ACTA ARITHMETICA
XLVI (1985)

Uniform distribution of recurrences in Dedekind domains

by

R. F. Tichy and G. Turnwald (Wien)

1. Introduction. Let R be a commutative ring with identity 1 and I an ideal of R such that the residue class ring R/I is finite. Then a sequence $\{u_k\}_{k=0}^{\infty}$ of elements of R is said to be *uniformly distributed modulo* I (u.d. $\bmod I$) if and only if (for short: iff) for every $r \in R$

$$\lim_{n\to\infty} \frac{A(n, r, I)}{n} = \frac{1}{N(I)}, \tag{1.1}$$

where $A(n, r, I)$ denotes the number of indices k such that $0 \leqslant k < n$ and $u_k \equiv r \bmod I$; $N(I)$ denotes the cardinality of the finite ring R/I. In the case that R is the ring of integers of an algebraic number field (of finite degree) $N(I)$ is the absolute norm of the ideal I. If I is a maximal ideal the sequence $\{u_k\}$ is u.d. $\bmod I$ if and only if $\{u_k + I\}$ is u.d. in the finite field R/I.

H. Niederreiter and J.-S. Shiue [6], [7] described all u.d. linear recurring sequences of orders 2, 3, and 4 with elements in finite fields. Uniform distribution of linear recurring sequences of rational integers has been studied by several authors (detailed references are given in [6]). R. T. Bumby [1] was the first to obtain a complete characterization of all u.d. recurrences of second order; in the case of third order linear recurrences (including second order) M. J. Knight and W. A. Webb [3] established a corresponding result for uniform distribution $\bmod m$ (i.e. modulo the principal ideal (m)) — provided that m is not divisible by 2, 3, and 5. A complete characterization of u.d. third order linear recurrences of algebraic integers has been obtained recently ([9], [10]). Since this result is rather complicated we formulate it only for rational integers:

THEOREM 1. *Let $\{u_k\}$ be a linear recurring sequence with characteristic polynomial $c(x) = x^3 - c_2 x^2 - c_1 x - c_0$. Then we have*

I. *$\{u_k\}$ is u.d.* $\bmod m$ *iff the following conditions hold:*

1. *$\{u_k\}$ is u.d.* $\bmod p^h$ *for every prime power divisor p^h of m.*

2. *There exists at most one odd prime p dividing m such that $c(x) \equiv (x-\alpha)^3 \bmod p$ and $u_2-2\alpha u_1+\alpha^2 u_0 \not\equiv 0 \bmod p$.*
3. *If there exists an odd prime with the properties stated in 2. and if m is even, then $u_0 \not\equiv u_2 \bmod 2$ and $c_0 \not\equiv 0 \bmod 2$; if $m \equiv 0 \bmod 4$ in addition we must have $c_1 \not\equiv -1 \bmod 4$.*

