If $M' = \pm\sqrt{2}$, $N' = 3$, and $r = 2$, then $M'^2 - 4N' = -10 \equiv 0 \pmod 5$. Also $5 \nmid R$ since $5 \nmid U'_r = U'_2 = \pm\sqrt{2}$. So $5 \| M^2 - 4N$. By Theorem A (iii) and (iv), we conclude that $m(d) \leqslant 4$. This completes the proof of Theorem 6.

References

[1] R. Alter and K. K. Kubota, *Multiplicities of second order linear recurrences* Trans. Amer. Math. Soc. 178 (1973), pp. 271–284.

[2] R. Apéry, *Sur une équation diophantienne*, Comptes Rendus, Paris, 251 (1960), pp. 1263–1264.

[3] Z. Borevič and I. R. Šafarevič, *Number Theory*, Academic Press, New York 1966.

[4] J. W. S. Cassels, *On the diophantine equation* $a^x - b^y = 1$, Amer. J. Math. 75 (1953), pp. 159–162.

[5] P. Chowla, S. Chowla, M. Dunton, and D. J. Lewis, *Some diophantine equations in quadratic number fields*, Det. Kong. Norske Videnskabers Selskabs Forhandlinger 31 (1958), pp. 181–183.

[6] S. Chowla, M. Dunton, and D. J. Lewis, *Linear recurrences of order two*, Pacific J. Math. 11 (1961), pp. 833–845.

[7] R. R. Laxton, *Linear recurrences of order two*, J. Austral. Math. Soc. 7 (1967), pp. 108–114.

[8] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), pp. 419–448.

[9] W. J. LeVeque, *On the equation* $a^x - b^y = 1$, Amer. J. Math. 74 (1952), pp. 325–331.

[10] D. J. Lewis, *Diophantine equations: p-adic methods*, Studies in Number Theory, Math. Assoc. of Amer., Washington, D. C., 1969.

[11] E. Lucas, *Théorie des fonctions simplement périodiques*, Amer. J. Math. 1 (1878), pp. 184–240.

[12] K. Mahler, *Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen*, Proc. Amsterdam Acad. 38 (1935), pp. 50–60.

[13] T. Nagell, *The Diophantine equation* $x^2 + 7 = 2^n$, Norsk Mat. Tidsskr. 30 (1948), pp. 62–64; Ark. f. Mat. 4 (1960), pp. 185–187.

[14] Th. Skolem, S. Chowla, and D. J. Lewis, *The diophantine equation* $2^{n+2} - 7 = x^2$ *and related problems*, Proc. Amer. Math. Soc. 10 (1959), pp. 663–669.

[15] M. F. Smiley, *On the zeros of a cubic recurrence*, Amer. Math. Monthly 63 (1956), pp. 171–172.

[16] R. Strassman, *Über der Wertevorrat von Potenzreihen in Gebiet det p-adischen Zahlen*, J. Reine Angew. Math. 159 (1928), pp. 13–28.

[17] S. B. Townes, *Note on the Diophantine equation* $x^2 + 7y^2 = 2^{n+2}$, Proc. Amer. Math. Soc. 13 (1962), pp. 864–869.

[18] M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J. 21 (1954), pp. 607–614.

Received on 23. 4. 1975
and in revised form on 30. 12. 1975 (698)

ACTA ARITHMETICA
XXXIII (1977)

On a conjecture of Morgan Ward, II

by

K. K. Kubota (Ann Arbor, Mich.)

1. Introduction. This is a continuation of a study [3] of the number of times an integer d occurs in a sequence $\{a_n\}$ of rational integers satisfying a second order linear recurrence relation

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

where M and N are constant integers.

The multiplicity of such a sequence is the supremum of the numbers $m(d)$ as d ranges through the rational integers. The standard conjecture due to Morgan Ward was that the multiplicity of a second order linear recurrence is either infinite or bounded above by five. This conjecture was verified in [3]. In earlier work [1], it was conjectured that in fact the bound of five could be improved to four, and this was verified in the case where $(M, N) = 1$, [3]. As will be seen, the general case is more troublesome and is the main result of this paper.

THEOREM. *The multiplicity of a second order linearly recurring sequence of rational integers is either infinite or bounded above by four.*

As in the first part of this paper, the proof uses Skolem's p-adic method, the only essential difference being a systematic use of exponential diophantine equations of kinds studied by Nagell and Ljunggren. Knowledge of the exact solution sets of these equations allows one to know the sequences for which certain "good" primes do not exist. Since the solutions are quite rare, the exceptional cases can be dealt with individually.

The proof is divided into several parts. In the next section, several reductions are made and the notation is established. The diophantine equations appear in Section 3; and the next two sections are devoted to several special classes of sequences needed in the proof given in the final section. Because we will constantly be making reference to results in [3], the numbering of lemmas begun there will be continued in this paper; any reference without a bracketed number is either to this paper or to [3].

2. Preliminary reductions. We establish here notation which will remain in effect throughout the paper. Let $\{a_n\}$ be a non-degenerate second order linear recurrence of rational integers satisfying

$$a_{n+2} = Ma_{n+1} - Na_n, \quad n \geqslant 0, \quad M, N \in \mathbf{Z}. \tag{1}$$

As in [3], the degenerate sequences are all easily dealt with, and so it suffices to show that the multiplicity $m(d)$ of any integer d in $\{a_n\}$ is at most four.

By Theorem A (i), we may assume that $M^2 - 4N < 0$. Also we may assume $(M, N) \neq 1$ by Theorem 3. If $d = 0$, and $a_n = a_m = d$ with $n < m$, then by [3, Eq. (9)], we have $a_{(m-n)k+n} = 0$ for all $k \geqslant 0$. But this contradicts Theorem 2. Thus $m(0) \leqslant 1$ and so we may assume d is non-zero. Clearly we may assume that $a_0 = d$ and $(a_0, a_1) = 1$. Next, write $d = d_1 d_2$ where no prime divisor of d_1 divides (M, N) and every prime divisor of d_2 divides (M, N). By Lemma 4, either $m(d) \leqslant 1$ or else there is a positive integer r_1 such that $d_1 | a_n$ exactly when $r_1 | n$. Thus the multiplicity of d in $\{a_n\}$ is the same as the multiplicity of d_2 in $\{a_{r_1 n}/d_1\}$. Therefore we may assume that every prime divisor of d also divides (M, N). Since the recurrence relation (1) implies that (M, N) divides a_n for $n \geqslant 2$, we may assume conversely that every prime divisor of (M, N) also divides d.

Let $\{U_n\}$ and $\{V_n\}$ be the Lucas sequences

$$U_{n+2} = MU_{n+1} - NU_n, \quad U_0 = 0, \quad U_1 = 1,$$
$$V_{n+2} = MV_{n+1} - NV_n, \quad V_0 = 2, \quad V_1 = 1.$$

If $U_2 = M$ has an odd prime divisor p which does not divide N, then $p \nmid Nd$ and so $m(d) \leqslant 2 + \delta + \varepsilon \leqslant 4$ by Theorem 2. If M is even and N is odd, then $2 \nmid Nd$ and so $m(d) \leqslant 4$ by Lemma 5. Thus we may assume that every prime divisor of M also divides N.

If p is a rational prime and a is a real number such that a^2 is a rational integer, then we denote by $v_p(a)$, the number of times p divides a. If $p | (M, N)$ and $v_p(M^2) < v_p(N)$, then $m(d) \leqslant 2$ by Theorem A (ii). So one can assume that $v_p(M^2) \geqslant v_p(N)$ for every prime divisor p of M. It follows that there is a positive real number R, an integer N', and a real number M' with

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

Note that the prime divisors of R^2 are precisely the same as the prime divisors of (M, N). Also since $M'^2 - 4N' = (M^2 - 4N)/R^2 < 0$, it must be that N' is positive.

Let $\{b_n\}, \{U'_n\}, \{V'_n\}$ be the Lehmer sequences defined by

$$a_n = R^{n-1} b_n, \quad U_n = R^{n-1} U'_n, \quad \text{and} \quad V_n = R^n V'_n.$$

Clearly these sequences satisfy the recurrence relations:

$$b_{n+2} = M'b_{n+1} - N'b_n, \quad b_0 = Ra_0, \quad b_1 = a_1,$$
$$U'_{n+2} = M'U'_{n+1} - N'U'_n, \quad U'_0 = 0, \quad U'_1 = 1,$$
$$V'_{n+2} = M'V'_{n+1} - N'V'_n, \quad V'_0 = 2, \quad V'_1 = M'.$$

Further, by [3, Eq. (14)], we have

$$a_n = a_1 U_n - Na_0 U_{n-1},$$
$$b_n = b_1 U'_n - N'Ra_0 U'_{n-1}. \tag{2}$$

Let P be defined by

$$P = \Big(\prod_{\substack{p \mid M \\ p \text{ prime}}} p\Big) \Big/ \Big(\prod_{\substack{\sqrt{p} \mid M' \\ p \text{ prime}}} p^{1/2}\Big).$$

By Theorem B (iv), there is a least positive integer r such that $P | U'_r$. Since $P | d = a_0$, Theorem B (iii) together with (2) shows that $P | b_n$ iff $P | U'_n$ iff $r | n$. Let $Q \subseteq Q'$ be sets of prime divisors of M, r' be the least positive integer with $\big(P, \prod_{p \in Q'} p\big) | U'_{r'}$, and t_i for $i \geqslant -1$ be defined by $t_{-1} = 1$ and

$$t_i = r\Big(\prod_{p \in Q} p\Big)^i \quad \text{for} \quad i \geqslant 0.$$

The significance of the integers r and t_i is shown by the following

LEMMA 7. *For each $i \geqslant 0$, the equation*

$$a_n = \pm d, \quad t_{i-1} | n, \ t_i \nmid n$$

has at most one solution $n \geqslant 0$.

