Conspectus materiae tomi XXXIII, fasciculi 2

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de
la Rédaction
et de l'échange

Address of the
Editorial Board
and of the exchange

Die Adresse der
Schriftleitung und
des Austausches

Адрес редакции
и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

TA ARITHMETICA
XXXIII (1977)

On a conjecture of Morgan Ward, III

by

K. K. Kubota (Lexington, Ky.)

In [2], the author has shown that, in a non-degenerate second order linear recurrence of rational integers, no integer occurs more than four times. The aim of this paper is to generalize this result to recurrences of algebraic integers and to apply the method to the problem of bounding the number of representations of unity by rank one binary biquadratic forms.

Throughout the paper, $\mathfrak{o}$ will be the ring of integers of an algebraic number field K of degree $[K:Q]$ over the rational number field Q. A *second order linear recurrence* in K is defined to be a sequence $\{a_n\}$ of integers in $\mathfrak{o}$ satisfying a relation

$$(1)\qquad a_{n+2} = Ma_{n+1}-Na_n, \quad n \geqslant 0,\ |a_0|+|a_1| \neq 0,$$

where M and $N \neq 0$ are fixed integers in $\mathfrak{o}$. Let β_1 and β_2 be the roots of the *companion polynomial*

$$(2)\qquad x^2-Mx+N = 0.$$

We say that the recurrence $\{a_n\}$ is *non-degenerate* if β_1, β_2 and β_1/β_2 are not roots of unity. The *multiplicity* of $\{a_n\}$ is defined to be the supremum taken over all integers of $\mathfrak{o}$ of the number $m(d)$ of times that d occurs in $\{a_n\}$. The first result may be stated as follows.

Theorem 1. *The multiplicity of a non-degenerate second order linear recurrence in an algebraic number field K is bounded above by an effectively computable integer $n(m)$ depending only on the degree $m = [K:Q]$.*

It would be interesting to know if there is an absolute bound independent of the degree $[K:Q]$. If it existed, then one would expect to be able to generalize the result to recurrences in the complex field C. However, the method of proof used below cannot give such an absolute bound. It can be shown that non-degenerate rational integer cubic recurrences can have no more than six zeros.

By a careful study of biquadratic units, T. Nagell has proved the following theorem ([5]):

THEOREM. *If $f(x, y)$ is an irreducible totally complex binary biquadratic form with integer coefficients such that the field generated by a root of $f(x, 1) = 0$ contains a quadratic subfield, then the diophantine equation $f(x, y) = 1$ has at most eight solutions.*

One expects that the condition about the existence of a quadratic subfield is unnecessary. The diophantine equation in question will be interpreted in terms of second order linear recurrences, and the following theorem will be obtained.

THEOREM 2. *With the possible exception of forms in a finite number of equivalence classes, an irreducible totally complex binary biquadratic form with integer coefficients represents unity at most eight times.*

The exceptional cases correspond to solutions of a manageable number of binary quintic diophantine equations. Since these may be solved by Runge's method, one can, at least in principle, list the exceptional equations.

It is possible to apply the Skolem p-adic method with a prime divisor $\mathfrak{p}$ of 2 to obtain an upper bound with no exceptional equations. This requires an examination of all possible decompositions of 2 in the splitting field of $f(x, 1)$, which in the cases not covered by the result of Nagell is a field of degree 12 or 24. The result, which will not be proved here, can be stated as follows.

THEOREM 3. *An irreducible totally complex binary biquadratic form with integer coefficients represents unity no more than twelve times.*

1. Linear recurrences in number fields. The proof of Theorem 1 uses Skolem's p-adic method in conjunction with a result of A. Schinzel, which in turn is based on Baker's method. The result of the p-adic argument can be summarized as follows:

