TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 301, Number 1, May 1987

UNIFORM DISTRIBUTION OF TWO-TERM RECURRENCE SEQUENCES

WILLIAM YSLAS VÉLEZ

ABSTRACT. Let u_0, u_1, A, B be rational integers and for $n \geqslant 2$ define $u_n = Au_{n-1} + Bu_{n-2}$. The sequence (u_n) is clearly periodic modulo m and we say that (u_n) is uniformly distributed modulo m if for every s, every residue modulo m occurs the same number of times in the sequence of residues $u_s, u_{s+1}, \ldots, u_{s+N-1}$, where N is the period of (u_n) modulo m. If (u_n) is uniformly distributed modulo m then m divides N, so we write $N = mf$. Several authors have characterized those m for which (u_n) is uniformly distributed modulo m. In fact in this paper we will show that a much stronger property holds when $m = p^k$, p a prime. Namely, if (u_n) is uniformly distributed modulo p^k with period $p^k f$, then every residue modulo p^k appears exactly once in the sequence $u_s, u_{s+f}, \ldots, u_{s+(p^k-1)f}$, for every s. We also characterize those composite m for which this more stringent property holds.

Let u_0, u_1, A, B be rational integers and define, for $n \geqslant 2$, $u_n = Au_{n-1} + Bu_{n-2}$. The sequence of integers (u_n) thus obtained is said to be a two-termed linear recurrence sequence. If m is a positive integer then the sequence (u_n) considered modulo m is clearly periodic.

DEFINITION. The sequence (u_n) is said to be uniformly distributed modulo m (henceforth denoted by UD(mod m)) if every residue modulo m occurs the same number of times in any period. That is, if N is the period of (u_n) modulo m, then for every s, every residue modulo m appears the same number of times among the residues $\{u_s, u_{s+1}, \ldots, u_{s+N-1}\}$.

Those m for which (u_n) is UD(mod m) have been determined by several authors and recently Narkiewicz [**2**] has collected these results together. We shall use the notation and results of Chapter 3 of [**2**] throughout this paper.

In order to state this characterization we begin by developing some terminology. Given (u_n), let $D = A^2 + 4B$ be the discriminant of $x^2 - Ax - B$. We can express u_n in terms of the roots of the quadratic in the following way (see Chapter 3 of [**2**]).

Case I, $D = 0$. Then $u_n = (c_0 + c_1 n)(A/2)^n$, for $n \geqslant 0$ and $c_0 = u_0$, $c_1 = (2u_1 - Au_0)A^{-1}$.

Case II, $D \neq 0$. Then $u_n = c_0((A + \sqrt{D})/2)^n + c_1((A - \sqrt{D})/2)^n$, where $c_0 = (u_0\sqrt{D} + (2u_1 - Au_0))/2\sqrt{D}$, $c_1 = (u_0\sqrt{D} - (2u_1 - Au_0))/2\sqrt{D}$.

Received by the editors August 5, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 10A35.
The author was supported in part by National Science Foundation Grant #PRM 82-13783.

THEOREM A. *The sequence* (u_n) *is* UD(mod m) *iff the following hold*:

(i) *If a prime p divides m then p divides D and $p \nmid B$.*

(ii) *If $p \geqslant 3$ then $p \nmid 2u_1 - Au_0$.*

(iii) *If $p = 3$ and $9 \mid m$ then $D \not\equiv 6 \pmod 9$.*

(iv) *If $p = 2$ then u_0, u_1 have opposite parity and if $4 \mid m$ then $A \equiv 2 \pmod 4$ and $B \equiv 3 \pmod 4$.*

If (u_n) is UD(mod m) then it is obvious that the period of (u_n) modulo m is divisible by m. Henceforth let us denote this period by mf.

If one specializes the above to the Fibonacci sequence, $u_0 = 0$, $u_1 = A = B = 1$, then (u_n) is UD(mod m) iff $m = 5^k$ and the period is $5^k \cdot 4$. For this sequence Erlebach and Vélez [**1**] discovered that in fact (u_n) satisfies an even more stringent property modulo 5^k, namely, for every s, every residue modulo 5^k occurs exactly once in the sequence $u_s, u_{s+4}, \ldots, u_{s+(5^k-1)4}$.