II. 1. *$\{u_k\}$ is u.d. $\bmod 2$ iff one of the following three conditions holds:*
1.1. $c(x) \equiv x(x-1)^2 \bmod 2$ *and* $u_1 \not\equiv u_2 \bmod 2$.
1.2. $c(x) \equiv (x-1)^3 \bmod 2$ *and* $u_2 \equiv u_0 \bmod 2$, $u_1 \not\equiv u_0 \bmod 2$.
1.3. $c(x) \equiv (x-1)^3 \bmod 2$ *and* $u_2 \not\equiv u_0 \bmod 2$.
2. *$\{u_k\}$ is u.d. $\bmod 4$ iff $\{u_k\}$ is u.d. $\bmod 2$ and one of the following conditions holds:*
2.1. $c(x) \equiv x(x-1)^2 \bmod 2$, $c_0+c_1+c_2 \equiv 1 \bmod 4$, $c_1 \not\equiv 1 \bmod 4$.
2.2. $c(x) \equiv (x-1)^3 \bmod 2$, $c_0+c_1+c_2 \not\equiv 1 \bmod 4$, $u_2 \equiv u_0 \bmod 2$.
2.3. $c(x) \equiv (x-1)^3 \bmod 2$, $c_0+c_1+c_2 \equiv 1 \bmod 4$, $u_2 \equiv u_0 \bmod 2$, $u_2 \not\equiv u_0 \bmod 4$, $c_1 \equiv 1 \bmod 4$.
2.4. $c(x) \equiv (x-1)^3 \bmod 2$, $c_0+c_1+c_2 \equiv 1 \bmod 4$, $u_2 \not\equiv u_0 \bmod 2$, $u_0 \not\equiv u_1 \not\equiv u_2 \bmod 4$, $c_0 \equiv 1 \bmod 4$, $c_1 \equiv -1 \bmod 4$.
2.5. $c(x) \equiv (x-1)^3 \bmod 2$, $c_0+c_1+c_2 \equiv 1 \bmod 4$, $u_2 \not\equiv u_0 \bmod 2$, $c_1 \not\equiv -1 \bmod 4$.
3. *$\{u_k\}$ is u.d. $\bmod 8$ iff $\{u_k\}$ is u.d. $\bmod 4$ and one of the following conditions holds:*
3.1. = 2.1.
3.2. = 2.2.
3.3.: 2.3. *and* $c_0+c_1+c_2 \equiv 1 \bmod 8$.
3.4.: 2.4. *and* $c_0+c_1+c_2 \equiv 1 \bmod 8$, $c_1 \not\equiv -1 \bmod 8$.
3.5. = 2.5.
4. *If $\{u_k\}$ is u.d. $\bmod 8$ then $\{u_k\}$ is u.d. $\bmod 2^h$ for every positive integer h.*

III. 1. *Let p be an odd prime; then $\{u_k\}$ is u.d. $\bmod p$ iff $c(x) \equiv (x-\alpha)^2 \times (x-\beta) \bmod p$ (for some integers α, β with $\alpha \not\equiv 0 \bmod p$) and one of the following conditions holds:*
1.1 $\alpha \not\equiv \beta \bmod p$, $u_2-(\alpha+\beta)u_1+\alpha\beta u_0 \not\equiv 0 \bmod p$.
1.2. $\alpha \equiv \beta \bmod p$, $u_2-2\alpha u_1+\alpha^2 u_0 \equiv 0 \bmod p$, $u_1-\alpha u_0 \not\equiv 0 \bmod p$.
1.3. $\alpha \equiv \beta \bmod p$, $u_2-2\alpha u_1+\alpha^2 u_0 \not\equiv 0 \bmod p$, $(u_2-4\alpha u_1+\alpha^2 u_0)^2 \equiv 4\alpha^2 u_0 u_2 \bmod p$ *and α is not a square* $\bmod p$.
2. *Let p be an odd prime; then $\{u_k\}$ is u.d. $\bmod p^2$ iff $\{u_k\}$ is u.d. $\bmod p$ and one of the following two conditions holds (where α and β have the same meaning as in 1.):*
2.1. *If $p = 3$ one of the following conditions must be satisfied:*
2.1.1. $\alpha \not\equiv \beta \bmod p$, $\beta \equiv 0 \bmod p$, $c(\alpha) \not\equiv 3\alpha \bmod p^2$.
2.1.2. $\alpha \not\equiv \beta \bmod p$, $\beta \not\equiv 0 \bmod p$, $c(\alpha) \not\equiv -3\alpha \bmod p^2$.

