ON THE CYCLE STRUCTURE OF REPEATED EXPONENTIATION MODULO A PRIME POWER

MIN SHA

Abstract. We obtain some results about the repeated exponentiation modulo a prime power from the viewpoint of arithmetic dynamical systems. In particular, we extend two asymptotic formulas about periodic points and tails in the case of modulo a prime to the case of modulo a prime power.

1. Introduction

For a positive integer M, denote by $\mathbb{Z}/M\mathbb{Z}$ the residue ring of $\mathbb{Z}$ modulo M and $(\mathbb{Z}/M\mathbb{Z})^*$ the unit group. For an integer $k \geq 2$, we consider the following endomorphism of $(\mathbb{Z}/M\mathbb{Z})^*$,

$$f\colon (\mathbb{Z}/M\mathbb{Z})^* \to (\mathbb{Z}/M\mathbb{Z})^*,\ x \to x^k.$$

For any initial value $x \in (\mathbb{Z}/M\mathbb{Z})^*$, we repeat the action of f, then we get a sequence

$$x_0 = x,\ x_n = x_{n-1}^k,\ n = 1, 2, 3, \ldots.$$

This sequence is known as the power generator of pseudorandom numbers. Studying such sequences in the cases that M is a prime or a product of two distinct primes, is of independent interest and is also important for several cryptographic applications, see [1, 6]. From the viewpoint of cryptography, there are numerous results about these sequences, see the papers mentioned in [2], more recently see [3] and its references.

If we view $(\mathbb{Z}/M\mathbb{Z})^*$ as a vertex set and draw a directed edge from a to b if $f(a) = b$, then we get a digraph. There are also many results in this direction, see [12] and the papers mentioned there, more recently see [8, 9, 10, 11].

As in [2], in this article we will study $(\mathbb{Z}/M\mathbb{Z})^*$ under the action of f from the viewpoint of arithmetic dynamical systems, where M is a prime power. Specifically we will extend two asymptotic formulas in [2] to the case of modulo a prime power.

It is easy to see that for any initial value $x \in (\mathbb{Z}/M\mathbb{Z})^*$ the corresponding sequence becomes eventually periodic, that is, for some positive integer $s_{k,M}(x)$ and *tail* $t_{k,M}(x) < s_{k,M}(x)$, the elements $x_0 = x$, x_1, $\ldots$, $x_{s_{k,M}(x)-1}$ are pairwise distinct and $x_{s_{k,M}(x)} = x_{t_{k,M}(x)}$. So we can define a *tail function* $t_{k,M}$ on $(\mathbb{Z}/M\mathbb{Z})^*$.

The sequence $x_{t_{k,M}(x)}, \ldots, x_{s_{k,M}(x)-1}$, ordered up to a cyclic shift, is called a *cycle*. The *cycle length* is $c_{k,M}(x) = s_{k,M}(x) - t_{k,M}(x)$. The elements in the cycle are called *periodic points* and their *periods* are $c_{k,M}(x)$. So we can define a *cycle length function* $c_{k,M}$ on $(\mathbb{Z}/M\mathbb{Z})^*$. In particular, [4, 5] gave lower bounds for the largest period.

We denote by $P_r(k, M)$ and $P(k, M)$, respectively the number of periodic points with period r and the number of periodic points in $(\mathbb{Z}/M\mathbb{Z})^*$. Also, we denote by $C_r(k, M)$ and $C(k, M)$, respectively the number of cycles with length r and the number of cycles in $(\mathbb{Z}/M\mathbb{Z})^*$. We denote the average values of $c_{k,M}(x)$ and $t_{k,M}(x)$ over all $x \in (\mathbb{Z}/M\mathbb{Z})^*$ by $c(k, M)$ and $t(k, M)$, respectively,

$$c(k,M)=\frac{1}{\varphi(M)}\sum_{x\in(\mathbb{Z}/M\mathbb{Z})^*}c_{k,M}(x), \qquad t(k,M)=\frac{1}{\varphi(M)}\sum_{x\in(\mathbb{Z}/M\mathbb{Z})^*}t_{k,M}(x),$$

where φ is the Euler totient function.

When M is an odd prime power, we will derive explicit formulas for $P_r(k,M)$ and $C_r(k,M)$ by the results in [10], and we will also derive explicit formulas for $c(k,M)$ and $t(k,M)$ which generalize those in [11].

