MODULAR PERIODICITY OF LINEAR RECURRENCE SEQUENCES

CURTIS BRIGHT

ABSTRACT. Integers which satisfy linear recurrence relations are always periodic modulo m. Many results on the period and pre-period length are summarized in this report, which have importance when studying some pseudo-random number generators as well as primality tests like the Lucas–Lehmer test for Mersenne primes. A Maple procedure is also provided allowing period calculation for arbitrary linear recurrences.

1. INTRODUCTION

An integer sequence (X_n) which satisfies the linear recurrence relation

$$X_n = a_1X_{n-1} + a_2X_{n-2} + \cdots + a_kX_{n-k} + a \tag{1}$$

for all $n \geq k$ is known as a *linear recurrence sequence*. We call the k-tuple

$$S_i = (X_i, X_{i+1}, \ldots, X_{i+k-1})$$

the ith *state* of the recurrence, so once (1) is given the value of X_{i+k} depends solely on S_i, and all values of the sequence are precisely defined by the *inital conditions* S_0. Furthermore, the residue of $X_{i+k} \pmod m$ depends only on the elementwise residues of S_i, and since there are m possible residues for each of the k components of state i, there are m^k possibilities for $S_i \pmod m$.

Since there are finitely many state residue classes, there must exist some $p > 0$ and $q \geq 0$ such that $S_q \equiv S_{q+p} \pmod m$. In fact, since $S_{i+1} \pmod m$ depends only on $S_i \pmod m$, we have

$$\text{for all } i \geq q, \qquad S_i \equiv S_{i+p} \pmod m, \tag{2}$$

which establishes that all linear recurrence sequences are eventually periodic.

There is a minimal pair (p, q) which satisfies (2)—dependant on m, S_0 and the recurrence parameters $\mathbf{a}$ in (1). Since the minimal p and q may be defined independently of each other the minimal pair is unique (e.g., it is not possible to accept an increase in p to decrease q).

2. PERIOD AND PRE-PERIOD

Definition 1. *The period $\lambda_X(m)$ is defined to be the minimal p which satisfies* (2) *and the pre-period $\mu_X(m)$ is defined to be the minimal q which satisfies* (2), *both with respect to the linear recurrence sequence (X_n). If the sequence is clear from context we may just refer to $\lambda(m)$ and $\mu(m)$.*

Note that $\mu(m) + \lambda(m) \leq m^k$ for all (X_n) because there are m^k states reduced modulo m and there can be no states repeated within the first $\mu(m) + \lambda(m)$ states (by period and pre-period minimality).

Lemma 1. *For $t \in \mathbb{N}$, $\lambda(m) \big| t$ if and only if $X_i \equiv X_{i+t} \pmod{m}$ for all $i \geq \mu(m)$.*

Proof. Repeatedly applying (2) with the period and pre-period yields

$$\text{for all } s \in \mathbb{N} \text{ and } i \geq \mu(m), \qquad X_i \equiv X_{i+s\lambda(m)} \pmod{m}, \tag{3}$$

which shows the forwards direction since we have $t = s\lambda(m)$.

Alternatively, by the division algorithm there exist integers q, r such that $t = q\lambda(m) + r$, with $0 \leq r < \lambda(m)$. Then

$$X_i \equiv X_{i+t} \equiv X_{i+q\lambda(m)+r} \equiv X_{i+r} \pmod{m},$$

where the final equivalence uses (3) with $s = q$. But then $X_i \equiv X_{i+r} \pmod{m}$ and $r < \lambda(m)$, so we have that $r = 0$ and $\lambda(m) \big| t$. □

Theorem 1. *For coprime m_1 and m_2, $\lambda(m_1 m_2) = \operatorname{lcm}(\lambda(m_1), \lambda(m_2))$.*

Proof. In the following, let i be any sufficiently large integer. To show equality we will show each side divides the other.

Firstly, by definition we have $X_i \equiv X_{i+\lambda(m_1 m_2)} \pmod{m_1 m_2}$, and thus

$$X_i \equiv X_{i+\lambda(m_1 m_2)} \pmod{m_1 \text{ and } m_2},$$

so by Lemma 1, $\lambda(m_1) \big| \lambda(m_1 m_2)$ and $\lambda(m_2) \big| \lambda(m_1 m_2)$ which implies $\operatorname{lcm}(\lambda(m_1), \lambda(m_2)) \big| \lambda(m_1 m_2)$.

