THE DISTRIBUTION OF RESIDUES OF TWO-TERM RECURRENCE SEQUENCES

Eliot Jacobson
Ohio University, Athens, OH 45701
(Submitted July 1988)

Let U_0, U_1, A, B be integers and define, for $n \geq 2$,

$$U_n = AU_{n-1} + BU_{n-2}.$$

For an integer $m > 1$, the sequence (U_n) considered modulo m is eventually periodic. We say (U_n) is *uniformly distributed* modulo m [notation: u.d.(mod m)] if every residue modulo m occurs with the same frequency in any period. In this case, it is clear that the length of any period will be a multiple of m. Conditions that (U_n) be u.d.(mod m) can be found in [2, Theorem A]. Suppose (U_n) is u.d.(mod p^k) where p is a prime and $k > 0$. Let $M \geq 2$ be any integer. We study the relationship between the distribution of U_n (mod M) and U_n (mod $M \cdot p^k$). For integers $N \geq 2$ and $0 \leq c < N$, denote by $\nu(N, c)$ the number of times that c occurs as a residue in one shortest period of U_n (mod N). Our main result can now be stated.

Theorem: Let p be a prime and $k > 0$ be an integer such that U_n is u.d.(mod p^k). Say U_n has shortest period of length $p^k f$ modulo p^k. Let $M \geq 2$, and assume that U_n is purely periodic modulo M, with shortest period of length Q. Assume $p \nmid Q$. Then, for any $0 \leq a < M$, and $0 \leq b < M \cdot p^k$ with $b \equiv a$ (mod M),

$$\nu(M \cdot p^k, b) = \frac{f}{(Q, f)} \cdot \nu(M, a).$$

We remark that (,) denotes the GCD. Also, observe that the hypothesis $p \nmid Q$ yields $p \nmid M$. To prove the Theorem, we make use of a recent result of Vélez [2], which we state here for the reader's convenience.

Lemma: Suppose that U_n is u.d.(mod p^k) with shortest period of length $p^k f$. Then, for any integer $s \geq 0$, the sequence U_{s+qf}, $q = 0, 1, \ldots, p^k - 1$, consists of a complete residue system modulo p^k.

Proof of Theorem: Let $0 \leq a < M$ and let $\nu(M, a) = d$. As the Theorem is vacuous if $d = 0$, assume $d \geq 1$. Let $w_1, w_2, \ldots, w_d$ be all of the integers $0 \leq w_i < Q$ such that $U_{w_i} \equiv a$ (mod M). Let $0 \leq b < M \cdot p^k$, say $b \equiv r$ (mod p^k) with $0 \leq r < p^k$. Assume $b \equiv a$ (mod M). Note that U_n has period length

$$\text{LCM}(Q, fp^k) = \frac{f}{(Q, f)} \cdot Q \cdot p^k \text{ modulo } M \cdot p^k.$$

For ease of notation, we set $z = f/(Q, f)$. As $(M, p^k) = 1$, it suffices, by the Chinese Remainder Theorem, to show that the system

$$(1) \qquad U_n \equiv \begin{cases} a \pmod{M} \\ r \pmod{p^k} \end{cases}$$

has exactly $z \cdot d$ solutions, $0 \leq n < z \cdot Q \cdot p^k$.

We begin by producing, for each w_i, solutions $v_{i1}, v_{i2}, \ldots, v_{iz}$ of the system. Fix i. Then

$$U_{w_i + eQ} \equiv a \pmod{M} \text{ for all } 0 \leq e < z \cdot p^k - 1.$$

Let $0 \leq s_{i1} < s_{i2} < \cdots < s_{iz} < f$ be all of the distinct integers such that

$$w_i \equiv s_{i1} \equiv s_{i2} \equiv \cdots \equiv s_{iz} \pmod{(Q, f)}.$$

By Vélez's lemma, there exist integers $0 \le q_{i1}, q_{i2}, \ldots, q_{iz} \le p^k - 1$ such that

$$U_{s_{ij}+q_{ij}f} \equiv r \pmod{p^k}, \text{ for all } j.$$

Then, also, for any $0 \le t \le Q/(Q, f) - 1$, we have

$$U_{s_{ij}+(q_{ij}+tp^k)f} \equiv r \pmod{p^k}.$$

The bounds on e, t guarantee that these subscripts are less than $z \cdot Q \cdot p^k$. For each i, j, we seek $e = e_{ij}$, $t = t_{ij}$ in these bounds such that

$$w_i + e_{ij}Q = s_{ij} + (q_{ij} + t_{ij}p^k)f.$$

Write $s_{ij} - w_i = (Q, f)m_{ij}$. Note that since $\left(z \cdot p^k, \dfrac{Q}{(Q, f)}\right) = 1$, the linear congruence

$$t \cdot z \cdot p^k \equiv -(m_{ij} + q_{ij}z) \left(\operatorname{mod} \frac{Q}{(Q, f)}\right)$$

