Записки научных
семинаров ПОМИ
Том 322, 2005 г.

**A. Dubickas**

# DIVISIBILITY PROPERTIES OF CERTAIN RECURRENT SEQUENCES

Abstract. Let $g$ and $m$ be two positive integers, and let $F$ be a polynomial with integer coefficients. We show that the recurrent sequence $x_0 = g$, $x_n = x_{n-1}^n + F(n)$, $n = 1, 2, 3, \ldots$, is periodic modulo $m$. Then a special case, with $F(z) = 1$ and with $m = p > 2$ being a prime number, is considered. We show, for instance, that the sequence $x_0 = 2$, $x_n = x_{n-1}^n + 1$, $n = 1, 2, 3, \ldots$, has infinitely many elements divisible by every prime number $p$ which is less than or equal to 211 except for three prime numbers $p = 23, 47, 167$ that do not divide $x_n$. These recurrent sequences are related to the construction of transcendental numbers $\zeta$ for which the sequences $[\zeta^{n!}]$, $n = 1, 2, 3, \ldots$, have some nice divisibility properties.

## 1. Introduction

There are several unsolved problems concerning the sequence $[\alpha^n]$, $n = 1, 2, 3, \ldots$, where $\alpha > 1$ is a fixed real number and where $[x]$ stands for the integral part of a real number $x$. It is indeed surprising that some of them are unsolved. For instance, if $\alpha$ is not an integer, even a simple question like whether the sequence $[\alpha^n]$, $n = 1, 2, 3, \ldots$, contains infinitely many *composite* numbers or not remains unsolved except for very few special cases. Of course, it is expected that there are infinitely many composite numbers of the form $[\alpha^n]$, $n \in \mathbb{N}$, for every $\alpha > 1$. See [12], where this was proved for $\alpha = 3/2$, $\alpha = 4/3$ and [10], where this result was proved for $\alpha = 5/4$. No other rational noninteger number $\alpha$ for which the sequence $[\alpha^n]$, $n = 1, 2, 3, \ldots$, is proved to contain infinitely many composite numbers is known. See also [6–8] for some other results in this direction concerning algebraic irrational numbers $\alpha$. Problem E19 in [13] raises the question whether the sequence $[\alpha^n]$, $n = 1, 2, 3, \ldots$, where $\alpha$ is a rational noninteger number, contains infinitely many *prime* numbers. Naturally, this problem is expected to be even more difficult. It

This research was supported in part by the Lithuanian State Studies and Science Foundation.

remains unsolved: not a single $\alpha$ with this property is known. However, see [16, 18], and [3] for some existence results.

One should remark that metrical results are well-known. They are not difficult to obtain and follow from an old work of Koksma [14]: for every $\xi \neq 0$, the sequence of fractional parts $\{\xi\alpha^n\}$, $n = 1, 2, 3, \ldots$, is uniformly distributed in the interval $[0, 1)$ for almost all $\alpha > 1$. Applying this result to $\xi = 1/2$, we see easily that, for such $\alpha$, $\{\alpha^n/2\} < 1/2$ for infinitely many $n$. So the sequence $[\alpha^n]$, $n = 1, 2, 3, \ldots$, has infinitely many even numbers for almost all $\alpha > 1$. (See also [4] for more recent metrical results.) Hence the results for integral parts are closely related to corresponding results for fractional parts. See, e.g., [1, 2, 5, 9, 11, 15, 17] for some results concerning the distribution of fractional parts $\{\xi\alpha^n\}$, $n = 1, 2, 3, \ldots$.