LEMMA 1. *Let $\{a_n\}$ be a non-degenerate second order linear recurrence in K satisfying (1), β_1 and β_2 be the roots of the companion equation (2), and $\mathfrak{p}$ be a prime ideal of the ring of integers of $K(\beta_1, \beta_2)$ such that $\mathfrak{p}\nmid N$. Suppose $\varkappa$ is a positive integer no smaller than $-\left[\frac{-3e}{p-1}\right]$ where p is the rational prime lying under $\mathfrak{p}$, e is the absolute ramification index of $\mathfrak{p}$, and the brackets denote the greatest integer function. Let q be a positive integer such that*

$$\beta_1^q \equiv \beta_2^q \equiv 1 \pmod{\mathfrak{p}^\varkappa};$$

and, if $\mathfrak{p}\,|\,2$, take q to be minimal subject to this condition. For every fixed d in $\mathfrak{o}$, consider the equation $a_{qn+i} = d$. For every fixed value of i, the equation has at most 2 solutions. If $\mathfrak{p}\nmid 2$ (resp. $\mathfrak{p}\,|\,2$) then there is at most one (resp. two) values of i in the range $0 \leqslant i < q$ for which there is more than one solution. If $\mathfrak{p}\,|\,2$ and the equation has 2 solutions when $i = i_1, i_2$ where $0 \leqslant i_1 < i_2 < q$, then $2(i_2 - i_1) = q$.

Proof. The proof of Theorem 1 of [2] can be used to prove this lemma. Note that there is considerable simplification since we do not need as sharp a result as in [2].

If A and B are non-zero integers of an algebraic number field L, then a prime ideal $\mathfrak{p}$ of the ring of integers of L is called a *primitive divisor* of $A^n - B^n$ if $\mathfrak{p}\,|\,A^n - B^n$ and $\mathfrak{p}\nmid A^s - B^s$ for all s in the range $0 < s < n$. Using Baker's method and a result of Blanksby and Montgomery ([1]), Schinzel ([8]) has proved the following result.

LEMMA 2. *If $(A, B) = 1$ and A/B is not a root of unity, then $A^n - B^n$ has a primitive divisor for all $n \geqslant n_0(d)$ where $n_0(d)$ is an effectively computable constant depending only on the upper bound d for the degree of A/B.*

Before showing how the lemmas lead to the theorem, let us set up some preliminary notation. Let $\{a_n\}$ be a second order non-degenerate linear recurrence in K satisfying (1). By a well known result ([3], p. 85), there is a finite extension K' of K containing integers M', N', and R with

$$M = M'R, \quad N = N'R^2, \quad \text{and} \quad (M', N') = 1.$$

Let $\{U_n\}$, $\{U'_n\}$, and $\{V_n\}$ be the Lucas sequences defined by

$$\begin{aligned} U_{n+2} &= MU_{n+1} - NU_n, & U_0 &= 0, & U_1 &= 1, \\ U'_{n+2} &= M'U'_{n+1} - N'U'_n, & U'_0 &= 0, & U'_1 &= 1, \\ V_{n+2} &= MV_{n+1} - NV_n, & V_0 &= 2, & V_1 &= M. \end{aligned} \tag{3}$$

Just as in [2], § 2, these sequences can be expressed as

$$U_n = R^{n-1}U'_n = \frac{\beta_1^n - \beta_2^n}{\beta_1 - \beta_2}, \quad U'_n = \frac{\beta_1'^n - \beta_2'^n}{\beta'_1 - \beta'_2}, \quad \text{and} \qquad V_n = \beta_1^n + \beta_2^n, \tag{4}$$

where β_1, β_2 (resp. β'_1, β'_2) are the roots of the companion polynomial (2) (resp. $x^2 - M'x + N' = 0$). Also, one has some obvious generalizations of formulas in [2], § 2:

$$a_n = U_na_1 - NU_{n-1}a_0, \tag{5}$$

$$\beta_1^n = V_n/2 + (\beta_1 - \beta_2)U_n/2 \quad \text{and} \quad \beta_2^n = V_n/2 - (\beta_1 - \beta_2)U_n/2, \tag{6}$$

$$a_{rn+i} = \left(\frac{V_r}{2}\right)^n \sum_{j=0}^{\infty} \left\{\frac{c_iU_r}{V_r}\binom{n}{2j+1} + a_i\binom{n}{2j}\right\}\left(\frac{DU_r^2}{V_r^2}\right)^j, \tag{7}$$

where $c_i = 2a_{i+1} - Ma_i$ and $D = M^2 - 4N$. Let $P = \prod_{\substack{\mathfrak{p}|R \\ \mathfrak{p}\nmid M'}} \mathfrak{p}$.