2.1.3. $\alpha \equiv \beta \bmod p$, $u_2-2\alpha u_1+\alpha^2 u_0 \equiv 0 \bmod p$, $\alpha^3-c_2\alpha^2-c_1\alpha-c_0 \equiv 0 \bmod p^2$, $3\alpha^2-2\alpha c_2-c_1 \not\equiv 3 \bmod p^2$.
2.1.4. $\alpha \equiv \beta \bmod p$, $u_2-2\alpha u_1+\alpha^2 u_0 \not\equiv 0 \bmod p$, $c_1 \not\equiv c_2 \bmod p^2$, $1+c_0 \not\equiv c_1 \bmod p^2$, $1+c_0 \not\equiv -c_2 \bmod p^2$.
2.2. *If $p \neq 3$ one of the following two conditions must be satisfied:*
2.2.1. $\alpha \not\equiv \beta \bmod p$.
2.2.2. $\alpha \equiv \beta \bmod p$, $u_2-2\alpha u_1+\alpha^2 u_0 \equiv 0 \bmod p$.
3. *If p is an odd prime and $\{u_k\}$ is u.d. $\bmod p^2$ then $\{u_k\}$ is u.d. $\bmod p^h$ for every positive integer h.*

In the present paper we investigate uniform distribution of recurrences with elements in an arbitrary Dedekind domain R. Furthermore we show how to deduce the characterization of u.d. third order linear recurrences in p-adic integers from Theorem 1. In a final section we generalize a result of Nagasaka [5] concerning the weak uniform distribution (w.u.d.) of a special sequence to the case of Dedekind domains. A sequence $\{u_k\}$ with elements in a ring R is said to be w.u.d. $\bmod I$ iff for every $\bmod I$ invertible element $r \in R$

$$\lim_{n\to\infty} \frac{A(n, r, I)}{n} = \frac{1}{N^*(I)}, \tag{1.2}$$

where $N^*(I)$ denotes the number of invertible elements of the finite ring R/I.

2. Linear recurring sequences in Dedekind domains. Let P be a non-zero prime ideal of a Dedekind domain R; we assume that R/P is finite. Then $N(P^h) = N(P)^h$ for every positive integer h ([8], Chapter 8, A; the proof given there only in the case of algebraic integers is valid for arbitrary Dedekind domains). We denote the characteristic of the finite field R/P by p and assume $p \neq 2$; the case $p = 2$ can be treated similarly but is more technical (for algebraic integers cf. [9], [10]). As in the introduction $\{u_k\}$ is an r-th order linear recurring sequence with characteristic polynomial

$$c(x) = x^r - c_{r-1}x^{r-1} - \ldots - c_0$$

(i. e. $u_{k+r} = c_{r-1}u_{k+r-1} + \ldots + c_0 u_k$ for all $k \geq 0$; it should be remarked that there may exist characteristic polynomials of smaller order).

Lemma 1. *Let e_0 be the multiplicity of x in the factorization of the characteristic polynomial $c(x) \bmod P$ and let e_i $(i \geq 1)$ be the multiplicities of the remaining irreducible factors of $c(x) \bmod P$. We choose t as the smallest non-negative integer such that $p^t \geq e_i$ $(i \geq 1)$. If v denotes the order of the multiplicative group of the splitting field of $c(x)$ over R/P, then $(v, p) = 1$. Setting $l = vp^t$ we have (for $k \geq 0$)*

$$u_{j+kp^h l} \equiv u_j + kp^h(u_{j+l}-u_j) \bmod P^{h+2} \quad \textit{for } h \geq 0,\ j \geq \max(2e_0, 3\cdot 2^{h-1}e_0). \tag{2.1}$$

(2.2) $\{u_k\}$ *is periodic* $\bmod P^{h+1}$ $(h \geqslant 0)$ *with preperiod* $2^h e_0$ *and period (length)* $p^h l$.

(2.3) *If* $e_i \leqslant 2$ $(i \geqslant 1)$, *then*

$$u_{j+kv} \equiv u_j + k(u_{j+v} - u_j) \bmod P \quad \text{for} \quad j \geqslant e_0.$$

(2.4) *If* $e_i \leqslant 2$ $(i \geqslant 1)$ *and* $p \geqslant 5$, *then*

$$u_{j+pv} \equiv u_j + p(u_{j+v} - u_j) \bmod P^2 \quad \text{for} \quad j \geqslant 2e_0.$$

Proof. See Section 2.2.1 of [9], [10].

