UNIFORM DISTRIBUTION (MOD m) OF RECURRENT SEQUENCES

STEPHAN R. CAVIOR
State University of New York at Buffalo, Buffalo, New York 14226

In this paper it is shown that, for any odd prime p, a sequence of integers can be found which is uniformly distributed (mod m) if and only if m is a power of p.

Suppose m is an integer greater than 1. We say that an infinite sequence of integers $\{T_n\}$ is *uniformly distributed* (mod m) if for $j = 0, 1, \cdots, m-1$

$$\lim_{n \to \infty} \frac{1}{n} A(n,j,m) = \frac{1}{m},$$

where $A(n,j,m)$ denotes the number of terms among $T_1, \cdots, T_n$ which satisfy the congruence

$$T_i \equiv j \pmod{m}.$$

The combined results of Kuipers and Shiue [1] and Niederreiter [2] establish the fact that the Fibonacci sequence $\{F_n\}$ is uniformly distributed (mod m) if and only if m is a power of 5. In this paper we show that, for any odd prime p, a sequence of integers can be defined by a linear recurrence of the second order which is uniformly distributed (mod m) if and only if m is a power of p.

We first prove

Lemma. Suppose p is an odd prime and that k is a positive integer. Then $p+1$ belongs to the exponent p^k (mod p^{k+1}).

Proof. We use induction.

For the case $k = 1$, note that

$$(p+1)^p = p^p + \cdots + \binom{p}{2}p^2 + p^2 + 1 \equiv 1 \pmod{p^2}.$$

Now if $p+1$ belongs to e (mod p^2), it follows that $e|p$, hence $e = p$.

Suppose now that $p+1$ belongs to p^k (mod p^{k+1}). Then

$$(p+1)^{p^k} = tp^{k+1} + 1$$

and

$$(p+1)^{p^{k+1}} = (tp^{k+1}+1)^p = (tp^{k+1})^p + \cdots + \binom{p}{2}(tp^{k+1})^2 + tp^{k+2} + 1.$$

Thus

(1) $$(p+1)^{p^{k+1}} \equiv 1 \pmod{p^{k+2}}.$$

So if $p+1$ belongs to e (mod p^{k+2}), then $e|p^{k+1}$. But from (1) it follows that

$$(p+1)^e \equiv 1 \pmod{p^{k+1}};$$

and by the inductive supposition, $p^k|e$. Therefore, $e = p^k$ or $e = p^{k+1}$.

Now

(2) $$(p+1)^{p^k} \equiv \binom{p^k}{k}p^k + \cdots + \binom{p^k}{2}p^2 + p^{k+1} + 1 \pmod{p^{k+2}}.$$

We next show that

(3) $$\binom{p^k}{j}$$

is divisible by p^{k-j+2} for $j = 2, 3, \cdots, k$. It will be useful to recall

(4) $$\binom{p^k}{j} = \frac{p^k(p^k-1)\cdots(p^k-j+1)}{j!}.$$

Let $p(n)$, $p(d)$, and $p(q)$ denote, respectively, the highest power of p dividing the numerator, the denominator, and the quotient in (4). When $j = 2$, $p(n) \geq k$, $p(d) = 0$, so $p(q) \geq k$. When $j = 3$, $p(n) \geq k$, $p(q) \leq 1$, so $p(q) \geq k - 1$. In general, $p(n) \geq k$, and by the customary formula

$$p(d) = \sum_{e=1}^{\infty} \left[\frac{j}{p^e}\right] \leq j \sum_{e=1}^{\infty} \frac{j}{p^e} = \frac{j}{p-1} \quad .$$

Since $p \geq 3$, we see that

$$p(d) \leq \frac{j}{2}\ ;$$

and since

$$\frac{j}{2} \leq j-2 \quad (j = 4, \cdots, k),$$

it follows that

$$p(q) \geq k-j+2 \quad (j = 2, 3, \cdots, k).$$

Returning to (2), we see that

$$\binom{p^k}{j} p^j \quad (j = 2, \cdots, k)$$

is divisible by p^{k+2}. Hence

$$(p+1)^{p^k} \equiv p^{k+1} + 1 \not\equiv 1 \quad (\text{mod } p^{k+2}),$$

and it follows finally that $e = p^{k+1}$, which completes the proof of the lemma.

We turn now to our major result.

Theorem. Let p be an odd prime and $\{T_n\}$ be the sequence defined by

$$T_{n+1} = (p+2)T_n - (p+1)T_{n-1}$$

and the initial values $T_1 = 0$, $T_2 = 1$. Then $\{T_n\}$ is uniformly distributed (mod m) if and only if m is a power of p.

Proof. We associate with $\{T_n\}$ the quadratic polynomial

$$x^2 - (p+2)x + p + 1$$

whose zeros over C are $p+1$ and 1. It can be shown [3] that T_n is expressible in terms of those zeros as

$$T_n = \frac{1}{p}\{(p+1)^{n-1} - 1\}\ .$$

PART 1. In this part of the proof we show that $\{T_n\}$ is uniformly distributed (mod p^k), $k = 1, 2, 3, \cdots$.

