References

[1] S. K. Aggarwal, *Transference theorems in the field of formal power series*, Monatsh. Math. 72 (1968), pp. 97–106.

[2] B. J. Birch, *A transference theorem in the geometry of numbers*, J. London Math. Soc. 31 (1956), pp. 248–251.

[3] J. W. S. Cassels, *An introduction to diophantine approximation*, Camb. Tracts 45, Cambridge University Press, 1957.

[4] I. S. Luthar and Meenakshi Duggal, *Minkowski's theorems in completions of A-fields non-zero characteristic*, to appear in Coll. Math.

[5] — — *A theorem of Mahler and some applications to transference theorems*, to appear in Coll. Math.

[6] K. Mahler, *Ein Übertragungsprinzip für lineare Ungleichungen*, Časopis Pest. Mat. 68 (1939), pp. 85–92.

[7] André Weil, *Basic number theory*, Springer-Verlag, New York 1967.

DEPARTMENT OF MATHEMATICS
PENJAB UNIVERSITY
Chandigarh, India

Received on 23. 3. 1976
and in revised form on 21. 5. 1977 (831)

ACTA ARITHMETICA
XXXVI (1980)

Uniform distribution of third order linear recurrence sequences

by

MELVIN J. KNIGHT and WILLIAM A. WEBB (Pullman, Wash.)

1. Introduction. Let $\{u_n\}$ be defined by

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \ldots + a_w u_{n-w} \quad \text{for} \quad n \geqslant w \tag{1}$$

and $u_0, u_1, \ldots, u_{w-1}$ given, where $u_0, u_1, \ldots, u_{w-1}, a_1, a_2, \ldots, a_w$ are all integers and $a_w \neq 0$. This is called a *linear recurrence* of order w.

A sequence is said to be *uniformly distributed modulo* m, written u.d. mod m, provided each residue modulo m appears with an asymptotic density of $1/m$.

Uniform distribution of recurrence sequences was first considered in the special case of the Fibonacci numbers. Kuipers and Shiue [2] showed that 5 is the only prime for which the Fibonacci numbers are uniformly distributed, and Niederreiter [6] showed that they are uniformly distributed mod 5^h for $h \geqslant 1$. Kuipers and Shiue [3] obtained sufficient conditions for a general second order recurrence to be uniformly distributed mod p^k. This question was completely settled when both necessary and sufficient conditions were obtained independently by Bumby [1], Nathanson [5], Long and Webb [7].

In this paper we consider uniform distribution of higher order sequences. The principal result, Theorem 3, gives necessary and sufficient conditions for a third order recurrence sequence $\{u_n\}$ to be uniformly distributed modulo M, where M is divisible only by primes $p > 5$.

2. General results on uniform distribution. The sequence $\{u_n\}$ is periodic modulo m for every m and is purely periodic mod m provided $(m, a_w) = 1$. It follows that $\{u_n\}$ is u.d. mod m if and only if each residue modulo m appears equally often in every period modulo m. Notice that in this paper, a period will not necessarily mean a least period.

The recurrence given in (1) has corresponding characteristic polynomial

$$\varphi(x) = x^w - a_1 x^{w-1} - a_2 x^{w-2} - \ldots - a_w$$

and discriminant

$$D = \prod_{i<j}(\alpha_i - \alpha_j)^2 \tag{2}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_w$ are the (not necessarily distinct) roots of $c(x)$ over the rationals Q.

The discriminant D can be defined in terms of the coefficients of $c(x)$ and thus is the same when $c(x)$ is considered over other fields. In particular, $c(x)$ factors completely in some finite extension of the finite field GF(p) and the roots of $c(x)$ over GF(p) are distinct if and only if $p \nmid D$.

THEOREM 1. *If $p \nmid D$, then $\{u_n\}$ is not u.d. mod p.*

Proof. Let $p \nmid D$, then the roots $r_1, r_2, \ldots, r_w$ of $c(x)$ over GF(p) are distinct and thus

$$u_n = c_1 r_1^n + c_2 r_2^n + \ldots + c_w r_w^n \quad \text{for } n \geqslant 0$$

for some constants $c_1, c_2, \ldots, c_w$ in GF(p^f). Since the non-zero elements of GF(p^f) form a cyclic group of order p^f-1, each non-zero root r of $c(x)$ satisfies $r^{p^f-1} = 1$. Therefore, $\{u_n\}$ has a period mod p of length p^f-1.

If $\{u_n\}$ were u.d. mod p, every period would have a length a multiple of p, which contradicts $\{u_n\}$ having a period of length p^f-1.

3. Linear recurrences of order three. Assume now that $\{u_n\}$ is third order with characteristic polynomial

$$c(x) = x^3 - a_1 x^2 - a_2 x - a_3.$$

Let $a = -(a_1^2+3a_2)/3$, $b = -(2a_1^3+9a_1a_2+27a_3)/27$, then the discriminant (2) of $c(x)$ is

$$D = -27b^2 - 4a^3.$$

Let p be a prime greater than 3 such that $p|D$. The polynomial $c(x)$ has two equal roots over the field GF(p) and since it is a cubic, it must have all three roots in GF(p).

It follows that $c(x) = (x-r_1)^2(x-r_2)$ where $r_1, r_2 \in \mathrm{GF}(p)$ and possibly $r_1 = r_2$. Furthermore, since $c(r_1) = c'(r_1) = 0$, we have $r_1 = (a_1 - 9b/2a)/3$ and $r_2 = (a_1 + 9b/a)/3$ provided $p \nmid a$. If $p|a$, then since $p|D$, we also have $p|b$. Thus $c(x+a_1/3) = x^3 + ax + b \equiv x^3 \pmod p$ and it follows that $r_1 = r_2 = a_1/3$ in this case. We will use r_1 and r_2 to denote the roots of $c(x)$ over GF(p) throughout the paper.