Proof. By Theorem B (iii), the t_i for $i \geqslant 1$ are characterized as being the least positive integers such that $v_p(U'_{t_i}) > v_p(U'_{t_{i-1}})$ for every prime $p \in Q$.

Suppose that for some fixed value of i the equation in question has a solution and that s is the least solution. Since $t_{i-1} | s$ and $t_i \nmid s$, there is a prime divisor p of (M, N) and in fact one in Q if $i \geqslant 1$ such that $v_p(U'_s) = v_p(U'_{t_{i-1}})$. By equation (2), it follows that

$$v_p(d) = v_p(a_s) = v_p(R^{s-1} b_s) = (s-1)v_p(R) + v_p(b_s)$$
$$= (s-1)v_p(R) + v_p(U'_s) = (s-1)v_p(R) + v_p(U'_{t_{i-1}}).$$

If t is any other solution of the equation, then one sees similarly that

$$v_p(d) = (t-1)v_p(R) + v_p(U'_t) \geqslant (t-1)v_p(R) + v_p(U'_{t_{i-1}}).$$

Since $t > s$, we have a contradiction. The lemma is proved.

As a first application of the lemma, note that if $U_r'^2$ has an odd prime divisor p which does not divide d, then $p \nmid N'$ and so $p \nmid R^2 dN' = Nd$. By Theorem 2, the subsequence $\{a_{rn}\}$ contains at most three occurrences of d. By the last lemma, it follows that $m(d) \leqslant 4$. Therefore we may assume that every odd prime divisor of U_r' also divides d (and hence R^2 and (M, N)).

Unless the contrary is explicitly stated, the notation in this section is preserved in the rest of the paper; further all of the additional hypotheses hich we have seen in this section are assumed to apply even though they may not be explicitly stated. Recall that the assumptions are that $\{a_n\}$ is a non-degenerate second order linear recurrence with $M - 4N < 0$, $(M, N) \neq 1$, $a_0 = d$, $(a_0, a_1) = 1$, $(M'^2, N') = 1$, $N' > 0$, $R > 0$, and that if p is a prime (resp. odd prime), then $p|d$ iff $p|(M, N)$ iff $p|R^2$ and that $p|M$ iff $v_p(M^2) \geqslant v_p(N) > 0$ (resp. $p|d$ iff $p|U_r'^2$).

3. Some diophantine equations. A number of results on certain rather special diophantine equations are collected here. In the proof of the theorem, it will be seen that the scarcity of solutions of these and other equations is reflected in the existence of good primes for the p-adic method.

LEMMA 8. *The diophantine equation*

$$9^m = 2x^2 + 1, \quad m, x > 0$$

has the unique solution $m = 1$, $x = 2$.

Proof. We have

$$(3^m + 1)(3^m - 1) = 2x^2$$

and $(3^m + 1, 3^m - 1) = 2$. By unique factorization, it follows that

$$3^m \pm 1 = 2u^2 \quad \text{and} \quad 3^m \mp 1 = v^2$$

where the signs are ordered, $uv = x$, $(u, v) = 1$, v is even, and both u and v are positive. If the upper signs hold, then since v is even, reducing the second equation modulo 4 shows that m is even. But then the second equation expresses 1 as a difference of two non-zero squares, which is absurd. So the lower signs must hold. The first equation can then be expressed as

$$u^2 = \frac{3^m - 1}{3 - 1}.$$

By a theorem of Ljunggren [5], the only solutions are $m = 1, 2$, and 5. But $m = 2$ and 5 are not solutions of the second equation. This proves the lemma.

LEMMA 9. *The diophantine equation*

$$2^k 3^m = x^2 - 1, \quad x, k > 0, \quad m \geqslant 0$$

has only the solutions $(k, m, x) = (3, 0, 3), (3, 1, 5), (4, 1, 7)$, *and* $(5, 2, 17)$.

Proof. Since $k > 0$, $(x-1, x+1) = 2$ and $k \geqslant 3$. Since

$$2^k 3^m = (x+1)(x-1),$$

unique factorization shows that either

$$x \pm 1 = 2^{k-1} 3^m, \quad x \mp 1 = 2$$

or else

$$x \pm 1 = 2^{k-1}, \quad x \mp 1 = 3^m 2$$

where in each case, the signs are ordered. Eliminating x from the first set of equations shows that $2^{k-1} 3^m = \pm 2 + 2$ which means that $m = 0$, $k = 3$, and the sign is positive. The corresponding value of x is 3. On the other hand, eliminating x from the second set of equations gives $3^m \pm 1 = 2^{k-2}$. By a theorem of LeVeque on the Catalan equation ([4], [2]), the only solutions of this last equation are $(k, m, \text{sign}) = (3, 0, +), (3, 1, -)$, $(4, 1, +)$ and $(5, 2, -)$. The corresponding values of x are 3, 5, 7, and 17 respectively. This proves the lemma.

LEMMA 10. *The diophantine equation*

$$x(x^2 - 3y^n) = \varepsilon 2^k$$

where $\varepsilon = \pm 1$, y *is odd and positive,* $n > 1$, *and* $x \neq \pm 1$ *has only the solutions* $(x, y, k, \varepsilon, n) = (2, 1, 1, 1, n)$ *and* $(-2, 1, 1, -1, n)$.

Proof. Since $x|2^k$, if $x \neq \pm 1$, then x is even, $k > 0$, and so $x^2 - 3y^n$ is odd. But then $x = \pm 2^k$. So the equation becomes

$$4^k - 2y^n = \pm \varepsilon.$$

This equation considered modulo three shows that $\pm \varepsilon = 1$. So

$$(2^k + 1)(2^k - 1) = 3y^n$$

and $(2^k + 1, 2^k - 1) = 1$. Unique factorization gives

$$2^k \pm 1 = 3u^n \quad \text{and} \quad 2^k \mp 1 = v^n \tag{3}$$

where $(3u, v) = 1$, $uv = y$, u and v are positive, and the signs are ordered.

By Cassels ([2], Corollary 2), the upper signs can only hold if $k = 1$ or $v = 1$. But then $k = v = u = y = 1$, and we have the stated solutions. If the lower signs hold, then by Cassels ([2], Theorem III), the second equation implies that any odd prime divisor p of n is bigger than k. So if $v > 2$, then $v^n \geqslant v^p > v^k > 2^k + 1$, which is absurd. Since $p > 0$, we know that $v = 2$ is impossible, and clearly $v = 1$ is not a solution. Therefore n must be a power of 2, and so

$$(v^{n/2} + 1)(v^{n/2} - 1) = 2^k,$$

$k > 1$, and $(v^{n/2} + 1, v^{n/2} - 1) = 2$. By unique factorization,

$$v^{n/2} \pm 1 = 2^{k-1} \quad \text{and} \quad v^{n/2} \mp 1 = 2$$

where the signs are ordered. Eliminating $v^{n/2}$ gives $2^{k-1} = 2 \pm 2$, and so $k = 3$; but then (3) implies that $7 = 3u^n$, an obvious impossibility. Thus the bottom signs could not have held, and the lemma is proved.

LEMMA 11. *The diophantine equation*

$$y^2 = \frac{x^m + \varepsilon}{x + \varepsilon'}, \quad m > 0 \text{ and odd}, \quad \varepsilon, \varepsilon' = \pm 1, \quad |x| > 1,$$

has only the solutions $(|y|, x, m, \varepsilon') = (3, 2\varepsilon, 3, -\varepsilon)$ *and* $(11, -3\varepsilon, 5, \varepsilon)$.

Proof. Since m is odd,

$$y^2 - \frac{x^m + \varepsilon'}{x + \varepsilon'} = \frac{\varepsilon - \varepsilon'}{x + \varepsilon'}$$

is an integer. So either $\varepsilon = \varepsilon'$ or else $\varepsilon \neq \varepsilon'$ and $x = \pm 2, \pm 3$.

If $\varepsilon = -\varepsilon'$ and $x = \pm 2$, the equation reads

$$y^2 = \frac{\pm 2^m + \varepsilon}{\pm 2 - \varepsilon} = \frac{2^m \pm \varepsilon}{2 \mp \varepsilon} = 2^m + 1 \text{ or } (2^m - 1)/3.$$

The second possibility is impossible since $3 \nmid 2^m - 1$ for m odd. The first possibility gives

$$|y| \pm 1 = 2^{m-1} \quad \text{and} \quad |y| \mp 1 = 2$$

where the signs are ordered. The bottom signs give no solution and the top signs give $|y| = m = 3$.

If $\varepsilon = -\varepsilon'$ and $x = \pm 3$, the equation reads

$$y^2 = \frac{\pm 3 + \varepsilon}{\pm 3 - \varepsilon} = \frac{3^m \pm \varepsilon}{3 \mp \varepsilon} = (3^m + 1)/2 \text{ or } (3^m - 1)/4.$$

Both possibilities are impossible by a congruence modulo 8 using the fact that m is odd.