In this paper we shall see that this same type of distribution holds for the more general cases of UD(mod p^k) and we shall also characterize those composite m for which the above property holds. With this in mind we make the following definition.

DEFINITION. Let (u_n) be UD(mod m) with period mf. Then we say that (u_n) is f-UD(mod m) if for every s every residue modulo m occurs exactly once in the sequence $u_s, u_{s+f}, \ldots, u_{s+(m-1)f}$.

As mentioned above we shall prove the following.

THEOREM B. *The sequence* (u_n) *is* UD(mod p^k) *with period $p^k f$ iff* (u_n) *is* f-UD(mod p^k). *Furthermore, $f = 1$ if $p = 2$ otherwise it is the multiplicative order of $A/2$ modulo p.*

It is obvious that if (u_n) is f-UD(mod m) then (u_n) is UD(mod m). Thus we only have to prove one direction. What we shall actually prove is that if (u_n) and p satisfy conditions (i)–(iv) then (u_n) is f-UD(mod p^k).

The method of proof will be as follows. We shall expand $((A \pm \sqrt{D})/2)^n$ using the binomial theorem and reduce the expression in the appropriate residue system. Before launching into a proof we must first deal with some technical matters.

For a prime p let $\nu_p(a)$ denote the exact power of p that divides the integer a. For a rational number a/b we set $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$.

LEMMA 1. *Suppose that conditions* (i)–(iv) *of A are satisfied, $D \neq 0$ and $j \geqslant 1$.*

If $p = 2$, $\nu_2((2j+1)!A^{2j}) = \nu_2((2j)!A^{2j}) < 4j \leqslant \nu_2(D^j)$.

If $p \geqslant 5$ or $\nu_p(D) > 1$, then $\nu_p((2j+1)!A^{2j}) < \nu_p(D^j)$.

If $p = 3$ and $\nu_3(D) = 1$, then

$$\nu_3\big((2j+1)!A^{2j}\big) \leqslant j = \nu_3(D^j).$$

Further $\nu_3((2j+1)!A^{2j}) = j$ iff $2j+1$ is a power of 3.

PROOF. It is well known that

$$\nu_p((2j+1)!) = \sum_{h=1}^{\infty} \left[\frac{2j+1}{p^h} \right],$$

where [ ] denotes the greatest integer function. Let s be defined by $p^s \leqslant 2j+1 < p^{s+1}$.

If $p = 2$ and $k \geqslant 2$ then since $A \equiv 2 \pmod 4$, $B \equiv 3 \pmod 4$ we see that $\nu_2(D) \geqslant 4$ and $\nu_2(A^{2j}) = 2j$, so

$$\nu_2\big((2j+1)!A^{2j}\big) = 2j + \nu_2\big((2j)!\big) = 2j + \sum_{h=1}^{s}\left[\frac{2j}{2^h}\right]$$
$$\leqslant 2j + \sum_{h=1}^{s}\frac{2j}{2^h} = 2j + 2j(1-2^{-s}).$$

However, since the left-hand side is an integer we have that

$$\nu_2\big((2j)!A^{2j}\big) = \nu_2\big((2j+1)!A^{2j}\big) < 4j \leqslant \nu_2(D^s).$$

The remaining cases follow the same pattern. □

LEMMA 2. *Suppose that* u_0, u_1 *satisfy conditions* (i)–(iv). *If we replace* u_0, u_1 *by* u_s, u_{s+1} *in* (i)–(iv), *then* u_s, u_{s+1} *also satisfy conditions* (i)–(iv).

PROOF. It is obvious that if u_0, u_1 have opposite parity then u_s, u_{s+1} also have opposite parity. Thus it only remains to show that $p \nmid (2u_{s+1} - Au_s)$, where p is an odd prime satisfying $p|D$ and $p \nmid B$. From this it follows that $p \nmid A$ and $(A/2)^2 \equiv -2B \pmod p$.