These few results concerning prime and composite numbers of the form $[\alpha^n]$ with explicit $\alpha$ which were known before have been proved for algebraic numbers $\alpha$ only. Recently, in [3] we constructed certain explicit transcendental numbers $\zeta$ for which not only $[\zeta^n]$ was proved to be composite for infinitely many integer $n$, but also some other arithmetical properties of the set $[\zeta^n]$, $n \in \mathbb{N}$, have been analyzed. We obtained such $\zeta$ as follows. Let $x_0$ be a positive integer and let $x_n = x_{n-1}^n + a_n$ for $n = 1, 2, 3, \ldots$, where $a_n$ is a sequence of nonnegative integers which increases not too fast. It is proved in [3] that $x_n^{1/n!}$ tends to a limit, say $\zeta$, and that this limit $\zeta$ is a transcendental number. Furthermore, it was shown that $[\zeta^{n!}] = x_n$ for every $n \in \mathbb{N}$. Therefore, the analysis of the arithmetical properties of the subsequence $[\zeta^{n!}]$, $n = 1, 2, \ldots$, of the sequence $[\zeta^n]$, $n = 1, 2, \ldots$, is, in fact, the analysis of the arithmetical properties of the sequence $x_n$, $n = 0, 1, 2, \ldots$. In particular, we took in [3] $x_0 = 2$ and $a_n = 2$ or $a_n = n - 1$. With the latter choice, one can easily show (which was done in [3]) that the sequence $x_n = x_{n-1}^n + n - 1$, $n = 1, 2, 3, \ldots$, has infinitely many elements divisible by every prime number $p$.

The sequences of this form seem to be of independent interest too. In this note, we further consider their divisibility properties. Suppose that $x_0$ and $m > 1$ are integers. Let also $F(z)$ be an arbitrary polynomial with integer coefficients. In the next section, we prove that the sequence $x_n = x_{n-1}^n + F(n)$, $n = 1, 2, 3, \ldots$, is ultimately periodic modulo $m$ and give upper bounds for the length of the period and for the length of the pre-periodic part. (Recall that the sequence $s_1, s_2, s_3, \ldots$ is called *ultimately periodic* if there is a $t \in \mathbb{N}$ such that $s_{n+t} = s_n$ for every sufficiently large integer $n$.) In Sec. 3, setting $F(z) = 1$, we analyze which

prime numbers $p$ occur as divisors of $x_n$ for infinitely many $n$. When we consider the sequence $x_0 = 2$, $x_n = x_{n-1}^n + 1$, $n = 1, 2, 3, \ldots$, the set of such primes seems to be nontrivial. There are just three exceptional primes $p = 23, 47, 167$ among the primes that do not exceed 211 which do not occur as divisors of this sequence.

## 2. Periodicity

**Theorem 1.** *Let $x_0$ and $m > 1$ be two integers and let $F(z)$ be an arbitrary polynomial with integer coefficients. Then the sequence defined by the recurrent relation $x_n = x_{n-1}^n + F(n)$, $n = 1, 2, 3, \ldots$, is ultimately periodic modulo $m$.*

**Proof.** Let $D_m$ be the set of divisors of $m$ greater than 1. For instance, $D_{12} = \{2, 3, 4, 6, 12\}$. Write $\ell(m)$ for the least common multiple of $m$ and the numbers $\varphi(d)$, where $d$ runs over every element of $D_m$. Here, $\varphi$ stands for Euler's function. In particular, $\ell(12) = 12$, because $\varphi(2) = 1$, $\varphi(3) = \varphi(4) = \varphi(6) = 2$ and $\varphi(12) = 4$.

Now, let $s$ be an integer greater than $\log_2 m$, e.g., $s = [\log_2 m] + 1$. We consider the sequence $x_{s+k\ell(m)}$, $k = 0, 1, 2, \ldots$, modulo $m$. Take two terms in this sequence, say, $x_t$ and $x_{t+u\ell(m)}$ which are equal modulo $m$. (It is possible to choose $u \leqslant m$ and $t \leqslant s + m = m + [\log_2 m] + 1$.) We claim that then $x_{n+u\ell(m)} - x_n$ is divisible by $m$ for each $n \geqslant t$, so the sequence $x_n$, $n = 1, 2, 3, \ldots$, modulo $m$ is ultimately periodic, as claimed. (Furthermore, the above bounds would imply that its period is of length $\leqslant m\ell(m)$ and its pre-periodic part is of length $\leqslant m + [\log_2 m] + 1$.)

