PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 96, Number 2, February 1986

UNIFORM DISTRIBUTION OF SECOND-ORDER LINEAR RECURRING SEQUENCES

G. TURNWALD

ABSTRACT. A complete classification is obtained for all second-order linear recurring sequences uniformly distributed modulo an ideal of a Dedekind domain.

1. Introduction. A sequence of rational integers is said to be uniformly distributed modulo m (u.d. mod m) if every residue class appears with the same asymptotic frequency. Uniform distribution of second-order linear recurring sequences was first investigated in special cases [**4**, **5**, **9**]; then several authors obtained (partial) results concerning u.d. modulo prime powers [**2**, **6**, **8**, **16**]. Finally, R. T. Bumby provided a complete solution [**1**]; cf. [**7**, Chapter III]. The corresponding problem for order three was solved by Knight and Webb under the additional hypothesis that m is relatively prime to $2, 3, 5$ [**3**]. Bumby remarks that his methods could possibly lead to a solution of the corresponding problem with algebraic integers. This is indeed the case (and was carried out by the author; unpublished), but the approach presented here leads to considerably more general results. Specializing to rational integers, our method yields an elementary proof of Bumby's result, totally avoiding algebraic number theory. It is also possible to obtain a characterization of u.d. third-order linear recurring sequences in a similar way; the result, however, becomes very complicated [**15**]. The special case of rational integers (formulated in [**13**]) completes the investigations of Knight and Webb. The method presented here also leads to partial results concerning u.d. modulo prime powers for linear recurring sequences of arbitrary order [**13**, **15**]. Uniform distribution modulo a prime ideal (of finite norm) in a Dedekind domain amounts to u.d. in a finite field, which was investigated by Niederreiter and Shiue for linear recurring sequences up to order four [**10**, **11**].

This paper is distilled from my thesis [**14**], written under the supervision of Dozent R. F. Tichy. The case of order two that is treated here was excluded in [**15**], where the larger part of the thesis is published. (The results of §§2 and 3 essentially appear in [**15**] too, but mostly without (complete) proof.)

2. Linear recurring sequences. Let R be a commutative ring with unit element; let (u_n) be a sequence of elements of R. A polynomial $\Sigma a_k x^k$ with coefficients in R is

Received by the editors March 5, 1985.
1980 *Mathematics Subject Classification*. Primary 10A35, 12A05.
Key words and phrases. Linear recurring sequences, uniform distribution in residue classes, algebraic integers, p-adic integers.

called a characteristic polynomial of (u_n) if $\Sigma a_k u_{n+k} = 0$ for all $n \geqslant 0$. If $a(x) = \Sigma a_k x^k$ is a characteristic polynomial and $b(x) = \Sigma b_k x^k$ is an arbitrary polynomial, then $a(x)b(x)$ again is a characteristic polynomial of (u_n), since

$$\sum_{i,j} a_i b_j u_{n+i+j} = \sum_j b_j \left(\sum_i a_i u_{n+i+j} \right) = 0.$$

If (u_n) admits a monic characteristic polynomial $c(x)$, we call (u_n) a linear recurring sequence with characteristic polynomial $c(x)$. We do not require that $c(x)$ has minimal degree. Even a restriction to monic characteristic polynomials of minimal degree would not guarantee uniqueness: In a ring of characteristic 4 the sequence $(2, 2, 0, 2, 2, 0, \ldots)$ admits the different monic characteristic polynomials $x^2 - x - 1$ and $x^2 + x + 1$ of degree two, but none of degree one. In a unique factorization domain, however, uniqueness can be proven [**14**, Proposition 1.1.4]. By an rth-order linear recurring sequence we mean a sequence that admits a monic characteristic polynomial of degree r; again, no minimality condition is assumed. Such a sequence (u_n) is uniquely determined by a characteristic polynomial of degree r and the initial terms $u_0, \ldots, u_{r-1}$.

LEMMA 1. *Let I be an ideal of R and let (u_n) be a linear recurring sequence with characteristic polynomial $c(x)$. If $\Sigma a_k x^k \equiv 0\ (c(x), I)$ then $\Sigma a_k u_{n+k} \equiv 0\ (I)$ for all $n \geqslant 0$.*

PROOF. By assumption there exists a polynomial $\Sigma b_k x^k$ with coefficients in I such that $\Sigma(a_k - b_k)x^k$ is a multiple of $c(x)$. Hence, $\Sigma(a_k - b_k)u_{n+k} = 0$ and $\Sigma a_k u_{n+k} \equiv \Sigma(a_k - b_k)u_{n+k} \equiv 0\ (I)$.

For the following calculations it is useful to observe that the congruences $f(x) \equiv 0\ (c(x), I)$ and $g(x) \equiv 0\ (c(x), J)$ imply $f(x)g(x) \equiv 0\ (c(x), IJ)$.

LEMMA 2. *Assume that $x^n(x^l - 1) \equiv 0\ (c(x), I)$. Then*

$$x^{2n}(x^{kl} - 1) \equiv x^{2n}k(x^l - 1)\ (c(x), I^2)$$

and

$$x^{3n}(x^{kl} - 1) \equiv x^{3n}k(x^l - 1) + x^{3n}\binom{k}{2}(x^l - 1)^2\ (c(x), I^3)$$

for $k > 0$.