In the following we investigate the uniform distribution of $\{u_k\}$ modulo powers of P. First we want to state two elementary properties of uniform distribution:

(2.5) If $\{u_k\}$ is u.d. $\bmod I$ and $I \subseteq J$, then $\{u_k\}$ is u.d. $\bmod J$.

(2.6) If $\{u_k\}$ is u.d. $\bmod I$, then the period length of $\{u_k\} \bmod I$ is divisible by $N(I)$.

Remark 1. If $e_i = 1$ $(i \geqslant 1)$ then in Lemma 1 we have $l = v$, and by (2.2) and (2.6) we conclude that $\{u_k\}$ is not u.d. $\bmod P$, since $(v, p) = 1$ and $N(P)$ is a power of p.

LEMMA 2. *Assume* $N(P) = p$ *and (in the notation of Lemma 1)* $u_{j+l} - u_j \not\equiv 0 \bmod P^2$ *for sufficiently large* j. *Then* $\{u_k\}$ *is u.d.* $\bmod P^2$ *provided that* $\{u_k\}$ *is u.d.* $\bmod P$; *if, in addition,* $p \not\equiv 0 \bmod P^2$ *then* $\{u_k\}$ *is u.d.* $\bmod P^h$ *for all* $h \geqslant 0$.

Proof. We proceed by induction and assume that $\{u_k\}$ is u.d. $\bmod P^{h+1}$ for some $h \geqslant 0$. By (2.2) the sequence $\{u_k\}$ has period-length $p^{h+1} l \bmod P^{h+2}$, and in order to prove uniform distribution $\bmod P^{h+2}$ we have to show that the number of indices n in a full period of length $p^{h+1} l$ with $u_n \equiv x \bmod P^{h+2}$ is independent of x.

We have $p^h \in P^h - P^{h+1}$ since this is trivial for $h = 0$ and follows from $p \in P - P^2$ for $h > 0$. Then $p^h(u_{j+l} - u_j) \in P^{h+1} - P^{h+2}$ and, since $u_{j+kp^h l} - u_j \equiv kp^h(u_{j+l} - u_j) \bmod P^{h+2}$ (by (2.1)), the congruence $u_{j+kp^h l} \equiv u_j \bmod P^{h+2}$ implies $k \equiv 0(P)$, i. e. k is divisible by p (all conclusions hold for sufficiently large j).

Since $N(P) = p$ yields

$$|P^{h+1}/P^{h+2}| = |R/P^{h+2}| : |R/P^{h+1}| = N(P^{h+2})/N(P^{h+1}) = N(P) = p,$$

this means that for fixed j the elements $u_{j+kp^h l}$ (for $k = 0, \ldots, p-1$) run through the residue classes $\bmod P^{h+2}$ which correspond to the residue class of $u_j \bmod P^{h+1}$. Thus the number of indices n in a full period of length $p^{h+1} l$ with $u_n \equiv x \bmod P^{h+2}$ is equal to the number of indices j in a full period of length $p^h l (\bmod P^{h+1})$ with $u_j \equiv x \bmod P^{h+1}$, and the last number is independent of x by assumption.

(In a condition like $p \not\equiv 0 \bmod P^2$ we interprete p as p times the unit element of R.)

THEOREM 2. *Let P be a prime ideal of the Dedekind domain R with corresponding prime* $p \neq 2$; $\{u_k\}$ *denotes a linear recurring sequence with characteristic polynomial* $c(x)$. *We assume that* $c(x)$ *splits into linear factors* $\bmod P$ *and that all factors different from x occur with multiplicity at most p (the multiplicity of x can be arbitrary). If* $\{u_k\}$ *is u.d.* $\bmod P$ *then*

1. $\{u_k\}$ *is u.d.* $\bmod P^2$ *iff* $u_{j+p(p-1)} - u_j \not\equiv 0 \bmod P^2$ *for sufficiently large* j.