For two integers $r,m\geq 1$, we call

$$\lim_{X\to\infty}\frac{1}{\pi(X)}\sum_{p\leq X}P_r(k,p^m)$$

the asymptotic mean number of periodic points with period r in $(\mathbb{Z}/p^m\mathbb{Z})^*$ for different choices of prime p, and we denote it by $AP_r(k,m)$. Similarly, we can define the asymptotic mean number for cycles with length r and denote it by $AC_r(k,m)$. We will derive explicit formulas for $AP_r(k,m)$ and $AC_r(k,m)$.

For an integer $m\geq 1$, following [11], we study the average values of $P(k,p^m)$ and $t(k,p^m)$ over all primes $p\leq N$,

$$S_0(k,m,N)=\frac{1}{\pi(N)}\sum_{p\leq N}P(k,p^m), \qquad S(k,m,N)=\frac{1}{\pi(N)}\sum_{p\leq N}t(k,p^m).$$

where, as usual, $\pi(N)$ is the number of primes $p\leq N$. Following the method in [2], we will get asymptotic formulas for $S_0(k,m,N)$ and $S(k,m,N)$.

2. Preparations

For two integers l and n, we denote their greatest common divisor by $\gcd(l,n)$. For a positive integer n, we denote by $\tau(n)$ the number of its positive divisors. Theorem 4.9 in [7] tells us that

$$\lim_{X\to\infty}\frac{1}{\pi(X)}\sum_{p\leq X}\gcd(p-1,n)=\tau(n). \tag{2.1}$$

For two integers $m\geq 1$ and $n\geq 2$, we denote the largest prime divisor of n by q. Then we have

$$\begin{aligned}
&\lim_{X\to\infty}\frac{1}{\pi(X)}\sum_{p\leq X}\gcd(p^{m-1}(p-1),n)\\
&=\lim_{X\to\infty}\frac{1}{\pi(X)}\sum_{q<p\leq X}\gcd(p^{m-1}(p-1),n)\\
&=\lim_{X\to\infty}\frac{1}{\pi(X)}\sum_{q<p\leq X}\gcd(p-1,n)\\
&=\tau(n).
\end{aligned} \tag{2.2}$$

Notice that if p is an odd prime, $\gcd(p^m-p^{m-1},n)$ is the number of solutions of the equation $x^n=1$ in $(\mathbb{Z}/p^m\mathbb{Z})^*$.

Given two integers a and n with $\gcd(a,n)=1$, following the method in the proof of formula (2) in [2], we can get

$$\sum_{\substack{p\le X\\ p\equiv a \pmod n}} p^m = \frac{X^{m+1}}{(m+1)\varphi(n)\ln X} + O(X^{m+1}\ln^{-2}X). \tag{2.3}$$

Then we have

$$\sum_{\substack{p\le X\\ p\equiv a \pmod n}} p^{m-1}(p-1) = \frac{X^{m+1}}{(m+1)\varphi(n)\ln X} + O(X^{m+1}\ln^{-2}X). \tag{2.4}$$

Following the same method in the proof of formula (4) in [2], we have

$$\sum_{\substack{p\le X\\ p\equiv a \pmod n}} p^{m-1}(p-1) = O\left(\frac{X^{m+1}}{n} + X^m\right). \tag{2.5}$$

3. Main Results

For two integers d and n satisfying $\gcd(d,n)=1$, we denote the multiplicative order of n modulo d by $\mathrm{ord}_d n$. For an integer n and a prime p, we denote $v_p(n)$ the exact power of p dividing n.

Let μ be the Möbius function. For a real number a, we denote $\lceil a\rceil$ the least integer which is not less than a.

Write $k=p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}\ge 2$, where $p_1,\dots,p_s$ are distinct primes, $p_1<p_2<\cdots<p_s$ and $n_1,\dots,n_s\ge 1$. Let m be a fixed positive integer.