Secondly, since $\lambda(m_1) \big| \operatorname{lcm}(\lambda(m_1), \lambda(m_2))$ and $\lambda(m_2) \big| \operatorname{lcm}(\lambda(m_1), \lambda(m_2))$ from Lemma 1 we have

$$X_i \equiv X_{i+\operatorname{lcm}(\lambda(m_1),\lambda(m_2))} \pmod{m_1 \text{ and } m_2}$$

and since m_1 and m_2 are coprime, by the Chinese Remainder Theorem,

$$X_i \equiv X_{i+\operatorname{lcm}(\lambda(m_1),\lambda(m_2))} \pmod{m_1 m_2}$$

so by Lemma 1, $\lambda(m_1 m_2) \big| \operatorname{lcm}(\lambda(m_1), \lambda(m_2))$. □

Theorem 2. *For coprime m_1 and m_2, $\mu(m_1 m_2) = \max\{\mu(m_1), \mu(m_2)\}$.*

Proof. By the Chinese Remainder Theorem, the smallest value of i which satisfies

$$X_i \equiv X_{i+\lambda(m_1 m_2)} \pmod{m_1 m_2},$$

will also be the smallest value of i which satisfies *both* of

$$X_i \equiv X_{i+\lambda(m_1 m_2)} \pmod{m_1 \text{ and } m_2}.$$

The smallest satisfying value of i will be $\mu(m_1)$ for the first and $\mu(m_2)$ for the second; thus the smallest satisfying both is $\max\{\mu(m_1), \mu(m_2)\}$. □

Corollary 1. *If $m = \prod p_i^{e_i}$ is the prime factorization, then $\lambda(m) = \operatorname{lcm}_i \lambda(p_i^{e_i})$ and $\mu(m) = \max_i \mu(p_i^{e_i})$.*

Proof. By repeated application of Theorems 1 and 2. □

Lemma 2. *Let (X_n) and (Y_n) satisfy the same recurrence, with (Y_n) having initial conditions $S_0 = (0, 0, \ldots, 0, 1)$, that is, the final entry of S_0 is 1 and all other entries (if any) are 0. Then $\lambda_X(m) \big| \lambda_Y(m)$.*

Proof. There exist constants $b_0, b_1, \dots, b_{k-1}$ such that

$$X_n = b_0 Y_n + b_1 Y_{n+1} + b_2 Y_{n+2} + \cdots + b_{k-1} Y_{n+k-1}$$

which may be found by solving the system

$$\begin{array}{rcccccccccc} X_0 & = & & & & & & & & & b_{k-1} \\ X_1 & = & & & & & & & b_{k-2} & + & b_{k-1}Y_k \\ X_2 & = & & & & & b_{k-3} & + & b_{k-2}Y_k & + & b_{k-1}Y_{k+1} \\ & \vdots & & & & & & & & & \\ X_{k-1} & = & b_0 & + & \cdots & + & b_{k-3}Y_{2k-4} & + & b_{k-2}Y_{2k-3} & + & b_{k-1}Y_{2k-2} \end{array}$$

Then for all $i \geq \mu_Y(m)$,

$$\begin{aligned} X_{i+\lambda_Y(m)} &\equiv b_0 Y_{i+\lambda_Y(m)} + \cdots + b_{k-1} Y_{i+\lambda_Y(m)+k-1} &&\pmod m \\ &\equiv b_0 Y_i + \cdots + b_{k-1} Y_{i+k-1} &&\pmod m \\ &\equiv X_i &&\pmod m \end{aligned}$$

and by Lemma 1, $\lambda_X(m) \big| \lambda_Y(m)$. ☐

Lemma 3. *Let (X_n) satisfy the homogeneous version of a recurrence satisfied by (Y_n), that is, their recurrences share the coefficients a_i but the (X_n) recurrence has $a = 0$. Then $\lambda_X(m) \big| \lambda_Y(m)$ when (Y_n) has initial conditions $(0, 0, \dots, 0, 1)$.*

