#A66 INTEGERS 13 (2013)

CYCLES IN REPEATED EXPONENTIATION MODULO p^n

Lev Glebsky
Instituto de Investigación en Comunicación Óptica Universidad Autónoma de San Luis Potosí Av. Karakorum 1470, Lomas 4a 78210 San Luis Potosi, Mexico
glebsky@cactus.iico.uaslp.mx

Received: 4/13/12, Revised: 6/16/13, Accepted: 9/1/13, Published: 10/10/13

Abstract

We consider a dynamical system generated by exponentiation modulo r, that is, by the map $u \mapsto f_q(u)$, where $f_q(u) \equiv q^u \pmod r$ and $0 \le f_g(u) \le r-1$. The number of cycles is estimated from above in the case when $r = p^n$ with a prime integer p and $\gcd(q,p) = 1$. Also a more general class of functions is considered.

1. Introduction and Formulation of Results

Given a number $r \in \mathbb{N}$, we consider a dynamical system generated by exponentiation modulo r, that is, by the map $u \mapsto f_q(u)$ where $f_q(u) \equiv q^u \pmod r$ and $0 \le f_q(u) \le r-1$. In [2] the author with Igor Shparlinski considered the case when r is prime. We gave some estimates for the number of $1-, 2-, 3-$periodic points of f. We believe that our estimates are very far from being strict (it seems that better estimates are not known). But the strictness is not the main issue. The technique we use does not work even for 4-periodic points. So, it is a challenging problem to prove any nontrivial estimate for the number of k-periodic points with $k \ge 4$. Maybe one of the difficulties is that f is not an algebraic factor of q^x: if, for example, $\gcd(r, \phi(r)) = 1$ then one can choose a representative $y \equiv x \mod r$ such that q^y has any possible value modulo r. The situation with large $\gcd(r, \phi(r))$ may be more tractable. In that case, instead of considering the function f, one may consider the graph with the edges from $x \in \mathbb{Z}_r = \mathbb{Z}/r\mathbb{Z}$ to all $q^y \mod r$, $y \equiv x \mod r$. We show that it works very well at least for $r = p^n$ with a prime p. Also, "additively close" to q^x functions are considered, see Corollary 5.

The main results of the present paper are Theorem 1, Theorem 2, and Theorem 4. A weaker result than Theorem 2 is proved in the author's preprint [1]. Then independently, among other things, a result equivalent to Theorem 2 is established in [3]. The authors of [3] use p-adic analysis and in the present article we use combinatorial methods. As it is shown in [3] the algebraic reason to consider a graph instead of a function is that $f(x) = q^x$ has the m-valued continuous extension on p-adic numbers where m is the multiplicative order of q modulo p. The results formulated in Theorem 1 and Theorem 4 do not appear in [3].

In what follows we suppose that $\gcd(q, p) = 1$. Let $\Gamma_{p,n,q}$ be a directed graph with the set of vertices $V(\Gamma) = \mathbb{Z}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$ and the set of edges $E = \{(x, q^y \mod p^n) \mid x \in \mathbb{Z}_{p^n},\ y \in \mathbb{Z},\ y \equiv x \mod p^n\}$.

Theorem 1. *Let* $\gcd(q, p) = \gcd(g, p) = 1$ *and the multiplicative orders of q and g modulo p^n coincide. Then the graphs $\Gamma_{p,n,q}$ and $\Gamma_{p,n,g}$ are isomorphic.*

Given a graph Γ, a sequence $v_1, v_2, \ldots, v_k, v_{k+1}$ with $v_j \in V(\Gamma)$, $(v_j, v_{j+1}) \in E(\Gamma)$, $v_1 = v_{k+1}$ is said to be a k-cycle (with initial vertex marked) in Γ. Let $C_{p,n,q}(k)$ be the number of k-cycles (with initial vertex marked) in $\Gamma_{p,n,q}$.