Proposition 3.1. *Let p be an odd prime and r be a positive integer. Write $p^m-p^{m-1}=p_1^{r_1}\cdots p_s^{r_s}\cdot\rho$, where $r_1,\dots,r_s\ge 0$ are integers and $\gcd(p_1\dots p_s,\rho)=1$. We have*

(1) $C_r(k,p^m)=\frac{1}{r}\sum_{d\mid r}\mu(d)\gcd(p^m-p^{m-1},k^{r/d}-1)$.
(2) $P_r(k,p^m)=\sum_{d\mid r}\mu(d)\gcd(p^m-p^{m-1},k^{r/d}-1)$.
(3) $P(k,p^m)=\rho$.
(4) $C(k,p^m)=\sum_{d\mid\rho}\frac{\varphi(d)}{\mathrm{ord}_d k}$.
(5) *For any $x\in(\mathbb{Z}/p^m\mathbb{Z})^*$, denote $\mathrm{ord}_{p^m}x$ by $\mathrm{ord}x$, $c_{k,p^m}(x)=\mathrm{ord}_{\gcd(\mathrm{ord}x,\rho)}k$.*
(6) $c(k,p^m)=\frac{1}{\rho}\sum_{d\mid\rho}\varphi(d)\mathrm{ord}_d k$.
(7) *For any $x\in(\mathbb{Z}/p^m\mathbb{Z})^*$, denote $\mathrm{ord}_{p^m}x$ by $\mathrm{ord}x$,*

$$t_{k,p^m}(x)=\max\left\{\left\lceil\frac{v_{p_1}(\mathrm{ord}x)}{n_1}\right\rceil,\left\lceil\frac{v_{p_2}(\mathrm{ord}x)}{n_2}\right\rceil,\dots,\left\lceil\frac{v_{p_s}(\mathrm{ord}x)}{n_s}\right\rceil\right\}.$$

(8) $t(k,p^m)=\frac{1}{p_1^{r_1}\cdots p_s^{r_s}}\sum_{d\mid p_1^{r_1}\cdots p_s^{r_s}}\varphi(d)\max\left\{\left\lceil\frac{v_{p_1}(d)}{n_1}\right\rceil,\dots,\left\lceil\frac{v_{p_s}(d)}{n_s}\right\rceil\right\}$.

Proof. (1) and (2) By Möbius inversion formula and Theorem 5.6 in [10].
(3) A special case of Corollary 3 in [12].
(4) By Theorem 2 and Theorem 3 in [12].
(5) By Lemma 3 and Theorem 2 in [12].

(6) Denote $p_1^{r_1}\cdots p_s^{r_s}$ by w, from (5), we have

$$\begin{aligned} c(k,p^m) &= \frac{1}{p^m-p^{m-1}} \sum_{x\in(\mathbb{Z}/p^m\mathbb{Z})^*} c_{k,p^m}(x) \\ &= \frac{1}{p^m-p^{m-1}} \sum_{d|\rho}\sum_{n|w} \varphi(dn)\mathrm{ord}_d k \\ &= \frac{1}{p^m-p^{m-1}} \sum_{n|w}\varphi(n) \sum_{d|\rho} \varphi(d)\mathrm{ord}_d k = \frac{1}{\rho}\sum_{d|\rho}\varphi(d)\mathrm{ord}_d k. \end{aligned}$$

(7) Let w_x be the factor of ord$x$ such that $\frac{\mathrm{ord}x}{w_x}$ is the largest factor relatively prime to k. By Lemma 3 in [12], we have $t_{k,p^m}(x)$ is the least non-negative integer l such that $w_x|k^l$. In other words, $t_{k,p^m}(x)$ is the least non-negative integer l such that $v_{p_i}(\mathrm{ord}\ x) \le l n_i$, for any $1 \le i \le s$. Then we get the desired result.

(8) Notice that for any $x \in (\mathbb{Z}/p^m\mathbb{Z})^*$, $\mathrm{ord}x|(p^m-p^{m-1})$, and there are $\varphi(\mathrm{ord}x)$ elements with the order ord$x$. By (7), we have

$$t(k,p^m) = \frac{1}{p^m-p^{m-1}} \sum_{d|(p^m-p^{m-1})} \varphi(d)\max\left\{\left\lceil\frac{v_{p_1}(d)}{n_1}\right\rceil, \left\lceil\frac{v_{p_2}(d)}{n_2}\right\rceil, \dots, \left\lceil\frac{v_{p_s}(d)}{n_s}\right\rceil\right\}.$$