PROOF. From

$$x^{kl} - 1 = \left(1 + (x^l - 1)\right)^k - 1 = \sum_{j=1}^{k} \binom{k}{j}(x^l - 1)^j$$

and $x^{2n}(x^l - 1)^2 \equiv 0\ (c(x), I^2)$ we deduce

$$x^{2n}(x^{kl} - 1) \equiv x^{2n}\binom{k}{1}(x^l - 1)\ (c(x), I^2).$$

Analogously, the second assertion follows from $x^{3n}(x^l - 1)^3 \equiv 0\ (c(x), I^3)$.

THEOREM 1. *Let I be an ideal of R and assume that $a \equiv 0\ (I)$ for a positive integer a. If $x^{n_0}(x^l - 1) \equiv 0\ (c(x), I^{h_0})$ $(n_0 \geqslant 0;\ l, h_0 > 0)$ then for every linear recurring sequence (u_n) with characteristic polynomial $c(x)$ we have*

(a) $u_{n+a^h l} \equiv u_n\ (I^{h_0+h})$ *for* $h \geqslant 0,\ n \geqslant 2^h n_0$,

(b) $u_{n+kl} \equiv u_n + k(u_{n+l} - u_n)\ (I^{2h_0})$ *for* $n \geqslant 2n_0$,

(c) $u_{n+ka^h l} \equiv u_n + ka^{h-1}(u_{n+al} - u_n)\ (I^{2h_0+h})$ *for* $h > 0,\ n \geqslant 3 \cdot 2^{h-1} n_0$,

(d) $u_{n+ka^h l} \equiv u_n + ka^h(u_{n+l} - u_n)\ (I^{2h_0+h})$ *for* $h > 0,\ n \geqslant 3 \cdot 2^{h-1} n_0$, *$a$ odd.*

PROOF. By Lemma 1 it suffices to show that

(a′) $x^{2^h n_0}(x^{a^h l} - 1) \equiv 0\ (c(x), I^{h_0+h})$,

(b′) $x^{2n_0}(x^{kl} - 1) \equiv x^{2n_0} k(x^l - 1)\ (c(x), I^{2h_0})$,

(c′) $x^{3 \cdot 2^{h-1} n_0}(x^{ka^h l} - 1) \equiv x^{3 \cdot 2^{h-1} n_0} ka^{h-1}(x^{al} - 1)\ (c(x), I^{2h_0+h})$,

(d′) $x^{3 \cdot 2^{h-1} n_0}(x^{ka^h l} - 1) \equiv x^{3 \cdot 2^{h-1} n_0} ka^h(x^l - 1)\ (c(x), I^{2h_0+h})$.

To simplify the notation we write n instead of n_0 in the sequel.

From $x^{2^h n}(x^{a^h l} - 1) \equiv 0\ (c(x), I^{h_0+h})$ we conclude that

$$x^{2^{h+1} n}\left(x^{a^{h+1} l} - 1\right) \equiv x^{2^{h+1} n} a\left(x^{a^h l} - 1\right)\ \left(c(x), I^{2h_0+2h}\right)$$

by Lemma 2. Since $x^{2^h n} a(x^{a^h l} - 1) \equiv 0\ (c(x), I^{h_0+h+1})$ and $h_0 + h + 1 \leqslant 2h_0 + 2h$, this proves (a′) by induction, the case $h = 0$ being trivial. Lemma 2, again, proves (b′).

Since $2h_0 + 1 \leqslant 3h_0$, Lemma 2 shows that

$$x^{3n}(x^{kal} - 1) \equiv x^{3n} k(x^{al} - 1) + x^{3n}\binom{k}{2}(x^{al} - 1)^2\ \left(c(x), I^{2h_0+1}\right).$$

From $x^n(x^{al} - 1) \equiv 0\ (c(x), I^{h_0})$ and $x^{2n}(x^{al} - 1) \equiv 0\ (c(x), I^{h_0+1})$ (case $h = 1$ of (a′)) we conclude

$$x^{3n}(x^{al} - 1)^2 \equiv 0\ \left(c(x), I^{2h_0+1}\right).$$

This gives case $h = 1$ of (c′). By (a′) we have $x^{2^h n}(x^{ka^h l} - 1) \equiv 0\ (c(x), I^{h_0+h})$ so that, by Lemma 2,

$$x^{3 \cdot 2^h n}\left(x^{aka^h l} - 1\right) \equiv x^{3 \cdot 2^h n} a\left(x^{ka^h l} - 1\right) + x^{3 \cdot 2^h n}\binom{a}{2}\left(x^{ka^h l} - 1\right)^2\ \left(c(x), I^{3(h_0+h)}\right).$$

Since $x^{2 \cdot 2^h n}(x^{ka^h l} - 1)^2 \equiv 0\ (c(x), I^{2(h_0+h)})$ and $2h_0 + h + 1 \leqslant 2(h_0 + h)$, the second term vanishes mod I^{2h_0+h+1}, and we obtain

$$x^{3 \cdot 2^h n}\left(x^{ka^{h+1} l} - 1\right) \equiv x^{3 \cdot 2^h n} a\left(x^{ka^h l} - 1\right)\ \left(c(x), I^{2h_0+h+1}\right).$$

The proof of (c′) now follows by induction since $a \equiv 0\ (I)$.