THEOREM 2. *Let p be a prime greater than 3. The sequence $\{u_n\}$ is u.d. mod p if and only if $p|D$ and one of the following holds:*

(i) $p \nmid a$ *and* $p \nmid r_1[u_0r_1r_2 - u_1(r_1+r_2) + u_2]$,

(ii) $p|a$, $p|[u_0r_1^2 - 2u_1r_1 + u_2]$, $p \nmid r_1[3r_1^2u_0 - 4r_1u_1 + u_2]$,

(iii) $p|a$, $p \nmid r_1[u_0r_1^2 - 2u_1r_1 + u_2]$,

$$p \left| \left\{ \begin{vmatrix} 1 & u_0 & 0 \\ r_1 & u_1 & r_1 \\ r_1^2 & u_2 & 4r_1^2 \end{vmatrix}^2 - 4u_0 \begin{vmatrix} 1 & 0 & u_0 \\ r_1 & r_1 & u_1 \\ r_1^2 & 2r_1^2 & u_2 \end{vmatrix} \right\}$$

and $\left(\frac{r_1}{p}\right) = -1$, *where* $\left(\frac{r_1}{p}\right)$ *is the Legendre symbol.*

Furthermore, the sequence has a period mod p of length $p(p-1)$. And for primes satisfying (i) *or* (ii) *and for each fixed value of d, the subsequence $\{u_{(p-1)k+d}\}$ is a nontrivial arithmetic progression mod p.*

Proof. Suppose $\{u_n\}$ is u.d. mod p, then by Theorem 1, $p|D$ and

$$c(x) \equiv (x-r_1)^2(x-r_2) \bmod p.$$

Case 1: $r_1 \neq r_2$. As was mentioned earlier, $r_1 \neq r_2$ if and only if $p \nmid a$. Since $c(x)$ has one repeated root over GF(p) it follows that in GF(p)

$$u_n = (b_1 + b_2 n) r_1^n + b_3 r_2^n$$

where b_1, b_2, b_3 are constants in GF(p). We claim this is u.d. mod p if and only if $r_1 b_2 \not\equiv 0 \bmod p$, which will give (i).

If $r_1 b_2 \equiv 0 \bmod p$, then $\{u_n\}$ has period of length $p-1$ and could not be u.d. mod p.

Therefore, assume $r_1 b_2 \not\equiv 0 \pmod p$, then $\{u_n\}$ has a period of length $p(p-1)$. Write $n = d + (p-1)k$, with $1 \leqslant d \leqslant p-1$. For each fixed value of d,

$$u_n = [b_1 + b_2 d + b_2(p-1)k] r_1^d + b_3 r_2^d$$

forms a nontrivial arithmetic progression mod p and thus $\{u_n\}$ is u.d. mod p.

Case 2: $r_1 = r_2$. In this case $p|a$ and the sequence mod p satisfies

$$u_n = (\beta_1 + \beta_2 n + \beta_3 n^2) r_1^n$$

for constants $\beta_1, \beta_2, \beta_3$ in GF(p).

Since $\{u_n\}$ is u.d. mod p, $r_1 \not\equiv 0 \bmod p$. Clearly $p(p-1)$ is a period.

Suppose first that $\beta_3 \equiv 0 \bmod p$, then as in Case 1 the sequence $\{u_n\}$ is u.d. mod p if and only if $\beta_2 \not\equiv 0 \bmod p$. Solving for β_2 and β_3 gives (ii).

Now suppose $\beta_3 \not\equiv 0 \bmod p$. Since $\{u_n\}$ is u.d. mod p, 0 must appear

in the sequence and thus the quadratic

$$\beta_1+\beta_2 n+\beta_3 n^2$$

must factor mod p. Since this quadratic has period p mod p, the residue 0 will appear too often in each period unless the quadratic is actually a perfect square. Therefore, we have $p|a$, $p\nmid r\beta_3$, and $\beta_1+\beta_2 n+\beta_3 n^2$ is a perfect square mod p and these are the respective conditions given in (iii).

If $(r_1/p)=+1$, only square residues would appear in $\{u_n\}$, so $(r_1/p)=-1$. An easy count shows that if $(r_1/p)=-1$, then $\{u_n\}$ is u.d. mod p.

For a fixed sequence $\{u_n\}$, we will refer to those primes of Theorem 2 satisfying (i), (ii), or (iii) as type I, type II, or type III, respectively.

THEOREM 3. *Let M be divisible only by primes greater than 5. The sequence $\{u_n\}$ is u.d.* mod M *if and only if $M=M_0$ or $M_0 q$, where M_0 is divisible only by powers of primes of type* I *or type* II *and q is any type* III *prime.*

The remainder of the paper is devoted to the proof of Theorem 3.

Note that Theorem 2 fails to hold for the primes 2 and 3, while the prime 5 is excluded from Theorem 3 because of our use of Lemmas 2 and 4 below. Because a complete discussion of these primes appears to require many cases, this has been postponed to a later paper.

4. Preliminary lemmas and notation. Let M be the modulus. We may assume the sequence $\{u_n\}$ is purely periodic mod M by possibly deleting a finite number of initial terms. Also, by altering the coefficients of $c(x)$ by multiples of M, the roots of $c(x)$ over Q may be assumed distinct, and so $D\neq 0$. Neither of these assumptions has any effect on uniform distribution mod M.

Let

$$K=Q(\alpha_1,\alpha_2,\alpha_3),$$

where $\alpha_1,\alpha_2,\alpha_3$ are the roots of $c(x)$. The field K might be of the first, second, third, or sixth degree over Q. Let Ω_K denote the integers of K and let

$$(p)=(\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g)^e$$

be the factorization of (p) into prime ideals of Ω_K.

