TSUKUBA J. MATH.
Vol. 9 No. 1 (1985). 159–166

WEAKLY UNIFORM DISTRIBUTION MOD M FOR CERTAIN RECURSIVE SEQUENCES AND FOR MONOMIAL SEQUENCES

By

Kenji NAGASAKA

0. Introduction.

In my preceding paper [2], recursive sequences defined by

(1) $$u_{n+1}\equiv a\cdot u_{n}+b\cdot u_{n}^{-1} \pmod m$$

were considered. We investigated conditions for which above defined recursive sequence with $a=b=1$ did not terminate and introduced the notion of uniform distribution in $(\boldsymbol{Z}/m\boldsymbol{Z})^{*}$ for non-terminating recursive sequences defined by (1). It was proved that every non-terminating recursive sequence defined by (1) was not uniformly distributed in $(\boldsymbol{Z}/m\boldsymbol{Z})^{*}$ except one special case.

In order to avoid the repetition of the word, "non-terminating", we define weakly uniform distribution mod m according to W. Narkiewicz [4]. Let $a=\{a_{n}\}_{n=1,2,}\cdots$ be a sequence of integers. For integers $N\geq 1$, $m\geq 2$, and j $(0\leq j\leq m-1)$, let us define $A_{N}(a;j,m)$ as the number of terms among $a_{1}, a_{2}, \cdots, a_{N}$ satisfying the congruence $a_{n}\equiv j \pmod m$ and similarly $B_{N}(a;m)$ as the number of terms a_{n}, $1\leq n\leq N$, that are relatively prime to m.

A sequence $a=\{a_{n}\}_{n=1,2,}\cdots$ of integers is said to be weakly uniformly distributed mod m if, for all j prime to m,

$$\lim_{N\to\infty}\frac{A_{N}(a;j,m)}{B_{N}(a;m)}=\frac{1}{\phi(m)},$$

provided

$$\lim_{N\to\infty}B_{N}(a;m)=\infty,$$

where $\phi(\cdot)$ denotes the Euler totient function.

For recursive sequences defined by (1), uniform distributions in $(\boldsymbol{Z}/m\boldsymbol{Z})^{*}$ are equivalent to weakly uniform distributions mod m.

In this note, we shall consider recursive sequences defined by

Received September 13, 1984.

(2) $$v_{n+1}\equiv a_k(v_n^k+v_n^{-k})+a_{k-1}(v_n^{k-1}+v_n^{-(k-1)})+\cdots$$
$$+a_1(v_n+v_n^{-1})+a_0 \pmod{m},$$

which is symmetric with respect to v_n and v_n^{-1}. We shall consider also recursive sequences defined by

(3) $$w_{n+1}\equiv a\cdot w_n^k+b\cdot w_n^{-k} \pmod{m}.$$

It will be proved that these recursive sequences are not weakly uniformly distributed mod m except for some special cases.

Uniform distribution properties mod m of monomial sequences are known by B. Zane [5]. We obtain almost similar results for weakly uniform distribution mod m of monomial sequences in the last section.

1. Symmetric recursion formula.

We considered in [2] a recursive sequence $u=\{u_n\}_{n=1,2,\cdots}$ defined by

(4) $$u_{n+1}\equiv u_n+u_n^{-1} \pmod{m}.$$

We introduced a function g_1 corresponding to the recursion formula (4) defined by $g_1(s)=s+s^{-1}$ on the multiplicative group $G_m=(\boldsymbol{Z}/m\boldsymbol{Z})^*$.

If the sequence u is weakly uniformly distributed mod m, then the corresponding function g_1 is necessarily bijective on G_m. The function g_1 satisfies a functional equation

(5) $$g_1(s)=g_1(s^{-1})$$

for all s in G_m, which gave Theorem 5 in [2] together with the bijectivety of g_1.

We now determine recursion formulae to which corresponding functions g satisfy the same functional equation as (5). Let us consider the function g_1 as a function h_1 with two variables, s and s^{-1}. The functional equation (5) is identical to the symmetricness of the function h_1. It is now enough to determine all symmetric functions of s and s^{-1}.

Every symmetric function can be represented as a polynomial of fundamental symmetric functions. In this case, two fundamental symmetric functions are $s+s^{-1}$ and $s\cdot s^{-1}=1$, and so every symmetric function $h(s, s^{-1})$ is a polynomial of $(s+s^{-1})$.

Applying Newton's binomial theorem to the expansion of $(s+s^{-1})^n$, the coefficient of s^k is $\binom{n}{(n+k)/2}$ which coincides with that of s^{-k}, where the symbol $\binom{x}{r}$ is the generalized binomial coefficient [1]. Hence the function satisfying (5) can be represented by

(6) $$g(s)=a_k(s^k+s^{-k})+a_{k-1}(s^{k-1}+s^{-(k-1)})+\cdots+a_1(s+s^{-1})+a_0,$$

and the corresponding recursion formula is (2).