Theorem 2. *Let m be the multiplicative order of q modulo p. Then $C_{p,n,q}(k) = m^k$ and the out-degree of any edge of the graph $\Gamma_{p,n,q}$ is m.*

Corollary 3. *The number of k-periodic points for $f(x) \equiv q^x \mod p^n$, $0 \leq f(x) < p^n$, is less than m^k where m is the multiplicative order of q modulo p.*

The same technique is used to estimate the number of k-cyclic points in "additive perturbations" of graph Γ. Precisely, let us define $\Gamma^r_{p,n,q}$ as follows: the set of vertices is $V(\Gamma) = \mathbb{Z}_{p^n}$ and the set of edges is $E = \{(x, q^y + c \mod p^n) \mid x \in \mathbb{Z}_{p^n},\ y \in \mathbb{Z},\ y \equiv x \mod p^n,\ c = -r, -r+1, \ldots, r\}$. Let $C^r_{p,n,q}(k)$ be the number of k-cycles (with the initial vertex marked) in $\Gamma^r_{p,n,q}$.

Theorem 4. $C^r_{p,n,q}(k) \leq p + 4krp[2(2r+1)(p-1)]^{k-1}(n-1)$.

So, $C^r_{p,n,q}$ grows no more than linearly in n (but the number of all vertices grows exponentially). Let us note that the estimate may be nontrivial even for $r > p$. For example, if k is fixed, $p > 2$, $r \sim p^{\epsilon n}$, and $\epsilon < 1/k$, then the estimate of the Theorem is nontrivial for large enough n.

Corollary 5. *Let $f : \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n}$ be such that $f(x) \equiv q^x + g(x) \mod p^n$, where $g : \mathbb{Z}_{p^n} \to \{-r, \ldots, r\}$. Then the number of k-periodic points of f is less than $p + 4krp[2(2r+1)(p-1)]^{k-1}(n-1)$.*

One could also consider other additive perturbations. For example, with $E = \{(x, q^y \mod p^n) \mid y \equiv x + j \mod p^n,\ \ j = -r, \ldots, r\}$. But it gives nothing new. Indeed, let Γ^r be the graph defined as $V(\Gamma^r) = \mathbb{Z}_{p^n}$ and $E(\Gamma^r) = \{(x, x + j \mod p^n),\ \ j = -r, \ldots, r\}$. Then both additive perturbations are composition of Γ^r and $\Gamma_{p,n,q}$, but with the different order. It is clear that the order does not change the number of cycles. The same is true for the composition $\Gamma^{r_1} - \Gamma_{p,n,q} - \Gamma^{r_2}$ (two-sided additive perturbation).

2. Proof of Theorem 2

In what follows we identify $\mathbb{Z}_{p^n}$ with $\{0,1,2,\ldots,p^n-1\}$. So, $y = (x \mod p^n)$ often means that $y \equiv x \mod p^n$ and $y \in \{0,1,\ldots p^n-1\}$.

Lemma 6. *Let $A_1, A_2, ..., A_r$ be elements of an associative (not necessarily commutative) ring $\mathcal{A}$. Let $M \in Mat_{n\times n}(\mathcal{A})$,*

$$M = \begin{pmatrix} A_1 & A_2 & \ldots & A_n \\ A_1 & A_2 & \ldots & A_n \\ \vdots & \vdots & \ldots & \vdots \\ A_1 & A_2 & \ldots & A_n \end{pmatrix}.$$

Then trace$(M^k) = (A_1 + A_2 + \cdots + A_r)^k$.

Proof.

$$M^k = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \left(\begin{pmatrix} A_1 & A_2 & \ldots & A_r \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \right)^{(k-1)} \begin{pmatrix} A_1 & A_2 & \ldots & A_r \end{pmatrix} =$$

$$(A_1 + A_2 + \cdots + A_r)^{k-1} \begin{pmatrix} A_1 & A_2 & \ldots & A_n \\ A_1 & A_2 & \ldots & A_n \\ \vdots & \vdots & \ldots & \vdots \\ A_1 & A_2 & \ldots & A_n \end{pmatrix}.$$

□

Lemma 7. *Let A_n be the adjacency matrix of $\Gamma_{p,n,q}$. Then*

1)

$$A_1 = \begin{pmatrix} 0 & a_1 & a_2 & \ldots & a_{p-1} \\ 0 & a_1 & a_2 & \ldots & a_{p-1} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & a_1 & a_2 & \ldots & a_{p-1} \end{pmatrix}$$

with $a_i \in \{0,1\}$ and $a_1 + a_2 \cdots + a_{p-1} = m$, where m is the multiplicative order of q modulo p;

2) *for $n > 1$ one has*

$$A_n = \begin{pmatrix} B_1^n & B_2^n & \ldots & B_p^n \\ B_1^n & B_2^n & \ldots & B_p^n \\ \vdots & \vdots & \ldots & \vdots \\ B_1^n & B_2^n & \ldots & B_p^n \end{pmatrix},$$

where $B_j^n \in Mat_{p^{n-1}\times p^{n-1}}(\{0,1\})$ and $B_1^n + B_2^n + ... + B_p^n = A_{n-1}$.