Furthermore, we have

$$\begin{aligned} t(k,p^m) &= \frac{1}{p^m-p^{m-1}} \sum_{d|p_1^{r_1}\dots p_s^{r_s}\rho} \varphi(d)\max\left\{\left\lceil\frac{v_{p_1}(d)}{n_1}\right\rceil, \dots, \left\lceil\frac{v_{p_s}(d)}{n_s}\right\rceil\right\} \\ &= \frac{1}{p^m-p^{m-1}} \sum_{i_1=0}^{r_1}\cdots\sum_{i_s=0}^{r_s}\sum_{d|\rho} \varphi(p_1^{i_1}\cdots p_s^{i_s}d)\max\left\{\left\lceil\frac{i_1}{n_1}\right\rceil, \dots, \left\lceil\frac{i_s}{n_s}\right\rceil\right\} \\ &= \frac{1}{p^m-p^{m-1}} \sum_{d|\rho}\varphi(d) \sum_{i_1=0}^{r_1}\cdots\sum_{i_s=0}^{r_s} \varphi(p_1^{i_1}\cdots p_s^{i_s})\max\left\{\left\lceil\frac{i_1}{n_1}\right\rceil, \dots, \left\lceil\frac{i_s}{n_s}\right\rceil\right\} \\ &= \frac{1}{p_1^{r_1}\cdots p_s^{r_s}} \sum_{d|p_1^{r_1}\cdots p_s^{r_s}} \varphi(d)\max\left\{\left\lceil\frac{v_{p_1}(d)}{n_1}\right\rceil, \dots, \left\lceil\frac{v_{p_s}(d)}{n_s}\right\rceil\right\}. \end{aligned}$$

□

Remark 3.2. If we put $k = 2$ and $m = 1$, then the formulas (3), (4), (6), and (8) correspond to Theorem 6 in [11].

Remark 3.3. Since the conclusions in [10] and [12] are about the general case of modulo a positive integer, it is easy to get similar formulas for the case of $p = 2$.

Proposition 3.4. *Let r be a positive integer, we have*

$$AP_r(k,m) = \sum_{d|r}\mu(d)\tau(k^{r/d}-1), \tag{3.1}$$

$$AC_r(k,m) = \frac{1}{r}\sum_{d|r}\mu(d)\tau(k^{r/d}-1). \tag{3.2}$$

Proof. Combining (2.2) and Proposition 3.1 (1) and (2), we can get the desired formulas. □

In the following, we denote by Ω the set of positive $\mathcal{S}$-units with $\mathcal{S} = \{p_1, \ldots, p_s\}$. Here a positive $\mathcal{S}$-unit means a positive integer whose prime divisors all belong to $\mathcal{S}$.

Proposition 3.5. *We have*

$$\lim_{N\to\infty} \frac{S_0(k,m,N)}{N^m} = \frac{1}{m+1}\left(\prod_{i=1}^{s} \frac{p_i^2}{p_i^2-1} - 1\right).$$

Proof. Let $Q = p_1p_2\ldots p_s$ and denote by $\mathcal{U}_Q$ the set of integers $u, 1 \le u \le Q$, and $\gcd(u,Q) = 1$.

For each odd prime p, let ρ_p be the largest divisor of $p^m - p^{m-1}$ coprime to $p_1p_2\ldots p_s$. It is easy to see

$$\lim_{N\to\infty} \frac{S_0(k,m,N)}{N^m} = \lim_{N\to\infty} \frac{1}{N^m\pi(N)} \sum_{p_s<p\le N} \rho_p.$$

Notice that if a prime $p > p_s$, then $v_{p_i}(p^m - p^{m-1}) = v_{p_i}(p-1)$ for any $1 \le i \le s$. Hence, following the method in Theorem 2 of [2], we have

$$\lim_{N\to\infty} \frac{S_0(k,m,N)}{N^m} = \lim_{N\to\infty} \frac{1}{N^m\pi(N)} \sum_{q\in\Omega} q^{-1} \sum_{u\in\mathcal{U}_Q} \sum_{\substack{p\le N \\ p\equiv qu+1 \pmod{qQ}}} (p^m - p^{m-1}).$$

Following the method in Theorem 2 of [2], we have

$$\lim_{N\to\infty} \frac{S_0(k,m,N)}{N^m} = \frac{1}{m+1}\sum_{q\in\Omega}\frac{1}{q^2}.$$