If a is odd, then $\binom{a}{2} = a(a-1)/2 \equiv 0\ (I)$. Hence

$$x^{3n}\binom{a}{2}(x^l - 1)^2 \equiv 0\ (I^{2h_0+1}),$$

and Lemma 2 gives

$$x^{3n}(x^{al} - 1) \equiv x^{3n} a(x^l - 1) + x^{3n}\binom{a}{2}(x^l - 1)^2 \equiv x^{3n} a(x^l - 1)\ \left(c(x), I^{2h_0+1}\right).$$

Since $a^{h-1} \equiv 0\,(I^{h-1})$, this implies

$$x^{3\cdot 2^{h-1}n}a^{h-1}(x^{al}-1) \equiv x^{3\cdot 2^{h-1}n}a^{h}(x^{l}-1)\,\big(c(x), I^{2h_0+h}\big).$$

Now (d′) follows from (c′).

3. Uniform distribution. From now on we assume that R is a Dedekind domain, i.e., an integral domain in which every nonzero ideal admits a (unique) representation as a product of prime ideals. Equivalently, a Dedekind domain may be defined to be a Noetherian integrally closed domain where every nonzero prime ideal is maximal. The examples we have in mind are p-adic integers or the ring of integers in an algebraic number field (of finite degree). We define the norm of an ideal I by $N(I) = |R/I|$. If I and J are ideals with finite norm, then $N(IJ) = N(I)N(J)$ (cf. [**12**, Chapter 8, A]). By the corresponding (rational) prime p of a nonzero prime ideal P, we mean the characteristic of the field R/P. If $N(P)$ is finite, it is a power of p.

A sequence (u_n) of elements of R is called uniformly distributed (u.d.) mod I if I is an ideal of finite norm and

$$\lim_{n\to\infty} n^{-1}\big|\{k \mid 0 \leqslant k < n,\ u_k \equiv x(I)\}\big| = 1/N(I)$$

for every element x of R. If (u_n) is u.d. mod I and I is contained in J, then (u_n) is u.d. mod J, since every residue class mod J consists of $N(I)/N(J)$ residue classes mod I. If (u_n) is periodic mod I and u.d. mod I, then every period must be divisible by $N(I)$.

Let (u_n) be a linear recurring sequence with characteristic polynomial $c(x)$. We assume that $c(x)$ splits into linear factors modulo P and that all factors incongruent to x occur with multiplicity at most two; P denotes a fixed prime ideal of R.

LEMMA 3. (a) *If (u_n) is u.d.* mod P, *then* $N(P) = p$,

$$u_{j+n(p-1)} \equiv u_j + n(u_{j+p-1} - u_j)\,(P), \qquad u_{j+p-1} - u_j \not\equiv 0\,(P) \quad \textit{for } j \geqslant j_0,$$

and $u_{j+p^h(p-1)} \equiv u_j(P^h)$ *for* $j \geqslant j_0(h)$ *and* $h \geqslant 1$.

(b) *If* $N(P) = p$ *and* $p > 2$, *then* $u_{j+np^h(p-1)} \equiv u_j + np^{h-1}(u_{j+p(p-1)} - u_j)\,(P^{h+1})$ *for* $j \geqslant j_0(h)$ *and* $h \geqslant 1$.

(c) *If* $N(P) = p$ *and* $p \geqslant 5$, *then* $u_{j+p(p-1)} \equiv u_j + p(u_{j+p-1} - u_j)\,(P^2)$ *for* $j \geqslant j_0$.

PROOF. By definition of u.d. mod P, $N(P)$ is finite. Let n_0 be the multiplicity of x in the factorization of $c(x)$ modulo P. Then setting $q = N(P)$ we have

$$x^{n_0}(x^{q-1}-1)^2 \equiv 0\,(c(x), P),$$

since every linear factor incongruent to x is a divisor of $x^{q-1}-1$ and the multiplicity is assumed to be at most 2. Hence,

$$x^{n_0}(x^{p(q-1)}-1) \equiv x^{n_0}(x^{q-1}-1)^p \equiv 0\,(c(x), P).$$

By Lemma 1 this implies that (u_n) has period $p(q-1)$ modulo P. If (u_n) is u.d. mod P every period length must be divisible by $q = N(P)$; hence, we conclude $q = p$. From

$$x^{n_0}(x^{n(p-1)}-1) = x^{n_0}\big((1+(x^{p-1}-1))^n - 1\big) = x^{n_0}\sum_{j=1}^{n}\binom{n}{j}(x^{p-1}-1)^j$$

and

$$x^{n_0}(x^{p-1}-1)^2 \equiv 0\ (c(x), P),$$

we deduce

$$x^{n_0}(x^{n(p-1)}-1) \equiv x^{n_0}n(x^{p-1}-1)\ (c(x), P).$$

Again, by Lemma 1 this implies $u_{j+n(p-1)} - u_j \equiv n(u_{j+p-1} - u_j)\ (P)$ for $j \geqslant j_0 = n_0$. We now apply Theorem 1 (with $I = P$, $a = p$, $h_0 = 1$, $l = p(p-1)$) to obtain (after a change of notation)

$$u_{j+p^h(p-1)} \equiv u_j\ (P^h) \quad \text{for } h \geqslant 1,\ j \geqslant j_0(h)$$

and

$$u_{j+np^h(p-1)} \equiv u_j + np^{h-1}(u_{j+p(p-1)} - u_j)\ (P^{h+1}) \quad \text{for } h \geqslant 1,\ j \geqslant j_0(h),\ p > 2.$$