If $\varepsilon = \varepsilon'$, the equation becomes

$$y^2 = \frac{(-\varepsilon x)^m - 1}{(-\varepsilon x) - 1}, \quad |x| > 1, \quad m \text{ odd},$$

which by a theorem of Ljunggren [5] has only the solutions $(-\varepsilon x, m) = (3, 5)$. This proves the lemma.

4. Special sequences. A certain number of recurrences do not fit into the general outline of the proof. In order that these not disturb the continuity of the proof, the special arguments required for these exceptional sequences are given in this section.

LEMMA 12. *One has* $m(d) \leqslant 4$ *in each of the following cases*:

(a) $N' = 2, M' = \pm 1, r \equiv 2 \pmod 4$,

(b) $N' = 2, M' = \pm 1, r = 4$,

(c) $N' = 2, M' = \pm\sqrt{7}, r \equiv 2 \pmod 4$,

(d) $N' = 2, M' = \pm\sqrt{3}, r = 2$.

Proof. For the first and third sequences, suppose first that $3 \mid r$. If $M' = \pm 1$ (resp. $M' = \pm\sqrt{7}$), then $U'_6 = \pm 5$ (resp. $\pm 5\sqrt{7}$). Since $6 \mid r$, Lemma 7 shows that there is at most one occurrence of d in $\{a_n\}$ not in $\{a_{6n}\}$. Since $(M'^2, N') = 1$ and $5 \mid U'_6$, we know that $5 \nmid N'$. Therefore, if $5 \nmid d$, then $5 \nmid R^2 d N' = Nd$ and so $a_{6n} = d$ has at most two solutions by Theorem 2. Thus either $m(d) \leqslant 3$ or else $5 \mid d$. But if $5 \mid d$, then by Lemma 7, all but at most two of the occurrences of d in $\{a_n\}$ lie in $\{a_{10n}\}$. But $U'_{10} = \mp 11$ (resp. $\mp 11\sqrt{7}$) if $M' = \pm 1$ (resp. $\pm\sqrt{7}$). If $11 \nmid d$, then as before, $a_{10n} = d$ has at most two solutions and so $m(d) \leqslant 4$. If $11 \mid d$, then $11 \mid U'_r$ and Theorem B (iii) allows one to check that $5 \mid r$. By Lemma 7, there is at most one occurrence of d in $\{a_{10n+i} \mid 0 < i < 10\}$. Since $57 \mid V'_{10}$ and $V'_{10} \mid U_{20}$, Theorem 2 applied to $p = 19$ shows that $\{a_{10n}\}$ contains at most three occurrences of d unless $19 \mid U'_r$. But in cases (a) and (c), $r/10$ is odd; thus $V'_{10} \mid V'_r$ and so $19 \nmid U'_r$ by Theorem B (i). Therefore, in these cases, if $3 \mid r$, then $m(d) \leqslant 4$.

If $3 \nmid r$ and $M' = \pm\sqrt{7}$, then since $5 \mid U'_3 = M'^2 - N'$, Theorem B (iii) implies that $\sqrt{5} \nmid U'_r$. Further, $5 \nmid N'$ since $(M'^2, N') = 1$. Thus $5 \nmid R^2 d N' = Nd$, and so $m(d) \leqslant 4$ by Theorem 2 applied with $p = 5$.

Suppose that $M' = \pm 1$, $r \equiv 2 \pmod 4$, and $3 \nmid r$. Since N' is even and M' is odd, V'_n for $n > 0$ is odd and so $V'_{2n} = V'^2_n - 2N'^n = V'^2_n - 2^{n+1} \equiv 1 \pmod 8$ for $n \geqslant 2$. If $9 \mid V'_r$, then $9 \mid U'_{2r} = V'_r U'_r$ and so $3 \mid 2r$ by Theorem B (iii) and the fact that $3 \parallel U'_4$; but this contradicts $3 \nmid r$. Since $3 \mid V'_2$, it follows that $3 \parallel V'_r$. We have already seen that $V'_r \equiv 1 \pmod 8$ if $r > 2$; and so, since V'_r is odd and $3 \parallel V'_r$, it has a prime divisor $p \geqslant 5$. Since $(V'_r, U'_r) \mid 2$, we have $p \nmid U'_r$ and so $p \nmid Nd$. By Theorem 2 and Lemma 7, it follows that $m(d) \leqslant 1 + 3 = 4$. On the other hand, if $r = 2$, then $U'_r = U'_2 = M' = \pm 1$ and so $(M, N) = 1$ contrary to the reduction hypotheses of Section 2.

Suppose that $M' = \pm 1$ and $r = 4$. Then $U'_4 = \mp 3$ and so R and d have only 3 as a prime divisor. By Lemma 7, there are at most 2 occurrences of d in $\{a_n\}$ but not in $\{a_{12n}\}$. Since $U'_{12} = \pm 3^2 5$, $5 \nmid N' d R^2 = Nd$ and so by Theorem 2, d occurs at most twice in $\{a_{12n}\}$; so $m(d) \leqslant 4$ in this case.

It remains to treat the case (d) where $M' = \pm\sqrt{3}$ and $r = 2$. Since $U'_r = U'_2 = M' = \pm\sqrt{3}$, R^2 and d are divisible by no primes other than three. By Lemma 7, each of the following three equations has at most one solution:

$$a_{2n_1+1} = d,$$
$$a_{6n_2+2i} = d, \quad i = 1 \text{ or } 2,$$
$$a_{18n_3+6j} = d, \quad j = 1 \text{ or } 2.$$

Now $U'_{18} = \pm 3^{5/2}19$ and so by Theorem 2 applied to $p = 19$, the sequence $\{a_{18n}\}$ contains at most two occurrences of d. Therefore, if $m(d) > 4$ then each of the three equations has a solution. Now $\sqrt{3} \| U'_2$ and $3^{3/2} \| U'_6$; so letting s be defined by $3^{s/2} \| R$, and using the fact that the 3-adic orders of a_{2n_1+1}, a_{6n_2+2i}, a_{18n_3+6j}, and d are all equal, we have by (2), Theorem B, and the definition of the sequence $\{b_n\}$ that

$$2n_1(s/2) = (6n_2+2i-1)(s/2)+1/2 = (18n_3+6j-1)(s/2)+3/2.$$

In particular, $s = 1$ and a congruence modulo 3 shows that $i = 1$. Solving for n_1 and n_2 in terms of n_3, we see that

$$a_{18n_3+6j} = a_{18n_3+6j+2} = a_{18n_3+6j+3} = d. \tag{4}$$

Further since $s = 1$, the recurrence relation is

$$a_{n+2} = \pm 3a_{n+1} - 6a_n.$$

The recurrence relation together with (4) allows one to solve for a_{18n_3+6j}. The result is $a_{18n_3+6j} = 0$ (resp. $d/6$) if $M' = \sqrt{3}$ (resp. $-\sqrt{3}$). So by (4), we see that $d = 0$ in both cases. By the assumptions made in Section 2, $d \neq 0$. So $m(d) \leqslant 4$, and the lemma is proved.

LEMMA 13. *One has $m(d) \leqslant 4$ in each of the following cases*:

(a) $N' = 3$, $r \equiv 2 \pmod 4$, *and* $M' = \pm\sqrt{2}$,

(b) $N' = 3$, $r = 2$, *and* $M' = \pm 2$,

(c) $N' = 3$, $r = 3$, *and* $M' = \pm 1$.

Proof. (a) First suppose that $M' = \pm\sqrt{2}$ and $r \equiv 2 \pmod 4$. One has $U'_2 = \pm\sqrt{2}$, $U'_4 = \mp 2^{5/2}$, $U'_8 = \pm 2^{7/2}$, and $U'_{16} = 2^{9/2}79$. Since both r and R^2 are even, Lemma 7 with $Q = Q' = \{2\}$ shows that for $s = 1, 2, 3$, and 4, there is at most one occurrence of d in the subsequence $\{a_{2^s n+2^{s-1}}\}$. If $79 | U'_r$, then $79 | U'_{(r,16)} = U'_2 = \pm\sqrt{2}$ by Theorem B (ii). So $79 \nmid U'_r$ and so $79 \nmid Nd$. By Theorem 2, d occurs at most twice in $\{a_{16n}\}$. Thus it suffices to prove that at most two of the subsequences $\{a_{2^s n+2^{s-1}}\}$ for $s = 1, \ldots, 4$ contain an occurrence of d.

By (2) and the definition of the sequence $\{b_n\}$, the condition that $\{a_{2^s n_s+2^{s-1}}\}$ and d have the same dyadic order is expressible as

$$v_2(d) = (2^s n_s + 2^{s-1} - 1)v_2(R) + v_2(U'_{2^{s-1}}). \tag{5}$$

Using the dyadic orders of the $U'_{2^{s-1}}$ listed above, we see that if (5) holds for $s = 3$ and 4 or for $s = 2$ and 3, then $v_2(R)$ is either only quarter integral or is an integer. But since $M = RM' = \pm R\sqrt{2}$ is an integer, $v_2(R)$ is exactly half integral. Thus, if at least three of the subsequences contain occurrences of d, then these subsequences must be those corresponding to $s = 1, 2$, and 4. From (5) with $s = 1$ and 2, we see that $v_2(R) = 1/2$,

and so solving for n_1 and n_2 in terms of n_4 yields

$$a_{16n_4+8} = a_{16n_4+14} = a_{16n_4+15} = d.$$

Since $v_2(R) = 1/2$, the recurrence relation is

$$a_{n+2} = \pm 2a_{n+1} - 6a_n,$$

and so

$$a_{16n_4+13} = \frac{\pm 2a_{16n_4+14} - a_{16n_4+15}}{6} = \left(\frac{\pm 2 - 1}{6}\right) d.$$

Now $3 | N'$ implies that $3 \nmid d$; and so, since a_{16n_4+13} is an integer, the sign must be negative, i.e. $M' = -\sqrt{2}$. But then using the recurrence relation, one can solve successively for a_{16n_4+12} and a_{16n_4+11} to see that

$$a_{16n_4+11} = d/12.$$

Since $d \neq 0$ and $3 \nmid d$, we have a contradiction which establishes $m(d) \leqslant 4$.