Moreover, we have

$$\begin{aligned}
\sum_{q\in\Omega}\frac{1}{q^2} &= \sum_{i_1,\ldots,i_s=0}^{\infty} \frac{1}{(p_1^{i_1}\cdots p_s^{i_s})^2} - 1\\
&= \sum_{i_1=0}^{\infty}\frac{1}{p_1^{2i_1}}\cdots\sum_{i_s=0}^{\infty}\frac{1}{p_s^{2i_s}} - 1\\
&= \prod_{i=1}^{s}\frac{p_i^2}{p_i^2-1} - 1.
\end{aligned}$$

Hence, we get the desired result. □

Corollary 3.6. *We have*

$$\frac{1}{k^2(m+1)} < \lim_{N\to\infty}\frac{S_0(k,m,N)}{N^m} < \frac{2^s-1}{m+1}.$$

Proof. Notice that for any prime p, we have

$$1 + p^{-2} < \frac{p^2}{p^2-1} = 1 + \frac{1}{p^2-1} < 2.$$

□

Given $q = p_1^{r_1}\cdots p_s^{r_s} \in \Omega$, we denote

$$\psi(q) = \frac{1}{q}\sum_{d|q}\varphi(d)\max\left\{\left\lceil\frac{v_{p_1}(d)}{n_1}\right\rceil, \ldots, \left\lceil\frac{v_{p_s}(d)}{n_s}\right\rceil\right\}.$$

Proposition 3.7. *We have*

$$\lim_{N\to\infty} S(k,m,N) = \sum_{q\in\Omega} \frac{\psi(q)}{q}.$$

Proof. Given $q = p_1^{r_1}\cdots p_s^{r_s} \in \Omega$. Suppose $r_1 \geq 1$. We want to estimate $\frac{1}{q}\sum_{d|q}\varphi(d)\left\lceil \frac{v_{p_1}(d)}{n_1}\right\rceil$. For simplicity, we replace p_1, r_1, and n_1 by p, r, and n, respectively. By the division algorithm, we write $r = ln + d$ with $0 \leq d < n$. We have

$$\begin{aligned}
\frac{1}{q}\sum_{d|q}\varphi(d)\left\lceil\frac{v_p(d)}{n}\right\rceil &= \frac{1}{p^r}\sum_{d|p^r}\varphi(d)\left\lceil\frac{v_p(d)}{n}\right\rceil \\
&= \frac{p-1}{p^r}\sum_{i=1}^{r} p^{i-1}\left\lceil\frac{i}{n}\right\rceil \\
&= \frac{p-1}{p^r}\left[\sum_{i=1}^{n} p^{i-1} + \sum_{i=n+1}^{2n} 2p^{i-1} + \cdots + \sum_{i=(l-1)n+1}^{ln} lp^{i-1} + \sum_{i=ln+1}^{ln+d}(l+1)p^{i-1}\right] \\
&= \frac{p^n-1}{p^r}\left[1 + 2p^n + \cdots + lp^{(l-1)n}\right] + \frac{(l+1)p^{ln}(p^d-1)}{p^r} \\
&= \frac{lp^{ln}}{p^r} - \frac{p^{ln}-1}{p^r(p^n-1)} + \frac{(l+1)p^{ln}(p^d-1)}{p^r} \\
&\leq l + (l+1) \leq 3r.
\end{aligned}$$

Hence, we have

$$\begin{aligned}
\psi(q) &\leq \frac{1}{q}\sum_{d|q}\varphi(d)\left(\left\lceil\frac{v_{p_1}(d)}{n_1}\right\rceil + \cdots + \left\lceil\frac{v_{p_s}(d)}{n_s}\right\rceil\right) \\
&\leq 3(r_1 + \cdots + r_s) \qquad (3.3)\\
&\leq \frac{3}{\ln 2}\ln q = O(\ln q).
\end{aligned}$$

Similarly to Proposition 3.5, by Proposition 3.1 (8), we have

$$\lim_{N\to\infty} S(k,m,N) = \lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{q\in\Omega}\psi(q)\sum_{u\in\mathcal{U}_Q}\sum_{\substack{p\leq N\\ p\equiv qu+1 \pmod{qQ}}} 1.$$

Then following the method in Theorem 2 of [2], we can get the desired result. □

Corollary 3.8. *We have*

$$\frac{1}{k} < \lim_{N\to\infty} S(k,m,N) < \frac{5\sqrt{p_1}\cdots\sqrt{p_s}}{(\sqrt{p_1}-1)\cdots(\sqrt{p_s}-1)}.$$