Suppose that $p \nmid 2u_k - Au_{k-1}$ and consider $2u_{k+1} - Au_k$. Since $u_{k+1} = Au_k + Bu_{k-1}$, we have that

$$2u_{k+1} - Au_k = Au_k + 2Bu_{k-1} \equiv Au_k - (A^2/2)u_{k-1}$$
$$\equiv (A/2)(2u_k - Au_{k-1}) \pmod p,$$

so $p \nmid 2u_{k+1} - Au_k$. □

The formulas appearing in Cases I and II are rather cumbersome. The next two lemmas will allow us to reduce the analysis to the case where $u_0 = 0$ and $u_1 = 1$.

LEMMA 3. *Suppose that* (u_n) *and* p *satisfy* (i)–(iv). *Given any* k *there exists an* n *such that* $\nu_p(u_n) \geqslant k$.

PROOF. *Case* I: $u_n = (c_0 + c_1 n)(A/2)^n$. From the assumptions we see that $(p, c_1) = (p, A/2) = 1$, so we can easily solve the linear congruence $c_0 + c_1 n \equiv 0 \pmod{p^k}$.

Case II. By applying the binomial theorem to $(A \pm \sqrt{D})^n$, we obtain

$$u_n = \left(\frac{A}{2}\right)^n\Big[u_0\Big(1 + \binom{n}{2}A^{-2}D + \binom{n}{4}A^{-4}D^2 + \cdots\Big)$$
$$+ (2u_1 - Au_0)\Big(\binom{n}{1}A^{-1} + \binom{n}{3}A^{-3}D + \binom{n}{5}A^{-5}D^2 + \cdots\Big)\Big].$$

First of all observe that by 1 all of the expressions involving the binomial coefficients are integral at p.

Let us write n in the form $n = p^{k-1}m$, where $k \geqslant 1$ and m is to be determined later. If $\nu_p(D^j/A^{2j+1}(2j+1)!) > 0$ or $\nu_p(D^j/A^{2j}(2j)!) > 0$, then

$$\nu_p\left(\binom{p^{k-1}m}{2j+1}A^{-2j-1}D^j\right) \geqslant k \quad\text{and}\quad \nu_p\left(\binom{p^{k-1}m}{2j}A^{-2j}D^j\right) \geqslant k.$$

Thus from Lemma 1 it follows that for $n = p^{k-1}m$,

$$u_0\left[1 + \binom{n}{2}A^{-2}D + \binom{n}{4}A^{-4}D^2 + \cdots\right] \equiv u_0 \pmod{p^k}.$$

Further, if $p \geqslant 5$ or $\nu_p(D) > 1$, then from Lemma 1 we have that

$$u_n \equiv (A/2)^n\left[u_0 + (2u_1 - Au_0)A^{-1}p^{k-1}m\right] \pmod{p^k}.$$

We will now induct on k. If $k = 1$, then if p is odd

$$u_m \equiv (A/2)^m\left[u_0 + (2u_1 - Au_0)A^{-1}m\right] \equiv 0 \pmod{p}$$

has a solution for some m since $((2u_1 - Au_0), p) = 1$. If $p = 2$, then u_0, u_1 have opposite parity, so at least one of u_0, u_1, is divisible by 2.

Thus, assume there is an s for which $u_s \equiv 0 \pmod{p^{k-1}}$. By Lemma 2 we may assume that $u_0 \equiv 0 \pmod{p^{k-1}}$. So let $u_0 = p^{k-1}v$. Then

$$u_n \equiv (A/2)^n\left[p^{k-1}v + (2u_1 - Au_0)A^{-1}p^{k-1}m\right] \equiv 0 \pmod{p^k}$$

iff

$$u_n p^{-k+1} \equiv (A/2)^n\left[v + (2u_1 - Au_0)A^{-1}m\right] \equiv 0 \pmod{p},$$

which clearly has a solution for some m. Thus the lemma is true if $p \geqslant 5$ or $\nu_p(D) > 1$.

Let us now consider $p = 3$ and $\nu_3(D) = 1$. Then if $j \geqslant 2$,

$$\nu_3\left((p^{k-1}m)!/(p^{k-1}m - (2j+1))\right) \geqslant k,$$

so

$$u_n \equiv (A/2)^n\left[u_0 + (2u_1 - Au_0)\left(A^{-1}3^{k-1}m + \binom{n}{3}A^{-3}D\right)\right] \pmod{3^k}.$$

Again we induct on k. Since (u_n) and 3 satisfy (i)–(iv) and $\nu_3(D) = 1$, we have that $D \equiv 3 \pmod 9$, so $D/3 \equiv 1 \pmod 3$.