If $\mathfrak{p}$ is any of the primes dividing p above, then

$$\Omega_K/\mathfrak{p}\cong \mathrm{GF}(p^f)$$

for some integer f and $efg=[K:Q]$. However, since $p|D$, the roots of $c(x)$ over $\mathrm{GF}(p)$ lie in $\mathrm{GF}(p)$. Therefore,

$$Z[\alpha_1,\alpha_2,\alpha_3]/\mathfrak{p}\cong \mathrm{GF}(p).$$

We will be considering the sequence $\{u_n\}$ as elements in $Z[\alpha_1,\alpha_2,\alpha_3]$ and study it modulo powers of $\mathfrak{p}$ instead of powers of p. The following lemma gives the relationship between these two approaches.

LEMMA 1. *For elements $a,b\in Z$, the congruences*

$$a\equiv b \bmod p^h \quad \textit{and} \quad a\equiv b \bmod \mathfrak{p}^{e(h-1)+1}$$

are equivalent.

Proof. If $a-b\in p^h$, then certainly $a-b\in\mathfrak{p}^{eh}$, which is stronger than stated result.

Conversely, every element of Z is contained in a power of $\mathfrak{p}^e$, because of the factorization of p. Therefore, if $a-b\in\mathfrak{p}^{e(h-1)+1}$, then $a-b\in\mathfrak{p}^{eh}$ and thus $a-b\in p^h$.

LEMMA 2. *If $p\geqslant 1+e$, $\alpha\in Z[\alpha_1,\alpha_2,\alpha_3]$, $\alpha\notin\mathfrak{p}$, then*

$$\alpha^{\varphi(p^h)}\equiv 1 \bmod \mathfrak{p}^{e(h-1)+1}.$$

Proof. Since $\alpha\in Z[\alpha_1,\alpha_2,\alpha_3]$, $\alpha\notin\mathfrak{p}$, there is an integer, a, prime to p, such that $\alpha-a\in\mathfrak{p}$.

The proof is by induction on h. For $h=1$,

$$\alpha^{p-1}\equiv a^{p-1}\equiv 1 \bmod \mathfrak{p}.$$

Let $\alpha^{\varphi(p^h)}=\beta+1$, where $\beta\in\mathfrak{p}^{e(h-1)+1}$, then

$$\alpha^{\varphi(p^{h+1})}=(\beta+1)^p=\beta^p+p\beta\delta+1\equiv 1 \bmod \mathfrak{p}^{eh+1}$$

provided $\beta^p\in\mathfrak{p}^{eh+1}$. This holds for $p\geqslant 1+e$.

Let $\mathrm{ord}_{\mathfrak{p}}(\beta)$ denote the highest power of $\mathfrak{p}$ containing β.

LEMMA 3. *If $e=6$, then $r_1=r_2$ and $\mathrm{ord}_{\mathfrak{p}}(\alpha_i-\alpha_j)\geqslant 2$ for each $i\neq j$.*

Proof. Since $e=6$, $[K:Q]=6$ and $\mathfrak{p}$ is the only prime of K dividing p.

Suppose $r_1\neq r_2$, then for some numbering of the roots $\alpha_1,\alpha_2,\alpha_3$, we have $\alpha_3-\alpha_2\in\mathfrak{p}$ and $(\alpha_3-\alpha_1)(\alpha_2-\alpha_1)\notin\mathfrak{p}$. However, the Galois group $G(K/Q)$ contains an automorphism σ which cyclically permutes the roots $\alpha_1\to\alpha_2\to\alpha_3$. Since $\mathfrak{p}$ is the only prime in K above p, $\sigma\mathfrak{p}=\mathfrak{p}$. Therefore, $\sigma(\alpha_3-\alpha_2)=\alpha_1-\alpha_3\in\mathfrak{p}$. This contradiction shows that $r_1=r_2$.

Suppose the roots of $c(x)$ are numbered so that

$$\mathrm{ord}_{\mathfrak{p}}(\alpha_3-\alpha_2)\geqslant\mathrm{ord}_{\mathfrak{p}}(\alpha_2-\alpha_1)\geqslant\mathrm{ord}_{\mathfrak{p}}(\alpha_1-\alpha_3),$$

then using σ again shows that these must all be equal.

Let $t=\mathrm{ord}_{\mathfrak{p}}(\alpha_3-\alpha_2)$, $L=Q(\alpha_1)$, $\mathfrak{P}=\mathfrak{p}\cap L$. Since $e(\mathfrak{p}/p)=6$, then $e(\mathfrak{P}/p)=[L:Q]=3$. Since

$$\mathfrak{D}_{L/Q}(\alpha_1)=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\in\mathfrak{P}^2$$

([4], p. 62) and $\mathfrak{P}\subseteq\mathfrak{p}^2$, it follows that

$$2t=\mathrm{ord}(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\geqslant 4.$$

Therefore, $t\geqslant 2$ and $(\alpha_i-\alpha_j)\in\mathfrak{p}^2$ for each $i\neq j$.

LEMMA 4. *Let p be a prime and $n \equiv m \bmod p^{h-1}$ for any $h \geqslant 2$. If $\Delta(j)$ is any number satisfying either*

(i) $e \leqslant 3$ *and* $\Delta(j) \in \mathfrak{p}^j$

or

(ii) $e \leqslant 6$ *and* $\Delta(j) \in \mathfrak{p}^{2j}$,

then

$$\left[\binom{n}{k} - \binom{m}{k}\right]\Delta(j) \in \mathfrak{p}^{e(h-1)+1}$$

for all $j > 0$ and $k < p$; and for all $j > 0$ and $k \leqslant j(p-1)/3$.

Proof. Since $n \equiv m \bmod p^{h-1}$,

$$\operatorname{ord}_p\left[\binom{n}{k} - \binom{m}{k}\right] \geqslant (h-1) - \operatorname{ord}_p k!.$$

If $k < p$, $\operatorname{ord}_p k! = 0$ and with $\Delta(j) \in \mathfrak{p}^j$

$$\operatorname{ord}_p\left[\binom{n}{k} - \binom{m}{k}\right]\Delta(j) \geqslant e(h-1)+j \geqslant e(h-1)+1$$

for $j > 0$.