(b) Suppose next that $M' = \pm 2$ and $r = 2$. Since $U'_r = \pm 2$, both R^2 and d have only 2 as a prime divisor. Now $U'_8 = \pm 2^3 7$, and so $7 \nmid Nd$. By Theorem 2 applied with $p = 7$, the equation $a_{8n} = d$ has at most two solutions. Therefore by Lemma 7, the only way that $m(d)$ could exceed 4 is if there are integers n_1, n_2, and n_3 with

$$a_{2n_1+1} = a_{4n_2+2} = a_{8n_3+4} = d.$$

Now $U'_2 = \pm 2$ and $U'_4 = \mp 4$; so by (2) and the definition of $\{b_n\}$, the equality of the dyadic orders of the numbers of this equation is expressible as

$$2n_1 v_2(R) = (4n_2+1)v_2(R)+1 = (8n_3+3)v_2(R)+2 = v_2(d).$$

The first equality implies that $v_2(R) = 1$, but then the second equality cannot hold by a congruence modulo 2. Thus $m(d) \leqslant 4$ in this case.

(c) Suppose that $M' = \pm 1$ and $r = 3$. Since $U'_3 = -2$, both R and d have only two as a prime divisor. Now $U'_{12} = \pm 2^5 5$ and $5 \nmid N'dR^2 = Nd$; so by Theorem 2 applied with $p = 5$, $\{a_{12n}\}$ contains at most two occurrences of d. By Lemma 7, each of the subsequences $\{a_{3n+i} | \ i = 1 \text{ or } 2\}$, $\{a_{6n+3}\}$, and $\{a_{12n+6}\}$ contain at most one occurrence of d each. Therefore if $m(d) > 4$, then there are integers m_1, m_2, and m_3 with $a_{3m_1+i} = a_{6m_2+3} = a_{12m_3+6} = d$ where $i = 1$ or 2. Since $2 \| U'_3$ and $2^4 \| U'_6$, the corresponding equality of dyadic orders is

$$\begin{aligned}(3m_1+i-1)v_2(R) &= (6m_2+2)v_2(R)+1 \\ &= (12m_3+5)v_2(R)+4 = v_2(d).\end{aligned}$$

From the first equality, since $v_2(R)$ is an integer, we have $v_2(R) = 1$, and so $i = 1$ by a congruence modulo 3. Solving for m_1 and m_2 in terms

of m_3 yields

$$a_{12m_3+6} = a_{12m_3+9} = a_{12m_3+10} = d.$$

Since $v_2(R) = 1$ and $R > 0$, we have $R = 2$ and so the recurrence relation is

$$a_{n+2} = \pm 2a_{n+1} - 12a_n.$$

It follows that

$$a_{12m_3+8} = \frac{\pm 2a_{12m_3+9} - a_{12m_3+10}}{12} = \left(\frac{\pm 2 - 1}{12}\right) d.$$

Since a_{12m_3+8} is an integer and $3 \nmid d$, the sign must be negative. But then the recurrence relation al ows one to solve for a_{12m_3+7}:

$$a_{12m_3+7} = \frac{-2(-d/4) - d}{12} = -\frac{d}{24}$$

which is not an integer. Thus $m(d) \leqslant 4$ and the lemma is proved.

LEMMA 14. *If* $N' = 17$, $r \equiv 2 \pmod 4$, *and* $M' = \pm\sqrt{10}$ *or* $\pm\sqrt{58}$, *then* $m(d) \leqslant 4$.

Proof. If $M' = \pm\sqrt{10}$ (resp. $\pm\sqrt{58}$), then $U_3' = -7$ (resp. 41) and $V_6' = -2^3 3^2 97$. If $U_3' \nmid d$, then since $(M'^2, N') = 1$, $U_3' \nmid N'$ and so $U_3' \nmid Nd$. By Theorem 2 applied with $p = |U_3'|$, $m(d) \leqslant 4$. By Theorem B (iii), if $U_3' | d$, then $3|r$ and so $6|r$. Since $r/6$ is odd, we have $V_6' | V_r'$. But then $97 | V_r'$ and so $97 \nmid U_r'$ by Theorem B (i). Therefore $97 \nmid Nd$ and $97 | U_{2r}'$. By Lemma 7 and Theorem 2 applied with $p = 97$, $m(d) \leqslant 3$. This establishes the lemma.

5. Some classes of recurrences. In this section, certain infinite classes of recurrences are treated. The first two lemmas are analogues of Lemmas 4, 5 and Theorem 2 of [1].

LEMMA 15. *If* N *is odd and* r *is even, then* $m(d) \leqslant 4$.

Proof. If in addition M is even, then this is a special case of Lemma 5; so we may assume that M is odd. If β_1 and β_2 are the roots of the companion equation $x^2 - Mx + N = 0$, then it is easy to verify that for $i = 1$ and 2,

$$\beta_i^6 = (M^2 - N)^3 \beta_i^2 - 2(M^2 - N)MN\beta_i + (MN)^2 \equiv 1 \pmod 4$$

and that if $-M \equiv N \equiv 1 \pmod 4$, then

$$\beta_i^3 = M(M\beta_i - N) - N\beta_i \equiv 1 \pmod 4.$$

We will apply Theorem 1 with $p = 2$ and q a factor of 6. Since r is even, Lemma 7 implies that $\{a_{2n+1}\}$ contains at most one occurrence of d; and so by Theorem 1, at most one subsequence $\{a_{qn+i}\}$ with $0 \leqslant i < q$ contains at least (and hence exactly) two occurrences of d. A straightforward computation shows that $\{a_n\}$ considered modulo 4 looks like repetitions of a constant odd multiple of one of the following segments:

$$\left.\begin{matrix} 0, 1, 1, 0, 3, 3 \\ 1, 3, 2, 3, 1, 2 \end{matrix}\right\} \quad \text{if} \quad M \equiv N \equiv 1 \pmod 4,$$

$$0, 1, 1, 2, 3, 1 \quad \text{if} \quad M \equiv -N \equiv 1 \pmod 4,$$

$$0, 1, 3, 2, 1, 1 \quad \text{if} \quad M \equiv -N \equiv 3 \pmod 4,$$

$$0, 1, 3 \text{ or } 1, 1, 2 \quad \text{if} \quad -M \equiv N \equiv 1 \pmod 4.$$

The lemma is now a consequence of Theorem 1 applied with $p = 2$.

LEMMA 16. *If either* $3|M$ *and* $3 \nmid N$ *or else* $N \equiv 1 \pmod 3$, *then* $m(d) \leqslant 4$.

Proof. Since $3 \nmid (M, N)$, we have $3 \nmid d$, R^2, $U_r'^2$. If 3 divides M but not N, then $3|U_2$ and $3 \nmid Nd$ and so $m(d) \leqslant 2 + \delta + \varepsilon \leqslant 4$ by Theorem 2. Suppose that $N \equiv 1 \pmod 3$ and $3 \nmid M$, then $3|U_3 = M^2 - N$ and $3 \nmid Nd$. A straightforward computation shows that the sequence $\{a_n\}$ considered modulo 3 looks like repetitions of a constant non-zero multiple of one of the following segments:

$$\left.\begin{matrix} 1, 1, 0, -1, -1, 0 \\ -1, 1, -1, 1, -1, 1 \end{matrix}\right\} \quad \text{if} \quad M \equiv 1 \pmod 3,$$

$$\left.\begin{matrix} 1, 1, 1, 1, 1, 1 \\ 1, -1, 0, 1, -1, 0 \end{matrix}\right\} \quad \text{if} \quad M \equiv -1 \pmod 3.$$

Theorem 2 applied with $p = 3$ to the first or last kind of sequence yields $m(d) \leqslant 3 + \varepsilon \leqslant 4$. For the second kind of sequence, all occurrences of d appear either in $\{a_{2n}\}$ or else all occur in $\{a_{2n+1}\}$. By [3, Eq. (9)], these subsequences satisfy a recurrence relation with coefficients $V_2 = M^2 - 2N \equiv -1 \pmod 3$ and $N^2 \equiv 1 \pmod 3$. Thus we are reduced to considering sequences of the third kind. But in this case, the roots β_1 and β_2 of the companion polynomial $x^2 - Mx + N = 0$ satisfy

$$0 = \beta_i^2 - M\beta_i + N \equiv \beta_i^2 - 2\beta_i + 1 = (\beta_i - 1)^2 \pmod 3$$

and so $\beta_i^3 \equiv 1 \pmod{3\pi}$ for $i = 1, 2$ where π is as in the statement of Theorem 2. By that theorem, it follows that $m(d) \leqslant 3 + \delta = 4$, and so the lemma is proved.

