INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A42

PERIODICITY OF SOME RECURRENCE SEQUENCES MODULO M

Artūras Dubickas
Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania
arturas.dubickas@mif.vu.lt

Tomas Plankis
Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania
topl@hypernet.lt

Received: 2/19/08, Accepted: 9/11/08, Published: 10/7/08

Abstract

We study the sequence of integers given by $x_1, \dots, x_d \in \mathbb{Z}$ and $x_{n+1} = F(x_n, \dots, x_{n-d+1})^{f(n)} + g(n)$, $n = d, d+1, d+2, \dots$, where F is a polynomial in d variables with integer coefficients, and $f : \mathbb{N} \mapsto \mathbb{N}$, $g : \mathbb{Z} \mapsto \mathbb{Z}$ are two functions. In particular, we prove that the sequence $x_1, x_2, x_3, \dots$ is ultimately periodic modulo m, where $m \geq 2$, if f and g are both ultimately periodic modulo every $q \geq 2$ and $\lim_{n\to\infty} f(n) = \infty$. We also give a result in the opposite direction for the sequence $x_1 \in \mathbb{Z}$, $x_{n+1} = x_n^{f(n)} + 1$, $n = 1, 2, 3, \dots$. If there is no infinite arithmetic progression $au+b$, $u = 0, 1, 2, \dots$, with $a, b \in \mathbb{N}$ such that $f(au+b)$, $u = 0, 1, 2, \dots$, is purely periodic modulo q for some $q \geq 2$, then $x_n \pmod m$, $n = 1, 2, 3, \dots$, is not ultimately periodic. Finally, we give some examples based on these two results.

1. Introduction

In this note, we are interested in sequences of integers given by the recurrence relations of the form

$$x_{n+1} = F(x_n, x_{n-1}, \dots, x_{n-d+1})^{f(n)} + g(n),$$

where $F(z_0, z_1, \dots, z_{d-1})$ is a polynomial in d variables with integer coefficients, $f : \mathbb{N} \mapsto \mathbb{N}$ and $g : \mathbb{Z} \mapsto \mathbb{Z}$. For example, the sequences

$$y_{n+1} = (y_n + 2y_{n-1}^3)^{n^2+2^n} + n, \quad n = 2, 3, 4, \dots, \quad \text{and} \quad u_{n+1} = u_n^{[n\sqrt{2}]} + 1, \quad n = 1, 2, 3, \dots,$$

where $y_1, y_2, u_1 \in \mathbb{Z}$, are of this form. (Throughout, $[x]$ stands for the integral part of a real number x.) Our results imply that the first sequence $y_1, y_2, y_3, \dots$ is ultimately periodic modulo m for every integer $m \geq 2$, whereas the second sequence $u_1, u_2, u_3, \dots$ is not ultimately periodic modulo m if m is not a power of 2. A sequence $s_1, s_2, s_3, \dots$ is called *ultimately periodic* if there are positive integers r and t such that $s_n = s_{n+t}$ for each $n \geq r$. If $r = 1$, then $s_1, s_2, s_3, \dots$ is called *purely periodic.*

The study of such recurrence sequences (in particular, of the sequence given by $x_{n+1} = x_n^{f(n)} + 1$, where $\lim_{n\to\infty} f(n) = \infty$) was motivated by the construction of some special transcendental numbers ζ for which the sequences of their integral parts $[\zeta^n]$, $n = 1, 2, 3, \dots$, have some divisibility properties [2], [4]. It seems very likely that, for each $\zeta > 1$, the sequence $[\zeta^n]$, $n = 1, 2, 3, \dots$, contains infinitely many composite elements (compare with Problem E19 on p. 220 in [6]), although such a statement is very far from being proved. One may consult [5] for the latest developments concerning this problem.

In [3], the first named author proved that the sequence given by $x_1 \in \mathbb{N}$ and $x_{n+1} = x_n^{n+1} + P(n)$ for $n \geq 1$, where $P(z)$ is an arbitrary polynomial with integer coefficients, is ultimately periodic modulo m for every $m \geq 2$.