has a unique solution $t = t_{ij}$ with $0 \le t_{ij} < \dfrac{Q}{(Q, f)} - 1$. But then

$$Q \mid (Q, f)(m_{ij} + q_{ij}z + t_{ij} \cdot z \cdot p^k);$$

thus, since $(Q, z \cdot Q \cdot p^k) = Q$, the linear congruence

$$eQ \equiv (Q, f)(m_{ij} + q_{ij}z + t_{ij} \cdot z \cdot p^k) \pmod{z \cdot Q \cdot p^k}$$

has Q solutions $0 \le e < z \cdot q \cdot p^k$. Hence, this congruence has a unique solution $e = e_{ij}$ satisfying $0 \le e_{ij} \le z \cdot p^k - 1$. With these values of e_{ij}, t_{ij}, we have

$$w_i + e_{ij}Q \equiv s_{ij} + (q_{ij} + t_{ij}p^k)f \pmod{z \cdot Q \cdot p^k},$$

so equality holds, since both sides are less than $z \cdot Q \cdot p^k$. Set $v_{ij} = w_i + e_{ij}Q$ for all i, j. Then $0 \le v_{ij} < z \cdot Q \cdot p^k$, and each v_{ij} is a subscript that satisfies the system (1), that is, $U_{v_{ij}} \equiv b \pmod{M \cdot p^k}$ for all i, j. We claim that the v_{ij} are distinct.

Suppose that $v_{ij} = v_{gh}$. Then $w_i + e_{ij}Q = w_g + e_{gh}Q$ implies $Q \mid (w_i - w_g)$. As $0 \le w_i, w_g < Q$, this gives $w_i = w_g$, so that $i = g$. Then

$$s_{ij} + (q_{ij} + t_{ij}p^k)f = s_{ih} + (q_{ih} + t_{ih}p^k)f,$$

so that $f \mid (s_{ij} - s_{ih})$. As $0 \le s_{ij}, s_{ih} < f$, we have that $s_{ij} = s_{ih}$; therefore, $j = h$. Thus, the v_{ij} are distinct. This shows that, for any $0 \le a < M$ and any $0 \le b < M \cdot p^k$, $\nu(M \cdot p^k, b) \ge z \cdot \nu(M, a)$. The proof is concluded by observing that

$$z \cdot Q \cdot p^k = \sum_{b=0}^{M \cdot p^k - 1} \nu(M \cdot p^k, b) = \sum_{a=0}^{M-1} \sum_{r=0}^{p^k-1} \nu(M \cdot p^k, b), \text{ where } b \equiv \begin{cases} a \pmod{M} \\ r \pmod{p^k} \end{cases}$$

$$\ge \sum_{a=0}^{M-1} \sum_{r=0}^{p^k-1} z \cdot \nu(M, a) = z \cdot p^k \sum_{a=0}^{M-1} \nu(M, a) = z \cdot p^k \cdot Q.$$

Hence, equality holds throughout, and the Theorem follows. □

Example: Let $A = B = 1$, $U_0 = 0$, $U_1 = 1$ so that U_n is the Fibonacci sequence. Then U_n is u.d.(mod 5). Take $M = 33$. Then U_n has period of length $Q = 40$ modulo 33, and one computes that $\nu(33, 1) = 5$, whereas $\nu(165, 1) = 3$. This justifies the hypothesis that $p \nmid Q$. Moreover, in this case, $\nu(33, a)$ assumes 5 values for $0 \le a < 33$, but $\nu(165, b)$ assumes only 4 values for $0 \le b < 165$.

In fact, our Theorem asserts that U_n has the same number of distinct distribution frequencies modulo M and $M \cdot p^k$, whenever M, p satisfy the hypotheses of the Theorem [that is, $\nu(M, *)$ and $\nu(M \cdot p^k, *)$ take on the same number of distinct values]. This provides an alternate method of obtaining the results in [1].

Note that the "purely periodic" hypothesis of the Theorem can be omitted if one substitutes asymptotic density for frequency, as the finite number of terms before U_n becomes periodic modulo M do not affect density. Our final result is well known but illustrates the Theorem's power.

Corollary: Suppose that U_n is u.d.(mod p^k) and is u.d.(mod M), where p is a prime that does not divide the length of the period of U_n (mod M). Then U_n is u.d.(mod $M \cdot p^k$).

References

1. E. Jacobson. "Almost Uniform Distribution of the Fibonacci Sequence." *Fibonacci Quarterly 27.4* (1989):335-37.
2. W. Y. Vélez. "Uniform Distribution of Two-Term Recurrence Sequences." *Trans. of the A.M.S. 301* (1987):37-45.

*****

Masaryk University in Brno, Czechoslovakia, is the only university in the country which subscribes to the *Fibonacci Quarterly.* Unfortunately, their set is not complete. They need volumes 1-9. If anyone would be interested in donating these volumes to Masaryk University please let the editor of this journal know and he will make arrangements.