Proof. Let $Z_n = Y_n - X_n$; then (Z_n) satisfies the same recurrence as (Y_n) so by Lemma 2, $\lambda_Z(m) \big| \lambda_Y(m)$. Then for all $i \geq \mu_Y(m)$,

$$X_{i+\lambda_Y(m)} \equiv Y_{i+\lambda_Y(m)} - Z_{i+\lambda_Y(m)} \equiv Y_i - Z_i \equiv X_i \pmod m,$$

and by Lemma 1, $\lambda_X(m) \big| \lambda_Y(m)$. ☐

The following theorems concern properties of the period function *for recurrences with initial conditions* $(0, 0, \dots, 0, 1)$.

Theorem 3. *For any prime p and $e \geq 1$, $\lambda(p^{e+1}) \big| p\lambda(p^e)$.*

Proof. For all $i \geq \mu(p^e)$ we have that $p^e \big| X_{i+\lambda(p^e)} - X_i$, so we may define the new integer sequence (Y_n) by

$$Y_n = \frac{X_{n+\lambda(p^e)+\mu(p^e)} - X_{n+\mu(p^e)}}{p^e}$$

which can be seen to satisfy the homogeneous version of the (X_n) recurrence. Since (X_n) has initial conditions $(0, 0, \dots, 0, 1)$, by Lemma 3 we have $\lambda_Y(m) \big| \lambda_X(m)$ or $Y_{i+\lambda_X(p^e)} \equiv Y_i \pmod{p^e}$ for sufficiently large i. Using this in the form $p^e Y_{i+\lambda(p^e)} \equiv p^e Y_i \pmod{p^{2e}}$ and the formula

$$X_{i+\lambda(p^e)+\mu(p^e)} = X_{i+\mu(p^e)} + p^e Y_i$$

we can show by induction that

$$X_{i+j\lambda(p^e)+\mu(p^e)} \equiv X_{i+\mu(p^e)} + jp^e Y_i \pmod{p^{2e}} \tag{4}$$

for $j \in \mathbb{N}$. Taking $j = p$ yields $X_{i+p\lambda(p^e)} \equiv X_i \pmod{p^{e+1}}$ for $2e \geq e + 1$ (i.e., $e \geq 1$), and the result follows. ☐

Corollary 2. *For any prime p and $e \geq 1$, $\lambda(p^{e+1}) = \lambda(p^e)$ or $\lambda(p^{e+1}) = p\lambda(p^e)$.*

Proof. An immediate consequence of Theorem 3 and the fact $\lambda(p^e) \big| \lambda(p^{e+1})$ (since $X_{i+\lambda(p^{e+1})} \equiv X_i \pmod{p^{e+1}}$ also holds modulo p^e). ☐

Theorem 4. *For any prime p and $e \geq 2$, if $\lambda(p^e) \neq \lambda(p^{e+1})$ then $\lambda(p^{e+1}) \neq \lambda(p^{e+2})$.*

Proof. Define (Y_n) as in the proof of Theorem 3. Notice from (4) we cannot have $p \big| Y_i$ for all arbitrarily large i, otherwise we would have $\lambda(p^e) = \lambda(p^{e+1})$. Thus, when $2e \geq e + 2$ (i.e., $e \geq 2$) we have

$$X_{i+\lambda(p^{e+1})+\mu(p^e)} \equiv X_{i+\mu(p^e)} + p^{e+1} Y_i \pmod{p^{e+2}}$$

and that there are arbitrarily large l such that $p \nmid Y_l$, so $\lambda(p^{e+1}) \neq \lambda(p^{e+2})$. □

Corollary 3. *For any prime p and $e \geq 2$, if $\lambda(p^e) \neq \lambda(p^{e+1})$ then $\lambda(p^{e+r}) = p^r \lambda(p^e)$ for $r \in \mathbb{N}$.*

Proof. By repeated application of Corollary 2 and Theorem 4. □

3. Example Use

It may be shown that if (U_n) is the Fibonacci sequence ($U_n = U_{n-1} + U_{n-2}$ with $U_0 = 0$ and $U_1 = 1$) then for all primes $p \neq 5$, $\lambda(p) \big| p^2 - 1$. So, for example, to show 91 is not a prime, we can calculate $\lambda(91)$ using the attached `calcperiod` function:

```
calcperiod([0, 1], [1, 1, 0], 91)[1];
```

returns 112. Since $91^2 \equiv 105 \not\equiv 1 \pmod{112}$, 91 is not prime. Under 1000, there are only 8 numbers which serve as 'psedoprimes': 161, 231, 323, 341, 377, 451, 671 and 903.