Proof. On one hand we have

$$\begin{aligned}
\sum_{q\in\Omega}\frac{\psi(q)}{q} &> \sum_{i_1\ge n_1,\cdots,i_s\ge n_s}\frac{\varphi(p_1^{i_1}\cdots p_s^{i_s})}{(p_1^{i_1}\cdots p_s^{i_s})^2}\\
&= \frac{(p_1-1)\cdots(p_s-1)}{p_1\cdots p_s}\sum_{i_1\ge n_1}^{\infty}\frac{1}{p_1^{i_1}}\cdots\sum_{i_s\ge n_s}^{\infty}\frac{1}{p_s^{i_s}}\\
&= \frac{1}{k}.
\end{aligned}$$

On the other hand, by (3.3) we have $\psi(q) < 5\ln q$, then we have

$$\begin{aligned}
\sum_{q\in\Omega}\frac{\psi(q)}{q} &< \sum_{q\in\Omega}\frac{5\ln q}{q}\\
&< 5\sum_{q\in\Omega}\frac{1}{\sqrt{q}}\\
&= 5\sum_{i_1=0,\cdots,i_s=0}\frac{1}{\sqrt{p_1^{i_1}\cdots p_s^{i_s}}}\\
&= \frac{5\sqrt{p_1}\cdots\sqrt{p_s}}{(\sqrt{p_1}-1)\cdots(\sqrt{p_s}-1)}.
\end{aligned}$$

□

4. Remarks on the General Case

In this section, we will give some remarks on the case of modulo a positive integer.

We can deduce formulas for $C_r(k,M)$ and $P_r(k,M)$ directly from Theorem 5.6 in [10]. Corollary 3 in [12] has given a formula for $P(k,M)$. We can also derive a formula for $C(K,M)$ directly by applying Theorem 2 and Theorem 3 in [12].

Following the same methods, we can easily determine the cycle length function $c_{k,M}(x)$ and the tail function $t_{k,M}(x)$ on $(\mathbb{Z}/M\mathbb{Z})^*$, then we can get formulas for $c(k,M)$ and $t(k,M)$.

In fact, [12] and [10] can tell us more information about the properties of repeated exponentiation modulo a positive integer.

5. Acknowledgment

We would like to thank Prof. I. E. Shparlinski for suggesting this problem and for his helpful advice.

References

[1] L. Blum, M. Blum, and M. Shub, *A simple unpredictable pseudo-random number generator*, SIAM J. Comp., **15** (1986), 364–383.
[2] W.-S. Chou and I. E. Shparlinski, *On the cycle structure of repeated exponentiation modulo a prime*, J. Number Theory, **107** (2004), 345–356.
[3] E. D. El-Mahassni, *On the distribution of the power generator over a residue ring for parts of the period*, Rev. Mat. Complut., **21** (2008), 319–325.
[4] J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Period of the power generator and small values of Carmichael's function*, Math. Comp., **70** (2001), 1591–1605.
[5] P. Kurlberg and C. Pomerance, *On the period of the linear congruential and power generators*, Acta Arith., **119** (2005), 149–169.

[6] J. C. Lagarias, *Pseudorandom number generators in cryptography and number theory*, Proc. Symp. in Appl. Math., Amer. Math. Soc., Providence, RI, **42** (1990), 115–143.

[7] M. Nilsson, *Cycles of monomials and perturbated monomial p-adic dynamical systems*, Ann. Math. Blaise Pascal, **7.1** (2000), 37–63.

[8] L. Somer and M. Křížek, *Structure of digraphs associated with quadratic congruences with composite moduli*, Discrete Math., **306** (2006), 2174–2185.

[9] L. Somer and M. Křížek, *On semiregular digraphs of the congruence $x^k \equiv y \pmod{n}$*, Comment. Math. Univ. Carolin., **48** (2007), 41–58.

[10] L. Somer and M. Křížek, *On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$*, Discrete Math., **309** (2009), 1999–2009.

[11] T. Vasiga and J. Shallit, *On the iteration of certain quadratic maps over $GF(p)$*, Discrete Math., **277** (2004), 219–240.

[12] B. Wilson, *Power digraphs modulo n*, The Fibonacci Quarterly, **36.3** (1998), 229–239.

MSC2010: 37P35, 11K45, 11B50

Institut de Mathematiques de Bordeaux, Universite Bordeaux 1, 33405 Talence Cedex, France
E-mail address: shamin2010@gmail.com