We shall prove the

THEOREM 1. *No recursive sequence* $v=\{v_n\}_{n=1,2,\cdots}$ *is weakly uniformly distributed mod* m *except for*

$$v_{n+1}\equiv v_n+v_n^{-1} \pmod 3$$

and for

$$v_{n+1}\equiv v_n^2+v_n+1+v_n^{-1}+v_n^{-2} \pmod 3).$$

NOTE. The sequence defined by the latter congruence is substantially identical with the sequence defined by the former, since

$$v_n^2\equiv v_n^{-2}\equiv 1 \pmod 3 \text{ for all } n.$$

PROOF. If a recursive sequence $v=\{v_n\}_{n=1,2,\cdots}$ is weakly uniformly distributed mod m, then the function g in (6) corresponding to the recursion formula (2) is necessarily bijective from $G_m=(\boldsymbol{Z}/m\boldsymbol{Z})^*$ to G_m. The function g satisfies $g(s)=g(s^{-1})$, from which and from the bijectivity of g we deduce that

$$s\equiv s^{-1} \pmod m,$$

or equivalently to

(7) $$s^2\equiv 1 \pmod m,$$

for all s in G_m.

(i) *Case of odd m's.* For any odd integer m, the multiplicative group G_m contains 2 as an element. Substituting 2 in (7), we obtain $m=3$.

From Fermat's theorem, $s^3\equiv s \pmod 3$ for all s in $\boldsymbol{Z}/3\boldsymbol{Z}$, then we may restrict ourselves to the following recursion formulae:

$$v_{n+1}\equiv a_2(v_n^2+v_n^{-2})+a_1(v_n+v_n^{-1})+a_0 \pmod 3.$$

Direct calculation shows that only the following two recursion formulae:

$$v_{n+1}\equiv v_n+v_n^{-1} \pmod 3$$

and

$$v_{n+1}\equiv v_n^2+v_n+1+v_n^{-1}+v_n^{-2} \pmod 3$$

generate weakly uniformly distributed sequences mod 3.

(ii) *Case of even m's.* We denote r the smallest positive odd integer other than the unit element in the multiplicative group $G_m=(\boldsymbol{Z}/m\boldsymbol{Z})^*$. Substituting r in (7), we have $m=r^2-1$. The smallestness of $r\neq 1$ in G_m assures that m is divisible by all primes p_j less than r, which signifies

(8) $$\Pi_{j=1}^{\pi(r)-1} p_j < r^2-1.$$

The inequality (8) holds, from the prime number theorem, for only small values of r. Indeed (8) is valid only for $r=3$, 5,7 and 9. Considering prime factors of r^2-1 for above values of r satisfying (8), it is enough to consider the following two cases: $m=8$ and $m=24$.

On $G_8=(\boldsymbol{Z}/8\boldsymbol{Z})^*$, the function $g_1(s)$ takes only two distinct values, from which g is not bijective on G_8. Similarly g is neither bijective on $G_{24}=(\boldsymbol{Z}/24\boldsymbol{Z})^*$. Thus we complete the proof.

2. Recursive sequences defined by $w_{n+1}\equiv a\cdot w_n^k+b\cdot w_n^{-k}$ (mod m).

We now consider recursive sequences $w=\{w_n\}_{n=1,2,\cdots}$ defined by

(3) $$w_{n+1}\equiv a\cdot w_n^k+b\cdot w_n^{-k} \pmod{m},$$

that is a generalization of the recursion formula (1) considered in [2]. We obtain

THEOREM 2. *No recursive sequence $w=\{w_n\}_{n=1,2,\cdots}$ defined by* (3) *is weakly uniformly distributed mod m except for $a=b=k=1$ and $m=3$.*

PROOF. The corresponding function f to the recursion formula (3) is

$$\begin{aligned} f(s)&=a\cdot s^k+b\cdot s^{-k}\\ &=a\cdot s^k+b(s^k)^{-1}. \end{aligned}$$

If a recursive sequence $w=\{w_n\}_{n=1,2,\cdots}$ is weakly uniformly distributed mod m, then the function f from $G_m=(\boldsymbol{Z}/m\boldsymbol{Z})^*$ is bijective to G_m, from which we deduce that the function f_k from G_m defined by

$$f_k(s)=s^k$$

is also bijective to G_m, since f may be considered as a function of s^k. Then the following congruential equation

(9) $$s^k\equiv c \pmod{m}$$

has only one solution in G_m for all c in G_m.