If $\mathfrak{p}$ is a prime of K' which divides N', then since $(M', N') = (\beta_1' + \beta_2', \beta_1'\beta_2') = 1$, one has $\mathfrak{p} \nmid \beta_1'^n - \beta_2'^n$ for all $n > 0$. If $\mathfrak{B}$ is any ideal of K' such that $(\mathfrak{B}, N') = 1$, then by (4), there is a least positive integer t such that $\mathfrak{B} \mid U_t'$. Now since $(\mathfrak{B}, N') = 1$, an easy induction using (3) together with $U_1' = 1$ shows that for every s, no prime divisor of $\mathfrak{B}$ can divide (U_s', U_{s-1}'). The natural generalization of (7) of [2.I] shows the identity

$$U_{ut+v}' = U_{ut}' U_{v+1}' - N' U_{ut-1}' U_v'$$

for all $u \geqslant 0$ and v in the range $0 \leqslant v < t$. Since $U_0' = 0$, it follows that $\mathfrak{B} \mid U_{ut}'$ for all $u \geqslant 0$. Now if there were a least positive $n = ut + v$ with $0 < v < t$ and $\mathfrak{B} \mid U_n'$, then the identity shows that $\mathfrak{B} \mid U_v'$ since $(\mathfrak{B}, N' U_{ut-1}') = 1$. This contradiction proves that for every $n \geqslant 0$, we have $\mathfrak{B} \mid U_n'$ iff $t \mid n$.

Proof of Theorem 1. With the notation of the last three paragraphs, let us bound the number of occurrences in $\{a_n\}$ of some integer $d \in \mathfrak{o}$. Clearly, we may assume that d occurs at least once in $\{a_n\}$, and so by translation that $a_0 = d$. One can factor the ideal generated by d as

$$(d) = \mathfrak{A}\mathfrak{B}\mathfrak{C}$$

where $\mathfrak{A} = (a_0, a_1)$, no prime divisor of $\mathfrak{B}$ divides (M, N), and every prime divisor of $\mathfrak{C}$ divides (M, N). Since $\mathfrak{A}(M, N) \mid a_n$ for all $n \geqslant 2$ by equation (1), it may be assumed that $\mathfrak{C}$ is divisible by (M, N). Since $(d) = (a_0) = \mathfrak{A}\mathfrak{B}\mathfrak{C}$, $(\mathfrak{B}, a_1\mathfrak{A}^{-1}) = 1$, and $(R, \mathfrak{B}) = 1$, we see by the last paragraph and (5) and (4) that for every $n \geqslant 0$, $\mathfrak{A}\mathfrak{B} \mid (a_n)$ iff $\mathfrak{B} \mid (U_n)$ iff $\mathfrak{B} \mid (U_n')$ if $t \mid n$ where t is the least positive integer with $p\mathfrak{B} \mid U_n'$.

The degree $D = [K(\beta_1, \beta_2): Q]$ is at most $2[K: Q]$. Further, each rational prime can split into at most D primes in $K(\beta_1, \beta_2)$, and the ramification indices of each of these primes is at most D ([3]). So certainly there are no more than $3D^2 \leqslant 12[K: Q]^2$ primes of $K(\beta_1, \beta_2)$ for which the quantity $\varkappa$ in Lemma 1 cannot be taken to be one. Also by [3], p. 85, there are algebraic numbers A, B and b such that