For $k = 1$, we have that $n = 3^{1-1}m = m$,

$$\begin{aligned} u_m &\equiv (A/2)^m\left[u_0 + (2u_1 - Au_0)(A^{-1}m + m(m-1)(m-2)A^{-3}(D/3)/2)\right] \\ &\equiv (A/2)^m\left[u_0 + (2u_1 - Au_0)(A^{-1}m)\right] \pmod 3, \end{aligned}$$

since $m(m-1)(m-2) \equiv 0 \pmod 3$. Since $(2u_1 - Au_0, 3) = 1$, there is certainly an m for which $u_m \equiv 0 \pmod 3$.

Thus by induction we may assume that there is an s for which $u_s \equiv 0 \pmod{3^{k-1}}$ and as before we may assume that $s = 0$ and $u_0 = 3^{k-1}v$. Thus

$$\begin{aligned} u_n 3^{-k+1} &\equiv (A/2)^n\left[v + (2u_1 - 3^{k-1}mA)(A^{-1}m + m(3^{k-1}m - 1)\right. \\ &\qquad \left.\cdot(3^{k-1}m - 2)A^{-3}(D/3)/2)\right] \pmod 3 \\ &\equiv (A/2)^n\left[v + 2u_1(A^{-1}m + m(-1)(-2)A^{-3}/2)\right] \\ &\equiv (A/2)^n\left[v + 2u_1A^{-1}m(1 + A^{-2})\right] \\ &\equiv (A/2)^n\left[v + u_1A^{-1}m\right] \pmod 3, \quad \text{since } A^2 \equiv 1 \pmod 3. \end{aligned}$$

Since $3 \mid u_0$ and $3 \nmid (2u_1 - Au_0)$, we have that $\nu_3(u_1 A^{-1}) = 0$ so there is an m for which $v + u_1 A^{-1} m \equiv 0 \pmod 3$ so the lemma is proven. □

REMARK. The reader will note that if $D/3 \equiv 2 \pmod 3$ then $1 + (D/3)A^{-2} \equiv 0 \pmod 3$ and the induction fails to go through.

COROLLARY 4. *Suppose that* (u_n) *and* p *satisfy* (i)–(iv). *Then if we are considering the sequence* (u_n) *modulo* p^k *we may assume that* $u_0 = 0$, $u_1 = 1$ *and* u_n *modulo* p^k *is given by the formulas*:

Case I. $u_n \equiv (A/2)^{n-1} n \pmod{p^k}$.

Case II. $u_n \equiv (A/2)^n (\binom{n}{1} + \binom{n}{3} A^{-2} D + \binom{n}{5} A^{-4} D^2 + \cdots) \pmod{p^k}$.

PROOF. From the previous lemmas we may assume that $u_0 \equiv 0 \pmod{p^k}$. Since $p \nmid 2u_1 - Au_0$ if p is odd, this implies that $p \nmid u_1$. Also if $p = 2$ then u_0, u_1 having opposite parity yields that $2 \nmid u_1$. Thus in all cases $p \nmid u_1$. If we multiply u_n by u_1^{-1} then $(u_1^{-1} u_n)$ satisfy (i)–(iv). □

Now that we have these preliminaries out of the way we can begin to obtain information about the periods of uniformly distributed sequences.

LEMMA 5. *Let the order of* $A/2$ *modulo* p *be* f. *If* (u_n) *is* UD(mod p^k) *its period is* $p^k f$.

PROOF. Without loss of generality we may assume that $u_0 = 0$ and $u_1 = 1$.

Case I. Since $u_n \equiv (A/2)^{n-1} n \pmod{p^k}$, we have that the order of $A/2$ modulo p^k is $p^j f$, where $j \leqslant k - 1$ and the period of n modulo p^k is p^k, so the assertion follows.

Case II. Then $u_n \equiv (A/2)^{n-1} B(n) \pmod{p^k}$, where $B(n) = \binom{n}{1} + \binom{n}{3} A^{-2} D + \binom{n}{5} A^{-4} D^2 + \cdots$, where of course the sum is finite.