2. *If* $\{u_k\}$ *is u.d.* $\bmod P^2$ *and* $p \not\equiv 0 \bmod P^2$, *then* $\{u_k\}$ *is u.d.* $\bmod P^h$ *for all* $h \geqslant 0$. *If* $p \equiv 0 \bmod P^2$ *then* $\{u_k\}$ *is not u.d.* $\bmod P^3$.

Proof. We use the notation of Lemma 1. From $e_i \leqslant p$ $(i \geqslant 1)$ we obtain $l = pv$ with $(p, v) = 1$. Since l must be divisible by $N(P)$ we obtain $N(P) = p$. By assumption $c(x)$ splits into linear factors and so $v = N(P) - 1 = p - 1$. If $u_{j+p(p-1)} - u_j \not\equiv 0 \bmod P^2$ then by Lemma 2 $\{u_k\}$ is u.d. $\bmod P^2$. Taking $h = 0$ in (2.1) from $u_{j+p(p-1)} - u_j \equiv 0 \bmod P^2$ we derive $u_{j+kl} \equiv u_j \bmod P^2$ (for all k); hence the residue $u_j \bmod P^2$ occurs at least p times (for $k = 0, \ldots, p-1$) in a period of length $pl \bmod P^2$. If $\{u_k\}$ were u.d. $\bmod P^2$ every residue $\bmod P^2$ would occur $pl/N(P^2) = p - 1$ times in a period of length pl, however. This proves 1.

The first part of 2. follows from 1. and Lemma 2. Taking $k = h = 1$ in (2.1) we obtain $u_{j+pl} \equiv u_j \bmod P^3$ from $p \equiv 0 \bmod P^2$ (observing $u_{j+l} - u_j \equiv 0 \bmod P$). Since pl is not divisible by $N(P)^3$, $\{u_k\}$ is not u.d. $\bmod P^3$.

Remark 2. By Lemma 1 the minimal period of $\{u_k\} \bmod P$ is not divisible by p if $c(x)$ has no multiple factors $\bmod P$ (except possibly the factor x). Hence in this case $\{u_k\}$ is not u.d. $\bmod P$.

Suppose $c(x)$ has degree at most 3; then the existence of multiple factors $\bmod P$ implies that $c(x)$ splits into linear factors $\bmod P$, and so in Theorem 2 it is sufficient to assume that $\{u_k\}$ is u.d. $\bmod P$.

Remark 3. As we saw in the proof the hypotheses of Theorem 2 imply $N(P) = p$ and $l = p(p-1)$.

The result $N(P) = p$ and the second half of part 2 of Theorem 2 remain valid if we just assume that $c(x)$ splits into irreducible factors $\bmod P$ with multiplicities at most p (with the possible exception of the factor x); we do not necessarily have $l = p(p-1)$, but $l \not\equiv 0 \bmod p^2$.

Remark 4. The proof of Theorem 2 is essentially taken from [9], [10] (cf. Sections 2.2.3 and 2.2.4). In the quoted papers only the case of algebraic integers is treated, but with minor changes the arguments presented there hold for arbitrary Dedekind domains; for example instead of assuming that p is ramified, we write $p \equiv 0 \bmod P^2$. Hence we obtain a classification of all $\bmod I$ u.d. third order linear recurring sequences $\{u_k\}$ with elements in a

Dedekind domain R, provided that I is an arbitrary ideal with finite norm $N(I)$.

The theorems concerning uniform distribution in a ring of algebraic integers can be used directly for the investigation of uniform distribution $\bmod I$ in an arbitrary Dedekind domain R if R/I is isomorphic to a residue class ring of a ring of algebraic integers. We illustrate this for the ring R of p-adic integers. As is well known every non-zero ideal I is a principal ideal (p^h) generated by a power of p, and R/I is isomorphic to $Z/p^h Z$ (Z denotes the ring of rational integers).