$$\beta_1 = Ab, \quad \beta_2 = Bb, \quad \text{and} \quad (A, B) = 1.$$

Clearly, $A/B = \beta_1/\beta_2$ has degree at most $2[K: Q]$. By Lemma 2, it follows that for r equal to at least one of the first $12[K: Q]^2 + 1$ multiples of t greater than $n_0(2[K: Q])$, the quantity $\beta_1^r - \beta_2^r = b^r(A^r - B^r)$ has a prime divisor $\mathfrak{p}$ which does not divide (M, N) and for which $\varkappa$ may be taken to be 1. By the paragraph preceding the beginning of the proof, $(\mathfrak{p}, N') = 1$; and so it follows that $\mathfrak{p} \nmid (N)$. Letting s denote the multiplicative order of $V_r/2 \pmod{\mathfrak{p}}$, we see by (6) that $\beta_1^{rs} \equiv \beta_2^{rs} \equiv 1 \pmod{\mathfrak{p}}$.

There is an integer a in an extension field of K such that $(a) = (a_0, a_t)$ ([3], p. 85). Letting $\{a_{nt}'\}$ be the sequence defined by $a_{nt}' = a_{nt}/a$, we see by (7) that

$$(8) \qquad a_{rn+ti}' \equiv \left(\frac{V_r}{2}\right)^n a_{ti}' \pmod{\mathfrak{p}}$$

for $n \geqslant 0$ and $0 \leqslant i < r/t$. Now by the choice of t, $(d/a) = (a_0') \mid \mathfrak{B}\mathfrak{C}$ and so $(\mathfrak{p}, a_0') = 1$. If $(a_{ti}', \mathfrak{p}) \neq 1$, then the congruence (8) shows that d/a cannot occur in the subsequence $\{a_{rn+ti}'\}$. On the other hand, if $(a_{ti}', \mathfrak{p}) = 1$, then the same congruence shows that for fixed i, there is at most one value of j in the range $0 \leqslant j < s$ such that d/a occurs in the subsequence $\{a_{rsn+rj+ti}'\}$. By Lemma 1 applied with $\{a_n\}$, $\mathfrak{p}$, and $q \mid rs$, we see that d can occur no more than $r/t + 2$ times in the sequence $\{a_{tn}\}$. By the first paragraph of the proof and the analogue of Lemma 7 in [2], d can occur at most once outside of this subsequence. Thus d occurs at most

$$\frac{r}{t} + 3 \leqslant \frac{n_0(2[K: Q]) + (12[K: Q]^2 + 2)t}{t} + 3$$
$$\leqslant n_0(2[K: Q]) + 12[K: Q]^2 + 5$$

times in $\{a_n\}$. Since this bound depends only on $[K: Q]$, Theorem 1 is proved.

2. Biquadratic forms. Let $f(x, y)$ be an irreducible totally complex binary biquadratic form with rational integer coefficients. It will first be shown under one additional assumption that if the diophantine equation

$$(9) \qquad f(x, y) = 1$$

has at least one solution, then the number of solutions is twice the number of times a certain quantity occurs in a particular second order linear recurrence.

Suppose equation (9) has at least one solution. Then after a unimodular change of variables, it may be assumed that $(x, y) = (1, 0)$ is a solution; hence $f(x, 1)$ is a monic polynomial. If η is a root of $f(x, 1) = 0$, then equation (9) can be interpreted as saying that $x - \eta y$ has norm one. By the Dirichlet unit theorem ([3]) and the assumption that $f(x, y)$ is totally complex and irreducible, the rank of the unit group of $\boldsymbol{Z}[\eta]$ is one. If ξ is a fundamental unit for $\boldsymbol{Z}[\eta]$, then $x - \eta y = \zeta\xi^n$ where n is an integer and ζ is a root of unity in $\boldsymbol{Z}[\eta]$. Further since η is irrational, each pair (ζ, n) corresponds to at most one solution of equation (9).