Now, for all k

$$\operatorname{ord}_p k! = \sum_{i \geqslant 1}\left[\frac{k}{p^i}\right] < \frac{k}{p-1}.$$

Hence, if $\operatorname{ord}_p \Delta(j) \geqslant tj$,

$$\operatorname{ord}_p\left[\binom{n}{k} - \binom{m}{k}\right]\Delta(j) > e(h-1) - \frac{ek}{p-1} + jt \geqslant e(h-1)$$

by either (i) or (ii).

The following property is fundamental for the uniform distribution of these sequences. Given a prime p and integer $h \geqslant 0$, let $\Phi(p^h) = p^h(p-1)$. The prime p satisfies *property h* for the sequence $\{u_n\}$ provided:

(i) $\{u_n\}$ has a period of length $\Phi(p^{h-1}) \bmod p^{h-1}$,

(ii) if $n \equiv m \bmod \Phi(p^{h-1})$ and $u_n \equiv u_m \bmod p^h$, then $n \equiv m \bmod \Phi(p^h)$.

Every prime is said to satisfy property 0.

Theorem 2 shows that type I and type II primes satisfy property 1, whereas from the proof of Theorem 2 it can be seen that type III primes do not satisfy property 1.

LEMMA 5. *Let p satisfy property h for $0 \leqslant h \leqslant H$, then $\{u_n\}$ is u.d. mod p^h with period $\Phi(p^h)$ for all such h.*

Proof. The proof is by induction on h. The result is trivially true for $h = 0$.

Now assume $\{u_n\}$ is u.d. mod p^{h-1} and has a period of length $(p-1)p^{h-1}$. Thus, in any period of this length, each residue appears exactly $p-1$ times.

Given an integer g, let $n_i(g)$, $i = 1, 2, \ldots, p-1$ be those $p-1$ values of $n \bmod (p-1)p^{h-1}$ for which $u_n \equiv g \bmod p^{h-1}$.

Fix k and let $n, m \in [k,\ k+(p-1)p^h-1]$ and $u_n \equiv u_m \equiv g \bmod p^h$. Then $n \equiv n_i$ and $m \equiv n_j \bmod (p-1)p^{h-1}$, for some values of i, j. But if $i = j$, then $n \equiv m \bmod (p-1)p^{h-1}$ and by condition (ii) $n \equiv m \bmod (p-1)p^h$, which implies $n = m$.

Hence there is at most one n for which $u_n \equiv g \bmod p^h$ and $n \equiv n_i \bmod (p-1)p^{h-1}$, and so at most $p-1$ values of n for which $u_n \equiv g \bmod p^h$. Since this is true for each g, it follows that there are exactly $p-1$ such n for each g and each residue appears equally often. Thus, $\{u_n\}$ is u.d. mod p^h and has period $(p-1)p^h$.

LEMMA 6. *If $p > 5$ satisfies property 1, then it satisfies property h for all $h \geqslant 1$.*

Lemma 6 is the principal tool needed to prove Theorem 3. The next two sections are devoted to the proofs of these two results.

5. Proof of Lemma 6. The case when $h = 1$ is trivial, so we will now complete the proof by induction on h. Since $c(x)$ has distinct roots, the sequence $\{u_n\}$ has general term $u_n = c_1\alpha_1^n + c_2\alpha_2^n + c_3\alpha_3^n$, where c_1, c_2, c_3 are uniquely determined by

$$\begin{aligned} c_1 + c_2 + c_3 &= u_0, \\ \alpha_1 c_1 + \alpha_2 c_2 + \alpha_3 c_3 &= u_1, \\ \alpha_1^2 c_1 + \alpha_2^2 c_2 + \alpha_3^2 c_3 &= u_2. \end{aligned}$$

Let $\sqrt{D} = (\alpha_3 - \alpha_2)(\alpha_3 - \alpha_1)(\alpha_2 - \alpha_1)$. Then we can solve for the c_i and rewrite u_n in the form $u_n = u_0C_0(n) - u_1C_1(n) + u_2C_2(n)$, where

$$\begin{aligned} \sqrt{D}C_0(n) &= (\alpha_2\alpha_3^2 - \alpha_2^2\alpha_3)\alpha_1^n + (\alpha_1^2\alpha_3 - \alpha_1\alpha_3^2)\alpha_2^n + (\alpha_1\alpha_2^2 - \alpha_1^2\alpha_2)\alpha_3^n, \\ \sqrt{D}C_1(n) &= (\alpha_3^2 - \alpha_2^2)\alpha_1^n + (\alpha_1^2 - \alpha_3^2)\alpha_2^n + (\alpha_2^2 - \alpha_1^2)\alpha_3^n, \\ \sqrt{D}C_2(n) &= (\alpha_3 - \alpha_2)\alpha_1^n + (\alpha_1 - \alpha_3)\alpha_2^n + (\alpha_2 - \alpha_1)\alpha_3^n. \end{aligned}$$

By the induction hypothesis, p satisfies properties 1 through $h-1$. Therefore, by Lemma 5, $\{u_n\}$ is u.d. mod p^{h-1} with period $\Phi(p^{h-1})$. This implies part (i) of the definition of property h. Also, $c(x)$ has a repeated root mod p, and two cases arise depending on whether $r_1 \neq r_2$ or $r_1 = r_2$.