Proof. For Item 1 it suffices to note that q^x modulo p takes m different values and depends on x modulo $p-1$ only (not on x modulo p). Let us prove Item 2. First of all we represent $x \in \mathbb{Z}_{p^n} = \{0,1,2,\ldots,p^n-1\}$ as $x = y + bp^{n-1}$, where $y \in \{0,1,\ldots,p^{n-1}-1\}$ and $b \in \{0,1,\ldots,p-1\}$. The block structure of A_n corresponds to the above described representation, such that b's are indexing our blocks and y's are indexing the elements inside the blocks. Let $O^n(x) = \{y \in Z_{p^n} \mid (x,y) \in E(\Gamma_{p,n,q})\}$. Item 2 follows from the following facts

(i) $O^n(x)$ is independent of blocks. That is $O^n(x) = O^n(z)$ if $x \equiv z \mod p^{n-1}$.

(ii) Let $\psi : \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^{n-1}}$ be defined as $\psi(x) \equiv x \mod p^{n-1}$. Then for any $y \in \{0,1,2,\ldots,p^{n-1}-1\}$ ψ defines a bijection $O^n(y) \leftrightarrow O^{n-1}(y)$.

Fact **i)**. To find $q^z \mod p^n$ it suffices to know $z \mod (p-1)p^{n-1}$. Let $P_x = \{z \in \mathbb{Z}_{(p-1)p^{n-1}} \mid \exists a \in \mathbb{Z}\ a \equiv z \mod (p-1)p^{n-1}$ and $a \equiv x \mod p^n\}$. One has that $O^n(x) = \{q^z \mod p^n \mid z \in P_x\}$. By Chinese Remainder Theorem $P_x = P_y$ if and only if $x \equiv y \mod p^{n-1}$.

Fact **ii)** Observe that $p^n \equiv 1 \mod p-1$. So, $O^n(y) = \{q^y q^{bp^n} \mod p^n \mid b \in \{0,1,\ldots,p-2\}\}$ and $O^{n-1}(y) = \{q^y q^{bp^{n-1}} \mod p^{n-1} \mid b \in \{0,1,\ldots,p-2\}\}$. Now, $q^{bp^{n-1}} \equiv q^{bp^n} \mod p^n$. Indeed, $bp^{n-1} - bp^n \equiv 0 \mod (p-1)p^{n-1}$. So, $O^n(y) = \{q^y q^{bp^{n-1}} \mod p^n \mid b \in \{0,1,\ldots,p-2\}\}$. It remains to prove that for $b_1, b_2 \in \{0,1,\ldots,p-2\}$ the congruence

$$q^{b_1 p^{n-1}} \equiv q^{b_2 p^{n-1}} \mod p^{n-1} \tag{1}$$

implies the congruence

$$q^{b_1 p^{n-1}} \equiv q^{b_2 p^{n-1}} \mod p^n. \tag{2}$$

Let $q \equiv g^r \mod p^n$ for primitive g. The first congruence is equivalent to $(b_1 - b_2)rp^{n-1} \equiv 0 \mod (p-1)p^{n-2}$. It implies $(p-1)|(b_1-b_2)r$. So, $(b_1-b_2)rp^{n-1} \equiv 0 \mod (p-1)p^{n-1}$ and the second congruence follows. Now, Fact **(i)** implies that all block rows in A_n are equal. Fact **(ii)** implies that the sum of the blocks in the first row is A_{n-1}. □

Now it is easy to finish the proof of Theorem 2. Firstly, $C_{p,n,q}(k) = trace((A_n)^k)$. Using Lemma 6, Lemma 7 and compatibility of the trace and multiplication with the block structure we get

$$trace((A_n)^k) = trace((A_{n-1})^k) = \cdots = trace((A_1)^k) = (a_1 + a_2 + \cdots + a_{p-1})^k.$$

The second statement of the theorem is a simple consequence of Lemma 7.