For $k = 1$, the period of $(A/2)^{n-1}$ is f and the period of $B(n)$ is p, thus the period of u_n is pf.

For general k we have that the period of (u_n) modulo p^k is $p^k h$, for some h. As before $(A/2)$ has period fp^j, where $j \leqslant k - 1$, so $f \mid h$. It is also clear that $\binom{n}{2j+1} A^{-2j} D^j$ has period a divisor of p^k. Thus the period of $(A/2)^{n-1} B(n)$ divides $p^k f$, so the period is $p^k f$. □

The determination of f-UD(mod p^k) involves the analysis of $(A/2)^{n-1} B(n) \pmod{p^k}$. A useful technical result will be the following.

LEMMA 6. *Let* $n = m + p^{k-1} m_1$. *If either* (a) $p \geqslant 5$, (b) $\nu_p(D) > 1$, *or* (c) $p = 3$, $\nu_3(D) = 1$ *and* $j \geqslant 2$, *then*

$$\binom{n}{2j+1} A^{-2j} D^j \equiv \binom{m}{2j+1} A^{-2j} D^j \pmod{p^k}.$$

PROOF. If $\nu_p(D^j / A^{2j}(2j+1)!) > 0$ then the result follows, and this occurs if $p \geqslant 5$ or $\nu_p(D) > 1$ or $p = 3$, $\nu_p(D) = 1$ and $2j + 1$ is not a power of 3, by Lemma 1.

Thus, let us consider $p = 3$, $\nu_p(D) = 1$ and $2j + 1 = 3^r$. Then

$$\alpha = D^j A^{-2j} / (2j+1)!$$

is integral at 3. Set $\lambda = n(n-1)\cdots(n-2j)$. A factor of λ is of the form $n-i$, where $i \in \{0,1,\ldots,2j\}$. Thus write $\lambda = (n-i)\lambda_i$. Now

$$\lambda = \left(m - i + p^{k-1}m_1\right)\lambda_i$$

and $3 \mid \lambda_i$ since $2j \geqslant 8$ (recall $2j = 3^r$, $r \geqslant 2$), so λ is the product of at least 8 consecutive integers. Thus $\lambda \equiv (m-i)\lambda_i$ and the result follows. □

We can now prove the main result on f-UD(mod p^k).

THEOREM 7. *Let* (u_n) *and* p^k *satisfy conditions* (i)–(iv). *If* $A/2$ *has order* f *modulo* p, *then* (u_n) *is* f-UD(mod p^k).

PROOF. We want to show that for any s, u_s, $u_{s+f}, \ldots, u_{s+f(p^k-1)}$ are all distinct residues modulo p^k. Let us first prove the assertion for $k = 1$. If $p = 2$ the assertion is obvious.

In either Case I or II we have that $u_n \equiv (A/2)^{n-1}n \pmod p$. Thus for $n = s + af$, $a \in \{0,1,\ldots,p-1\}$ we have that

$$u_n \equiv (A/2)^{s-1}(A/2)^{af}(s+af) \equiv (A/2)^{s-1}(s+af) \pmod p,$$

since $(A/2)^f \equiv 1 \pmod p$. Since $f \mid p-1$, $s + af$ runs through the distinct residues modulo p as a runs through $\{0,1,\ldots,p-1\}$. Thus we have the result is true for $k = 1$ and now let us assume that the result is true for $k-1$.

For $k > 1$ and $a \in \{0,1,\ldots,p^k-1\}$ let us write a in the form $a = b + cp^{k-1}$, where $b \in \{0,1,\ldots,p^{k-1}-1\}$, $c \in \{0,1,\ldots,p-1\}$. Thus

$$\begin{aligned} u_{s+af} &\equiv (A/2)^{s-1}(A/2)^{bf}(A/2)^{cfp^{k-1}}B(s+af) \\ &\equiv (A/2)^{s-1}(A/2)^{bf}B(s+af) \pmod{p^k}. \end{aligned}$$

If we consider u_{s+af} modulo p^{k-1}, then $B(s+af) \equiv B(s+bf) \bmod(p^{k-1})$, so $u_{s+af} \equiv (A/2)^{s-1}(A/2)^{bf}B(s+bf) \pmod{p^{k-1}}$. Thus the induction hypothesis yields that as b ranges through the set $\{0,1,\ldots,p^{k-1}\}$, these are all distinct modulo p^{k-1}.