More generally, let $f : \mathbb{N} \mapsto \mathbb{N}$, $g : \mathbb{Z} \mapsto \mathbb{Z}$ be two functions, and let x_n, $n = 1, 2, 3, \dots$, be a sequence of integers given by $x_1 \in \mathbb{Z}$ and $x_{n+1} = x_n^{f(n)} + g(n)$ for each $n \geq 1$. Suppose that $m \geq 2$ is a positive integer. Our aim is to investigate the conditions on f and g under which the sequence $x_n \pmod m$, $n = 1, 2, 3, \dots$, is ultimately periodic. Are there some 'simple' functions f, g for which this sequence is not ultimately periodic?

In the next section, we shall prove that this sequence is ultimately periodic provided that the functions f and g are ultimately periodic sequences themselves modulo every $q \geq 2$. In fact, Theorem 1 is more general, whereas the above result is its corollary with $d = 1$ and the polynomial $F(z) = z$. We also prove a result in the opposite direction assuming that no subsequence of $f(n)$, $n = 1, 2, 3, \dots$, having the form of infinite arithmetic progression is ultimately periodic modulo $q \geq 2$. Finally, in Section 3 we shall give some examples.

2. Results

Theorem 1 *Let d be a positive integer, $F(z_0, \dots, z_{d-1}) \in \mathbb{Z}[z_0, \dots, z_{d-1}]$, $f : \mathbb{N} \mapsto \mathbb{N}$ and $g : \mathbb{Z} \mapsto \mathbb{Z}$. Suppose that f and g are ultimately periodic modulo q for every integer $q \geq 2$, and $\lim_{n\to\infty} f(n) = \infty$. Let $x_1, \dots, x_d \in \mathbb{Z}$ and*

$$x_{n+1} = F(x_n, \dots, x_{n-d+1})^{f(n)} + g(n)$$

for $n = 1, 2, 3, \dots$. Then, for each $m \geq 2$, the sequence $x_n \pmod m$, $n = 1, 2, 3, \dots$, is ultimately periodic.

Proof. Let D_m be the set of divisors of m greater than 1 including m itself. Put M for the least common multiple of the numbers $\{\varphi(j) \ : \ j \in D_m\}$, where φ is Euler's function.

Since g is ultimately periodic modulo m and f is ultimately periodic modulo M, there are $n_0, s, \ell \in \mathbb{N}$ such that $m | (g(n+s) - g(n))$ and $M | (f(n+\ell) - f(n))$ for every integer

$n \geq n_0$. Set $l = s\ell$. It follows that $m|(g(n+ul)-g(n))$ and $M|(f(n+ul)-f(n))$ for $n \geq n_0$ and each $u \in \mathbb{N}$.

We assert that there is an integer $n_1 \geq n_0$ such that $m|(a^{f(n+l)} - a^{f(n)})$ for each $n \geq n_1$ and each $a \in \{0, 1, \dots, m-1\}$. Then the theorem easily follows by induction on n. Indeed, the sequence of vectors $(x_{n_1+kl}, \dots, x_{n_1+kl-d+1})$, $k = 0, 1, 2, \dots$, contains some two equal elements modulo m, because there are only m^d different vectors. The corresponding values of polynomials $F(x_{n_1+k_1l}, \dots, x_{n_1+k_1l-d+1})$ and $F(x_{n_1+k_2l}, \dots, x_{n_1+k_2l-d+1})$ are also equal modulo m. Setting

$$a = F(x_{n_1+k_1l}, \dots, x_{n_1+k_1l-d+1}) \pmod m = F(x_{n_1+k_2l}, \dots, x_{n_1+k_2l-d+1}) \pmod m,$$

where $k_1 > k_2 \geq 0$, $n = n_1 + k_2 l$, $u = k_1 - k_2$, and subtracting $x_{n+1} = F(x_n, \dots, x_{n-d+1})^{f(n)} + g(n)$ from $x_{n+ul+1} = F(x_{n+ul}, \dots, x_{n+ul-d+1})^{f(n+ul)} + g(n+ul)$, we find that $x_{n+ul+1} - x_{n+1}$ modulo m equal to $a^{f(n+ul)} - a^{f(n)}$ modulo m. By the above assertion, this is zero, because $a^{f(n+ul)} - a^{f(n)} = \sum_{k=1}^{u}(a^{f(n+kl)} - a^{f(n+(k-1)l)})$. Hence $x_{n+ul+1} \pmod m = x_{n+1} \pmod m$. Consequently, by induction on n, the sequence $x_n \pmod m$, $n = 1, 2, 3, \dots$, is ultimately periodic.

