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. Especially, 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 $(\mathbb{Z}/M\mathbb{Z})^*$,

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

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 [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. Especially 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.

2010 Mathematics Subject Classification. Primary 37P35; Secondary 11K45, 11B50.

Key words and phrases. Repeated powering, Periodic point, Tail, Primes in arithmetic progressions.
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,

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

where $\varphi$ 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 the limit of $\lim_{X \to \infty} \frac{1}{\pi(X)} \sum_{p \leq X} P_r(k, p^m)$ 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 $P_r(k, p^m)$ and $t(k, p^m)$ over all primes $p \leq N$, \[ S_0(k, m, N) = \frac{1}{\pi(N)} \sum_{p \leq N} P(k, p^m), \quad S(k, m, N) = \frac{1}{\pi(N)} \sum_{p \leq N} t(k, p^m). \]

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

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

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

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

\[
(2.3) \quad \sum_{\substack{p \leq X \\ (\text{mod } n) \atop p \mid a}} p^m = \frac{X^{m+1}}{(m+1)\phi(n)\ln X} + O(X^{m+1}\ln^{-2}X).
\]

Then we have

\[
(2.4) \quad \sum_{\substack{p \leq X \\ (\text{mod } n) \atop p \mid a}} p^{m-1}(p-1) = \frac{X^{m+1}}{(m+1)\phi(n)\ln X} + O(X^{m+1}\ln^{-2}X).
\]

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

\[
(2.5) \quad \sum_{\substack{p \leq X \\ (\text{mod } n) \atop p \mid a}} p^{m-1}(p-1) = O\left(\frac{X^{m+1}}{n} + X^m\right).
\]

### 3. Main Results

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

Let \( \mu \) be the Möbius function. For a real number \( a \), we denote \( \lfloor a \rfloor \) the least integer which is not less than \( a \).

Write \( k = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} \geq 2 \), where \( p_1, \ldots, p_s \) are distinct primes, \( p_1 < p_2 < \cdots < p_s \) and \( n_1, \ldots, n_s \geq 1 \). 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 \( r_1, \ldots, r_s \geq 0 \) are integers and \( \gcd(p_1 \cdots p_s, \rho) = 1 \). 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. \( C(k, p^m) = \sum_{d \mid p} \frac{\varphi(d)}{\text{ord}_d k} \).
5. For any \( x \in (\mathbb{Z}/p^m \mathbb{Z})^* \), denote \( \text{ord}_{p^m} x \) by \( \text{ord}_x \), \( c_{k, p^m}(x) = \text{ord}_{\text{gcd}(\text{ord}_x, \rho)} k \).
6. \( c(k, p^m) = \frac{1}{\rho} \sum_{d \mid p} \varphi(d)\text{ord}_d k \).
7. For any \( x \in (\mathbb{Z}/p^m \mathbb{Z})^* \), denote \( \text{ord}_{p^m} x \) by \( \text{ord}_x \),

\[
t_{k, p^m}(x) = \max \left\{ \left\lfloor \frac{v_{p_1}(\text{ord}_x)}{n_1} \right\rfloor, \left\lfloor \frac{v_{p_2}(\text{ord}_x)}{n_2} \right\rfloor, \ldots, \left\lfloor \frac{v_{p_s}(\text{ord}_x)}{n_s} \right\rfloor \right\}.
\]

8. \( t(k, p^m) = \frac{1}{p_1^{r_1} \cdots p_s^{r_s}} \sum_{d \mid p_1^{r_1} \cdots p_s^{r_s}} \varphi(d) \max \left\{ \left\lfloor \frac{v_{p_1}(d)}{n_1} \right\rfloor, \left\lfloor \frac{v_{p_2}(d)}{n_2} \right\rfloor, \ldots, \left\lfloor \frac{v_{p_s}(d)}{n_s} \right\rfloor \right\} \).