Case I. Suppose exactly two of the roots are congruent mod p, then we have $\alpha_1-\alpha_2\in\mathfrak{p}$ for some prime $\mathfrak{p}|p$ and we will write $\alpha_1=\alpha$, $\alpha_2=\alpha+\delta$, $\alpha_3=\beta$, where $\delta\in\mathfrak{p}$, $\alpha-\beta\notin\mathfrak{p}$, and $\alpha\notin\mathfrak{p}$, since $r_1\not\equiv 0 \bmod p$. Therefore, $\sqrt{D}=(\beta-\alpha-\delta)(\beta-\alpha)\delta$ and

$$\begin{aligned}\sqrt{D}C_0(n) &= (\alpha+\delta)\beta(\beta-\alpha-\delta)\alpha^n-\alpha\beta(\beta-\alpha)(\alpha+\delta)^n+\alpha(\alpha+\delta)\delta\beta^n\\ &= \alpha\beta(\beta-\alpha)\alpha^n-\alpha\beta\delta\alpha^n+\delta\beta(\beta-\alpha-\delta)\alpha^n+\alpha(\alpha+\delta)\delta\beta^n-\\ &\qquad -\alpha\beta(\beta-\alpha)\sum_{j\geqslant 0}\binom{n}{j}\alpha^{n-j}\delta^j,\end{aligned}$$

from expanding $(\alpha+\delta)^n$. This simplifies to

$$\sqrt{D}C_0(n)=\delta\beta(\beta-2\alpha-\delta)\alpha^n+\delta\alpha(\alpha+\delta)\beta^n-\alpha\beta(\beta-\alpha)\sum_{j\geqslant 1}\binom{n}{j}\alpha^{n-j}\delta^j.$$

Similarly,

$$\sqrt{D}C_1(n)=(\beta^n-\alpha^n)(2\alpha\delta+\delta^2)-(\beta^2-\alpha^2)\sum_{j\geqslant 1}\binom{n}{j}\alpha^{n-j}\delta^j,$$

$$\sqrt{D}C_2(n)=\delta(\beta^n-\alpha^n)-(\beta-\alpha)\sum_{j\geqslant 1}\binom{n}{j}\alpha^{n-j}\delta^j.$$

To show that p satisfies part (ii) of the definition of property h, let $n\equiv m \bmod (p-1)p^{h-1}$ and $u_n\equiv u_m \bmod p^h$. By Lemma 1, $u_n\equiv u_m \bmod \mathfrak{p}^{e(h-1)+1}$, therefore noting that $\delta^{-1}\sqrt{D}=(\beta-\alpha)(\beta-\alpha-\delta)\notin\mathfrak{p}$ and using Lemma 2 to replace α^m by α^n, we have the following congruences, all modulo $\mathfrak{p}^{e(h-1)+1}$,

$$\begin{aligned}u_n-u_m\equiv 0 \equiv u_0\alpha\beta(\alpha-\beta)&\sum_{j\geqslant 1}\left[\binom{n}{j}-\binom{m}{j}\right]\alpha^{n-j}\delta^{j-1}-\\ -u_1(\alpha^2-\beta^2)&\sum_{j\geqslant 1}\left[\binom{n}{j}-\binom{m}{j}\right]\alpha^{n-j}\delta^{j-1}+\\ +u_2(\alpha-\beta)&\sum_{j\geqslant 1}\left[\binom{n}{j}-\binom{m}{j}\right]\alpha^{n-j}\delta^{j-1}.\end{aligned}$$

Lemma 3 shows that $e\leqslant 3$ and then Lemma 4 shows that all terms in the above sums for $j\geqslant 2$ are in $\mathfrak{p}^{e(h-1)+1}$, so

$$\begin{aligned}0\equiv u_0\alpha\beta(\alpha-\beta)&\left[\binom{n}{1}-\binom{m}{1}\right]\alpha^{n-1}-u_1(\alpha^2-\beta^2)\left[\binom{n}{1}-\binom{m}{1}\right]\alpha^{n-1}+\\ &+u_2(\alpha-\beta)\left[\binom{n}{1}-\binom{m}{1}\right]\alpha^{n-1}\\ \equiv (n-m)(\alpha-\beta)\alpha^{n-1}&[u_0\alpha\beta-u_1(\alpha+\beta)+u_2].\end{aligned}$$

However, $\{u_n\}$ satisfies (i) of Theorem 2, since it is u.d. mod p and $r_1\neq r_2$, so $u_0\alpha\beta-u_1(\alpha+\beta)+u_2\notin\mathfrak{p}$. It follows that $n-m\in\mathfrak{p}^{e(h-1)+1}$ and thus $n\equiv m \bmod p^h$ by Lemma 1. Hence p satisfies property h.

Case II. Suppose all three roots are congruent mod p. We note that this condition and the fact that p satisfies property 1 implies p is of type II. We may assume without loss of generality that

$$\operatorname{ord}_{\mathfrak{p}}(\alpha_2-\alpha_1)\leqslant\operatorname{ord}_{\mathfrak{p}}(\alpha_3-\alpha_1)\leqslant\operatorname{ord}_{\mathfrak{p}}(\alpha_3-\alpha_2).$$

Suppose $\operatorname{ord}_{\mathfrak{p}}(\alpha_2-\alpha_1)<\operatorname{ord}_{\mathfrak{p}}(\alpha_3-\alpha_1)$, then since $\alpha_3-\alpha_2=(\alpha_3-\alpha_1)-(\alpha_2-\alpha_1)$, $\operatorname{ord}_{\mathfrak{p}}(\alpha_3-\alpha_2)=\operatorname{ord}_{\mathfrak{p}}(\alpha_2-\alpha_1)<\operatorname{ord}_{\mathfrak{p}}(\alpha_3-\alpha_1)$. This contradiction shows that if we write $\alpha_1=\alpha$, $\alpha_2=\alpha+\delta_2$, $\alpha_3=\alpha+\delta_3$, then $\operatorname{ord}_{\mathfrak{p}}\delta_2=\operatorname{ord}_{\mathfrak{p}}\delta_3\geqslant 1$.