In order to prove the assertion we need to show that m divides $a^{f(n)}(a^{f(n+l)-f(n)} - 1)$. This is obvious if $a = 0$ or $a = 1$. Suppose that $a \geq 2$. If $\gcd(a, m) > 1$, write $a = a' p_1^{u_1} \dots p_k^{u_k}$ and $m = m' p_1^{v_1} \dots p_k^{v_k}$, where $p_1, \dots, p_k$ are some prime numbers, $u_1, \dots, u_k, v_1, \dots, v_k \in \mathbb{N}$ and $\gcd(a', m') = 1$. (Otherwise, if $\gcd(a, m) = 1$, take $a' = a$ and $m' = m$.)

Assume that $f(n+l) \geq f(n)$. Using $\lim_{n\to\infty} f(n) = \infty$, we see that $p_1^{v_1} \dots p_k^{v_k}$ divides $a^{f(n)}$ for each sufficiently large n, say, for $n \geq n_1 \geq n_0$. This proves the claim if $m' = 1$. Suppose that $m' \geq 2$. By Euler's theorem, $m'|(a^{\varphi(m')} - 1)$, because $\gcd(a, m') = 1$. So it remains to show that $f(n+l) - f(n)$ is divisible by $\varphi(m')$. But $\varphi(m')|M$, by the choice of M. Since, by the above, we have $M|(f(n+l) - f(n))$, it follows that $\varphi(m')$ divides $f(n+l) - f(n)$, as claimed. The proof of this statement when $f(n+l) < f(n)$ is the same, because $a^{f(n)}(a^{f(n+l)-f(n)} - 1)$ can be written as $a^{f(n+l)}(1 - a^{f(n)-f(n+l)})$. This completes the proof of the theorem. □

We remark that the assertion of Theorem 1 is true under weaker assumptions on f and g. We do not need them to be ultimately periodic modulo every $q \geq 2$. It is sufficient that $g : \mathbb{Z} \mapsto \mathbb{Z}$ is ultimately periodic modulo m and $f : \mathbb{N} \mapsto \mathbb{N}$ is ultimately periodic modulo M, where M is defined in the proof of Theorem 1 and is given in terms of m only.

The following corollary generalizes the main result of [3]:

Corollary 2 *Let $f : \mathbb{N} \mapsto \mathbb{N}$ and $g : \mathbb{Z} \mapsto \mathbb{Z}$ be two functions which are ultimately periodic modulo q for every integer $q \geq 2$, and $\lim_{n\to\infty} f(n) = \infty$. Suppose that $x_1 \in \mathbb{Z}$ and*

$$x_{n+1} = x_n^{f(n)} + g(n)$$

for $n = 1, 2, 3, \dots$. Then, for each $m \geq 2$, the sequence $x_n \pmod m$, $n = 1, 2, 3, \dots$, is ultimately periodic.

We also give a statement in the opposite direction:

Theorem 3 *Let* $m \geq 3$ *be an integer, which is not a power of* 2*, and let* $f : \mathbb{N} \mapsto \mathbb{N}$*. Suppose that* $x_1 \in \mathbb{Z}$ *and*

$$x_{n+1} = x_n^{f(n)} + 1$$

for $n = 1, 2, 3, \ldots$*. If the sequence* $x_n \pmod{m}$, $n = 1, 2, 3, \ldots$, *is ultimately periodic, then there are positive integers* q, b, t*, where* $2 \leq q \leq m - 1$*, such that the sequence* $f(b + ut) \pmod{q}$, $u = 0, 1, 2, \ldots$, *is purely periodic.*