Assume now that $\boldsymbol{Z}[\eta]$ contains no roots of unity other than ± 1. Since η is of degree 4, this is equivalent to assuming that $\boldsymbol{Z}[\eta]$ contains no primitive cube, fourth, or fifth roots of unity. For every integer n, we have

$$(10)\qquad \xi^n \equiv c_{0n}+c_{1n}\eta+c_{2n}\eta^2+c_{3n}\eta^3$$

where the c_{in} are rational integers. The assumption implies that the number of solutions of equation (9) is twice (one for each value of $\zeta = \pm 1$) the number of solutions of $c_{2n} = c_{3n} = 0$.

Applying automorphisms to equation (10) mapping $(\eta, \xi) = (\eta_1, \xi_1)$ to the conjugate pairs (η_i, ξ_i), $i = 2, 3, 4$, one obtains a system of linear equations

$$\xi_i^n = \sum_{j=0}^{3} c_{jn}\eta_i^j, \qquad i = 1, \ldots, 4,$$

in the variables $c_{0n}, \ldots, c_{3n}$. By Cramer's rule and the fact that the discriminant of η is non-zero, the condition that $c_{2n} = c_{3n} = 0$ is equivalent to

$$\det(1, \eta_i, \eta_i^2, \xi_i^n) = \det(1, \eta_i, \xi_i^n, \eta_i^3) = 0$$

which can be written as

$$\sum_{i=1}^{4} A_i\xi_i^n = \sum_{i=1}^{4} B_i\xi_i^n = 0,$$

where A_i and B_i are the appropriate minors. For fixed k, it follows that

$$(11)\qquad d_n = B_k\sum_{i=1}^{4} A_i\xi_i^n - A_k\sum_{i=1}^{4} B_i\xi_i^n = \sum_{i\neq k}(A_iB_k-A_kB_i)\,\xi_i^n = 0.$$

Now it is easy to verify that

$$(12)\qquad \frac{B_k}{A_k} = \frac{(-1)^{k+3}\det(1, \eta_i, \eta_i^3)_{i\neq k}}{(-1)^{k+4}\det(1, \eta_i, \eta_i^2)_{i\neq k}} = -\sum_{i\neq k}\eta_i = \eta_k - \mathrm{Tr}(\eta) \notin \boldsymbol{Q}.$$

Since

$$c_{2n} = \Delta^{-1}\sum_{i=1}^{4} A_i\xi_i^n \quad \text{and} \quad c_{3n} = \Delta^{-1}\sum_{i=1}^{4} B_i\xi_i^n$$

(where $\Delta = \det(1, \eta_i, \eta_i^2, \eta_i^3)$) are rational integers, it follows by linear independence and (11) and (12) that $c_{2n} = c_{3n} = 0$ if and only if $d_n = 0$. Rearranging equation (11) we see that the number of solutions of equation (9) is twice the number of solutions of

$$(13)\qquad a_n = \sum_{i\neq j,k}(A_iB_k-A_kB_i)(\xi_i/\xi_j)^n = A_kB_j - A_jB_k$$

where $j \neq k$ is fixed. Now this last equation has at least one solution (viz. $n = 0$) but cannot have infinitely many solutions since equation (9) has but finitely many solutions by a theorem of A. Thue [9]; hence the left member of (13) cannot be identically zero. This establishes the assertion made in the first paragraph of this section.

It may happen that ξ is only of degree two. In this case, we may assume that the notation has been chosen so that $\xi_1 = \xi_3$, $\xi_2 = \xi_4$, $j = 3$, and $k = 4$. Equation (12) and its analogue with k replaced with 2 shows that the coefficient of ξ_2/ξ_j in (13) is non-zero. Since $\xi_1/\xi_3 = 1$ and $n = 0$ is a solution of (13), it follows that the other solutions are multiples of the multiplicative order of ξ_2/ξ_3. Since the other solutions are finite in number, it follows that there cannot be any. Therefore in this case equation (9) has but two solutions. Assume henceforth that ξ is of degree four.

Consider now the case where the linear recurrence in (13) is degenerate. For some pair i, j with $i \neq j$, one has $\xi_i/\xi_j = \zeta$ where ζ is a primitive rth root of unity. Since $\boldsymbol{Q}(\xi_i, \xi_j)$ is of degree at most three over $\boldsymbol{Q}(\xi_j)$, the only possible values for r are 2, 3, 4, and 6.