References

[1] H. Engstrom, On Sequences Defined by Linear Recurrence Relations, *Transactions of the American Mathematical Society* **33** (1931), 210–218.
[2] P. Freyd, K. Brown, The Period of Fibonacci Sequences Modulo m, *The American Mathematical Monthly* **99** (1992), 278–279.
[3] D. Knuth, *The Art of Computer Programming Volume 2: Seminumerical Algorithms*, Third Edition (1997), 7, 16–23, 37.
[4] M. Renault, Properties of the Fibonacci Sequence Under Various Moduli, Master's Thesis, Wake Forest University (1996).
[5] D. Robinson, A Note on Linear Recurrent Sequences Modulo m, *The American Mathematical Monthly* **73** (1966), 619–621.
[6] M. Ward, The Arithmetical Theory of Linear Recurring Series, *Transactions of the American Mathematical Society* **35** (1933), 600–628.

Maple Code 1 Auxiliary function for `calcperiod`; tests if two lists x and y have all equal elements with respect to the given index offsets.

```
equal := proc(x::list, xoffset::nonnegint, y::list, yoffset::nonnegint)
  local i, k;
  k := nops(x);
  for i from 1 to k do
    if x[i+xoffset mod k+1] <> y[i+yoffset mod k+1] then
      break;
    end if;
  end do;
  return evalb(i=k+1);
end;
```

Maple Code 2 Returns the period and pre-period modulo m of a linear recurrence sequence (X_n) using Floyd's cycle-finding algorithm. Input x as the list $X_0, X_1, \dots, X_{k-1}$ and a as the list $a_k, a_{k-1}, \dots, a_1, a$.

```
calcperiod := proc(x::list, a::list, m::posint)
  local k, i, j, X, Y, Z, n, period, preperiod;
  k := nops(x);
  X := x mod m;
  Y := X;
  Z := X;

  for i from 0 do
    if equal(X, i mod k, Y, 2*i mod k) and i>0 then
      n := i;
      period := i;
      break;
    end if;
    X[i mod k+1] := X[i mod k+1]*a[k] + a[k+1] mod m;
    Y[2*i mod k+1] := Y[2*i mod k+1]*a[k] + a[k+1] mod m;
    for j from 1 to k-1 do
      X[i mod k+1] := X[i mod k+1] + X[i+j mod k+1]*a[k-j] mod m;
      Y[2*i mod k+1] := Y[2*i mod k+1] + Y[2*i+j mod k+1]*a[k-j] mod m;
    end do;
    Y[2*i+1 mod k+1] := Y[2*i+1 mod k+1]*a[k] + a[k+1] mod m;
    for j from 1 to k-1 do
      Y[2*i+1 mod k+1] := Y[2*i+1 mod k+1] + Y[2*i+1+j mod k+1]*a[k-j] mod m;
    end do;
  end do;

  for i from 0 do
    if equal(X, n+i mod k, Z, i mod k) then
      preperiod := i;
      break;
    end if;
    X[n+i mod k+1] := X[n+i mod k+1]*a[k] + a[k+1] mod m;
    Z[i mod k+1] := Z[i mod k+1]*a[k] + a[k+1] mod m;
    for j from 1 to k-1 do
      X[n+i mod k+1] := X[n+i mod k+1] + X[n+i+j mod k+1]*a[k-j] mod m;
      Z[i mod k+1] := Z[i mod k+1] + Z[i+j mod k+1]*a[k-j] mod m;
    end do;
    if equal(X, i mod k, Y, n+i mod k) and period=n then
      period := i+1;
    end if;
  end do;
  return period, preperiod;
end;
```