Setting $c=a$ and $c=b$, we denote the unique solution in (9) a_0 and b_0, respectively. Then the function f corresponding to (3) satisfies a functional equation:

(10) $$f(s)=f(b_0\cdot a_0^{-1}\cdot s^{-1})$$

for all s in G_m. The bijectivity of f and (10) shows that

(11) $$s \equiv b_0 \cdot a_0^{-1} \cdot s^{-1} \pmod{m}$$

for all s in the multiplicative group G_m.

Substituting for $s=1$, we have

$$c \equiv d \pmod{m},$$

which is a special case in Theorem 1. Thus the proof is completed.

3. Monomial Sequences.

In the preceding section, the solvability of (9) is a necessary condition for weakly uniform distribution mod m of $w=\{w_n\}_{n=1,2,\cdots}$. Thus we are naturally led to consider distribution properties of monomial sequences.

Let us consider, for nonnegative integer k, monomial sequences $m(k\,;a)=\{a\cdot n^k\}_{n=1,2,\cdots}$. If a monomial sequence $m(k\,;a)$ is weakly uniformly distributed mod m, then the following congruential equation

(12) $$a \cdot s^k \equiv c \pmod{m}$$

has a unique solution in $G_m=(\boldsymbol{Z}/m\boldsymbol{Z})^*$ for all c in G_m and a is necessarily prime to m. Then multiplying a^{-1} to (12), it is enough to consider the unique solvability of (9) for all c in the multiplicative group G_m.

Let m be a composite integer such that

(13) $$m=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_r^{\alpha_r}\ (\alpha_i \geq 1),$$

where $p_1, p_2, \cdots, p_r$ are distinct primes. Then (9) has only one solution if and only if

(14) $$s^k \equiv c \pmod{p_i^{\alpha_i}}$$

has only one solution for each i, $1 \leq i \leq r$. In order to determine whether a monomial sequence $m(k\,;a)$ is weakly uniformly distributed mod m, it is enough to consider (14) for each i.

Starting from small values of k, we trivially obtain from the theory of linear congruences

THEOREM 3. *Monomial sequence $m(1\,;a)$ of degree one is weakly uniformly distributed mod m if and only if a is relatively prime to m.*

Likewise to uniformly distributed sequences of integers, we call an integer sequence $b=\{b_n\}_{n=1,2,\cdots}$ to be weakly uniformly distributed if b is weakly uniformly distributed mod m for all integers $m \geq 2$. Dirichlet's prime number theorem asserts us that the sequence of prime numbers is an example of weakly uniformly distributed sequences of integers.

From Theorem 3, we derive

COROLLARY. *$m(1;a)$ is not weakly uniformly distributed except for $a=\pm 1$.*

For monomial sequences $m(2l;a)$ of even degree, we get a negative answer to weakly uniform distribution mod m.

THEOREM 4. *No monomial sequence $m(2l;a)$ of even degree is weakly uniformly distributed mod m except for $m=2$ and odd integer a.*

PROOF. For the case of $l=0$, the statement of the Theorem is evident.

Setting now that $l\geq 1$ and we suppose that a monomial sequence $m(2l;a)$ is weakly uniformly distributed mod m, where m is of the form (13). Then, the congruence

$$s^{2l}\equiv c \pmod{p_i^{\alpha_i}} \tag{15}$$

has only one solution. From the unique existence of (15) for all c in $G_{p_i^{\alpha_i}}=(\boldsymbol{Z}/p_i^{\alpha_i}\boldsymbol{Z})^*$, we deduce that $2l$ and $\varphi(p_i^{\alpha_i})$ are relatively prime, which is impossible for odd prime p.

We now restrict ourselves to the modulus of the form 2^α and next Proposition (Theorem 63 in [3]) is useful.

PROPOSITION. *The numbers $\pm 5, \pm 5^2, \cdots, \pm 5^{2^{\beta-2}}$ form a reduced residue system modulo 2^β when $\beta\geq 3$.*

That signifies

$$G_{2^\alpha}=(\boldsymbol{Z}/2^\alpha\boldsymbol{Z})^*=\{\pm 5, \pm 5^2, \cdots, \pm 5^{2^{\alpha-2}}\}. \tag{16}$$

Suppose further that

$$2l=2^r\cdot l', \text{ where } l' \text{ is an odd integer,} \tag{17}$$

and consider the following congruence

$$s^{2l}\equiv c \pmod{2^\alpha}. \tag{18}$$

From (16), we may put, for $\alpha\geq 3$,

$$c\equiv(-1)^\lambda\cdot 5^h \pmod{2^\alpha}, \tag{19}$$

$$s\equiv(-1)^\mu\cdot 5^x \pmod{2^\alpha}, \tag{20}$$

where h, x, λ and μ are nonnegative integers. By introducing (19) and (20) in (18), we get

$$5^{2\chi l}\equiv(-1)^{\lambda}\cdot 5^{h} \pmod{2^{\alpha}}.$$

Hence the number λ is even. Then again from (16) and introducing (17), we obtain

$$2^{r}\cdot l'\cdot \chi\equiv h \pmod{2^{\alpha-2}}.$$

This implies $h\equiv 0 \pmod{2^{r}}$.