Let $\{u_k\}$ be a linear recurring sequence with characteristic polynomial $c(x) = x^r - c_{r-1}x^{r-1} - \ldots - c_0$. We choose rational integers u'_k $(0 \leqslant k \leqslant r-1)$, c'_j $(0 \leqslant j \leqslant r-1)$ such that the residue classes $u'_k + p^h Z$, $c'_j + p^h Z$ correspond to the residue classes $u_k + I$, $c_j + I$. If we define the linear recurring sequence $\{u'_k\}$ of rational integers by the initial values $u'_0, \ldots, u'_{r-1}$ and the characteristic polynomial $x^r - c'_{r-1}x^{r-1} - \ldots - c'_0$, then for all k the residue class $u'_k + p^h Z$ corresponds to $u_k + I$ and $\{u_k\}$ is u.d. $\bmod I$ iff $\{u'_k\}$ is u.d. $\bmod p^h Z$.

For any $m \leqslant h$ the elements of R with residue classes $\bmod I$ corresponding to residue classes $(\bmod p^h Z)$ of elements of $p^m Z$ are just the elements of $p^m R$. Hence congruences concerning u'_k, $c'_j \bmod p^m$ (i. e. $\bmod p^m Z$) may be interpreted as congruences concerning u_k, $c_j \bmod p^m R$. In the case $r = 3$ from Theorem 1 we obtain:

THEOREM 3. *Let $\{u_k\}$ be a third order linear recurring sequence in p-adic integers. If $p \neq 2$ and $\{u_k\}$ is u.d. $\bmod p^2$ then $\{u_k\}$ is u.d. $\bmod p^h$ for all $h \geqslant 1$. If $p = 2$ and $\{u_k\}$ is u.d. $\bmod p^3$ then $\{u_k\}$ is u.d. $\bmod p^h$ for all $h \geqslant 1$.*

Remark 5. By uniform distribution $\bmod p^h$ we, of course, mean uniform distribution $\bmod p^h R$. The conditions for u.d. $\bmod p$, $\bmod p^2$ and $\bmod p^3$ (for $p = 2$) may be seen from Theorem 1, II $(p = 2)$ and III $(p \neq 2)$; the congruences have to be interpreted in p-adic integers.

Remark 6. As another example we can apply the above argumentation to the ring of formal power series over Z/pZ, p prime. Every ideal is of the form (x^r) and the residue class ring is isomorphic to R/P if P is a prime divisor of p in the $(p-1)p^{r+1}$-th cyclotomic fields.

Let R be the ring of algebraic integers of the mth cyclotomic field, $m = p^f - 1$ (p prime, f arbitrary). Then pR splits into $g = \varphi(m)/f$ distinct prime ideals P_i of residue class degree f (cf. [8], Chapter 13, 4.B) and (by the Chinese remainder theorem) R/pR is isomorphic to the g-fold product of the finite field $\mathrm{GF}(p^f)$. Hence the above considerations can be applied to uniform distribution modulo an ideal with residue class ring isomorphic to such a product of a finite field.

Finally we want to remark that not every finite residue class ring of a commutative ring with unit element is isomorphic to a residue class ring of a Dedekind domain. It clearly suffices to construct a finite commutative ring R with unit element which is not the homomorphic image of a Dedekind domain. We take $R = \{(a, a+2b)\colon a, b \in Z/4Z\}$ with componentwise operations and make use of the fact that every ideal of a proper residue class ring of a Dedekind domain is generated by one element (cf. [8], Chapter 7.I). We consider the ideal I of R generated by $(0, 2)$ and $(2, 2)$. Obviously every element of I has the form $(2a, 2a+2b)$; since conversely

$$(b, b)\cdot(0, 2) + (a, a)\cdot(2, 2) = (2a, 2a+2b),$$

every element of this form belongs to I. As I contains elements with non-zero first and second component, the only possible generator of I is $(2, 2)$. But $(0, 2)$ is not a multiple of $(2, 2)$ since $(a, a+2b)\cdot(2, 2) = (2a, 2a)$ has equal components. Hence I is not generated by one element.