Thus let us now let b be fixed and let c range through the set $\{0,1,\ldots,p-1\}$. So we have $u_{s+af} \equiv (A/2)^{s-1}(A/2)^{bf}B(s+bf+cfp^{k-1}) \pmod{p^k}$. So these are all incongruent iff $B(s+bf+cfp^{k-1}) \pmod{p^k}$ are all incongruent.

By Lemma 6 we have that if $p \geqslant 5$ or $\nu_p(D) > 0$, then

$$B(s+af) \equiv \binom{s+bf+cfp^{k-1}}{1} + C(s,b) \pmod{p^k},$$

where $C(s,b)$ depends only on b and s and not on c. Thus $B(s+af)$ are clearly all incongruent as c ranges through the set $\{0,1,\ldots,p-1\}$.

If $p = 3$ and $\nu_3(D) = 1$, then

$$B(s+af) \equiv \binom{s+bf+c3^{k-1}}{1} + \binom{s+bf+c3^{k-1}}{3}A^{-2}D + C_1(s,b) \pmod{3^k},$$

where again $C_1(s,b)$ depends only on b and s and not on c. Set $B_1(s+af) \equiv B(s+af) - C_1(s,b)$, and we shall prove the assertion for $B_1(s+af)$.

If $k \geqslant 3$ then condition (iii) gives that $D \not\equiv 6 \pmod 9$. Since we are also assuming that $\nu_3(D) = 1$, this implies that $D \equiv 3 \pmod 9$, so $A^{-2}D/3 \equiv 1 \pmod 3$.

Let $c_1 = cf$, then since $(f, 3) = 1$, c_1 ranges over the residue system $\{0, 1, 2\}$ as c ranges over the same residue system. Set $m = s + bf$. Then

$$\begin{aligned} B_1(s + af) &\equiv m + c_1 3^{k-1} + \left(m + c_1 3^{k-1}\right)\left(m - 1 + c_1 3^{k-1}\right) \\ &\qquad \cdot\left(m - 2 + c_1 3^{k-1}\right) A^{-2}D/(2 \cdot 3) \\ &\equiv m + c_1 3^{k-1} + \left[m(m-1)(m-2) + c_1 3^{k-1}\right. \\ &\qquad \left.\cdot\left(m(m-1) + m(m-2) + (m-1)(m-2)\right)\right] A^{-2}D/(2 \cdot 3) \\ &\equiv m + c_1 3^{k-1} + \left[m(m-1)(m-2) + 2c_1 3^{k-1}\right] A^{-2}D/(2 \cdot 3) \\ &\equiv C_2(s, b) + c_1 3^{k-1} \pmod{3^k}, \end{aligned}$$

where $C_2(s, b)$ collects together all those terms which do not contain c_1.

Thus it is obvious that $B_1(s + af)$ are all distinct as c_1 runs through the residue system module 3. □

We have proved Theorem B and in so doing we have proven A for the case m a prime power. It has already been observed that if (u_n) is UD(mod p^k) for every p^k dividing m, p a prime, then (u_n) is UD(mod m). We shall not prove this result again (though at the end of this paper we shall make some remarks about a different proof), rather we shall assume the validity of A and characterize when (u_n) is f-UD(mod m).

Let $m = P_1 \cdots P_r$, where each P_i is a prime power, $(P_i, P_j) = 1$ if $i \neq j$. We shall assume that u_n is UD(mod P_i), with period $P_i f_i$, for each i (thus by Theorem B, (u_n) is f_i-UD(mod P_i)).

The period of (u_n) modulo m is the l.c.m.$\{P_1 f_1, \ldots, P_r f_r\}$, which we shall write as mf.

We shall need the following technical result to arrive at this characterization.

LEMMA 8. *Suppose that* (u_n) *is* f-UD(mod m), *then* $u_s, u_{s+hf}, u_{s+2hf}, \ldots, u_{s+(m-1)hf}$ *are all distinct modulo* m *iff* $(h, m) = 1$.