**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 \( p_1^{s_1} \cdots p_r^{s_r} \) by \( w \), from (5), we have

\[
c(k, p^m) = \frac{1}{p^m - p^{m-1}} \sum_{x \in (\mathbb{Z}/p^m \mathbb{Z})^*} c_{k, p^m}(x)
\]

\[
= \frac{1}{p^m - p^{m-1}} \sum_{d|p^m} \sum_{n|w} \phi(d) \text{ord}_k
\]

\[
= \frac{1}{p^m - p^{m-1}} \sum_{d|p^m} \sum_{n|w} \phi(d) \text{ord}_k \frac{d}{\phi(d)} \sum_{\nu=0}^{\text{ord}_k} \nu \frac{w^{\nu}}{n^\nu}
\]

Furthermore, we have

\[
t(k, p^m) = \frac{1}{p^m - p^{m-1}} \sum_{d|p^m} \phi(d) \max \left\{ \left\lfloor \frac{v_{p_1}(d)}{n_1} \right\rfloor, \left\lfloor \frac{v_{p_2}(d)}{n_2} \right\rfloor, \ldots, \left\lfloor \frac{v_{p_s}(d)}{n_s} \right\rfloor \right\}
\]

(7) Let \( w_x \) be the factor of \( \text{ord}_x \) such that \( \frac{\text{ord}_x}{w_x} \) 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 \( v_{p_x}(\text{ord}_x) \leq ln_x \), for any \( 1 \leq i \leq s \). Then we get the desired result.

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

\[
t(k, p^m) = \frac{1}{p^m - p^{m-1}} \sum_{d | (p^m - p^{m-1})} \phi(d) \max \left\{ \left\lfloor \frac{v_{p_1}(d)}{n_1} \right\rfloor, \left\lfloor \frac{v_{p_2}(d)}{n_2} \right\rfloor, \ldots, \left\lfloor \frac{v_{p_s}(d)}{n_s} \right\rfloor \right\}
\]

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] we apply 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

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

(3.1)

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

(3.2)

Proof. Combing (2.2) and Proposition 3.1 (1) and (2), we can get the desired formulas. \( \square \)

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

Proposition 3.5. We have

\[
\lim_{N \to \infty} \frac{S_0(k, m, N)}{N^m} = \frac{1}{m+1} \left( \prod_{i=1}^{s} \frac{p_i^2}{p_i^2 - 1} - 1 \right).
\]
ON THE CYCLE STRUCTURE OF REPEATED EXPONENTIATION MODULO A PRIME POWER

Proof. Put \( Q = p_1 p_2 \cdots p_s \) and denote by \( \mathcal{U}_Q \) the set of integer \( u, 1 \leq u \leq Q \), such that \( \gcd(u, Q) = 1 \).

For each odd prime \( p \), let \( \rho_p \) be the largest divisor of \( p^m - p^{m-1} \) coprime to \( p_1 p_2 \cdots p_s \). It is easy to see

\[
\lim_{N \to \infty} \frac{S_0(k, m, N)}{N^m} = \frac{1}{N^{m \pi(N)}} \sum_{p \leq N} \rho_p.
\]

Notice that if a prime \( p > p_s \), then \( v_p(p^m - p^{m-1}) = v_p(p-1) \) for any \( 1 \leq i \leq s \).

Hence, following the method in Theorem 2 of [2], we have

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

Moreover, we have

\[
\sum_{q \in \Omega} \frac{1}{q^2} = \sum_{i_1, \ldots, i_s = 0}^{\infty} \frac{1}{(p_1^{i_1} \cdots p_s^{i_s})^2} - 1
\]

\[
= \sum_{i_1 = 0}^{\infty} \cdots \sum_{i_s = 0}^{\infty} \frac{1}{p_1^{i_1} \cdots p_s^{i_s}} - 1
\]

\[
= \prod_{i=1}^{s} \frac{p_i^2}{p_i^2 - 1} - 1.
\]

Hence, we get the desired result.

\[\square\]

Corollary 3.6. We have \( \frac{1}{k^x(m+1)} \frac{k^x}{N^m} < \lim_{N \to \infty} \frac{S_0(k, m, N)}{N^m} < \frac{2^x - 1}{m+1} \).

Proof. Notice that for any prime \( p \), we have

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

\[\square\]

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

\[
\psi(q) = \frac{1}{q} \sum_{d | q} \varphi(d) \max \left\{ \left\lfloor \frac{v_{p_1}(d)}{n_1} \right\rfloor, \ldots, \left\lfloor \frac{v_{p_s}(d)}{n_s} \right\rfloor \right\}
\]

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 \( \frac{1}{q} \sum_{d|q} \varphi(d) \left[ \frac{\nu_k(d)}{n_1} \right] \).

