ON PERIODS MODULO A PRIME OF SOME CLASSES OF SEQUENCES OF INTEGERS

Juan Pla
315 rue de Belleville 75019 Paris, France
(Submitted July 1995)

In [2] and [3] we used the T transformation of sequences of integers (u_n), defined by $T(u_n) = xu_{n+k} - u_n$, to prove in a simple way properties of periodicity modulo a given prime p for (u_n) satisfying several types of second-order linear recurrences.

The aim of this note is to extend these early results to more general forms of the transformation and of the sequence (u_n).

Theorem 1: Let $u_n, n \geq 0$, be the general term of a given sequence of integers and define the transformation $T_{(x,y,k)}(u_n)$ as $T_{(x,y,k)}(u_n) = xu_{n+k} + yu_n$ for every $n \geq 0$, k being a positive integer.

Then, if x and y are nonzero integers and there exists a positive prime number p which divides $T_{(x,y,k)}(u_n)$ for every $n \geq 0$ and is relatively prime to x, the distribution of the residues of (u_n) modulo p is either constant or periodic with period $k(p-1)$.

Proof: If $(T(u_n))^{(m)}$ denotes the m^{th} iterate of the transformation $T_{(x,y,k)}$ on (u_n) for given x, y, and k, it is quite easy to prove by induction that, for any n and m,

$$(T(u_n))^{(m)} = \sum_{r=0}^{m} \binom{m}{r} (x)^r (y)^{m-r} u_{n+rk}.$$

Put $m = p$ in this formula. Since p is prime, the binomial coefficients are all divisible by p, except the two extreme ones (see [1], p. 417). Therefore,

$$(T(u_n))^{(p)} \equiv x^p u_{n+pk} + y^p u_n \pmod{p}.$$

Since by construction $(T(u_n))^{(p)}$ is a sum of terms all supposedly divisible by p, this entails that $x^p u_{n+pk} + y^p u_n \equiv 0 \pmod{p}$.

Since p is prime, by Fermat's little theorem, $x^p \equiv x \pmod{p}$ and $y^p \equiv y \pmod{p}$, and the previous congruence becomes $xu_{n+pk} + yu_n \equiv 0 \pmod{p}$.

By hypothesis, for any n, $xu_{n+k} + yu_n \equiv 0 \pmod{p}$, and from the difference with the previous congruences we obtain $x(u_{n+pk} - u_{n+k}) \equiv 0 \pmod{p}$. Since, by hypothesis, p and x are relatively prime, this implies $u_{n+pk} - u_{n+k} \equiv 0 \pmod{p}$ for any n. This proves Theorem 1.

Examples:

(1) Theorem 1 contains known properties for particular second-order linear sequences. For instance, let us consider the following one, with a and b being arbitrary nonzero integers:

$$u_{n+2} - au_{n+1} + bu_n = 0. \tag{R1}$$

An equivalent form of this recursion is $u_{n+2} + bu_n = au_{n+1}$.

If we take arbitrary integral values for u_0 and u_1, all u_n are integers; therefore, if p divides a, Theorem 1 may be applied with $x = 1$, $y = b$, and $k = 2$, which proves that the distribution of the residues of (u_n) modulo p is either constant or periodic with period $2(p-1)$. This was shown in [4] by Lawrence Somer, for a particular case of (u_n). The reader is also referred to [5] and [6] for other results about the periods of residues modulo a prime on examples of second-order (u_n) more restricted than ours but with more detailed results.

(2) The scope of Theorem 1 is not limited to *second*-order linear recursions (not even to *linear* ones). For instance, let us consider the third-order recursion

$$u_{n+3}+au_{n+2}+bu_{n+1}+cu_n=0$$

with nonzero integers as coefficients and initial values. If the prime p divides both a and b, then, by Theorem 1, the distribution of the residues of (u_n) modulo p is either constant or periodic with period $3(p-1)$. For p dividing both a and c, the corresponding period will be $2(p-1)$; it will be $p-1$ for p dividing both b and c.

(3) The T transformation allows a fresh look at the fundamental recursion (R1) and helps to provide an easy demonstration on a periodicity modulo a prime p property of sequences of the type $(2u_{n+1}-au_n)$.

If $\Delta=a^2-4b$, we may replace b in (R1) by $(a^2-\Delta)/4$ and, after simple computation, we obtain $\Delta u_n=4u_{n+2}-4au_{n+1}+a^2u_n$, where we recognize the right-hand side to be $T^2_{(2,-a,1)}(u_n)$, which is the result of the first iteration of the transformation $T_{(2,-a,1)}$. Therefore, by applying Theorem 1 to the sequence $(2u_{n+1}-au_n)=(T_{(2,-a,1)}(u_n))$, with $k=1$, $x=2$, and $y=-a$, we see that if p is any *odd* positive prime divisor of Δ, the discriminant of (R1), supposed nonzero, the distribution of the residues of $(2u_{n+1}-au_n)$ modulo p is either constant or periodic with period $p-1$ for any (u_n) satisfying (R1) and made up of integers. (In that case, the condition that p be odd is necessary to insure that p and $x=2$ are relatively prime.) The interesting fact here is that *any* member of the set of the sequences $(2u_{n+1}-au_n)$ exhibits the same periodicity property with regard to *any number* in the set of odd prime divisors of Δ.