The next three results are concerned with some cases in which r is small.

LEMMA 17. *If* $r = 2$, $V_r' = \pm 2^k$, *and* $M' \not\equiv 2 \pmod 4$, *then* $m(d) \leqslant 4$.

Proof. By Lemma 15, it suffices to treat the case in which N is even. Now $U_3' = M'^2 - N'$ is odd. In fact, if $M'^2 = (U_r')^2$ is odd, then R^2 is odd and so N' is even; and if M'^2 is even, then $v_2(M'^2) \geqslant v_2(N')$ and

so N' is odd. In both cases, $2 \nmid M'^2 - N'$. If $3 | M'^2 - N'$ then $3 \nmid M'^2$ since $(M'^2, N') = 1$. Since $\sqrt{3} \nmid U'_r = M'$, we have $3 \nmid R$ and so $3 | M^2 - N$ and $3 \nmid M$. Thus $N \equiv 1 \pmod 3$ and $m(d) \leqslant 4$ by the last lemma. If $U'_3 = M'^2 - N'$ has a prime divisor $p \geqslant 5$, then $\sqrt{p} \nmid M' = U'_r$ and $p \nmid N'$; so $p \nmid Nd$. Applying Theorem 2 with this prime shows then that $m(d) \leqslant 4$. It follows that either $m(d) \leqslant 4$ or else

$$M'^2 - N' = \varepsilon, \quad \varepsilon = \pm 1.$$

Since also

$$M'^2 - 2N' = V'_r = \pm 2^k,$$

we have

$$N' = \varepsilon \mp 2^k \quad \text{and} \quad M'^2 = 2\varepsilon \mp 2^k.$$

Since $M'^2 \not\equiv 2 \pmod 4$, it must be that $k = 0$ or 1. If $k = 1$, then since $N' > 0$, $N' = \varepsilon + 2$ and $M'^2 = 2\varepsilon + 2$. Now $\varepsilon = -1$ corresponds to a degenerate recurrence; and so, if $k = 1$, then

$$\varepsilon = 1, \quad N' = 3, \quad \text{and} \quad M' = \pm 2.$$

If $k = 0$, then since $N' > 0$, $N' = 1 + 1 = 2$ and $M'^2 = 3$. By Lemmas 12 and 13, $m(d) \leqslant 4$ and so the lemma is proved.

LEMMA 18. *$m(d) \leqslant 4$ in each of the following cases:*
(a) *$r = 4$, N even, M odd, and $V'_4 = \pm 2^k$,*
(b) *$r = 4$, N even, and $V'_4 = \pm 2$.*

Proof. Begin by reducing to the case where $U'_3 = \pm 1$. Note that $U'_3 = M'^2 - N'$ is odd. In fact, if $M = M'R$ is odd, then M'^2 and R^2 are odd, and so $N' = N/R^2$ is even. On the other hand, if $\pm 2 = V'_4 = M'^4 - 4M'^2N' + 2N'^2$, then M'^2 is even, $v_2(M'^2) \geqslant v_2(N)$ and so N' is odd. In either case $M'^2 - N'$ is odd. If p is an odd prime divisor of U'_3, then Theorem B (iii) shows that $\sqrt{p} \nmid U'_4 = U'_r$, and so $\sqrt{p} \nmid R^2 dN' = Nd$. If $p \geqslant 5$, then $m(d) \leqslant 4$ by Theorem 2. If $p = 3$, then $\sqrt{p} \nmid RM' = M$ and so $p | U'_3 R^2 = M^2 - N$ implies $N \equiv 1 \pmod 3$. By Lemma 16, it follows that $m(d) \leqslant 4$. Thus we have reduced to the case where

$$M'^2 - N' = U'_3 = \varepsilon', \quad \varepsilon' = \pm 1.$$

It follows that

$$V'_4 = M'^4 - 4M'^2N' + 2N'^2 = (M'^2 - N')^2 - 2N'(M'^2 - N') - N'^2$$
$$= 1 - 2\varepsilon' N' - N'^2.$$

If $V'_r = V'_4 = 2\varepsilon$, $\varepsilon = \pm 1$, then solving for N' yields

$$N' = -\varepsilon' \pm \sqrt{2(1 - \varepsilon)}.$$

Since $N' > 0$, we have $(\varepsilon, \varepsilon', N') = (1, -1, 1)$, $(-1, 1, 1)$, or $(-1, -1, 3)$. The corresponding values for $M'^2 = N' + \varepsilon'$ are 0, 2, and 2 respectively.

Now the first two cases are degenerate; in the third case $U'_2 = \pm\sqrt{2}$ and $U'_4 = \mp 4\sqrt{2}$ which, by the definition of r, excludes the possibility that $r = 4$. So this case does not occur.

If M is odd and N is even, then V_n and a fortiori V'^2_n is odd for all $n > 0$. So $V'_4 = \varepsilon = \pm 1$. If $\varepsilon = -1$, then solving for N' gives $N' = -\varepsilon \pm \pm\sqrt{3}$, which is impossible since N' is an integer. Therefore $\varepsilon = 1$, and so $N' = -2\varepsilon' = 2$ since $N' > 0$. Also $M'^2 = N' + \varepsilon' = 1$. But then $m(d) \leqslant 4$ by Lemma 12. This completes the proof of the lemma.

LEMMA 19. *The multiplicity $m(d)$ of d is at most four if*

$$M' = \pm 1, \quad N' = \frac{1 + 2^{2s+1}}{3}, \quad r = 3, \quad s \geqslant 0.$$

Proof. The case $s = 0$ is a degenerate sequence, and the case $s = 1$ has already been proved in Lemma 13; so we may assume $s > 1$.

1) Suppose first that d is odd. Since R must then also be an odd integer and $N' \equiv 3 \pmod 8$, we have $N \equiv 3 \pmod 8$. Also, since

$$V'_3 = M'(M'^2 - 3N') = \mp 2^{2s+1} \equiv 0 \pmod 8,$$

we have $8 | V_3$. By [3, Eq. (9)], it follows that

$$a_{3(n+2)} \equiv 5a_{3n} \pmod 8.$$

Therefore at most one of the subsequences $\{a_{12n}\}$ and $\{a_{12n+6}\}$ and at most one of the subsequences $\{a_{12n+3}\}$ and $\{a_{12n+9}\}$ can contain an occurrence of d.

If $1 - 4^{s+1} = \pm 3^{m+1}$, then the sign must be negative and $m = 0$ by a theorem of LeVeque ([4], [2]). But then $s = 0$ contrary to hypotesis. Therefore, since

$$V'_2 = M'^2 - N' = (1 - 4^{s+1})/3$$

is odd, there is a prime divisor $p \geqslant 5$ of V'_2. Since $p | U'_4 = V'_2 U'_2$, Theorem B (iii) shows that $p \nmid U'_3 = U'_r$. Thus $p \nmid R^2 dN' = Nd$ and so by Theorem 2, none of the subsequences $\{a_{4n+i}\}$ where $0 \leqslant i < 4$ contain more than two occurrences of d and at most one contains more than one occurrence of d. But then the same must be true of the subsequences $\{a_{12n+3i}\}$ where $0 \leqslant i < 4$. So by the result of the last paragraph, $\{a_{3n}\}$ contains at most three occurrences of d. By Lemma 7, it follows that $m(d) \leqslant 4$, and the lemma is proved in the case where d is odd.

2) Suppose now that d is even. As in part 1) of the proof, the diophantine equation $1 - 4^s = \pm 3^{m+1}$ has no solutions with $s > 1$. Hence $U'_3 = 2(1 - 4^s)/3$ has a prime divisor $p \geqslant 5$.

In order to see that $3 \nmid V'_p$, first note that $3 | U'_3$ if $s \equiv 0 \pmod 3$, $3 | U'_4$ if $s \equiv 2 \pmod 3$, and $3 \nmid U'_n$ for $n > 0$ if $s \equiv 1 \pmod 3$ (since $3 | N'$ in

this last case). Now if $3|V'_p$, then $3|U'_{2p} = V'_p U'_p$, and so in particular $s \not\equiv 1 \pmod 3$. In the other cases, we would have $3|U'_{(2p,3)} = U'_1 = 1$ and $3|U'_{(2p,4)} = U'_2 = \pm 1$ respectively. So $3 \nmid V'_p$.

Since M' and N' are both odd, it is easy to verify using Theorem B (iii) that $2|V'_n$ if and only if $3|n$; so in particular V'_p is odd. Since $M' = V'_1 = \pm 1$, Lemma 1 shows that $V'_p \neq \pm 1$. Therefore there exists a prime divisor $q \geqslant 5$ of V'_p. As before, if $q|U'_3 = U'_r$, then $q|U'_{(3,2p)} = U'_1 = 1$. So $q \nmid U'_r$ and hence $q \nmid R^2 dN' = Nd$. By Theorem 2 applied with the prime q, it follows that d occurs at most twice in $\{a_{2pn}\}$. Since $2p|d$, the integer d occurs at most twice in $\{a_n | 2pr \nmid n\}$ by Lemma 7. Thus $m(d) \leqslant 4$ and the lemma is proved.