For simplicity, we replace \( p_1, r_1 \) and \( n_1 \) by \( p, r \) and \( n \) respectively. By division algorithm, we write \( r = ln + d \) with \( 0 \leq d < n \). We have

\[
\frac{1}{q} \sum_{d|q} \varphi(d) \left[ \frac{\nu_k(d)}{n} \right] = \frac{1}{p^r} \sum_{d|p^r} \varphi(d) \left[ \frac{\nu_k(d)}{n} \right]
\]

\[
= \frac{p-1}{p^r} \sum_{i=1}^{\lfloor \frac{n}{p^r} \rfloor} p^{i-1} \left[ \frac{1}{n} \right]
\]

\[
= \frac{p-1}{p^r} \left( \sum_{i=1}^{n} p^{i-1} + \sum_{i=n+1}^{2n} 2p^{i-1} + \cdots + \sum_{i=(l-1)n+1}^{ln} lp^{i-1} + \sum_{i=ln+1}^{ln+d} (l+1)p^{i-1} \right)
\]

\[
= \frac{p-1}{p^r} \left[ 1 + 2p^n + \cdots + lp^{(l-1)n} \right] + \frac{(l+1)p^n (p^r-1)}{p^r}
\]

\[
\leq l + (l + 1) \leq 3r.
\]

Hence, we have

\[
\psi(q) \leq \frac{1}{q} \sum_{d|q} \varphi(d) \left( \left[ \frac{\nu_k(d)}{n_1} \right] + \cdots + \left[ \frac{\nu_k(d)}{n_s} \right] \right)
\]

\[
(3.3)
\]

\[
\leq 3(kr_1 + \cdots + kr_s)
\]

\[
\leq \frac{3}{\ln 2} \ln q = O(\ln q).
\]

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

\[
\lim_{N \to \infty} S(k, m, N) = \lim_{N \to \infty} \frac{1}{\pi(N)} \sum_{q \in \Omega} \psi(q) \sum_{u \in U_q} \sum_{p \leq N \ (p \equiv q u + 1 \text{ (mod $q$)})} 1.
\]

Then following the method in Theorem 2 of [2], we can get the desired result. \( \square \)

**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

\[
\sum_{q \in \Omega} \frac{\psi(q)}{q} > \sum_{i_1 \geq n_1, \ldots, i_s \geq n_s} \frac{\psi(p_1^{i_1} \cdots p_s^{i_s})}{(p_1^{i_1} \cdots p_s^{i_s})^2}
\]

\[
= \frac{(p_1 - 1) \cdots (p_s - 1)}{p_1 \cdots p_s} \sum_{i_1 \geq n_1} \frac{1}{i_1} \cdots \sum_{i_s \geq n_s} \frac{1}{p_s}
\]

\[
= \frac{1}{k}.
\]

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

\[
\sum_{q \in \Omega} \frac{\psi(q)}{q} < \sum_{q \in \Omega} \frac{5 \ln q}{q}
\]

\[
< 5 \sum_{q \in \Omega} \frac{1}{q}
\]

\[
= 5 \sum_{i_1 = 0, \ldots, i_s = 0} \frac{1}{p_1^{i_1} \cdots p_s^{i_s}}
\]

\[
= \frac{5}{\sqrt{p_1} \cdots \sqrt{p_s}} \left( \frac{1}{\sqrt{p_1} - 1} \cdots \frac{1}{\sqrt{p_s} - 1} \right).
\]

\( \square \)
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, M. Křížek, Structure of digraphs associated with quadratic congruences with composite moduli, Discrete Math. 306 (2006) 2174-2185.
9. L. Somer, M. Křížek, On semiregular digraphs of the congruence $x^k \equiv y \pmod{m}$, Comment. Math. Univ. Carolin. 48 (2007), 41-58.
10. L. Somer, M. Křížek, On symmetric digraphs of the congruence $x^k \equiv y \pmod{m}$, Discrete Math. 309 (2009) 1999-2009.
11. T. Vasiga, 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, Fibonacci Quart. 36 (1998) 229-239.