Then we derive that the congruential equation (18) has solutions if $c\equiv 5^{h} \pmod{2^{\alpha}}$ with $h\equiv 0 \pmod{2^{r}}$; otherwise it has no solution. We henceforth conclude that no monomial sequence $m(2l\,;\,a)$ is weakly uniformly distributed mod 2^{α} when $\alpha\geq 3$.

For $\alpha=1$ and $\alpha=2$, we examine $m(2l\,;\,a)$ directly and obtain that $m(2l\,;\,a)$ is weakly uniformly distributed mod 2 for odd a. Thus we complete the proof.

For monomial sequences of odd degree we obtain first positive answers to weakly uniform distribution mod m.

THEOREM 5. *Monomial sequences $m(k\,;\,a)$ of odd degree are weakly uniformly distributed mod 2^{α} for every $\alpha\geq 1$, provided a is odd.*

PROOF. For $\alpha=1$ and $\alpha=2$, direct calculations gives the statement of the Theorem 5.

For $\alpha\geq 3$, using the same representations as in (19) and (20),

$$s^{k}\equiv c \pmod{2^{\alpha}} \tag{21}$$

may be rewritten by

$$(-1)^{\mu}\cdot 5^{\chi k}\equiv(-1)^{\lambda}\cdot 5^{h} \pmod{2^{\alpha}}.$$

Hence $\mu\equiv\lambda \pmod 2$ and again from Proposition

$$\chi\cdot k\equiv h \pmod{2^{\alpha-2}}.$$

Since k is odd, this linear congruential equation has only one solution. Therefore, the congruence (21) has exactly one solution for all c in $G_{2^{\alpha}}$, which completes the the proof.

THEOREM 6. *If k is odd, then there exist infinitely many primes p such that a monomial sequence $m(k\,;\,a)$ is weakly uniformly distributed mod p^{α} for all $\alpha\geq 1$, provided a and p are relatively prime.*

PROOF. Theorem 3 asserts the statement of Theorem 6 for $k=1$. Hence we suppose that k is greater than 1.

From the proof of Theorem 4 and Theorem 5, we know that $m(k\,;\,a)$ is weakly uniformly distributed mod p^{α} if k is prime to $\phi(p^{\alpha})$. By Dirichlet's theorem the arithmetic progression

$$2+k,\ 2+2k, \cdots,\ 2+mk, \cdots$$

contains an infinite number of primes. Let $p=2+mk$ be any such prime satisfying $p>a$. If d is a divisor of $p-1=1+mk$ and if d is also a divisor of k, then k must be a divisor of 1. It follows that k is relatively prime to $\phi(p^a)=p^{a-1}(p-1)$. The proof is now completed.

We get, however, a negative answer to weakly uniform distribution mod m for monomial sequences of odd degree greater than one.

THEOREM 7. *If k is an odd integer greater than one, then there exist infinitely many primes p such that $m(k; a)$ is not weakly uniformly distributed mod p.*

PROOF. It is enough to prove the existence of an infinite number of primes p for which $p-1$ are not prime to k. Again by Dirichlet's theorem, there exist infinitely many primes p in the following arithmetic progression

$$1+k,\ 1+2k, \cdots,\ 1+mk, \cdots.$$

Let $p=1+mk>k$ be any such prime, then

$$(k,\ p-1)=(k,\ mk)=k>1,$$

where (a, b) denotes the greatest common divisor of two integers a and b. Thus the proof is finished.

REMARK. No monomial sequence $m(k; a)$ is weakly uniformly distributed except for $m(1; \pm 1)$.

References

[1] Feller, W., An Introduction to Probability Theory and Its Applications. Vol. 1. Third Ed. John Wiley and Sons, New York et al. 1968.

[2] Nagasaka, K., Distribution property of recursive sequences defined by $u_{n+1}\equiv u_n+u_n^{-1}$ (mod m). Fibonacci Q. **22** (1984), 76–81.

[3] Nagell, Y., Introduction to Number Theory. Chelsea Publishing Company, New York 1964.

[4] Narkiewicz, W., Uniform distribution of sequences of integers. Journées Arithmétiques 1980. Edited by J.V. Armitage. London Mathematical Society Lecture Note Series 56. Cambridge University Press, London (1982), 202–210.

[5] Zane, B., Uniform distribution modulo m of monomials. Amer. Math. Monthly **71** (1964), 162–164.

Department of Mathematics
Faculty of Education
Shinsyu University
Nagano Pref.
380 Japan