \pm b_1d)i\theta]^2 + [ab_1 - 37cd_1 \mp a_1b \pm 37c_1d + (b_1c + ad_1 \mp a_1d \mp bc_1)i\theta]^2.$$

Since $a \pm d$ and $a_1 \pm d_1$ are always divisible by 4, we have, as well for the upper as for the lower sign,

$$ac_1 + a_1c \pm (bd_1 + b_1d) \equiv 0 \pmod 4$$

and

$$ab_1 - 37cd_1 \mp (a_1b - 37c_1d) \equiv 0 \pmod 4.$$

Let us choose the sign such that the number $cc_1 \mp bb_1$ is divisible by 4. Then we clearly obtain

$$aa_1 - 37cc_1 \pm (bb_1 - 37dd_1) \equiv 0 \pmod 4$$

and

$$b_1c + ad_1 \mp (a_1d + bc_1) \equiv 0 \pmod 4.$$

This proves the lemma.

Lemma 7. *If ω is an F-prime, 2ω is not an A-number.*

Proof. Suppose ω given by (6), where a and d are even, b and c odd. Then we have

$$8\omega = 4\omega(1^2+1^2) = [a+b+(c+d)i\theta]^2 + [a-b+(c-d)i\theta]^2.$$

If 2ω were an A-number, it should exist a unit E in $\mathbf{K}(\theta, i\theta)$ such that

$$E[a+b+(c+d)i\theta + i(a-b) - (c-d)\theta] = a_1 + c_1 i\theta + i(b_1 + d_1 i\theta),$$

where the rational integers a_1, b_1, c_1 and d_1 were all even. It is sufficient to take $E=6+\theta$. Then we get $a_1=6a+6b-37(c-d)$. Hence a_1 is odd, and 2ω is not an A-number.

10. *Summary.* As a consequence of the discussions in the preceding sections, we may state the following results.

Theorem 3. *All the prime ideals in* $\mathbf{K}(i\theta)$ *are principal except the prime ideal divisors of 2 and of the odd rational primes p satisfying the relations, in* $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right)=-1, \quad \left(\frac{-37}{p}\right)=+1.$$

Theorem 4. *The prime* ω *in* $\mathbf{K}(i\theta)$ *is an A-number only in the following cases:*
(i) $w=\pm p$ *where p is an odd rational prime such that, in* $\mathbf{K}(1)$,

$$\left(\frac{-37}{p}\right)=-1,$$

except when $p\equiv -1 \pmod 4$ *and the equation* $p=x^2-37y^2$ *has no solutions in rational integers x and y.*

(ii) ω *is of the form* $u+vi\theta$, *where u and v are rational integers, u odd, v even, such that* u^2+37v^2 *is a rational prime, except when the A-number* 4ω *has a representation of the form*

$$4\omega=(a+ci\theta)^2+(b+di\theta)^2, \tag{10}$$

a, b, c and d being rational integers such that one of the numbers a^2+d^2 *and* b^2+c^2 *is divisible by 9 and the other one only by 2.*

By means of this theorem it may always be decided if a given prime is an A-prime or not. This is evident in the first case. In the second case it follows from section 5 that equation (10) is always solvable when ω is a prime of the type in question. Thus a solution of (10) may be found by trial.

It is now possible to determine the necessary and sufficient conditions for a given integer α in the field to be an A-number. To arrive at a result of that sort it should, however, be necessary to develop a great number of lemmata on certain products of the type

$$\omega_1\omega_2\omega_3\ldots\omega_\nu,$$

where ω_i is either a B-prime, or a C-prime, or an F-prime, or a number $u+vi\theta$ defined in lemma 4, and finally ω_i may also be $=2$ or $=i\theta$. It should furthermore be necessary to distinguish two kinds of C-primes. (The lemmata 1, 2, 4, 6 and 7 are of the type in question.) Since the discussions in that matter should be too extensive we terminate with these remarks.

11. *Numerical examples in* $\mathbf{K}(i\theta)$. The numbers 3 and 11 are B-primes since

$$3=\tfrac{1}{4}(7^2-37\cdot 1^2) \quad \text{and} \quad 11=\tfrac{1}{4}(9^2-37\cdot 1^2).$$

The number $2+3i\theta$ is a C-prime since

$$2+3i\theta=\tfrac{1}{4}[3^2+(6+i\theta)^2],$$

and since $N(2+3i\theta)=337$ is a prime.

The number $-16+i\theta$ is a C-prime of another kind since

$$-16+i\theta=\tfrac{1}{4}[(3+i\theta)^2+(1-i\theta)]^2,$$

and since $N(-16+i\theta)=293$ is a prime.

The number $-3+2i\theta$ is an F-prime since

$$-3+2i\theta=\tfrac{1}{4}[4+i\theta)^2+3^2],$$

and since $N(-3+2i\theta)=157$ is a prime.

The number $-13+2i\theta$ is an A-prime since

$$-13+2i\theta=(6+i\theta)^2+(5-i\theta)^2,$$

and since $N(-13+2i\theta)=313$ is a prime.

REFERENCES

1. NAGELL, T., On the representations of integers as the sum of two integral squares in algebraic, mainly quadratic fields, Nova Acta Soc. Sci. upsal., Ser. IV, Vol. 15, No. 11, Uppsala 1953.
2. NAGELL, T., On the sum of two integral squares in certain quadratic fields, Arkiv f. matematik, Bd. 4, nr. 20, Uppsala 1960.
3. NAGELL, T., Sur quelques questions dans la théorie des corps biquadratiques, Arkiv f. matematik, Bd. 4, nr. 26, Uppsala 1961.

Tryckt den 13 juni 1962

Uppsala 1962. Almqvist & Wiksells Boktryckeri AB