If $r = 3, 4$, or 6, then the minimal polynomial for ξ_i over $\boldsymbol{Q}(\xi_j)$ is

$$x^2+\xi_j^2 = 0 \quad \text{or} \quad x^2 \pm \xi_j x + \xi_j^2 = 0.$$

Further if ξ_k denotes the other solution of this equation, then the fourth conjugate ξ_m lies in $\boldsymbol{Q}(\xi_j)$. Applying any automorphism mapping ξ_i to ξ_m gives $\xi_m/\xi_n = \zeta^{\pm 1}$ where $n \neq m$. Thus

$$\xi_m/\xi_j = (\xi_m/\xi_n)(\xi_n/\xi_j) = \zeta^{\pm 1+\varepsilon}$$

where $\varepsilon = 0, 1$, or -1 depending on the value of n. It follows that

$$1 = \xi_i\xi_j\xi_k\xi_m = (\zeta\xi_j)\,\xi_j(\zeta^{-1}\xi_j)(\zeta^{\pm 1+\varepsilon}\xi_j),$$

and so ξ_j is a root of unity, which is absurd. Therefore $r = 2$ and $\xi_i/\xi_j = -1$. Applying an automorphism mapping ξ_i to ξ_k where $k \neq i, j$ one gets $\xi_k/\xi_m = -1$. Since the ξ's are distinct, one has $m \neq i, j, k$. The product of the conjugates of ξ is one; so it follows that the four conjugates are of the form $\xi, \xi^{-1}, -\xi, -\xi^{-1}$. Now (12) for $k = 1, \ldots, 4$ shows that the coefficients $A_iB_k - A_kB_i$ in equation (13) are all non-zero. With the notation of that equation, the form of the ξ's makes it clear that ξ_i/ξ_j is -1 for one value of $i \neq j, k$ and is a power of ξ for the other such value of i (and so in particular is not a root of unity). It follows that equation (13) has at most one solution of each parity. Thus, if the recurrence is degenerate, then equation (9) has at most four solutions.

Next it will be shown that, if for $v = 2$ or 3, there is a prime ideal $\mathfrak{p}$ of the ring of integers of $\boldsymbol{Q}(\xi_1, \ldots, \xi_4)$ such that

$$(\xi_1^v - \xi_2^v)/(\xi_1 - \xi_2) \equiv 0 \pmod{\mathfrak{p}^{\varkappa}}$$

where

$$\varkappa = \begin{cases} -\left[\dfrac{-3e}{p-1}\right] & \text{if} \quad \mathfrak{p}\nmid 2, \\ 4e & \text{if} \quad \mathfrak{p}\,|\,2 \end{cases}$$

and e is the ramification index of $\mathfrak{p}$ over the rational prime p which lies under it, then any non-degenerate second order linear recurrence whose companion polynomial has roots ξ_1/ξ_3 and ξ_2/ξ_3 is of multiplicity at most four. This in turn will imply that equation (9) has at most eight solutions in this case. To avoid repetition, the reader is referred to the relevant parts of the proof of Theorem 1.

Suppose first that $\mathfrak{p}\nmid 2$. Let $\beta_i = \xi_i/\xi_3$ for $i = 1, 2$. Since ξ_3 is a unit, one has

$$(\beta_1^v - \beta_2^v)/(\beta_1 - \beta_2) \equiv 0 \pmod{\mathfrak{p}^{\varkappa}}.$$

The argument of Theorem 1 can now be repeated letting $r = tv$ and s be the multiplicative order of $V_r/2 \pmod{\mathfrak{p}^{\varkappa}}$.