The divisibility of $x_{n+u\ell(m)} - x_n$ by $m$ is proved by induction on $n$. By the above, this is the case for $n = t$. Assume that it holds for $n := n - 1$, that is, $x_{n-1}$ and $x_{n-1+u\ell(m)}$ are both equal modulo $m$, say, both equal to $r$ modulo $m$, where $0 \leqslant r \leqslant m - 1$. Note that $F(n + u\ell(m)) - F(n)$ is divisible by $m$, because $m | \ell(m)$. Hence, from the equalities

$$x_{n+u\ell(m)} = x_{n-1+u\ell(m)}^{n+u\ell(m)} + F(n + u\ell(m))$$

and $x_n = x_{n-1}^n + F(n)$, using $m | (F(n + u\ell(m)) - F(n))$, we derive that $x_{n+u\ell(m)} - x_n$ modulo $m$ is equal to

$$r^{n+u\ell(m)} - r^n = r^n(r^{u\ell(m)} - 1)$$

modulo $m$. We see immediately that it is zero modulo $m$ if $r = 0$. Assume that $r > 0$. Write

$$r = r' p_1^{u_1} \ldots p_k^{u_k}, \qquad m = m' p_1^{v_1} \ldots p_k^{v_k},$$

where $p_1, \ldots, p_k$ are prime numbers, $u_1, \ldots, u_k, v_1, \ldots, v_k \geqslant 1$, $\gcd(r'm', p_1 p_2 \ldots p_k) = 1$, and $\gcd(r', m') = 1$.

Since $n \geqslant t \geqslant s > \log_2 m$, we have $p_i^{u_i n} \geqslant p_i^n \geqslant 2^n > m \geqslant p_i^{v_i}$. Hence the number $r^n$ is divisible by $p_1^{u_1} p_2^{u_2} \ldots p_k^{u_k}$. It remains to show that the number $r^{u\ell(m)} - 1$ is divisible by $m'$. Indeed, $\gcd(m', r) = 1$, so, by Euler's theorem, $r^{\varphi(m')} - 1$ is divisible by $m'$. But $\varphi(m')$ divides $\ell(m)$, so $r^{u\ell(m)} - 1$ is divisible by $m'$, as claimed. This completes the proof of the theorem. □

## 3. Divisibility of a sequence of shifted powers

In this section, we consider the sequence

$$x_0 = g, \quad x_n = x_{n-1}^n + 1, \quad n = 1, 2, 3, \ldots.$$

Given a prime number $p$, is it true that this sequence contains infinitely many elements divisible by $p$? In general, the answer is "no", but the exceptional primes occur rarely. Evidently, this sequence has infinitely many even elements for any $g$, so assume that $p > 2$. We will write $X_g(p)$ for the string $x_0, x_1, \ldots, x_{p-2}$ modulo $p$. For instance, $X_4(5)$ is the string (or list) $4, 0, 1, 2$. Let also $e(X_g(p))$ be the last element of the list $X_g(p)$, so that $e(X_4(5)) = 2$. Sometimes, when it is clear (like in Theorem 2 below), we shall write for brevity $X_g$ instead of $X_g(p)$.

**Theorem 2.** *Assume that $p > 2$ is a prime number and $0 \leqslant g \leqslant p - 1$. The sequence $x_0 = g$, $x_n = x_{n-1}^n + 1$, $n = 1, 2, \ldots$, modulo $p$ is*

(1) $X_g X_2 X_2 X_2 X_2 \ldots$, *if* $e(X_g) \neq 0$, $e(X_2) \neq 0$;
(2) $X_g X_2 X_1 X_1 X_1 X_1 \ldots$, *if* $e(X_g) \neq 0$, $e(X_2) = 0$, $e(X_1) = 0$;
(3) $X_g X_2 X_1 X_2 X_1 X_2 X_1 X_2 X_1 \ldots$, *if* $e(X_g) \neq 0$, $e(X_2) = 0$, $e(X_1) \neq 0$;
(4) $X_g X_1 X_2 X_2 X_2 X_2 \ldots$, *if* $e(X_g) = 0$, $e(X_1) \neq 0$, $e(X_2) \neq 0$;
(5) $X_g X_1 X_1 X_1 X_1 \ldots$, *if* $e(X_g) = 0$, $e(X_1) = 0$;
(6) $X_g X_1 X_2 X_1 X_2 X_1 X_2 X_1 X_2 \ldots$, *if* $e(X_g) = 0$, $e(X_1) \neq 0$, $e(X_2) = 0$.