Proof. Since m is not a power of 2, it has an odd prime divisor, say, p. The sequence $x_n \pmod{m}$, $n = 1, 2, 3, \ldots$, is ultimately periodic, so the sequence $x_n \pmod{p}$, $n = 1, 2, 3, \ldots$, must be an ultimately periodic sequence too. Hence there are n_1 and t such that $p|(x_{n+t} - x_n)$ for each $n \geq n_1$. Fix any $b \geq n_1$ for which $a = x_b \pmod{p} \notin \{0, 1\}$. Such b exists, because $p \geq 3$, so each 0 of the sequence $x_n \pmod{p}$, $n = 1, 2, 3, \ldots$, is followed by 1, which is followed by 2. Clearly, $x_{b+ut} \pmod{p} = a$ for each nonnegative integer u.

Subtracting $x_{b+1} = x_b^{f(b)} + 1$ from $x_{b+ut+1} = x_{b+ut}^{f(b+ut)} + 1$, we obtain $p|(a^{f(b+ut)} - a^{f(b)})$. Since $2 \leq a \leq p - 1$ and p is a prime number, we have $\gcd(a, p) = 1$. It follows that $p|(a^{|f(b+ut)-f(b)|} - 1)$. Let q be the least positive integer for which $p|(a^q - 1)$. Since $a < p$, we have $2 \leq q \leq \varphi(p) = p - 1 \leq m - 1$. Furthermore, q divides the difference $|f(b + ut) - f(b)|$ for every integer $u \geq 0$. Thus the sequence $f(b + ut) \pmod{q}$, $u = 0, 1, 2, \ldots$, is purely periodic, as claimed. □

The condition that m is not a power of 2 is essential. Evidently, any sequence given by $x_{n+1} = x_n^{f(n)} + 1$, where $f : \mathbb{N} \mapsto \mathbb{N}$, is purely periodic modulo 2. If $m = 2^s$, where $s \geq 2$, we can take any function $f : \mathbb{N} \mapsto \mathbb{N}$ satisfying $f(n) \geq s$ for each sufficiently large n. It is easy to see that, starting from some n_0, the sequence $x_n \pmod{2^s}$ is $1, 2, 1, 2, 1, 2, \ldots$, so $x_n \pmod{2^s}$, $n = 1, 2, 3, \ldots$, is ultimately periodic.

In general, the problem of periodicity of residues of a recurrence sequence can be very difficult even for a 'simply looking' sequence. In [1], the authors considered the sequence $x_{n+1} = -[\lambda x_n] - x_{n-1}$, $n = 1, 2, 3, \ldots$. It is conjectured that, for any $x_0, x_1 \in \mathbb{Z}$ and $\lambda \in [-2, 2]$, the sequence x_n, $n = 0, 1, 2, \ldots$ is purely periodic. The nontrivial case is when $\lambda \in (-2, 2) \setminus \{-1, 0, 1\}$. For $\lambda = 1/2$, the sequence is given by $x_0, x_1 \in \mathbb{Z}$, $x_{n+1} = -[x_n/2] - x_{n-1}$ for $n = 1, 2, 3, \ldots$. Note that $[x_n/2] = x_n/2$ for even x_n and $[x_n/2] = (x_n - 1)/2$ for odd x_n. Hence the sequence x_n, $n = 0, 1, 2, \ldots$ is purely periodic, if and only if, the sequence $x_n \pmod{2}$, $n = 0, 1, 2, \ldots$, is ultimately periodic. However, even the statement concerning the periodicity of $x_n \pmod{2}$, $n = 0, 1, 2, \ldots$, seems to be out of reach.