LEMMA 20. *The multiplicity $m(d)$ of d is at most 4 if*

$$V'_r = \pm 2^k, \quad N' = 2^k + (-1)^{k+1}, \quad M'^2 = 2\left(2^{k-1} + (-1)^{k+1}\right),$$
$$k \geqslant 3, \quad \textit{and} \quad r \equiv 2 \pmod 4.$$

Proof. The sequence $\{V'_{2n}\}$ satisfies a linear recurrence relation whose characteristic polynomial [3, § 2] has discriminant

$$U'^2_2(M'^2 - 4N') = 2M'^2\left(-2^{k-1}3 + (-1)^k\right).$$

Since $k \geqslant 3$, the last factor has a prime divisor $p \geqslant 5$; so $\{V'_{2n}\}$ has multiplicity at most two by Theorem A (iv). Also $V'_2 = M'^2 - 2N'$ is even, $r \equiv 2 \pmod 4$, and $V'_r = \pm 2^k$. By Theorem B (iii), it follows that $2^k \| V'_2$ and hence that $2^k \| V'_{4n+2}$ for all $n \geqslant 0$.

Suppose that for some odd integer m, we have $V'_{2m} = \varepsilon 2^k$ where $\varepsilon = \pm 1$. Then since $2^{k-1} \equiv (-1)^k \pmod{M'^2/2}$, we have

$$\begin{aligned} V'^2_m = V'_{2m} + 2N'^m &= 2\left\{\varepsilon 2^{k-1} + \left(2^k + (-1)^{k+1}\right)^m\right\} \\ &\equiv 2\left\{\varepsilon(-1)^k + \left(2(-1)^k + (-1)^{k+1}\right)^m\right\} \\ &= 2(-1)^k(\varepsilon + 1)^m \pmod{M'^2/2}. \end{aligned}$$

But also since m is odd, $M' = V'_1 | V'_m$ and so $V'^2_m \equiv 0 \pmod{M'^2/2}$. Now $M'^2/2 \neq \pm 1$ and is odd; combining results, it follows that $\varepsilon = -1$. Since $3|N'$ and $3 \nmid M'^2$, we also know that $3 \nmid V'^2_n$ for all $n \geqslant 0$. Therefore for every $n \geqslant 0$, either there is a prime divisor $p \geqslant 5$ of V'_{4n+2} or else $V'_{4n+2} = -2^k$.

Now suppose that there is an odd prime divisor m of U'^2_r. If $m|r$, then $V'_{2m} | V'_r = \pm 2^k$ and so by the last paragraph, $V'_{2m} = -2^k$. If $m \nmid r$, then again by the last paragraph, either $V'_{2m} = -2^k$ or else V'_{2m} has an odd prime divisor $p \geqslant 5$. Now $p \nmid N'$ and if $\sqrt{p} | U'_r$, then $\sqrt{p} | U'_{(r,4m)} = U'_2 = M'$ by Theorem B (ii). But $M' = V'_1 | V'_m$ and $V'_{2m} = V'^2_m - 2N'^m$; so we have $p|N'$ which we know to be false. Therefore $\sqrt{p} \nmid U'_r$ and so $p \nmid N'R^2 d = Nd$. Since $p | V'_{2m} U'_{2m} R^{4m-1} = U_{4m}$, Theorem 2 implies that

$\{a_{4mn}\}$ contains at most two occurrences of d. By Lemma 7 with $r' = r$ and $Q = \{2, m\}$, there are at most two occurrences of d in $\{a_n\}$ not contained in $\{a_{4mn}\}$; and so $m(d) \leqslant 4$. We have shown that if m is an odd prime divisor of U'^2_r, then either $m(d) \leqslant 4$ or else $V'_{2m} = -2^k$.

Since $V'_2 = M'^2 - 2N' = -2^k$ and V'_{2n} is of multiplicity 2, the last paragraph shows that $m(d) \leqslant 4$ if U'^2_r is divisible by at least two distinct odd primes. Now $M'^2 = 2\left(2^{k-1} + (-1)^{k+1}\right)$ is divisible for $k \geqslant 3$ by an odd prime, say m. By the minimality of r, either $r = 2$ or else U'^2_r is divisible by some odd prime not dividing M'^2. Therefore, we may assume $r = 2$ and $M'^2 = 2m^w$.

Suppose that V'^2_m is divisible by an odd prime $p \neq m$. Since $3|N'$ and $p \nmid U'^2_r = M'^2$, we have $p \geqslant 5$ and $p \nmid Nd$; thus by Theorem 2, d occurs at most twice in $\{a_{2mn}\}$. Lemma 7 applied with $r' = r$ and $Q = \{m\}$ shows that there are at most two occurrences of d not in $\{a_{2mn}\}$, and so $m(d) \leqslant 4$. Assume therefore that V'^2_m is divisible by no primes other than 2 and m. By Theorem B, $m^{w+2} \| U'^2_{2m} = U'^2_m V'^2_m$ and $m \nmid U'^2_m$; so $m^{w+2} \| V'^2_m$. Similarly, $2 \| V'^2_m$. Thus

$$V'^2_m = \pm 2m^{w+2} = \varepsilon m^2 M'^2, \quad \varepsilon = \pm 1.$$

By the third paragraph of the proof, we may assume that $V'_{2m} = -2^k$. But then

$$-2^k = V'_{2m} = V'^2_m - 2N'^m = \varepsilon m^2 M'^2 - 2N'^m,$$

and so by the definitions of N' and M',

$$2\left(N'^m + (-1)^{k+1}\right) = (\varepsilon m^2 + 1)M'^2.$$

Since $2m^w = M'^2 = N' + (-1)^{k+1}$, this gives

$$\begin{aligned} m^{wm} &\leqslant 2\left(\left(2m^w + (-1)^k\right)^m + (-1)^{k+1}\right) = 2\left(N'^m + (-1)^{k+1}\right) \\ &= (\varepsilon m^2 + 1)M'^2 = 2(\varepsilon m^2 + 1)m^w \leqslant 4m^{w+2}. \end{aligned}$$

Since $w \geqslant 1$, this gives $m^{m-3} \leqslant m^{w(m-1)-2} \leqslant 4$ and so $m < 5$. But m was an odd prime divisor of M'^2, and so $m \neq 3$. This contradiction proves the lemma.

6. Proof of the theorem. The notation and assumptions of Section 2 are retained. Suppose that there is an odd prime p with $\sqrt{p} | V'_r$. Since $(M'^2, N') = 1$, we have $\sqrt{p} \nmid N'$. Also $\sqrt{p} \nmid U'_r$ since $(U'_r, V'_r) | 2$ by Theorem B (ii); and so $p \nmid N'dR^2 = Nd$. By Lemma 7, there is at most one occurrence of d in $\{a_n\}$ which does not lie in $\{a_{rn}\}$. If $p \geqslant 5$, then, since $p | V'_r U'_r R^{2r-1} = U_{2r}$, Theorem 2 implies that d occurs no more than three times in $\{a_{rn}\}$. So $m(d) \leqslant 4$. Thus we may assume that $V'_r = \pm 2^k 3^m$ where $2k$ and $2m$ are integers.

Next we treat the case where $m > 0$. We have seen that this implies that $3 \nmid Nd$. By Lemma 16, we may assume that $3 \nmid M$ and that $N \equiv 2$

(mod 3). The sequence $\{V_n\}$ considered modulo three then looks like repetitions of the segment

$$2, M, 0, M, 1, 2M, 0, 2M;$$

so that $r \equiv 2 \pmod 4$ and $\sqrt{3} \nmid V_4'$. Since $M \equiv \pm 1 \pmod 3$, one can verify that $\{a_n\}$ considered modulo three looks like repetitions of the segment

$$1, 1, 2, 0, 2, 2, 1, 0;$$

and so at most three of the subsequences $\{a_{8n+i}\}$, $0 \leqslant i < 8$ contain occurrences of d.

Suppose that there is a prime $p \geqslant 5$ with $\sqrt{p} | V_4'$. If $\sqrt{p} | U_r'$, then by Theorem B (ii), $\sqrt{p} | (U_r', U_8') = |U_{(8,r)}'| = |U_2'| = |M'|$; and since $\sqrt{p} | V_4' = M'^4 - 4M'^2N' + 2N'^2$, we also have $\sqrt{p} | N'$, which contradicts $(M'^2, N') = 1$. Therefore $\sqrt{p} \nmid U_r'$ and so $\sqrt{p} \nmid d, R$. Also since $\sqrt{p} | V_4'$ and $(M'^2, N') = 1$, we have $p \nmid N'$, and so $p \nmid dR^2N' = Nd$. Since also $p | V_4' U_4' R^7 = U_8$, Theorem 2 together with the last paragraph shows that $m(d) \leqslant 4$. So we may assume that no prime $p \geqslant 5$ divides V_4'.

Since we have already seen that $\sqrt{3} \nmid V_4'$, we must have $V_4' = \varepsilon 2^u$ where $\varepsilon = \pm 1$ and $u \in \boldsymbol{Z}$. Since $r/2$ is odd, we have $V_2' | V_r'$ and so $V_2' = \varepsilon' 2^{k'm'}$ where $\varepsilon' = \pm 1$, $k', m' \in \boldsymbol{Z}$. We have

$$\varepsilon 2^u = V_4' = V_2'^2 - 2N'^2 = 4^{k'} 9^{m'} - 2N'^2. \tag{6}$$

If $u = 0$, then $k' = 0$ and the equation considered modulo 3 shows that either $m' > 0$ and $\varepsilon = 1$ or else $m' = 0$. In the second case, the fact that $N' > 0$ shows that $\varepsilon = -1$, $N'^2 = 1$, and $V_2' = \pm 1$; but this is impossible since by [3, Eq. (9)] it follows that the sequence $\{a_{2n}\}$ and therefore $\{a_n\}$ is degenerate. By Lemma 8, the first case occurs only when $m' = 1$ and $N' = 2$. But then since $M'^2 - 2N' = V_2' = 3\varepsilon'$, we see that $M' = \pm\sqrt{7}$ or ± 1; so $m(d) \leqslant 4$ by Lemma 12.