As a more concrete example of application, let (U_n) and (V_n) be, respectively, the *generalized* Fibonacci and Lucas sequences of (R1). If $u_n=U_n$, then, by a well-known formula, we get $2u_{n+1}-au_n=V_n$. This proves that the distribution of the residues of V_n modulo any odd prime divisor p of Δ is either constant or periodic with period $p-1$.

(4) We may generalize this set to set relationship by studying the composition of two T transformations with different integral parameters. For any sequence (u_n), we have

$$T_{(v,w,1)}(T_{(x,y,1)}(u_n))=vxu_{n+2}+(vy+wx)u_{n+1}+wyu_n,$$

which proves that the composition of these transformations is commutative.

If (u_n) satisfies (R1), this expression is equal to $(vy+wx+avx)u_{n+1}+(wy-bvx)u_n$, and by applying Theorem 1 we prove that if p is any positive prime divisor of the gcd of $vy+wx+avx$ and $wy-bvx$ (if one exists), and is relatively prime with both x and v, then the sequences of the residues modulo p of $(xu_{n+1}+yu_n)$ and $(vu_{n+1}+wu_n)$ are either constant or periodic with period $p-1$.

Here we have two different sets of sequences that display the same behavior, in terms of periodicity, regarding a given set of prime numbers (the prime divisors of the gcd of $vy+wx+avx$ and $wy-bvx$).

(5) The period provided by Theorem 1 is not necessarily the *shortest* one, as shown in [3]. The following example shows how this situation may occur. Let us suppose that we have a sequence (u_n) of integers satisfying the recursion (R1), and two nonzero integers x and y such that $xu_{n+2}+yu_n$ is divisible by a prime number p for every n, p being prime with both x and a. The application of Theorem 1 to this situation yields $2(p-1)$ as the corresponding period. But $xu_{n+2}+yu_n = axu_{n+1}+(y-bx)u_n$, which means that the right-hand side is also divisible by p for every n; this time, applying Theorem 1 to this situation yields $p-1$ as the corresponding period. This proves, with the result of Example 1, that the primes p for which there exist integers x and y, x prime with p, such that p divides every $xu_{n+2}+yu_n$, and the distribution of the residues of (u_n) mod p has a corresponding *shortest* period of $2(p-1)$, are necessarily divisors of a.

Therefore, when $a=\pm 1$, for any prime p such that there exist integers x and y such that $xu_{n+2}+yu_n \equiv 0 \pmod{p}$ for every n, x prime with p, the corresponding shortest period is $p-1$ or less. For instance, if (L_n) and (F_n) are, respectively, the classifal Lucas and Fibonacci sequences, the shortest period mod 5 for (L_n) is precisely $p-1=4$, in accordance with the fact that $L_{n+2}+L_n$ is divisible by 5 for every n and $a=1$.

For (F_n), the shortest period mod 5 is 20, which means that, when $0<k<5$, integers x and y, x prime with 5 and such that $xF_{n+k}+yF_n$ is divisible by 5 for every n, do not exist because, in that case, $k(p-1)=4k<20$.

For $k=5$, we easily find that $F_{n+5}+2F_n$ is divisible by 5 for every n, and the corresponding period is $k(p-1)=20$.

ACKNOWLEDGMENT

The author wishes to express his deepest thanks to the editor for drawing his attention to references [5] and [6], and to Professor Lawrence Somer for providing the texts of his quoted papers and for an interesting discussion about them during one of his visits to France. Also, the important contribution of the referee to a better presentation of this paper is also gratefully acknowledged.

REFERENCES

1. Edouard Lucas. *Théorie des nombres*. Paris, 1891; rpt. Paris: Editions Jacques Gabay, 1991.
2. Juan Pla. "Some Conditions for 'All or None' Divisibility of a Class of Fibonacci-Like Sequences." *The Fibonacci Quarterly* **33.5** (1995):464-65.
3. Juan Pla. "On the Possibility of Programming the General 2-by-2 Matrix on the Complex Field." *The Fibonacci Quarterly*.
4. Lawrence Somer. "The Divisibility Properties of Primary Lucas Recurrences with Respect to Primes." *The Fibonacci Quarterly* **18.4** (1980):316-34.
5. Lawrence Somer. "Distribution of Residues of Certain Second-Order Linear Recurrences Modulo *p*." In *Applications of Fibonacci Numbers* **3**:311-24. Dordrecht: Kluwer, 1994.
6. Lawrence Somer. "Distribution of Residues of Certain Second-Order Linear Recurrences Modulo *p*—II." *The Fibonacci Quarterly* **29.1** (1991):72-78.

AMS Classification Numbers: 11B37, 11B39

❖❖❖