3. Examples

Let $a, m \geq 2$ be integers. The functions $f(n) = a^n$, $f(n) = P(n)$, where $P(z) \in \mathbb{Z}[z]$, $P(n) \geq 1$ for $n \geq 1$, $f(n) = n!$ and their linear combinations are ultimately periodic modulo m. Thus, by Theorem 1, the sequence given by $y_1, y_2 \in \mathbb{Z}$ and $y_{n+1} = (y_n + 2y_{n-1}^3)^{n^2+2^n} + n$ for $n \geq 2$ (see Section 1) is ultimately periodic modulo m. Similarly, for instance, the sequence given by $x_1 \in \mathbb{Z}$ and $x_{n+1} = x_n^{n^a} + 1$, where $n \geq 1$, is ultimately periodic modulo m. The same is true for the sequence $x_1 \in \mathbb{Z}$, $x_{n+1} = x_n^{a^n} + 1$, $n = 1, 2, 3, \ldots$.

Let $\alpha > 0$ be an irrational number and $\beta \geq 0$. Consider the sequence $x_1 \in \mathbb{Z}$,

$$x_{n+1} = x_n^{[\alpha n + \beta]} + 1$$

for $n = 1, 2, 3, \ldots$. We claim that this sequence is not ultimately periodic modulo m, if $m \neq 2^s$ with integer $s \geq 0$.

Suppose that the sequence $x_n \pmod{m}$, $n = 1, 2, 3, \ldots$, is ultimately periodic. By Theorem 3, there exist positive integers q, b, t, where $2 \leq q \leq m-1$, such that the sequence $[\alpha(b+ut)+\beta] \pmod{q}$, $u = 0, 1, 2, \ldots$, is purely periodic. Suppose that the length of the period is $\ell \geq 1$. Then q divides the difference $[\alpha(b+ut+\ell t)+\beta] - [\alpha(b+ut)+\beta]$. For any real numbers x, y, we have $[x+y] = [x]+[y]$ if the sum of the fractional parts $\{x\}+\{y\}$ is smaller 1 and $[x+y] = [x]+[y]+1$ if $\{x\}+\{y\} \geq 1$. Setting $x = \alpha(b+ut)+\beta$ and $y = \alpha\ell t$, we find that

$$[\alpha(b+ut+\ell t)+\beta] - [\alpha(b+ut)+\beta] = \begin{cases} [\alpha\ell t] & \text{if } \{\alpha(b+ut)+\beta\} < 1 - \{\alpha\ell t\}, \\ [\alpha\ell t]+1 & \text{if } \{\alpha(b+ut)+\beta\} \geq 1 - \{\alpha\ell t\}. \end{cases}$$

Since $\alpha t \notin \mathbb{Q}$, by Weyl's criterion, the sequence $\{\alpha(b+ut)+\beta\}$, $u = 0, 1, 2, \ldots$, is uniformly distributed in $[0, 1]$ (see, e.g., [8] or Section 2.8 in [7]). In particular, it is everywhere dense in $[0, 1]$. Hence the sets S_1 and S_2 of $u \in \mathbb{N}$ for which the first or the second alternative holds, respectively, are both not empty. Setting $N = [\alpha\ell t]$, we deduce that $q|N$, because S_1 is not empty, and $q|(N+1)$, because S_2 is not empty, a contradiction.

Since $\sqrt{2} \notin \mathbb{Q}$, this implies that the sequence given by $u_{n+1} = u_n^{[n\sqrt{2}]} + 1$, $n = 1, 2, 3, \ldots$, and some $u_1 \in \mathbb{Z}$ (see Section 1) is not ultimately periodic modulo m if m is not a power of 2.

One can give more 'natural' examples of sequences which are not ultimately periodic modulo m using the following:

Lemma 4 *Let $f : \mathbb{N} \mapsto \mathbb{N}$ be a non-decreasing function satisfying $\lim_{n\to\infty} f(n) = \infty$ with the property that, for every $l \in \mathbb{N}$, there is an integer n_l such that $f(n+l) - f(n) \leq 1$ for each $n \geq n_l$. Then there is no arithmetic progression $au+b$, $u = 0, 1, 2, \ldots$, with $a, b \in \mathbb{N}$ such that, for some $q \geq 2$, the sequence $f(au+b) \pmod{q}$, $u = 0, 1, 2, \ldots$, is ultimately periodic.*

Proof. Suppose there are positive integers a, b and $q \geq 2$ such that $f(au+b) \pmod q$, $u = 0, 1, 2, \ldots$, is ultimately periodic. Then there are $r, \ell \in \mathbb{N}$ such that q divides the difference $f(a(u+\ell)+b) - f(au+b)$ for each $u \geq r$. By the condition of the lemma, there is an integer $v \geq r$ such that $d_u = f(au+b+a\ell) - f(au+b) \leq 1$ for every $u \geq v$. If $d_v = 1$, then q does not divide d_v, a contradiction. Thus $d_v = 0$.