We have $\sqrt{D}=(\delta_3-\delta_2)\delta_3\delta_2$ and

$$\begin{aligned}\sqrt{D}C_1(n) &= (\delta_3-\delta_2)(2\alpha+\delta_2+\delta_3)\alpha^n-(2\alpha+\delta_3)\delta_3(\alpha+\delta_2)^n+\\ &\qquad +(2\alpha+\delta_2)\delta_2(\alpha+\delta_3)^n\\ &= (\delta_3-\delta_2)(2\alpha+\delta_2+\delta_3)\alpha^n-(2\alpha+\delta_3)\delta_3\sum_{j\geqslant 0}\binom{n}{j}\alpha^{n-j}\delta_2^j+\\ &\qquad +(2\alpha+\delta_2)\delta_2\sum_{j\geqslant 0}\binom{n}{j}\alpha^{n-j}\delta_3^j\\ &= -(2\alpha+\delta_3)\delta_3\sum_{j\geqslant 1}\binom{n}{j}\alpha^{n-j}\delta_2^j+(2\alpha+\delta_2)\delta_2\sum_{j\geqslant 1}\binom{n}{j}\alpha^{n-j}\delta_3^j\\ &= -(2\alpha+\delta_3)\delta_3\binom{n}{1}\alpha^{n-1}\delta_2+(2\alpha+\delta_2)\delta_2\binom{n}{1}\alpha^{n-1}\delta_3+\\ &\qquad +\sum_{j\geqslant 2}\binom{n}{j}\alpha^{n-j}[2\alpha\delta_2\delta_3(\delta_3^{j-1}-\delta_2^{j-1})+\delta_2^2\delta_3^2(\delta_3^{j-2}-\delta_2^{j-2})]\\ &= -n\alpha^{n-1}\delta_2\delta_3(\delta_3-\delta_2)+\sum_{j\geqslant 2}\binom{n}{j}\alpha^{n-j}[2\alpha\delta_2\delta_3(\delta_3^{j-1}-\delta_2^{j-1})+\\ &\qquad +\delta_2^2\delta_3^2(\delta_3^{j-2}-\delta_2^{j-2})].\end{aligned}$$

Write $\Delta(j-1)$ for $(\delta_3^j-\delta_2^j)/(\delta_3-\delta_2)$, then

$$C_1(n)=-n\alpha^{n-1}+\sum_{j\geqslant 2}\binom{n}{j}\alpha^{n-j}[2\alpha\Delta(j-2)+\delta_2\delta_3\Delta(j-3)].$$

Similar calculations give

$$C_2(n)=\sum_{j\geqslant 2}\binom{n}{j}\alpha^{n-j}\Delta(j-2)$$

and

$$C_0(n)=\alpha(\alpha+\delta_2)(\alpha+\delta_3)\sum_{j\geqslant 2}\binom{n-1}{j}\alpha^{n-1-j}\Delta(j-2).$$

As in Case I, we use these expressions to show that p satisfies (ii) of the definition of property h.

Suppose $n \equiv m \bmod \Phi(p^{h-1})$ and $u_n \equiv u_m \bmod p^h$. We then have the following congruences mod $\mathfrak{p}^{e(h-1)+1}$.

$$u_n - u_m \equiv 0 \equiv u_0\alpha(\alpha+\delta_2)(\alpha+\delta_3)\sum_{j\geqslant 2}\left[\binom{n-1}{j}-\binom{m-1}{j}\right]\alpha^{n-1-j}\Delta(j-2)-$$

$$-u_1\left\{-(n-m)\alpha^{n-1}+\sum_{j\geqslant 2}\left[\binom{n}{j}-\binom{m}{j}\right]\alpha^{n-j}\times\right.$$

$$\left.\times[2\alpha\Delta(j-2)+\delta_2\delta_3\Delta(j-3)]\right\}+$$

$$+u_2\sum_{j\geqslant 2}\left[\binom{n}{j}-\binom{m}{j}\right]\alpha^{n-j}\Delta(j-2).$$

Using Lemmas 3 and 4, all terms in the sums are congruent to 0 except those for $j=2$. Hence

$$0 \equiv u_0\alpha^3\alpha^{n-3}\left[\binom{n-1}{2}-\binom{m-1}{2}\right]-u_1\left\{2\alpha\alpha^{n-2}\left[\binom{n}{2}-\binom{m}{2}\right]\right\}+$$

$$+u_1\alpha^{n-1}(n-m)+u_2\alpha^{n-2}\left[\binom{n}{2}-\binom{m}{2}\right].$$

Again $\alpha \notin \mathfrak{p}$, since $\{u_n\}$ is u.d. mod p, so

$$0 \equiv u_0\alpha^2[(n^2-3n+2)-(m^2-3m+2)]-u_1\{2\alpha[(n^2-n)-(m^2-m)]\}+$$

$$+2u_1\alpha(n-m)+u_2[(n^2-n)-(m^2-m)]$$

or

$$0 \equiv (n-m)[(n+m-3)u_0\alpha^2-2(n+m-2)u_1\alpha+(n+m-1)u_2]. \tag{3}$$

It will follow that $n \equiv m \bmod \mathfrak{p}^{e(h-1)+1}$, provided

$$[(n+m-3)u_0\alpha^2-2(n+m-2)u_1\alpha+(n+m-1)u_2] \notin \mathfrak{p}.$$

However, $n \equiv m \bmod \mathfrak{p}$, so it suffices to show

$$(2n-3)u_0\alpha^2-2(2n-2)u_1\alpha+(2n-1)u_2 \notin \mathfrak{p}$$

for any n. This may be rewritten as

$$2n(u_0\alpha^2-2u_1\alpha+u_2)-(3u_0\alpha^2-4u_1\alpha+u_2) \notin \mathfrak{p}.$$

Since p satisfies condition (ii) of Theorem 2,

$$(u_0\alpha^2-2u_1\alpha+u_2) \in \mathfrak{p} \quad \text{and} \quad (3u_0\alpha^2-4u_1\alpha+u_2) \notin \mathfrak{p}$$

and this is the desired result. Hence p satisfies property h.