PROOF. If $(h, m) = 1$ then $0, h, \ldots, (m-1)h$ are all distinct modulo m. Given j, let $k(j)$ be the least residue between 0 and m congruent to jh modulo m. Thus $jhf \equiv k(j)f + l(j)mf$. However, (u_n) has period mf modulo m, so $u_{s+jhf} \equiv u_{s+k(j)f}$ (mod m) and since $u_s, u_{s+f}, \ldots, u_{s+(m-1)f}$ are all distinct modulo m the result follows.

Conversely, if $(h, m) \neq 1$, there exist $0 < i < j < m$ such that $ih \equiv jh \pmod m$, so $ihf = jhf + lmf$ and $u_{s+ihf} \equiv u_{s+jhf} \pmod m$. Thus $u_s, u_{s+hf}, \ldots, u_{s+(m-1)hf}$ are not all distinct modulo m. □

THEOREM 9. *Suppose that* $m = P_1 \cdots P_r$ *and that* (u_n) *is* f_i-UD(mod P_i), $i = 1, \ldots, r$. *Let* l.c.m.$\{P_1 f_1, P_2 f_2, \ldots, P_r f_r\} = mf$. *Then* (u_n) *is* f-UD(mod m) *iff* $(f, m) = 1$.

PROOF. Let p_i be the prime corresponding to P_i, that is, P_i equals p_i to some positive exponent. We shall number the P_i so that $p_1 < p_2 < \cdots < p_r$.

Assume that $(f, m) = 1$. We shall prove the theorem by inducting on r. For $r = 1$ this is Theorem B. Set $F = P_1$, $L = P_2 \cdots P_r$ and consider the matrix

$$A = \begin{bmatrix} u_s & u_{s+f} & \cdots & u_{s+(F-1)f} \\ u_{s+Ff} & u_{s+(F+1)f} & \cdots & u_{s+(2F-1)f} \\ \vdots & & & \\ u_{s+(L-1)Ff} & u_{s+((L-1)F+1)f} & \cdots & u_{s+(m-1)f} \end{bmatrix}.$$

Since $P_1 f_1 \mid P_1 \cdots P_r f$, we have that $f_1 \mid P_2 \cdots P_r f$. However, $f_1 \mid p_1 - 1$ since f_1 is the multiplicative order of $A/2$ modulo p_1 if p_1 is odd, otherwise $f_1 = 1$. Since $p_1 < p_2 < \cdots < p_r$, this implies that $(f_1, P_2 \cdots P_r) = 1$, so $f_1 \mid f$, and we write $f = h_1 f_1$. By assumption, $(f, P_1) = 1$, so $(h_1, P_1) = 1$ and from Lemma 8 we may conclude that each row of the matrix A represents all of the distinct residues modulo P_1 and in fact all of the rows of A are identical modulo P_1.

Now let us consider the columns of A modulo L. Set l.c.m.$\{P_2 f_2, \ldots, P_r f_r\} = Lf'$. From the hypothesis that $(m, f) = 1$, it follows easily that $(L, f') = 1$. Thus the induction hypothesis allows us to conclude that $u_s, u_{s+f'}, \ldots, u_{s+(L-1)f'}$ are all distinct modulo L. Obviously $Lf' \mid mf$, thus $f' \mid P_1 f$ and let us write $Ff = P_1 f = hf'$. Since $(f, m) = 1$, this implies that $(h, L) = 1$, thus we may apply Lemma 8 to conclude that each of the entries of any column of A are distinct modulo L.

The Chinese Remainder Theorem can now be invoked to conclude that $u_s, u_{s+f}, \ldots, u_{s+(m-1)f}$ are all distinct modulo m.

Now assume that $(m, f) \neq 1$. Then there exists a smallest v such that $(P_i, f) = 1$ for $i < v$ and $(P_v, f) \neq 1$. Set $L = P_v \cdots P_r$ and $F = m/L$, and consider the matrix A with these new values of F and L.

Just as in the preceding case it follows that each row of A represents all of the distinct residues modulo F and that all of the rows are identical modulo F.

Thus by the Chinese Remainder Theorem, all of the entries of the matrix are distinct modulo m iff all of the entries in any column (which are constant modulo F) are distinct modulo L. We shall show that the entries in the first column are not distinct modulo L.