Note that $d_v + d_{v+\ell} + \ldots + d_{v+k\ell} = f(av+b+a(k+1)\ell) - f(av+b)$. Clearly, $\lim_{n\to\infty} f(n) = \infty$ implies that $d_v + d_{v+\ell} + \ldots + d_{v+k\ell} \to \infty$ as $k \to \infty$. Therefore, there exists a positive integer t such that $d_v = d_{v+\ell} = \ldots = d_{v+(t-1)\ell} = 0$ and $d_{v+t\ell} = 1$. Since q divides d_u for every $u \geq v$, it must divide the sum $d_v + d_{v+\ell} + \ldots + d_{v+(t-1)\ell} + d_{v+t\ell} = 1$, a contradiction. □

It is easy to see that the functions $f(n) = [\gamma \log n]$, $f(n) = [\alpha n^\sigma]$, where $\alpha, \gamma > 0$ and $0 < \sigma < 1$, satisfy the conditions of the lemma. (Of course, the fact that several first values of f can be zero makes no difference in our arguments.) Hence, by Theorem 3 and the remark following its proof, the sequences given by $x_1 \in \mathbb{Z}$ and, for $n \geq 1$,

$$x_{n+1} = x_n^{[\gamma \log n]} + 1 \text{ or } x_{n+1} = x_n^{[\alpha n^\sigma]} + 1$$

are ultimately periodic modulo $m \in \mathbb{N}$, if and only if, $m = 2^s$ with some integer $s \geq 0$.

In conclusion, let us consider the sequence $x_1 = 0$, $x_{n+1} = x_n^n + 1$ for $n = 1, 2, 3, \ldots$. The sequence $x_n \pmod 3$, $n = 1, 2, 3, \ldots$, is $0, 1, 2, 0, 1, 2, \ldots$, so it is purely periodic. By the main lemma of [2], the limit $\zeta = \lim_{n\to\infty} x_n^{1/n!}$ exists, it is a transcendental number, and, furthermore, $[\zeta^{n!}] = x_n$ for every $n \in \mathbb{N}$. Hence the sequence $[\zeta^{n!}]$, $n = 1, 2, 3, \ldots$, has infinitely many elements of the form $3k_0$, $3k_1 + 1$ and $3k_2 + 2$, where $k_0, k_1, k_2 \in \mathbb{N}$.

References

[1] S. Akiyama, H. Brunotte, A. Pethö and W. Steiner, *Remarks on a conjecture on certain integer sequences,* Period. Math. Hungar. **52** (2006), 1–17.

[2] G. Alkauskas and A. Dubickas, *Prime and composite numbers as integer parts of powers,* Acta Math. Hung. **105** (2004), 249–256.

[3] A. Dubickas, *Divisibility properties of some recurrent sequences,* Zapiski Nauchn. Semin. POMI **322** (2005), 76–82. (*Reprinted in:* J. Math. Sciences **137** (2006), 4654–4657.)

[4] A. Dubickas, *On the powers of some transcendental numbers,* Bull. Austral. Math. Soc. **76** (2007), 433–440.

[5] A. Dubickas and A. Novikas, *Integer parts of powers of rational numbers,* Math. Z. **251** (2005), 635–648.

[6] R.K. Guy, *Unsolved problems in number theory,* Springer-Verlag, New York, 1994.

[7] O. Strauch and Š. Porubský, *Distribution of sequences: A sampler,* Schriftenreihe der Slowakischen Akademie der Wissenschaften 1, Peter Lang, Frankfurt, 2005.

[8] H. Weyl, *Über die Gleichverteilung von Zahlen modulo Eins,* Math. Ann. **77** (1916), 313–352.