If $u_{j+p-1} - u_j \equiv 0\ (P)$ for some $j \geqslant j_0$, from $u_{j+n(p-1)} - u_j \equiv n(u_{j+p-1} - u_j)\ (P)$ we see that the residue $u_j \bmod P$ appears at least p times (for $n = 0, \ldots, p-1$) in a period of length $p(p-1)$; but if (u_n) is u.d. mod P every residue must appear $p-1$ times, since the number of residues is $p = N(P)$. This concludes the proof of (a) and (b). To prove (c) we first remark that

$$\begin{aligned} x^{2n_0}(x^{p(p-1)}-1) &= x^{2n_0}\sum_{j=1}^{p}\binom{p}{j}(x^{p-1}-1)^j \\ &\equiv x^{2n_0}\big(p(x^{p-1}-1) + (x^{p-1}-1)^p\big)\ (c(x), P^2), \end{aligned}$$

since $\binom{p}{j} \equiv 0\ (P)$ for $1 \leqslant j \leqslant p-1$ and $x^{n_0}(x^{p-1}-1)^2 \equiv 0\ (c(x), P)$. For $p \geqslant 5$ we have $x^{2n_0}(x^{p-1}-1)^p \equiv 0\ (c(x), P^2)$; hence,

$$x^{2n_0}(x^{p(p-1)}-1) \equiv x^{2n_0}p(x^{p-1}-1)\ (c(x), P^2),$$

which implies $u_{j+p(p-1)} - u_j \equiv p(u_{j+p-1} - u_j)\ (P^2)$ for $j \geqslant 2n_0$.

REMARK. If $c(0) \not\equiv 0\ (P)$, then we may take $n_0 = 0$; hence the conditions given in the lemma hold for $j \geqslant 0$.

LEMMA 4. *Assume that $p = 2$ and (u_n) is u.d.* mod P^2. *If $p \equiv 0\ (P^2)$, then (u_n) is not u.d.* mod P^3; *if $p \not\equiv 0\ (P^2)$, (u_n) is u.d.* mod P^h *for all $h \geqslant 1$.*

PROOF. As in the proof of the preceding lemma, we conclude that $x^{n_0}(x-1)^2 \equiv 0\ (c(x), P)$, since (u_n) is u.d. mod P. We define $r(x) = \sum r_k x^k$ to be the residue of $x^{n_0}(x^2-1)$ modulo $c(x)$. From $x^{n_0}(x^2-1) \equiv x^{n_0}(x-1)^2 \equiv 0\ (c(x), P)$ we see that $r(x) \equiv 0\ (c(x), P)$. Hence, $r(x)$ is divisible by $c(x) \bmod P$, which implies $r_k \equiv 0\ (P)$ for all k, since the degree of $r(x) \bmod P$ is smaller than the degree of $c(x) \bmod P$ $(= \deg(c(x))$ since the leading coefficient is 1). Observing that $x^{n_0}(x^{2k}-1) \equiv 0\ (c(x), P)$, we see that this implies

$$\begin{aligned} x^{n_0}r(x)^2 &\equiv x^{n_0}\sum r_k^2 x^{2k} \equiv \sum r_k^2\big(x^{n_0}(x^{2k}-1) + x^{n_0}\big) \\ &\equiv x^{n_0}\sum r_k^2 \equiv x^{n_0}\Big(\sum r_k\Big)^2\ (c(x), P^3). \end{aligned}$$

From $x^{n_0}(x^2-1) \equiv r(x) \bmod (c(x))$ we deduce

$$x^{2n_0}(x^2-1)^2 \equiv r(x)^2 \bmod (c(x)).$$

Hence,

$$x^{3n_0}(x^4-1) = 2x^{3n_0}(x^2-1) + x^{3n_0}(x^2-1)^2 \equiv 2x^{3n_0}(x^2-1) + x^{n_0}r(x)^2$$
$$\equiv 2x^{3n_0}(x^2-1) + x^{n_0}\left(\sum r_k\right)^2 (c(x), P^3),$$

and, by Lemma 1,

$$u_{j+3n_0+4} - u_{j+3n_0} \equiv 2(u_{j+3n_0+2} - u_{j+3n_0}) + u_{j+n_0}\left(\sum r_k\right)^2 (P^3).$$

From $x^{n_0}(x^2-1) \equiv 0\,(c(x), P)$ and

$$x^{2n_0}(x^4-1) \equiv 2x^{2n_0}(x^2-1) + x^{2n_0}(x^2-1)^2 \equiv 0\,(c(x), P^2),$$

we see that $u_{j+2} \equiv u_j\ (P)$ and $u_{j+4} \equiv u_j\ (P^2)$ for $j \geqslant j_0 = 2n_0$. Since (u_n) is u.d. mod P^2, each of the four residues mod P^2 must appear once in a period, which implies $u_{j+2} \not\equiv u_j\ (P^2)$ for $j \geqslant j_0$, i.e., $u_{j+2} - u_j$ lies in the unique residue class mod P^2 that belongs to P but not to P^2. We conclude that $u_{j+3} - u_{j+1} \equiv u_{j+2} - u_j$ (P^2) for $j \geqslant j_0$. Since $u_{j+1} - u_j \equiv 1\ (P)$, we finally obtain

$$\sum r_k \equiv \sum r_k(u_{j+1+k} - u_{j+k}) \equiv (u_{j+n_0+3} - u_{j+n_0+1}) - (u_{j+n_0+2} - u_{j+n_0}) \equiv 0\ (P^2)$$