From the first column of A construct a new matrix

$$B = \begin{bmatrix} u_s & u_{s+Ff} & \cdots & u_{s+(P_v-1)Ff} \\ u_{s+P_v Ff} & \cdots & & \\ \vdots & & & \\ u_{s+(P_{v+1}\cdots P_r-1)P_v Ff} & \cdots & & u_{s+(L-1)Ff} \end{bmatrix}.$$

Now $P_v f_v \mid FLf$, so $f_v \mid FP_{v+1} \cdots P_r f$. Further, since $f_v \mid p_v - 1$ and $p_v < p_{v+1} < \cdots < p_r$, we have that $(f_v, P_{v+1} \cdots P_r) = 1$, so $f_v \mid Ff$, thus the rows are identical modulo P_v. Set $Ff = hf_v$. By assumption $p_v \mid f$ and since $(p_v, f_v) = 1$, we must have that $p_v \mid h$. However, we can now apply Lemma 8 to conclude that the rows of B are not all distinct modulo P_v, which in turn implies that the entries of B are not all distinct modulo L. □

As we pointed out it has been proved that if (u_n) is UD(mod P_i), $i = 1, \ldots, r$, then (u_n) is UD(mod m), where $m = P_1 \cdots P_r$. The proof of Theorem 9 did not need this result and in fact we can use Theorem 9 to prove this result on UD(mod m). We shall not give a complete proof but rather just indicate how Theorem 9 can be used.

Suppose that (u_n) is UD(mod P_i), then by Theorem B, (u_n) is f_i-UD(mod P_i), where $f_i \mid p_i - 1$. Let $mf = \text{l.c.m.}\{P_1 f_1, \ldots, P_r f_r\}$. If $(f, m) = 1$, then by Theorem 9, (u_n) is f-UD(mod m) and thus (u_n) is UD(mod m).

If $(f, m) \neq 1$ then there are technical complications. However, if we assume that $P_i \neq 2$ or 3 for all i, then we can apply Theorem 9 quite easily as the following argument shows.

If $P_i \neq 2$ or 3 and (u_n) is f_i-UD(mod P_i) then by Theorem A, (u_n) is f_i-UD(mod P_i^e), for all e.

Thus since $(m, f) \neq 1$, let e be a sufficiently large integer so that $\text{l.c.m.}\{P_1^e f_1, \ldots, P_r^e f_r\} = P_1^e \cdots P_r^e f' = m^e f'$, where $(f', m) = 1$. Thus by Theorem 9, (u_n) is f'-UD(mod m^e), so (u_n) is UD(mod m^e) and it then follows that (u_n) is UD(mod m).

If $P_i = 2$ or 3 for some i then we cannot use the above argument since it is possible that (u_n) is UD modulo 2 or 3, yet (u_n) is not UD modulo 2^2 or 3^2, respectively.

Thus, if $P_i = 2$ or 3 then we would set $F = P_1$, $L = P_2 \cdots P_r$ if exactly *one* of the P_i is 2 or 3 and we would set $F = P_1 P_2$, $L = P_3 \cdots P_r$ if $P_1 = 2$, $P_2 = 3$.

If $(f, L) \neq 1$ then we can replace L by L^e for e sufficiently large (just as in the preceding argument) so that $\text{l.c.m.}\{F, L^e, f_i, i = 1, \ldots, r\} = FL^e f'$, where $(f', L) = 1$. Thus if (u_n) is UD(mod FL^e), then (u_n) is UD(mod FL). So we can assume that $(f, L) = 1$, yet $(f, F) \neq 1$; thus there are three possibilities (i) $2 \mid f$, $3 \mid f$, (ii) $2 \mid f$, $3 \nmid f$, (iii) $2 \nmid f$, $3 \mid f$. All of these cases entail the same kind of analysis which we will not discuss further.

References

1. Lee Erlebach and William Yslas Vélez, *Equiprobability in the Fibonacci sequence*, Fibonacci Quart. **21** (1983), 189–191.

2. Władysław Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Math., vol. 1087, Springer-Verlag, New York, 1984.

Department of Mathematics, University of Arizona, Tucson, Arizona 85721