Now suppose that $\mathfrak{p}\,|\,2$. With β_i defined as before, one has

$$U_v = (\beta_1^v - \beta_2^v)/(\beta_1 - \beta_2) \equiv 0 \pmod{\mathfrak{p}^{4e}}.$$

Let t be as in the first paragraph of the proof of Theorem 1 and set $r = tv$. Then $U_v\,|\,U_r$ and so $V_r/2 = U_r(\beta_1 - \beta_2)/2 + \beta_2^r$ is a $\mathfrak{p}$-adic unit. It follows that $U_r/V_r \equiv 0 \pmod{\mathfrak{p}^{3e}}$. Therefore by (7), one still has (8) holding true modulo $\mathfrak{p}^{3e}$. Letting s denote the multiplicative order of $V_r/2 \pmod{\mathfrak{p}^{3e}}$, the argument of the first and third paragraph of the proof of Theorem 1 shows that d occurs only in the subsequence $\{a_{tn}\}$, and for each i with $0 \leqslant i < v$, there is at most one j in the range $0 \leqslant j < s$ such that d occurs in the subsequence $\{a_{rsn+rj+ti}\}$. In particular, it follows by Lemma 1 that d occurs at most twice in each subsequence $\{a_{rn+ti}\}$. If $v = 2$, then one has consequently $m(d) \leqslant 4$.

Assuming that $v = 3$, the same conclusion may be drawn as soon as one knows that at most one of the subsequences contains more than one occurrence of d. Working now with the linear recurrence $\{a_{tn}\}$, let q be the least positive integer such that $\beta_1^{tq} \equiv \beta_2^{tq} \equiv 1 \pmod{\mathfrak{p}^{3e}}$. Since $\mathfrak{p}^{4e}\,|\,U_3$, one has $\mathfrak{p}\nmid \beta_1 - \beta_2$; and for every $n \geqslant 0$, $\mathfrak{p}\,|\,U_n$ iff $\mathfrak{p}^{4e}\,|\,U_n$ iff $3\,|\,n$. Thus $\mathfrak{p}\,|\,U_{qt}$ and $3\,|\,qt$. If $3\,|\,t$, then $\mathfrak{p}^{4e}\,|\,U_t$ and the argument of the last paragraph with t replacing r shows that $m(d) \leqslant 2$. Assume therefore that $3\,|\,q$ and that two subsequences $\{a_{rsn+ti}\}$ and $\{a_{rsn+tj}\}$ where $0 \leqslant i < j < 3s$ both contain two occurrences of d. Since $tq\,|\,rs$, there are two subsequences, say $\{a_{tqn+tk}\}$ and $\{a_{tqn+tm}\}$ (where $0 \leqslant k < m < q$) both containing two occurences of d. By Lemma 1, this means that $2(k-m) = q \equiv 0 \pmod 3$, and so both subsequences are contained in a single subsequence $\{a_{rn+wt}\}$ where $w \equiv k \equiv m \pmod 3$. Therefore this subsequence contains four occurrences of d, contradicting the result of the last paragraph. Thus $m(d) \leqslant 4$ in this case also.

It remains to investigate conditions under which appropriate prime ideals can be shown to exist. The non-existence of appropriate primes will be shown to correspond to solutions of one of a finite number of binary quintic diophantine equations. To do this, note first that since the ramification index of any prime is certainly no larger than the field degree, the definition of $\varkappa$ shows that there are at most a finite number of prime ideals for which $\varkappa$ can be greater than one. Taking norms, it follows that if

$$N_v = \prod_{i<j} (\xi_i^v - \xi_j^v)/(\xi_i - \xi_j) \quad \text{for} \quad v = 2 \text{ or } 3$$

is not one of some finite set of values, then a suitable prime exists.