(taking into account that $x^{n_0}(x^2-1) \equiv \sum r_k x^k \bmod (c(x))$ implies $u_{j+n_0+2} - u_{j+n_0} \equiv \sum r_k u_{j+k}$). Hence, $(\sum r_k)^2 \equiv 0\ (P^3)$ and

$$u_{j+3n_0+4} - u_{j+3n_0} \equiv 2(u_{j+3n_0+2} - u_{j+3n_0})\ (P^3).$$

If $2 \equiv 0\ (P^2)$, this means that (u_n) has period 4 mod P^3; since 4 is not divisible by $N(P^3) = 2^3$, (u_n) is not u.d. mod P^3. Now let us assume $2 \not\equiv 0\ (P^2)$; then the above relation yields $u_{j+4} - u_j \not\equiv 0\ (P^3)$ for sufficiently large j. Theorem 1 now gives $(I = P,\ a = 2,\ h_0 = 1, l = 2,\ k = 1)$

$$u_{j+2^{h+1}} \equiv u_j + 2^{h-1}(u_{j+4} - u_j)\ (P^{h+2}) \quad \text{for } h > 0,\ j \geqslant 3 \cdot 2^{h-1}n_0.$$

Hence,

$$u_{j+2^{h+1}} \equiv u_j\ (P^{h+1}) \quad \text{and} \quad u_{j+2^{h+1}} \not\equiv u_j\ (P^{h+2}) \qquad \text{for } j \geqslant j_0(h),\ h > 0.$$

By assumption, (u_n) is u.d. mod P^2, i.e., every residue appears once in a period of length 4. Since $u_{j+4} \not\equiv u_j\ (P^3)$, this implies that every residue mod P^3 appears once in a period of length 8. Inductively we conclude the analogous statement modulo P^h for all h, i.e., (u_n) is u.d. mod P^h for all h.

THEOREM 2. *Let I be a proper ideal of the Dedekind domain R and let (u_n) be a linear recurring sequence (of elements of R) with characteristic polynomial $c(x)$. Assume that for every prime divisor P of I, $c(x)$ splits into linear factors modulo P and that the factors incongruent to x appear with multiplicity at most two. Then (u_n) is u.d. mod I if and only if the following conditions hold*:

(1) *If $P|I$ then (u_n) is u.d. mod P; if $P^2|I$ and $p = 2$ or $p = 3$, then (u_n) is u.d. mod P^2.*

(2) *If $P^2|I$ and $p \geqslant 5$, then $p \not\equiv 0\ (P^2)$; if $P^3|I$ and $p = 2$ or $p = 3$, then $p \not\equiv 0$ (P^2).*

(3) *If $P_i|I$ $(i = 1, 2)$ and $P_1 \neq P_2$, then $N(P_1) \neq N(P_2)$.*

PROOF. We assume first that (u_n) is u.d. mod I. Then (u_n) is u.d mod every divisor of I. This proves (1). For $P^2|I$ and $p \geqslant 5$ we deduce

$$u_{j+p(p-1)} \equiv u_j + p(u_{j+p-1} - u_j)\ (P^2)$$

from Lemma 3(c). Assume $p \equiv 0\ (P^2)$; then $u_{j+p(p-1)} \equiv u_j\ (P^2)$ (for sufficiently large j), which is impossible since the period must be divisible by $N(P^2) = p^2$. If $P^3|I$ and $p = 2$, the preceding lemma implies $p \not\equiv 0\ (P^2)$. For the remaining case $p = 3$ we use Lemma 3(b) to obtain

$$u_{j+p^2(p-1)} \equiv u_j + p(u_{j+p(p-1)} - u_j)\ (P^3)$$

so that

$$u_{j+p^2(p-1)} \equiv u_j(P^3) \quad \text{if } p \equiv 0\ (P^2).$$

Since $p^2(p-1)$ is not divisible by $N(P^3) = p^3$, (u_n) cannot be u.d. mod P^3; hence P^3 cannot divide I. This concludes the proof of (2).

Assume $P_i|I$ $(i = 1, 2)$ and $P_1 \neq P_2$; then P_1P_2 divides I. Hence, the period of (u_n) modulo P_1P_2 must be divisible by $N(P_1P_2)$. By Lemma 3(a) we have $N(P_i) = p_i$ and (u_n) has period $p_i(p_i - 1) \bmod P_i$. From $N(P_1) = N(P_2)$ we obtain $p_1 = p_2 = p$, so that (u_n) has period $p(p-1) \bmod P_1P_2 = P_1 \cap P_2$. Since $p(p-1)$ is not divisible by $N(P_1P_2) = p^2$, we arrive at a contradiction. Hence, $N(P_1) \neq N(P_2)$.