**Proof.** The sequence $x_0, x_1, x_2, \ldots$ modulo $p$ begins with $X_g$, by the definition of $X_g = X_g(p)$. The last element of the list $X_g$ is either nonzero or zero. Suppose first that it is nonzero, i.e., $e(X_g) \neq 0$. Then, by the Little Fermat theorem, $x_{p-1} = x_{p-2}^{p-1} + 1$ is equal to 2 modulo $p$. Similarly, $x_p = x_{p-1}^p + 1$ is equal to 3 modulo $p$ and so on. Using the fact that $b^{p-1+k}$ is equal to $b^k$ modulo $p$ for each $k \geqslant 1$, we get the next string $X_2$ (after $X_g$). Now, if $e(X_2) \neq 0$, the next element $x_{2(p-1)} = x_{2(p-1)-1}^{2(p-1)} + 1$ is

equal to 2 modulo $p$. So, as above, the next string is $X_2$ again, and so on. This proves (1). If however $e(X_2)=0$, then $x_{p-1}=x_{p-2}^{p-1}+1$ is equal to 1 modulo $p$. Then the next string after $X_gX_2$ is $X_1$. Now, further sequence depends on whether $e(X_1)$ is equal to zero or not. Suppose that $e(X_1)\neq 0$. Then, we further compute $x_{2(p-1)}=x_{2(p-1)-1}^{2(p-1)}+1$ which is equal to 2 modulo $p$. Hence the next string is $X_2$. Now, as $e(X_2)=0$, the next string is $X_1$, then $X_2$ again, because $e(X_1)\neq 0$, and so on. In this way we get the sequence $X_gX_2X_1X_2X_1X_2X_1\ldots$; this proves (3). Alternatively, if $e(X_1)=0$, we obtain $X_gX_2X_1X_1X_1\ldots$, that is, case (2).

Cases (4)–(6) corresponding to $e(X_g)=0$ (so the next string after $X_g$ being $X_1$), are obtained as above. □

For instance, applying Theorem 2 to $g=2$ and $p=3$, we obtain case (6) of the theorem, namely, that $x_0,x_1,x_2,x_3,\ldots$ modulo 3 is the following purely periodic sequence $2,0,1,2,2,0,1,2,2,0,1,2,\ldots$ (with period 4).

Of course, the "generic" situation is that $e(X_g)\neq 0$. So, case (1) is the "generic" case of Theorem 2. In particular, we have the following corollary.

**Corollary 3.** *Suppose that $p>3$ is a prime number, and let $x_0=2$, $x_n=x_{n-1}^n+1$, $n=1,2,3\ldots$. Suppose that $x_{p-2}$ is not divisible by $p$. Then the sequence $x_0,x_1,x_2,\ldots$ contains either infinitely many elements divisible by $p$ (precisely when $x_1x_2\ldots x_{p-3}$ is divisible by $p$) or it contains no elements divisible by $p$ (precisely when $x_1x_2\ldots x_{p-3}$ is not divisible by $p$).*

Indeed, $x_{p-2}$ is not divisible by $p$ iff $e(X_2)\neq 0$. So, by part (1) of Theorem 2, the sequence $x_0,x_1,x_2,\ldots$ modulo $p$ is $X_2X_2X_2\ldots$, where $X_2$ is the string $x_0,x_1,\ldots,x_{p-2}$ modulo $p$. This implies the corollary.