Letting $g(x) = x^4 - bx^3 + cx^2 - dx + e$ be the minimal polynomial for ξ, one can compute

$$N_2 = bcd - d^2 - b^2 e \tag{14 }$$

using the cubic resolvant ([10], p. 181). As for N_3, note that

$$\begin{aligned} N_3 &= \prod_{i<j} (\xi_i^2 + \xi_i\xi_j + \xi_j^2) = \prod_{i<j} (\xi_j - \zeta^2\xi_i)(\xi_i - \zeta^2\xi_j) \\ &= \frac{1}{e(1-\zeta^2)^4} \prod_{i,j} (\xi_i - \zeta^2\xi_j) = \frac{\zeta}{e(1-\zeta)^4} \prod_{i,j} (\xi_i - \zeta^2\xi_j) \\ &= \frac{1}{e(1-\zeta)^4} \operatorname{Res}\big(g(x), g(\zeta x)\big) \end{aligned}$$

where ζ is a primitive cube root of unity and Res denotes the resultant. A straightforward but somewhat lengthy calculation of the determinant defining the resultant shows that

$$-N_3 = y^3 - c^2y^2 - 3c^2ey + c^3(d^2 + b^2e - ce)$$

where $y = bd - e$. Since $e = 1$, combining this with equation (14) yields

$$-N_3 = y^3 - c^2y^2 - 3c^2y + c^3(cy - N_2). \tag{15}$$

These quintics for the various exceptional values of N_2 and N_3 are the desired set of diophantine equations.

To complete the proof of the theorem, note first that if $\boldsymbol{Z}[\eta]$ contains non-real roots of unity, then equation (9) has at most eight solutions by the theorem of T. Nagell quoted in the introduction. Further, a given ξ can be the fundamental unit of at most finitely many rings $\mathbf{Z}[\eta]$, and for a given value of ξ these can be effectively determined ([4]). Therefore in order to prove Theorem 2, it suffices to prove that each of the equations (15) has but a finite number of solutions. But this follows from a theorem of C. Runge ([7]) and the following lemma.

LEMMA. *The polynomial*

$$y^3 - x^2y^2 - 3x^2y + x^4y - Ax^3 + B$$

where $A \neq 0$ and B are integers is irreducible over the field $\mathbf{Q}$ of rational numbers.

Proof. If not, then it is a product of two polynomials whose leading forms must be monomial factors of x^4y. Substituting any complex value for x or for y yields a polynomial in one variable which is not identically zero; hence the polynomial in question has no non-trivial factors involving only one variable. In particular, there are no linear factors. If there is a factor with leading coefficient x^2, then there is one of the form $ax^2 + bx + c - y$ where $a \neq 0$ is rational. Substituting $y = ax^2 + bx + c$ into the polynomial gives a sextic polynomial in x with leading coefficient $a^3 - a^2 + a$. Since this polynomial is identically zero and $a \neq 0$ is rational, we have a contradiction. If there is a factor with leading form axy, say $axy - bx + cy - d$, then substituting $y = (bx+d)/(ax+c)$ into the polynomial and clearing denominators shows that $ax + c \mid bx + d$. So there must be a linear factor, which we have already seen to be untrue. This exhausts all possibilities; so the lemma, and hence Theorem 2 are proved.

References

[1] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. 18 (1971), pp. 355–369.

[2] K. K. Kubota, *On a conjecture of Morgan Ward*, I and II, ibid. 33 (1977), pp. 11–28; 29–48.

[3] H. B. Mann, *Introduction to Algebraic Number Theory*, Ohio State Univ. Press, Columbus, Ohio, 1955.

[4] T. Nagell, *Quelques propriétés des nombres algébriques du quatrième degré*, Ark. för Mat. 7 (1967–9), pp. 517–525.

[5] — *Sur les représentations de l'unité par les formes binaires biquadratiques du premier rang*, ibid. 5 (1963–5), pp. 477–521.

[6] — *Sur les unités dans les corps biquadratiques primitifs du premier rang*, ibid. 7 (1967–9), pp. 359–394.

[7] C. Runge, *Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen*, J. f. Math. 100 (1887), pp. 425–435.

[8] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. 268/9 (1974), pp. 27–33.

[9] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, ibid. 135 (1909), pp. 284–305.

[10] B. L. van der Waerden, *Modern Algebra*, vol. I, Frederick Ungar Publ. Co., New York 1949.

Received on 23. 4. 1975
and in revised form on 30. 12. 1975 (700)