Now we assume (1)–(3). If $P|I$ then, by (1), (u_n) is u.d. mod P, so that Lemma 3(a) shows $N(P) = p$ and $u_{j+p^h(p-1)} \equiv u_j(P^h)$ for $h \geqslant 1$, $j \geqslant j_0(h)$. By (3), a rational prime p belongs only to one prime ideal. Hence, every divisor of I may be written in the form $\prod P_i^{h_i} \cdot P^k$, $p_1 < p_2 < \cdots < p$; $\prod P_i^{h_i}$ may be the empty product. In order to prove that (u_n) is u.d. mod I, we may therefore proceed inductively and show that (u_n) is u.d. mod $\prod P_i^{h_i} \cdot P^{k+1}$ provided (u_n) is u.d. mod $\prod P_i^{h_i} \cdot P^k$, $P^{k+1}|I$, and $p_1 < p_2 < \cdots < p$. The first step is given by the first part of (1). If $p = 2$, the assertion follows from (1), (2), and Lemma 4. In the following we assume $p > 2$. Define $l = \prod p_i^{h_i}(p_i - 1)$; then (u_n) has period l modulo $\bigcap P_i^{h_i} = \prod P_i^{h_i}$, so that $u_{j+nl} - u_j \equiv n(u_{j+l} - u_j)\ (\prod P_i^{h_i})$ for sufficiently large j. By Lemma 3 we have

$$u_{j+np^k(p-1)} - u_j \equiv n(u_{j+p^k(p-1)} - u_j)\ (P^{k+1}) \quad \text{for } k \geqslant 0,\ j \geqslant j_0(k).$$

Hence,

$$u_{j+nlp^k(p-1)} - u_j \equiv n(u_{j+lp^k(p-1)} - u_j)\ \left(\prod P_i^{h_i} \cdot P^{k+1}\right).$$

If we can prove $u_{j+lp^k(p-1)} - u_j \not\equiv 0\ (P^{k+1})$, then the last congruence means that $u_{j+nlp^k(p-1)}$ $(n = 0, \ldots, p-1)$ runs through the p residues mod $\prod P_i^{h_i} \cdot P^{k+1}$ belonging to the residue u_j mod $\prod P_i^{h_i} \cdot P^k$. Since (u_n) has period $lp^k(p-1) \bmod \prod P_i^{h_i} \cdot P^k$, this implies that (u_n) is u.d. mod $\prod P_i^{h_i} \cdot P^{k+1}$ provided (u_n) is u.d. mod $\prod P_i^{h_i} \cdot P^k$. From $u_{j+lp^k(p-1)} - u_j \equiv l(u_{j+p^k(p-1)} - u_j)\ (P^{k+1})$ and $(l, p) = 1$ (since $p_i < p$ for all i), we see that it remains to prove $u_{j+p^k(p-1)} - u_j \not\equiv 0$ (P^{k+1}). If $k = 0$, this follows from Lemma 3(a). If $k \geqslant 1$ and $p \geqslant 5$ we have, by Lemma 3,

$$u_{j+p^k(p-1)} - u_j \equiv p^{k-1}(u_{j+p(p-1)} - u_j) \equiv p^k(u_{j+p-1} - u_j)\ (P^{k+1}).$$

Since, by (2), $p \not\equiv 0\ (P^2)$ and $u_{j+p-1} - u_j \not\equiv 0\ (P)$, this proves the assertion in this case. Now suppose $p = 3$. By (1), (u_n) is u.d. mod P^2. If $u_{j+p(p-1)} - u_j \equiv 0\ (P^2)$ for some $j \geqslant j_0$, then $u_{j+np(p-1)} - u_j \equiv n(u_{j+p(p-1)} - u_j)\ (P^2)$ implies that the residue u_j appears p times (for $n = 0, \ldots, p-1$) in a period of length $p^2(p-1)$. Since there are p^2 residues mod P^2, each of them must appear $(p-1)$ times. Hence, $u_{j+p(p-1)} - u_j \not\equiv 0\ (P^2)$ for all sufficiently large j. Consequently, the assertion is equivalent to $p^{k-1} \not\equiv 0\ (P^k)$, i.e., $p \not\equiv 0\ (P^2)$ if $k > 1$. To conclude the proof we remark that $k > 1$ and $P^{k+1}|I$ imply $P^3|I$; hence, $p \not\equiv 0\ (P^2)$ follows from (2).

REMARK. (1) Let (u_n) be a linear recurring sequence with arbitrary characteristic polynomial $c(x)$, and let P be a prime ideal with finite norm. Assume that $c(x)$ has no multiple factors mod P except possibly the factor x, whose multiplicity we denote by n_0. If d is the degree of the splitting field of $c(x)$ over R/P, $c(x)$ divides $x^{n_0}(x^{N(P)^d-1} - 1)$ mod P, i.e., $x^{n_0}(x^{N(P)^d-1} - 1) \equiv 0\ (c(x), P)$. Then, by Lemma 1, (u_n) has period $N(P)^d - 1$ mod P. Since this number is not divisible by $N(P)$, (u_n) cannot be u.d. mod P. Hence, in order that (u_n) be u.d. mod P, $c(x)$ must have a nontrivial multiple factor mod P.

(2) Conditions (2) and (3) of the theorem are satisfied trivially if R is the ring of rational integers.

4. The case $\deg(c(x)) = 2$. Apart from a substantial simplification of the proof of Lemma 4, restriction to second-order linear recurring sequences would only have entailed minor simplifications (mainly due to the fact that we could assume $n_0 = 0$) in the preceding investigations. The restriction is essential for the following complete classification, however.