As the first step we prove that $\{T_1, T_2, \cdots, T_{p^k}\}$ forms a complete residue system (mod p^k). Accordingly, suppose that $T_i \equiv T_j$ (mod p^k), or equivalently,

$$\frac{1}{p}\{(p+1)^{i-1} - 1\} \equiv \frac{1}{p}\{(p+1)^{j-1} - 1\} \quad (\text{mod } p^k),$$

where $1 \leq i, j \leq p^k$. Then

$$(p+1)^{i-1} \equiv (p+1)^{j-1} \quad (\text{mod } p^{k+1}).$$

Supposing $i \geq j$, we write

$$(p+1)^{j-1}(p+1)^e \equiv (p+1)^{j-1} \quad (\text{mod } p^{k+1}),$$

where $0 \leq e \leq p^k - 1$, and it follows that

$$(p+1)^e \equiv 1 \quad (\text{mod } p^{k+1}).$$

But by the Lemma, $p+1$ belongs to the exponent p^k (mod p^{k+1}), so that $e = 0$ and $i = j$.

In this section of Part 1, we prove that $\{T_n\}$ (mod p^k) has period p^k. Specifically, we prove that

$$T_{p^k+1} \equiv T_1 \quad \text{and} \quad T_{p^k+2} \equiv T_2$$

(mod p^k). It will follow that

$$T_i \equiv T_{i+p^k} \quad (\text{mod } p^k)$$

for $i = 1, 2, 3, \cdots$. Note first that the congruence

$$T_{p^k+1} = \frac{1}{p}\left\{(p+1)^{p^k} - 1\right\} \equiv 0 \pmod{p^k}$$

is equivalent to

(5) $$(p+1)^{p^k} \equiv 1 \pmod{p^{k+1}}$$

which follows from the Lemma. Note next that the congruence

$$T_{p^k+2} = \frac{1}{p}\left\{(p+1)^{p^k+1} - 1\right\} \equiv 1 \pmod{p^k}$$

is equivalent to

$$(p+1)^{p^k+1} \equiv p+1 \pmod{p^{k+1}}$$

which reduces to (5).

Combining the results of Part 1, we see that the complete residue system (mod p^k) occurs in the first and all successive blocks of p^k terms of $\{T_n\}$, proving that $\{T_n\}$ is uniformly distributed (mod p^k).

PART 2. In this part of the proof we show that $\{T_n\}$ is not uniformly distributed (mod m) if m is not a power of p.

If $\{T_n\}$ is uniformly distributed (mod m), then it is uniformly distributed (mod q) for every prime divisor q of m. We show here that $\{T_n\}$ is not uniformly distributed (mod q) for any prime $q \neq p$. There are two cases to consider according to whether $(p+1, q) = 1$ or q.

If $(p+1, q) = 1$, we can prove

(6) $$T_q \equiv 0 \pmod{q}$$

and

(7) $$T_{q+1} \equiv 1 \pmod{q}.$$

Equation (6) is equivalent to

$$T_q = \frac{1}{p}\{(p+1)^{q-1} - 1\} \equiv 0 \pmod{q}$$

or

(8) $$(p+1)^{q-1} \equiv 1 \pmod{pq}$$

which is equivalent to the *pair* of congruences

(9) $$(p+1)^{q-1} \equiv 1 \pmod{p}$$

and

(10) $$(p+1)^{q-1} \equiv 1 \pmod{q}.$$

Equation (9) is trivial, and (10) is proved by Fermat's theorem. Equation (7) is equivalent to

$$\frac{1}{p}\{(p+1)^q - 1\} \equiv 1 \pmod{q}$$

or

$$(p+1)^q \equiv p+1 \pmod{pq}$$

which reduces to (8). Now (6) and (7) evidently imply that the period of $\{T_n\}$ (mod q) is a divisor of $q-1$, consequently at least one residue will not occur in the sequence.

If on the other hand $(p+1, q) = q$, then

$$T_{n+1} = (p+2)T_n - (p+1)T_{n-1} \equiv T_n \pmod{q};$$

thus $\{T_n\}$ (mod q) becomes $\{0, 1, 1, \cdots\}$ which plainly is not uniformly distributed (mod q). This completes the proof of the theorem.

R. T. Bumby has found conditions for a sequence defined by a second-order linear recurrence to be uniformly distributed to all powers of a prime p.

REFERENCES

1. L. Kuipers and Jau-Shyong Shiue, "A Distribution Property of the Sequence of Fibonacci Numbers," *The Fibonacci Quarterly,* Vol. 10, No. 4 (December 1972), pp. 375–376.
2. Harald Niederreiter, "Distribution of Fibonacci Numbers mod 5^k," *The Fibonacci Quarterly,* Vol. 4, No. 4 (December 1972), pp. 373–374.
3. Francis D. Parker, "On the General Term of a Recursive Sequence," *The Fibonacci Quarterly,* Vol. 2, No. 1 (February 1964), pp. 67–71.

****