3. A special non-linear recurring sequence. Let m be an integer greater than 1 and $\{u_k\}_{k=0}^{\infty}$ be a sequence of $\bmod m$ invertible integers satisfying the recurrence $u_{k+1} \equiv u_k + u_k^{-1} \bmod m$ (u_k^{-1} denotes the inverse $\bmod m$). In a recent paper [5] K. Nagasaka proved that such a sequence is w.u.d. $\bmod m$ only if $m = 3$. We give a generalization to arbitrary Dedekind domains.

THEOREM 4. *Let I be an ideal of a Dedekind domain R with finite norm $N(I) > 1$ and $\{u_k\}_{k=0}^{\infty}$ be a sequence of $\bmod I$ invertible elements of R satisfying the recurrence $u_{k+1} \equiv au_k + bu_k^{-1} \bmod I$ with $\bmod I$ invertible elements a, b of R (u_k^{-1} denotes a representative of the inverse of $u_k + I$). Then $\{u_k\}$ is w.u.d. $\bmod I$ if and only if I is a prime ideal with $N(I) = 3$ and $a \equiv b \equiv 1 \bmod I$.*

In the proof we make use of the following

LEMMA 3. *Let I be an ideal of a Dedekind domain R with finite norm $N(I)$ and $\{u_k\}$ be a sequence w.u.d. $\bmod I$. If J is an ideal containing I then $\{u_k\}$ is w.u.d. $\bmod J$.*

Proof of Lemma 3. We may write $I = \prod P_i^{\alpha_i}$ and $J = \prod P_i^{\beta_i}$ with distinct prime ideals P_i of R and $\alpha_i \geqslant \beta_i \geqslant 0$. We have to show that the number of invertible residue classes $\bmod I$ corresponding to an invertible residue class $a + J$ is independent of a. The residue class $x + I$ corresponds to $a + J$ iff $x \equiv a \bmod P_i^{\beta_i}$ (for $\beta_i \neq 0$); in this case $x + I$ is invertible iff x is invertible $\bmod P_i$ for all indices i such that $\beta_i = 0$ (since invertibility $\bmod P_i^{\beta_i}$ with $\beta_i \neq 0$ implies invertibility $\bmod P_i^{\alpha_i}$ and an element is invertible $\bmod I$ iff it is invertible $\bmod P_i^{\alpha_i}$ for all indices i). So the number of possible residue classes of $x \bmod P_i^{\alpha_i}$ is $N(P_i)^{\alpha_i - \beta_i}$ for $\beta_i \neq 0$ and $(N(P_i) - 1)N(P_i)^{\alpha_i - 1}$ for $\beta_i = 0$. By the Chinese remainder theorem the number of solutions for $x \bmod I$ is the product of these numbers, hence independent of a.

Proof of Theorem 4. Let $\{u_k\}$ be w.u.d. $\bmod I$. Then for every $\bmod I$ invertible element c there exists an invertible residue class $u_k + I$ such that $au_k + bu_k^{-1} \equiv c \bmod I$, and $ac + bc^{-1}$ $(\equiv u_{k+2} \bmod I)$ is again invertible $\bmod I$. Hence the function f defined $(\bmod I)$ by $f(s) \equiv as + bs^{-1} \bmod I$ (for $\bmod I$

invertible elements s) induces a bijection on the finite set $(R/I)^*$. Since obviously $f(s) \equiv f(ba^{-1}s^{-1})$, we obtain $s \equiv ba^{-1}s^{-1} \bmod I$. Setting $s = 1$ yields $1 \equiv ba^{-1} \bmod I$; hence $s^2 \equiv 1 \bmod I$ for all $\bmod I$ invertible elements s. Since $f(1) \equiv a+b \equiv 2a \bmod I$ implies that 2 is invertible $\bmod I$, we conclude $2^2 \equiv 1 \bmod I$, i. e. $3 \equiv 0 \bmod I$.