THEOREM 3. *Let I be a proper ideal of the Dedekind domain R and let (u_n) be a linear recurring sequence (of elements of R) with characteristic polynomial $c(x) = x^2 - c_1x - c_0$. Then (u_n) is u.d.* mod *I if and only if the following conditions hold*:

(1) *If $P|I$, then $N(P) = p$, $c_1^2 + 4c_0 \equiv 0\ (P)$, $c_0 \not\equiv 0\ (P)$; $2u_1 \not\equiv c_1u_0\ (P)$ for $p > 2$, $u_1 \not\equiv u_0\ (P)$ for $p = 2$. If $P^2|I$ and $p = 2$, then $c_1 \not\equiv 0\ (P^2)$, $c_0 \not\equiv 1\ (P^2)$; if $P^2|I$ and $p = 3$ then $c_0 + c_1^2 \not\equiv 0\ (P^2)$.*

(2) *If $P^2|I$ and $p \geqslant 5$, then $p \not\equiv 0\ (P^2)$; if $P^3|I$ and $p = 2$ or $p = 3$, then $p \not\equiv 0\ (P^2)$.*

(3) *If $P_i|I$ $(i = 1, 2)$ and $P_1 \neq P_2$, then $N(P_1) \neq N(P_2)$.*

PROOF. By part (1) of the last remark we only have to show that (1) is equivalent to condition (1) of Theorem 2. Let P be a prime ideal. If (u_n) is u.d. mod P then $N(P) = p$ by Lemma 3(a). The conditions $c_0 \not\equiv 0\ (P)$ and $c_1^2 + 4c_0 \equiv 0\ (P)$ again follow from the above-cited remark since they are equivalent to $c(x) \equiv (x-a)^2\ (P)$ for some $a \not\equiv 0\ (P)$. From $c(x) \equiv (x-a)^2$ we conclude

$$au_n \equiv ((u_1 - au_0)n + au_0)a^n\ (P).$$

Since $a^{p-1} = a^{N(P)-1} \equiv 1\ (P)$, we obtain

$$a(u_{j+n(p-1)} - u_j) \equiv n(u_1 - au_0)(p-1)a^j \equiv -n(u_1 - au_0)a^j\ (P).$$

If $u_1 - au_0 \equiv 0\ (P)$, this means that (u_n) has period $p-1 \bmod P$; hence (u_n) is not u.d. mod P. If $u_1 - au_0 \not\equiv 0\ (P)$, then the subsequences $(u_{j+n(p-1)})$ $(j = 0, \ldots, p-2)$ are u.d. mod P, being nontrivial arithmetic sequences mod P. Since (u_n) is the union of these subsequences, we finally obtain that (u_n) is u.d. mod P if and only if $u_1 - au_0 \not\equiv 0\ (P)$. For $p = 2$ this means $u_1 - u_0 \not\equiv 0\ (P)$; for $p > 2$ the condition is equivalent to $2u_1 \not\equiv c_1 u_0\ (P)$ since $2 \not\equiv 0\ (P)$ and $2a \equiv c_1\ (P)$.

Let (u_n) be u.d. mod P. Assume $p = 2$ first. We have to show that (u_n) is u.d. mod P^2 if and only if $c_0 \not\equiv 1\ (P^2)$ and $c_1 \not\equiv 0\ (P^2)$. Since (u_n) is u.d. mod P, we have $c_0 \equiv 1\ (P)$, $c_1 \equiv 0\ (P)$, and $u_{j+1} \equiv u_j + 1\ (P)$ for $j \geqslant 0$. By Lemma 3(a) and the following remark, $u_{j+4} \equiv u_j\ (P^2)$ for $j \geqslant 0$. Hence, (u_n) is u.d. mod P^2 if and only if $u_0 \not\equiv u_2\ (P^2)$ and $u_1 \not\equiv u_3\ (P^2)$. The second condition may be replaced by $u_3 - u_1 \equiv u_2 - u_0\ (P^2)$. Since

$$\begin{aligned}(u_3 - u_1) - (u_2 - u_0) &= (c_1 u_2 + (c_0 - 1)u_1) - (c_1 u_1 + (c_0 - 1)u_0) \\ &\equiv c_1(u_2 - u_1) + (c_0 - 1)(u_1 - u_0) \equiv c_1 + (c_0 - 1)\ (P^2)\end{aligned}$$

and

$$\begin{aligned}u_2 - u_0 &= c_1 u_1 + (c_0 - 1)u_0 \equiv c_1(u_0 + 1) + (c_0 - 1)u_0 \\ &\equiv (c_1 + c_0 - 1)u_0 + c_1\ (P^2),\end{aligned}$$

we obtain the conditions $c_1 + (c_0 - 1) \equiv 0\ (P^2)$ and $c_1 \not\equiv 0\ (P^2)$, which are equivalent to $c_0 - 1 \not\equiv 0\ (P^2)$ and $c_1 \not\equiv 0\ (P^2)$.

