UNIFORM DISTRIBUTION FOR PRESCRIBED MODULI

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

In [1] the author proves the following

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.

The proof of the theorem rests on a lemma which states that if p is an odd prime and k is a positive integer, $p+1$ belongs to the exponent p^k (mod p^{k+1}). The lemma is also proved in [1].

Since for each positive integer k, 3 belongs to the exponent 2^{k-1}(mod 2^{k+1}), (see [2, §90]), the lemma and the theorem cannot be extended to the case $p = 2$. It is the object of this paper to find a sequence of integers which is uniformly distributed (mod m) if and only if m is a power of 2.

We will need the following

Lemma. For each positive integer k, 5 belongs to the exponent 2^k (mod 2^{k+2}).

Proof. See [2, §90].

Theorem. The sequence $\{T_n\}$ defined by

$$T_{n+1} = 6T_n - 5T_{n-1}$$

and the initial values $T_1 = 0$ and $T_2 = 1$ is uniformly distributed (mod m) if and only if m is a power of 2.

Proof. The formula of the Binet type for the terms of $\{T_n\}$ is

$$T_n = \tfrac{1}{4}(5^{n-1} - 1) \quad n = 1, 2, 3, \cdots.$$

To prove this, note that the zeros of the quadratic polynomial

$$x^2 - 6x + 5$$

associated with $\{T_n\}$ are 5 and 1. Solving for c_1 and c_2 in

$$c_1 \cdot 5 + c_2 = 0$$
$$c_1 \cdot 5^2 + c_2 = 1,$$

we find $c_1 = 1/20$ and $c_2 = -1/4$. Therefore

$$T_n = \frac{1}{20}5^n - \frac{1}{4} \qquad n = 1, 2, 3, \cdots,$$

which agrees with the result above. Similar derivations are discussed in [3].

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

First we prove that $\{T_i : i = 1, \cdots, 2^k\}$ is a complete residue system (mod 2^k). Accordingly, suppose that

$$T_i \equiv T_j \pmod{2^k},$$

where $1 \leqslant i, j \leqslant 2^k$. Then

$$\tfrac{1}{4}(5^{i-1} - 1) \equiv \tfrac{1}{4}(5^{j-1} - 1) \pmod{2^k}$$

or

$$5^{i-1} \equiv 5^{j-1} \pmod{2^{k+2}}.$$

Assuming $i \geqslant j$, we write

$$5^{j-1} \cdot 5^e \equiv 5^{j-1} \pmod{2^{k+2}},$$

where $0 \leqslant e \leqslant 2^k - 1$. Then

$$5^e \equiv 1 \pmod{2^{k+2}}.$$

But by the lemma, 5 belongs to the exponent 2^k (mod 2^{k+2}), so $e = 0$ and $i = j$.

Next, we note that as a consequence of the lemma,

$$5^{2^k+i-1} \equiv 5^{i-1} \pmod{2^{k+2}} \quad i = 1, 2, 3, \cdots$$

or

$$T_{2^k+i} \equiv T_i \pmod{2^{k+2}} \quad i = 1, 2, 3, \cdots.$$

Thus we see that the complete residue system (mod 2^k) occurs in the first and all successive blocks of length 2^k in $\{T_n\}$, proving that $\{T_n\}$ is uniformly distributed (mod 2^k).

PART 2. We prove in this part that $\{T_n\}$ is not uniformly distributed (mod m) unless m is a power of 2.

If $\{T_n\}$ is uniformly distributed (mod m), it is uniformly distributed (mod q) for each prime divisor q of m. We show that $\{T_n\}$ is not uniformly distributed (mod q) if $q \neq 2$.

Suppose first that $q = 5$. Then

$$T_{n+1} = 6T_n - 5T_{n-1} \equiv T_n \pmod 5.$$

Hence $\{T_n\}$ (mod 5) is $\{0, 1, 1, 1, \cdots\}$.

Suppose finally that $q \neq 2, 5$. We show that

(1) $$T_q \equiv 0 \pmod q$$

and

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

Note (1) is equivalent to

$$\tfrac{1}{4}(5^{q-1} - 1) \equiv 0 \pmod q$$

or

(3) $$5^{q-1} \equiv 1 \pmod{4q}$$

which is equivalent to the pair

$$5^{q-1} \equiv 1 \pmod 4$$

and

$$5^{q-1} \equiv 1 \pmod q$$

both of which are elementary. Eq. (2) also reduces to (3). Equations (1) and (2) imply that the period of $\{T_n\}$ (mod q) divides $q - 1$, so at least one residue will not occur in the sequence. Therefore, the distribution of $\{T_n\}$ (mod q) is not uniform.

REFERENCES

1. Stephan R. Cavior, "Uniform Distribution (mod m) of Recurrent Sequences," *The Fibonacci Quarterly,* Vol. 15, No. 3 (October 1977), pp.
2. C. F. Gauss, *Disquisitiones Arithmeticae,* Yale University Press, New Haven, 1966.
3. Francis D. Parker, "On the General Term of a Recursive Sequence," *The Fibonacci Quarterly,* Vol. 2, No. 1 (February 1964), pp. 67–71.

****