Let P be a prime divisor of I. By Lemma 3 $\{u_k\}$ is w.u.d. $\bmod P$, and the above arguments (applied to P instead of I) show that $s^2 \equiv 1 \bmod P$ for $s \not\equiv 0(P)$ and $3 \equiv 0 \bmod P$, i. e. the finite field R/P has characteristic 3 and the multiplicative group has at most two elements. Hence $N(P) = 3$ and $\{u_k\}$ has period length 2 $\bmod P$. If P^2 divides I, then $\{u_k\}$ is w.u.d. $\bmod P^2$ by Lemma 3. But for $\pi \in P - P^2$ we have $f(1) \equiv 2a \bmod P^2$ and $f(1+\pi) \equiv a(1+\pi)+a(1-\pi) \equiv 2a \bmod P^2$; since $1 \not\equiv 1+\pi \bmod P^2$ this is impossible. Hence I is the product of distinct prime factors $P_1, \ldots, P_m$. Since $\{u_k\}$ has period length 2 $\bmod P_i$ for all i, $\{u_k\}$ has period length 2 modulo $I = \prod P_i = \bigcap P_i$. The number of invertible residue classes $\bmod I$ is

$$\prod_{i=1}^{m} (N(P_i)-1) = 2^m,$$

and so we must have $m = 1$, i. e. I is a prime ideal with $N(I) = 3$. In this case there are only four possibilities for $\{u_k\} \bmod I$:

$$u_0 \equiv 1, \quad a \equiv 1 \bmod I: \quad \{u_k\} \equiv \{1, 2, 1, 2, \ldots\} \bmod I,$$
$$u_0 \equiv 1, \quad a \equiv 2 \bmod I: \quad \{u_k\} \equiv \{1, 1, 1, 1, \ldots\} \bmod I,$$
$$u_0 \equiv 2, \quad a \equiv 1 \bmod I: \quad \{u_k\} \equiv \{2, 1, 2, 1, \ldots\} \bmod I,$$
$$u_0 \equiv 2, \quad a \equiv 2 \bmod I: \quad \{u_k\} \equiv \{2, 2, 2, 2, \ldots\} \bmod I.$$

Since just the first and the third sequence are w.u.d. $\bmod I$, this proves our theorem.

References

[1] R. T. Bumby, *A distribution property for linear recurrence of the second order*, Proc. Amer. Math. Soc. 50 (1975), pp. 101–106.
[2] E. Hlawka, *Theorie der Gleichverteilung*, Bibl. Inst. Mannheim–Wien–Zürich 1979.
[3] M. J. Knight and W. A. Webb, *Uniform distribution of third order linear recurrence sequences*, Acta Arith. 36 (1980), pp. 7–20.
[4] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, John Wiley and Sons, New York 1974.
[5] K. Nagasaka, *Distribution property of recursive sequences defined by* $u_{n+1} \equiv u_n + u_n^{-1} \pmod m$, Fibonacci Quart. 22 (1984), pp. 76–81.
[6] H. Niederreiter and J.-S. Shiue, *Equidistribution of linear recurring sequences in finite fields*, Indag. Math. 39 (1977), pp. 397–405.
[7] — — *Equidistribution of linear recurring sequences in finite fields, II*, Acta Arith. 38 (1980), pp. 197–207.
[8] P. Ribenboim, *Algebraic Numbers*, John Wiley and Sons, New York 1972.

[9] G. Turnwald, *Gleichverteilung linearer Rekursionen*, Techn. Univ. Wien, Diss., 1984.
[10] — *Gleichverteilung von linearen rekursiven Folgen*, Sitzungsber. Österr. Akad. Wiss., math.-naturwiss. Kl., 193 (1984), pp. 201–245.

INSTITUT FÜR ANALYSIS, TECHNISCHE
MATHEMATIK UND VERSICHERUNGSMATHEMATIK
TECHNISCHE UNIVERSITÄT WIEN
WIEDNER HAUPTSTRASSE 6-10
A-1040 WIEN
AUSTRIA

Received on 4.8.1984 (1451)