If $u = 1$, then $k' > 0$ by (6). If $m' > 0$, then reducing (6) modulo 3 shows that $\varepsilon = -1$. If $m' = 0$ and $k' \geqslant 2$, then reducing (6) modulo 16 shows that N' is odd and $\varepsilon = -1$. If finally $m' = 0$, $k' = 1$, and $\varepsilon = 1$, then $N'^2 = 1$ and $V_2' = 2\varepsilon'$ which means that $\{a_{2n}\}$ and so $\{a_n\}$ is degenerate. Thus we may assume that $\varepsilon = -1$. By Lemma 9, the only solutions of (6) are then $(k', m', N') = (2, 0, 3)$ and $(3, 1, 17)$. The first solution does not apply since we have $3 \nmid N'$. Using $M'^2 - 2N' = V_2' = \varepsilon' 2^{k'} 3^{m'}$ to solve for M', shows that the corresponding values of M' are $\pm\sqrt{10}$ and $\pm\sqrt{58}$. So $m(d) \leqslant 4$ by Lemma 14.

If $u > 1$, then (6) implies that $k' > 0$ and N' is even. But then $2 | \varepsilon' 2^{k'} 3^{m'} + 2N' = V_2' + 2N' = M'^2$ which contradicts $(M'^2, N') = 1$. Thus the argument of these last six paragraphs shows that we may assume that $m = 0$, i.e. $V_r' = \pm 2^k$.

The next part of the proof is concerned with the case where r is odd. Since r is odd, $V_1' | V_r' = \pm 2^k$; and so, if $k = 0$, then we would have a contradiction with Lemma 1. Therefore $k > 0$. In particular, it cannot be the case that N is even and M is odd, since this would imply that V_n is odd for all $n > 0$. Also if both N and M'^2 are even, then (M, N) is even and so $U_r'^2$ must also be even. But then since $U_2'^2 = M'^2$ is even. Theorem B (iii) shows that $U_n'^2$ is even exactly when n is even; so it follows that r cannot be odd. Finally if N is odd and M is even, then $m(d) \leqslant 4$ by Lemma 5. Thus we may assume that if r is odd, then both M'^2 and N' are odd.

Now $V_n'^2$ is even exactly when $3 | n$; so $3 | r$. We have by [3, Eq. (4)],

$$V_{r/3}' (V_{r/3}'^2 - 3N'^{r/3}) = V_r' = \pm 2^k.$$

Here k is an integer since $V_{r/3}' / M'$ is an integer and $\sqrt{2} \nmid M'$. Now $V_{r/3}'^2$ is an integer, and so this last equation implies that $V_{r/3}'$ is also an integer. By Lemma 10, either $r = 3$ or else $N' = 1$ and $V_r' = \pm 2$. By [3, Eq. (9)], the second possibility implies that $\{a_{rn}\}$ and so $\{a_n\}$ are degenerate contrary to hypothesis. Thus $r = 3$, and so $V_{r/3}' = M' = \varepsilon$ where $\varepsilon = \pm 1$. Solving for N' gives $N' = (1 \mp \varepsilon 2^k)/3$. Since $N' > 0$ is an integer, it must be that $\mp \varepsilon = 1$ and k is odd. But then Lemma 19 shows that $m(d) \leqslant 4$. This completes the proof in case r is odd.

Therefore we may assume that r is even; by Lemma 15, we can also assume that N is even. Suppose in addition that M is odd. Then V_n for $n > 0$ and a fortiori $V_r'^2$ are odd; so $V_r' = \pm 1$. If $2^s \| r$, then $r/2^s$ is odd, and so $V_{2^s}' | V_r' = \pm 1$. By Lemma 1, it follows that $2^s = r$. We have

$$V_{r/2}'^2 - 2N'^{r/2} = V_r' = \pm 1.$$

If $s \geqslant 2$, then $V_{r/2}'$ is an integer and so reducing the equation modulo 8 and using the parity of N', we see that the sign is positive. If $s \geqslant 3$, we therefore have a solution of the diophantine equation $y^2 = 2x^4 + 1$, which by a theorem of Mordell [7] has $(x, y) = (0, \pm 1)$ as its only solutions. Since $N' \neq 0$, this case cannot occur. Therefore $s = 1$ or 2, and so $m(d) \leqslant 4$ by Lemmas 17 and 18.

Assume from now on that r, M, and N are all even. We first treat the case where $2 \| V_r'$. If r is not a power of two, then $r = 2mu$ where m is odd and greater than one. We have

$$V_{mu}'^2 - 2N'^{mu} = V_r' = 2\varepsilon,$$

$$V_u'^2 - 2N'^u = V_{2u}' = 2\varepsilon' \text{ or } \varepsilon'$$

where $\varepsilon, \varepsilon' = \pm 1$.

First consider the case where $V_{2u}' = \varepsilon'$. Since N' and $V_u'^2$ are odd, it is easy to check by the recurrence relation that $V_{nu}'^2$ is even precisely

when $3|n$; therefore $3|m$, $V'_{6u}|V'_r = 2\varepsilon$, $2|V'_{6u}$, and hence $V'_{6u} = 2\varepsilon''$ with $\varepsilon'' = \pm 1$. But then

$$2\varepsilon'' = V'_{6u} = V'_{2u}(V'^2_{2u} - 3N'^u) = \varepsilon'(1 - 3N'^u);$$

and so $N'^u = (1 - 2\varepsilon'\varepsilon'')/3$. Since N'^u is an integer, we have $\varepsilon'\varepsilon'' = -1$ and $N'^u = 1$. But then since $V'_{2u} = \varepsilon' = \pm 1$, the sequence $\{a_{2un}\}$ and hence $\{a_n\}$ is degenerate, contrary to hypothesis.

Now consider the case where $V'_{2u} = 2\varepsilon'$. Since m is odd, $V'_u|V'_{mu}$ and $a = V'_{mu}/V'_u$ is a rational integer. Using the above equations to solve for a^2 gives

$$a^2 = \frac{(N'^u)^m + \varepsilon}{N'^u + \varepsilon'}.$$

Since $N' > 0$, Lemma 11 shows that either $N' = 1$ or else $(N', a, m, u, \varepsilon, \varepsilon') = (2, \pm 3, 3, 1, 1, -1)$ or $(3, \pm 11, 5, 1, -1, -1)$. If $N' = 1$, then $V'_u = 0$ or ± 2; and so by [3, Eq. (9)], $\{a_{un}\}$ is degenerate contrary to hypothesis. In the other cases, $2\varepsilon' = V'_{2u} = V'_2 = M'^2 - 2N'$ can be solved for M'^2; and so we have

$$N' = 2,\ M' = \pm\sqrt{2} \quad \text{or} \quad N' = 3,\ M' = \pm 2,\ r = 10.$$

The first case does not occur since $(M'^2, N') = 1$, and the second case also does not occur since $V'_r = V'_{10} = -482 \neq \pm 2^k$. Thus, if $2\|V'_r$, then r must be a power of two. In particular, since N' is odd, $2|V'_r$ and $3 \nmid r$; it must be that M'^2 is even. Using [3, Eq. (9)], it is easy to verify then that $2\|V'_{4n}$ for $n \geqslant 0$.

Suppose now that, in addition, we have $8|r$. Then with $x = V'_{r/2}/2$, we have

$$2\varepsilon = V'_r = V'^2_{r/2} - 2N'^{r/2} = 4x^2 - 2(N'^{r/8})^4$$

where x is odd and $\varepsilon = \pm 1$. Reducing modulo 8 shows that $\varepsilon = 1$, and so we have a solution of a diophantine equation

$$y^4 + 1 = 2x^2,$$

which by Mordell [6, p. 18] has solutions only when $x^2 = (N'^{r/8})^2 = 1$. But then $N'^{r/2} = 1$, and $V'_{r/2} = \pm 2$; so the sequence $\{a_{rn/2}\}$ is degenerate contrary to hypothesis. Thus, if $2\|V'_r$, we must have $r = 2$ or 4. If $r = 4$, then $m(d) \leqslant 4$ by Lemma 18. If $r = 2$, then $M'^2 = V'_2 + 2N' \equiv 0 \pmod 4$ and so $m(d) \leqslant 4$ by Lemma 17. Thus we may assume henceforth that two does not exactly divide V'_r; and so $V'_r = \pm 2^k$ with $k \geqslant 2$.

Next we show that $\sqrt{2}\|M'$. If M'^2 were odd, then since N' is odd and U'^2_r is even, we have $3|r$. But then $6|r$, and so $2\sqrt{2}|U'_r$ by Theorem B (iii). By Theorem B (ii), it follows that $V'_r|2$. On the other hand, if $2|M'$, then since N' is odd, we have $V'_{2n} \equiv 2 \pmod 4$ for all $n \geqslant 0$. In either case,

we have a contradiction with the assumption made at the end of the last paragraph. Therefore we have $\sqrt{2}\|M'$.