6. Conclusion of the proof of Theorem 3. Using Lemmas 5 and 6, we now have that $\{u_n\}$ is u.d. mod p^h for all $h \geqslant 1$ when p is a type I or type II prime.

Suppose now that p is a type III prime, then $\{u_n\}$ is u.d. mod p with period $p(p-1)$. We show that $\{u_n\}$ is not u.d. mod p^h for any $h>1$. It suffices to prove it for $h=2$.

Let $n \equiv m \bmod p(p-1)$, so $u_n \equiv u_m \bmod p$. The calculations used in Case II of Section 5, namely (3) show that

$$u_n - u_m \equiv (n-m)T \bmod \mathfrak{p}^{e+1},$$

where

$$T = 2n(u_0\alpha^2-2u_1\alpha+u_2)-(3u_0\alpha^2-4u_1\alpha+u_2).$$

Since p is type III, $u_0\alpha^2-2u_1\alpha+u_2 \notin \mathfrak{p}$ and there is an n for which $T \in \mathfrak{p}$. For this fixed value of n,

$$u_n - u_m \equiv (n-m)T \equiv 0 \bmod \mathfrak{p}^{e+1}$$

for each $m \equiv n \bmod p(p-1)$. Thus, $u_n \equiv u_m \bmod p^2$ by Lemma 1 and the residue u_n appears mod p^2 with a frequency greater than $1/p^2$. It follows that $\{u_n\}$ is not u.d. mod p^2.

Now suppose M is any integer not divisible by 2, 3, or 5 for which $\{u_n\}$ is u.d. If p^h divides M, then $\{u_n\}$ is also u.d. mod p^h, so M is necessarily the product of powers of type I or type II primes times a product of first powers of some type III primes. In fact, two distinct type III primes cannot divide M. Suppose q_1, q_2 are these two primes and look at $\{u_n\}$ mod q_1q_2. The proof of Theorem 2 showed that $\{u_n\} \equiv (\gamma_i n+n_i)^2 r_i^n$ mod q_i for some residues γ_i, n_i and r_i mod q_i and $\left(\frac{r_i}{q_i}\right) = -1$. Therefore, u_n is a square mod q_i if and only if n is even. It follows that the residue R does not appear in $\{u_n\}$ mod q_1q_2, if R satisfies $\left(\frac{R}{q_1}\right) = +1, \left(\frac{R}{q_2}\right) = -1$, since otherwise n would be even by the first condition and odd by the second. Such a residue obviously exists. Thus, M must be as described in Theorem 3. To show that all such numbers do work, we prove the following lemma.

LEMMA 7. *Let* $N = \prod_{i=1}^{k} p_i^{a_i}$ *where each* p_i *is type* I, *or type* II. *Then* $\{u_n\}$ *is u.d.* mod N *with a period of* $N\prod_{i=1}^{k}(p_i-1)$. *Each residue appears* $\prod(p_i-1)$ *times in any such period at subscripts which are half odd and half even.*

Let q *be any type* III *prime and* N *as above with* $q > p_i$ *for each* i. *Then* $\{u_n\}$ *is u.d.* mod Nq.

Proof. By induction on k. For $k = 1$, everything has been proved except the statement on the subscripts. Such primes satisfy property 1, so each residue appears $p-1$ times in a period at subscripts which are distinct mod $p-1$. Since $p-1$ is even, this gives the result.

So suppose the result is true for $k-1$ and number the primes so $p_k > p_i$ for $i = 1, 2, \ldots, k-1$.

Write $N = N_0 p_k^{a_k}$ and $p^a = p_k^{a_k}$. Then for any R, $u_n \equiv R \bmod N_0$ if and only if $n \equiv n_1, \ldots, n_Q \bmod \Phi(N_0)$, where $Q = \Phi(N_0)/N_0$. Also, $u_n \equiv R \bmod p^a$ if and only if $n \equiv m_1, \ldots, m_{p-1} \bmod \Phi(p^a)$.

We want to show that $u_n \equiv R \bmod N$, $(p-1)Q$ times in the period of length $\Phi(N) = \Phi(N_0)\Phi(p^a)$.

It is possible to solve

$$\begin{aligned} n &\equiv n_i \bmod \Phi(N_0), \\ n &\equiv m_j \bmod \Phi(p^a) \end{aligned} \tag{4}$$

if and only if $d = (\Phi(N_0), \Phi(p^a))$ divides $n_i - m_j$. Since $p > p_i$ for $i = 1, 2, \ldots, k-1$, $d = (\Phi(N_0), p^a(p-1)) = (\Phi(N_0), p-1)$, and so $d \mid (p-1)$.

Fix n_i and vary m_j. The values of m_j form a complete residue system mod $p-1$ by property 1 and thus $n_i - m_j$ is divisible by d a total of $(p-1)/d$ times for this choice of n_i. By varying n_i, a total of $Q\left(\frac{p-1}{d}\right)$ pairs (n_i, m_j) are found for which the system (4) has a solution. In each case, this solution is unique modulo LCM $(\Phi(N_0), \Phi(p^a)) = \Phi(N_0)\Phi(p^a)/d$ and thus leads to d solutions modulo $\Phi(N) = \Phi(N_0)\Phi(p^a)$. Therefore, the residue R mod N appears $Q\left(\frac{p-1}{d}\right)d = Q(p-1)$ times. The fact on the parity of the subscripts follows since it held for N_0 by induction, n_i and m_j are the same parity, and each such pair n_i, m_j leads to d new solutions of the same parity as m_j. Now suppose q is a type III prime and N as before. If we write $p = q$, then again we are led to the system (4) with $a = 1$. Here, for $(R, p) = 1$, $u_n \equiv R \bmod p$ if and only if