We computed the sets $X_2(p)$ for every prime number $p\leqslant 211$. For every such $p\geqslant 5$ we found that $x_{p-2}$ is not divisible by $p$. All lists $X_2(p)$, that is, the elements $x_0,x_1,\ldots,x_{p-2}$ modulo $p$ contain at least one zero element except when $p=23,47,167$. For instance, for $p=23$, the list $X_2(23)$ is

$$2,3,10,12,14,16,5,18,17,8,4,2,3,10,13,19,13,7,19,15,10,8.$$

Hence the recurrent sequence $x_0=2$, $x_n=x_{n-1}^n+1$, $n=1,2,\ldots$, contains infinitely many elements of the form $23k+l$, where

$$l\in\{2,3,4,5,7,8,10,12,13,14,15,16,17,18,19\},$$

and no elements of the form $23k + l$, where

$$l \in \{0, 1, 6, 9, 11, 20, 21, 22\},$$

at all.

We conclude with the following two questions concerning the sequence $x_0 = 2$, $x_n = x_{n-1}^n + 1$, $n = 1, 2, 3, \ldots$:

**Question 4.** *Is there a prime number $p > 3$ such that $p | x_{p-2}$?*

**Question 5.** *Is the set of prime numbers $p \in \{23, 47, 167, \ldots\}$ that do not divide the product $x_1 x_2 \ldots x_{p-2}$ finite or infinite?*

## References


1. S. D. Adhikari, P. Rath, N. Saradha, *On the sets of uniqueness of the distribution function of $\{\xi(p/q)^n\}$.* (submitted).
2. S. Akiyama, C. Frougny, J. Sakarovitch, *On number representation in a rational base.* (submitted).
3. G. Alkauskas, A. Dubickas, *Prime and composite numbers as integer parts of powers.* — Acta Math. Hung. **105** (2004), 249–256.
4. R. C. Baker, G. Harman, *Primes of the form $[c^p]$.* — Math. Zeitschr. **221** (1996), 73–81.
5. Y. Bugeaud, *Linear mod one transformations and the distribution of fractional parts $\{\xi(p/q)^n\}$.* — Acta Arith. **114** (2004), 301–311.
6. D. Cass, *Integer parts of powers of quadratic units.* — Proc. Amer. Math. Soc. **101** (1987), 610–612.
7. A. Dubickas, *Integer parts of powers of Pisot and Salem numbers.* — Archiv der Math. **79** (2002), 252–257.
8. A. Dubickas, *Sequences with infinitely many composite numbers.* — in: Analytic and Probabilistic Methods in Number Theory, Palanga, 2001 (eds. A. Dubickas et al.), TEV, Vilnius (2002), pp. 57–60.
9. A. Dubickas, *Arithmetical properties of powers of algebraic numbers.* — Bull. London Math. Soc. (to appear).
10. A. Dubickas, A. Novikas, *Integer parts of powers of rational numbers.* — Math. Zeitschr. (to appear).
11. L. Flatto, J. C. Lagarias, A. D. Pollington, *On the range of fractional parts $\{\xi(p/q)^n\}$.* — Acta Arith. **70** (1995), 125–147.
12. W. Forman, H. N. Shapiro, *An arithmetic property of certain rational powers.* — Comm. Pure Appl. Math. **20** (1967), 561–573.
13. R. K. Guy, *Unsolved Problems in Number Theory.* — Springer–Verlag, New York (1994).
14. J. F. Koksma, *Ein mengen-theoretischer Satz über Gleichverteilung modulo eins.* — Compositio Math. **2** (1935), 250–258.
15. K. Mahler, *An unsolved problem on the powers of 3/2.* — J. Austral. Math. Soc. **8** (1968), 313–321.

16. H. W. Mills, *A prime representing function.* — Bull. Amer. Math. Soc. **53** (1947), 604.
17. T. Vijayaraghavan, *On the fractional parts of the powers of a number.* — J. London Math. Soc. **15** (1940), 159–160.
18. E. M. Wright, *A prime representing function.* — Amer. Math. Monthly **58** (1951), 616–618.

Department of Mathematics
and Informatics Vilnius University

Institute of Mathematics and Informatics
Lithuania

*E-mail*: arturas.dubickas@maf.vu.lt

Поступило 5 марта 2005 г.