Let us show that $2\|r$ and $3 \nmid r$. Since $V'_4 = M'^4 - 4M'^2N' + 2N'^2 \equiv 2 \pmod 4$ and $N'^4 \equiv 1 \pmod 4$, we have by [3, Eq. (9)] that

$$V'_{4(n+2)} \equiv 2V'_{4(n+1)} - V'_{4n} \pmod 4.$$

Since $V'_0 \equiv V'_4 \equiv 2 \pmod 4$, it follows that

$$V'_{4n} \equiv 2 \pmod 4 \quad \text{for all } n \geqslant 0.$$

So $4 \nmid r$ as asserted. It follows that $r/2$ is odd and so if $3|r$, then $V'_6|V'_r = \pm 2^k$. But it is easy to verify that

$$V'_6 = V'_2(M'^4 - 4M'^2N' + N'^2) = V'_2\gamma,$$

and $\gamma \equiv 5 \pmod 8$ since $\sqrt{2}\|M'$ and N' is odd. Since no factor of $\pm 2^k$ is congruent to 5 modulo 8, we have a contradiction, thus proving that $3 \nmid r$.

Now we can reduce to the case where $U'_3 = \pm 1$. In fact, $U'_3 = M'^2 - N'$ is odd; and so in the contrary case, U'_3 has an odd prime divisor p. Since $(M'^2, N') = 1$, we have $p \nmid N'$; and since $3 \nmid r$, Theorem B (iii) shows that $p \nmid U'_r$. Therefore $p \nmid N'R^2d = Nd$ and $p|U'_3R^2 = U_3$. If $p \geqslant 5$, Theorem 2 shows that $m(d) \leqslant 3 + \delta \leqslant 4$. If $p = 3$, then $N \equiv 1 \pmod 3$ since $3|M^2 - N = R^2(M'^2 - N')$ and $3 \nmid M = RM'$; therefore $m(d) \leqslant 4$ by Lemma 16. Thus we may assume that $M'^2 - N' = \varepsilon$, $\varepsilon = \pm 1$.

Since $2\|r$, $V'_2|V'_r = \pm 2^k$. Now $V'_2 = M'^2 - 2N'$ is divisible by 4, and so $V'_2 = \varepsilon' 2^m$ where $2 \leqslant m \leqslant k$, $\varepsilon' = \pm 1$. Also, $\sqrt{2}\|M' = U'_2$ and so $\sqrt{2}\|U'_r$ by Theorem B (iii). Therefore $2^{m+1/2}\|U'_2V'_2 = U'_4$ and $2^{k+1/2}\|U'_rV'_r = U'_{2r}$. Since $4\|2r$, Theorem B (iii) shows that $m + 1/2 = k + 1/2$. Thus $V'_2 = \varepsilon' 2^k = M'^2 - 2N'$. Since also $M'^2 - N' = \varepsilon$, we have

$$(7) \qquad N' = \varepsilon - \varepsilon' 2^k = \varepsilon + 2^k \quad \text{and} \quad M'^2 = 2(\varepsilon - \varepsilon' 2^{k-1}) = 2(\varepsilon + 2^{k-1})$$

where one has $\varepsilon' = -1$ because $N' > 0$.

Suppose that $3 \nmid N'$. Then $\varepsilon = (-1)^k$, and so $3|M'^2 = U'^2_2$. Therefore $\sqrt{3}|U'_r$ and so $3|R^2, d$. Since d is even, Lemma 7 implies that there are at most two occurrences of d in $\{a_n\}$ which do not lie in the subsequence $\{a_{6rn}\}$. Since $2|r$, we are reduced to showing that d occurs at most twice in $\{a_{12n}\}$. If there is a prime divisor $q \geqslant 5$ of $M'^2 - 3N'$, then $q \nmid M'^2, N'$ since $(M'^2, N') = 1$. Also $q|U'_6 = U'_3V'_3 = U'_3M'(M'^2 - 3N')$. If $\sqrt{q}|U'_r$, then by Theorem B (ii),

$$\sqrt{q}|(U'_r, U'_6) = |U'_{(r,6)}| = |U'_2| = |M'|$$

which is a contradiction. Thus $\sqrt{q} \nmid U'_r$ and so $q \nmid R^2dN' = Nd$. Since $q|U_6$, Theorem 2 shows that d occurs at most twice in $\{a_{6n}\}$, and so $m(d) \leqslant 4$.

Therefore we may assume that $M'^2-3N' = \pm 3^v$. Using $\varepsilon = (-1)^k$ and (7), we see this can be written as

$$\pm 3^v + 2^{k+1} = (-1)^{k+1}.$$

The sign surely must be negative; and so by a theorem of LeVeque ([4], [2]), we have $(v, k) = (2, 2)$, $(1, 1)$, or $(1, 0)$. We have already seen that $k \geqslant 2$. So $k = 2$ and the corresponding values of N' and M' are

$$N' = 5 \quad \text{and} \quad M' = \pm\sqrt{6}.$$

But then $V'_6 = 236$ which is divisible by 59. If $\sqrt{59} | U'_r$, then $\sqrt{59} | (U'_{12}, U'_r) = |U'_{(12,r)}| = |M'|$. But then since $59 | V'_6 = \{M'(M'^2-3N')\}^2 - 2N'^3$, we have $59 | N'$ contrary to $(M'^2, N') = 1$. So $59 \nmid Nd$, and Theorem 2 shows that $\{a_{12n}\}$ contains no more than two occurrences of d; therefore $m(d) \leqslant 4$.

The only remaining case is that in which $3 | N'$. By (7), we see then that $\varepsilon = (-1)^{k+1}$ and so

$$M'^2 = 2\left(2^{k-1} + (-1)^{k+1}\right) \quad \text{and} \quad N' = 2^k + (-1)^{k+1}.$$

If $k = 2$, then $m(d) \leqslant 4$ by Lemma 13. For $k \geqslant 3$, the result follows from Lemma 20, and so the proof of the theorem is complete.

References

[1] R. Alter and K. K. Kubota, *Multiplicities of second order linear recurrences*, Trans. Amer. Math. Soc. 178 (1973), pp. 271–284.

[2] J. W. S. Cassels, *On the diophantine equation* $a^x - b^y = 1$, Amer. J. Math. 75 (1953), pp. 159–162.

[3] K. K. Kubota, *On a conjecture of Morgan Ward, I*, Acta Arith., this volume, pp. 11–28.

[4] W. J. LeVeque, *On the equation* $a^x - b^y = 1$, Amer. J. Math. 74 (1952), pp. 325–331.

[5] W. Ljunggren, *Noen setninger om ubestemte likninger av formen* $(x^n - 1)/(x - 1) = y^q$, Norsk Mat. Tidsskr. 25 (1943), pp. 17–20.

[6] L. J. Mordell, *Diophantine Equations*, Academic Press, London 1969.

[7] — *The diophantine equation* $y^2 = Dx^4 + 1$, J. London Math. Soc. 39 (1964), pp. 161–164.

Received on 23. 4. 1975
and in revised form on 30. 12. 1975 (699)

ACTA ARITHMETICA
XXXIII (1977)

Proper solutions of the imbedding problem with restricted ramification

by

OLAF NEUMANN (Berlin)

Let k be a field, $\bar{k}$ its separable algebraic closure with the Galois group $\mathfrak{G} = \mathrm{Gal}(\bar{k}/k)$. An imbedding problem is defined by a diagram

(1)
$$\begin{array}{ccccccccc} & & & & & & \mathfrak{G} & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ \{1\} & \longrightarrow & A & \longrightarrow & G & \xrightarrow{j} & F & \longrightarrow & \{1\} \end{array}$$

where A, G, F denote finite groups. All arrows are group homomorphisms and the horizontal sequence is exact. We assume φ surjective. Hence, the kernel of φ, $\mathfrak{G}_0 = \mathrm{Ker}\varphi$, determines a finite normal extension K/k with $\mathrm{Gal}(K/k) \cong F$. A solution of the imbedding problem (1) is by definition a homomorphism $\psi\colon \mathfrak{G} \to G$ satisfying the condition $j \circ \psi = \varphi$. ψ is called a *proper solution* if and only if it is surjective.

Let k be a global field, i.e., a finite algebraic number field or an algebraic function field of one variable over a finite constant field. By k_S we denote the maximal normal extension of k unramified outside the given set of primes S. Let $\mathfrak{G}_S$ be the group $\mathrm{Gal}(k_S/k)$. If S contains all ramification points of the extension K/k occurring in the diagram (1), we can factorize φ through the group $\mathfrak{G}_S$:

(1_S)
$$\begin{array}{ccccccccc} & & & & & & \mathfrak{G} & \xrightarrow{\pi_S} & \mathfrak{G}_S \\ & & & & & & & & \downarrow{\scriptstyle \varphi_S} \\ \{1\} & \longrightarrow & A & \longrightarrow & G & \xrightarrow{j} & F & \longrightarrow & \{1\}. \end{array}$$

We say (1) admits a solution ψ unramified outside S if and only if (1_S) admits a solution $\psi_S\colon \mathfrak{G}_S \to G$ with $j \circ \psi_S = \varphi_S$ and $\psi = \psi_S \circ \pi_S$ where π_S denotes the canonical epimorphism $\mathfrak{G} \to \mathfrak{G}_S$.

The main result of the present paper is the following