$$n \equiv m_1, \ldots, m_{p-1} \bmod \Phi(p)$$

where the m_i are all even if $\left(\frac{R}{p}\right) = +1$, odd otherwise, and each of the possible $\left(\frac{p-1}{2}\right)$ residues mod $p-1$ appears twice. The argument used before works if altered slightly. Fixing n_i and varying m_j will work only if $n_i \equiv m_j \bmod 2$. This is true for one half of the n_i by result on subscripts already proved. For the $Q/2$ values of n which will work with the m_j, we have $n_i - m_j$ divisible by d a total of $2\left(\frac{p-1}{d}\right)$ times, since the residues

mod $p-1$ appear twice. So as before, we get $Q(p-1)$ solutions to (4) in each period.

The residue zero mod p appears at subscripts which form a complete residue system mod $p-1$, so the proof is the same as for type I and II primes.

Lemma 7 essentially completes the proof of Theorem 3, except it was assumed that $q > p_i$ for each i. Let M be as in the hypothesis of Theorem 3. Suppose $p_1 < p_2 < \ldots < p_k < q < p_{k+1} < \ldots < p_s$. By Lemma 7, $\{u_n\}$ is u.d. mod N, $N = p_1^{a_1} \ldots p_k^{a_n} q$. This N can be used in the proof of Lemma 7 for each of the primes $p_{k+1}, \ldots, p_s$ to prove that u_n is u.d. mod M, although the subscripts no longer satisfy the same property.

It should be noted that there is a significant difference in the behavior of third order recurrent sequences as compared to second order sequences. In the case of second order sequences, $\{u_n\}$ is u.d. mod p^h if and only if it is u.d. mod p, except for $p = 2$ or 3. However, for third order sequences and any prime $p > 5$, there is a sequence which is u.d. mod p and not u.d. mod p^h for any $h > 1$.

In [5], it is proved that a second order recurrence is u.d. mod m for every integer m if and only if the sequence is u.d. modulo every prime. As a result of the difference between second order and third order sequences mentioned above, the corresponding theorem no longer holds. In particular, the sequence $\{u_n\}$ satisfying

$$u_n = 4u_{n-1} + 11u_{n-2} + 6u_{n-3}, \quad n \geqslant 3$$

with $u_0 = 0$, $u_1 = 3$, $u_2 = 16$ is uniformly distributed modulo every prime, but is not u.d. mod 7^2.

The methods used here should give at least partial results on higher order recurrences. However, the behavior of third order sequences seems to indicate that any necessary and sufficient conditions for an arbitrary nth order recurrent sequence to be uniformly distributed mod p^h, for an $n > 3$ will be quite complex.

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] L. Kuipers and J. Shiue, *A distribution property of the sequence of Fibonacci numbers*, Fibonacci Quarterly 10 (1972), pp. 375–392.

[3] — — *A distribution property of a linear recurrence of the second order*, Atti Accad. Naz. Lincei, Rend. Cl. Sci. fis. mat. nat., 52 (1972), pp. 6–10.

[4] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading 1970.

[5] Melvyn B. Nathanson, *Linear recurrence and uniform distribution*, Proc. Amer. Math. Soc. 48 (1975), pp. 289–291.

[6] H. Niederreiter, *Distribution of Fibonacci numbers* mod 5^k, Fibonacci Quarterly 10 (1972), pp. 373–374.

[7] William A. Webb and Calvin T. Long, *Distribution modulo p^h of the general linear second order recurrence*, Atti. Accad. Naz. Lincei, Rend. Cl. Sci. fis. mat. nat., 58 (1975), pp. 92–100.

WASHINGTON STATE UNIVERSITY

Received on 22. 10. 1976
and in revised form on 24. 5. 1977 (884)

ACTA ARITHMETICA
XXXVI (1980)

On the greatest prime factor of (ax^m+by^n)

by

T. N. Shorey (Bombay, India)

1. Suppose that f is a polynomial with rational coefficients and has at least two distinct roots. Schinzel and Tijdeman [4] proved that the equation $y^m = f(x)$ (with $x, y, m \in \mathbf{Z}$, $|y| > 1$) implies that m is bounded. In [5], it is shown that the polynomial f can be replaced by a binary form $f(x, z)$ (where $f(1, 0) \neq 0$) with at least two distinct linear factors, with $(x, z) = 1$ and z composed solely of powers of primes from a fixed set. In this paper, we prove a generalization of this result. The purpose of this generalization is to strengthen Theorem 3 of [5] on the greatest prime factor of (ax^m+by^n). All these results depend on Gelfond–Baker theory of linear forms in logarithms.

2. For a real number c between 0 and 1 and for an integer m greater than 1, set

$$A = \max\left(2, \exp\left(c\left((\log m)(\log\log m)\right)^{1/2}\right)\right),$$
$$B = \max\left(2, c\left((\log m)(\log\log m)\right)^{1/2}\right).$$

Denote by S the set of all non zero integers composed of primes not exceeding B. Let $f(x, y) \in \mathbf{Q}[x, y]$ be a binary form of degree n with $f(1, 0) \neq 0$. Assume that $f(x, 1)$ has at least two distinct roots. We define the height of a rational number a/b, $(a, b) = 1$, as $\max(|a|, |b|)$. Assume that the maximum of the heights of the coefficients of f is not greater than A. Then we have:

THEOREM. *Let d be a positive integer. Then there exist effectively computable positive constants c, c_1 depending only on n and d such that the equation*

$$wz^m = f(x, y) \tag{1}$$

in integers m, w, x, y, z with $w \in S$, $y \in S$, $(x, y) = d$, $|z| > 1$ implies that

$$m < c_1.$$