Now assume $p = 3$. We prove that (u_n) is u.d. mod P^2 if and only if $c_0 + c_1^2 \not\equiv 0$ (P^2). By Lemma 3 we have $u_{j+6} \equiv u_j\ (P)$ and $u_{j+6n} \equiv u_j + n(u_{j+6} - u_j)\ (P^2)$ for $j \geqslant 0$. If, for some j, $u_{j+6} - u_j \equiv 0\ (P^2)$, then u_j appears three times (for $n = 0, 1, 2$) in a period of length 18; hence, (u_n) is not u.d. mod P^2 in this case. If $u_{j+6} - u_j \not\equiv 0$ (P^2), then u_{j+6n} $(n = 0, 1, 2)$ runs through the three residues mod P^2 belonging to the residue class of u_j mod P. Since (u_n) is u.d. mod P and $u_{j+6} \equiv u_j\ (P)$, this implies that (u_n) is u.d. mod P^2 provided $u_{j+6} \not\equiv u_j\ (P^2)$ for all j. As in the first part of the proof we have $c(x) \equiv (x-a)^2\ (P)$, $a \not\equiv 0\ (P)$; hence $c_0 \equiv -a^2\ (P)$, $c_1 \equiv 2a\ (P)$. From $c(x) = c(a) + (2a - c_1)(x - a) + (x - a)^2$ we conclude that $c(a)(x - a) + (x - a)^3 \equiv 0\ (c(x), P^2)$, since $(2a - c_1) \equiv 0\ (P)$, and $(x - a)^2 \equiv 0$ $(c(x), P)$. Observing that

$$x^3 - a^3 = (x - a)^3 + 3ax(x - a) \quad \text{and} \quad x(x - a) \equiv a(x - a)\ (c(x), P),$$

we obtain

$$x^3 - a^3 \equiv -c(a)(x - a) + 3a^2(x - a) \equiv (3a^2 - c(a))(x - a)\ (c(x), P^2).$$

Since $x^3 - a^3 \equiv (x - a)^3 \equiv 0\ (c(x), P)$ and $x^3 + a^3 = x^3 - a^3 + 2a^3 \equiv 2a^3$ $(c(x), P)$, this yields

$$x^6 - a^6 = (x^3 - a^3)(x^3 + a^3) \equiv 2a^3(3a^2 - c(a))(x - a)\ (c(x), P^2).$$

From $a^2 = a^{N(P)-1} \equiv 1\ (P)$ we obtain

$$a^6 = 1 + 3(a^2 - 1) + 3(a^2 - 1)^2 + (a^2 - 1)^3 \equiv 1\ (P^2).$$

Hence (by Lemma 1),

$$u_{j+6} - u_j \equiv 2a^3(3a^2 - c(a))(u_{j+1} - au_j)\ (P^2).$$

Since $u_{j+1} - au_j \equiv a(u_j - au_{j-1}) \equiv \cdots \equiv a^j(u_1 - au_0)\ (P)$ and $u_1 - au_0 \not\equiv 0\ (P)$, $u_{j+6} - u_j \not\equiv 0\ (P^2)$ is seen to be equivalent to $3a^2 - c(a) \not\equiv 0\ (P^2)$. Taking $a = 2c_1$ (a was only subject to the condition $c_1 \equiv 2a\ (P)$), we finally conclude that (u_n) is u.d. mod P^2 if and only if

$$c_1^2 + c_0 \equiv 3 \cdot 4c_1^2 - (4c_1^2 - 2c_1^2 - c_0) \not\equiv 0\ (P^2).$$

References

1. R. T. Bumby, *A distribution property for linear recurrence of the second order*, Proc. Amer. Math. Soc. **50** (1975), 101–106.

2. P. Bundschuh and J.-S. Shiue, *Solution of a problem on the uniform distribution of integers*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **55** (1973), 172–177.

3. M. J. Knight and W. A. Webb, *Uniform distribution of third order linear recurrence sequences*, Acta Arith. **36** (1980), 7–20.

4. L. Kuipers and J.-S. Shiue, *A distribution property of the sequence of Fibonacci numbers*, Fibonacci Quart. **10** (1972), 375–376, 392.

5. _____, *A distribution property of the sequence of Lucas numbers*, Elem. Math. **27** (1972), 10–11.

6. _____, *A distribution property of a linear recurrence of the second order*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **52** (1972), 6–10.

7. W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Math., vol. 1087, Springer-Verlag, Berlin and New York, 1984.

8. M. B. Nathanson, *Linear recurrences and uniform distribution*, Proc. Amer. Math. Soc. **48** (1975), 289–291.

9. H. Niederreiter, *Distribution of Fibonacci numbers mod* 5^k, Fibonacci Quart. **10** (1972), 373–374.

10. H. Niederreiter and J.-S. Shiue, *Equidistribution of linear recurring sequences in finite fields*, Indag. Math. **39** (1977), 397–405.

11. _____, *Equidistribution of linear recurring sequences in finite fields*, II, Acta Arith. **38** (1980), 197–207.

12. P. Ribenboim, *Algebraic numbers*, Wiley, New York, 1972.

13. R. F. Tichy and G. Turnwald, *Uniform distribution of recurrences in Dedekind domains*, Acta Arith. **46** (1985), 81–89.

14. G. Turnwald, *Gleichverteilung linearer Rekursionen*, Dissertation, Techn. Univ. Wien, 1984.

15. _____, *Gleichverteilung von linearen rekursiven Folgen*, Sitzungsber. Österr. Akad. Wiss. Math.-Naturwiss. Kl. **193** (1984), 201–245.

16. W. A. Webb and C. T. Long, *Distribution modulo* p^h *of the general linear second order recurrence*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **58** (1975), 92–100.

Institut für Analysis, Technische Mathematik und Versicherungsmathematik, Technische Universität Wien, Wiedner Hauptstr, 8–10, A - 1040 Vienna, Austria