3. Proof of Theorem 1

Adopting the notation of the previous section for different q, let $O^n_q(x) = \{y \in \mathbb{Z}_{p^n} \mid (x,y) \in E(\Gamma_{p,n,q})\}$.

Lemma 8. *Let M be the multiplicative order of q modulo p^n. Let r be the greatest r such that $p^r|M$. Then the following statements are equivalent:*

1) $O_q^n(x_1) \cap O_q^n(x_2) \neq \emptyset$*;*

2) $x_1 - x_2 \equiv 0 \mod p^r$*;*

3) $O_q^n(x_1) = O_q^n(x_2)$*.*

Proof. 1)$\Longrightarrow$2). Let $q^{y_1} \equiv q^{y_2} \mod p^n$ and $x_j \equiv y_j \mod p^n$, $j = 1, 2$. This implies that $y_1 \equiv y_2 \mod M$ and $x_1 \equiv x_2 \mod p^r$.
2)$\Longrightarrow$3). The values of $q^x \mod p^n$ depend on $x \mod (p-1)p^r$. So, the implication follows by the Chinese Reminder Theorem.
The last implication is trivial. □

Under our conditions the multiplicative orders of q and $g \mod p^k$, $k \leq n$, coincide. So, we inductively construct isomorphisms $h_k : \mathbb{Z}_{p^k} \to \mathbb{Z}_{p^k}$ of graphs $\Gamma_{p,k,q}$ and $\Gamma_{p,k,g}$. Let $\psi : \mathbb{Z}_{p^{k+1}} \to \mathbb{Z}_{p^k}$ be the natural projection (as in the previous section). We inductively keep the following properties:

1. h_k is an isomorphism of $\Gamma_{p,k,q}$ and $\Gamma_{p,k,g}$. In particular, it implies that h_k is a bijection.

2. The following diagram is commutative:

$$\begin{tikzcd}
\mathbb{Z}_{p^{k+1}} \arrow[r, "h_{k+1}"] \arrow[d, "\psi"] & \mathbb{Z}_{p^{k+1}} \arrow[d, "\psi"] \\
Z_{p^k} \arrow[r, "h_k"] & Z_{p^k}
\end{tikzcd}$$

Trivially, $h_1 = \text{id}$ (the identity map) satisfies our hypothesis. Assume that h_k is constructed. Let $x \in \{0, 1, \ldots, p^k - 1\} = \mathbb{Z}_{p^k}$. Since ψ and h_k are bijections on $O^k(x)$, there is a unique h_{k+1}^x making the following diagram commute:

$$\begin{tikzcd}
O_q^{k+1}(x) \arrow[r, "h_{k+1}^x"] \arrow[d, "\psi"] & O_g^{k+1}(h_k(x)) \arrow[d, "\psi"] \\
O_q^k(x) \arrow[r, "h_k"] & O_g^k(h_k(x))
\end{tikzcd}$$

Let $X = \bigcup_{x \in \mathbb{Z}_{p^k}} O_q^{k+1}(x) = \bigcup_{x \in \mathbb{Z}_{p^{k+1}}} O_q^{k+1}(x)$ and $Y = \bigcup_{x \in \mathbb{Z}_{p^k}} O_g^{k+1}(x)$. Lemma 8 implies that $O_q^{k+1}(x)$, $x \in \mathbb{Z}_{p^k}$ forms a partition of X and $O_q^{k+1}(x_1) = O_q^{k+1}(x_2)$ if and only if $O_g^{k+1}(h_k(x_1)) = O_g^{k+1}(h_k(x_2))$. So, the set of functions h_{k+1}^x, $x \in$

$\mathbb{Z}_{p^k}$, define bijection $h_{k+1} : X \to Y$. By construction, the following diagram is commutative:

$$\begin{tikzcd} X \arrow[r, "h_{k+1}"] \arrow[d, "\psi"] & Y \arrow[d, "\psi"] \\ \psi(X) \arrow[r, "h_k"] & \psi(Y) \end{tikzcd}$$

So, we can define $h_{k+1} : \mathbb{Z}_{p^{k+1}} \setminus X \to \mathbb{Z}_{p^{k+1}} \setminus Y$ making the corresponding diagram commute. Taking into account that $O^{k+1}(x) = O^{k+1}(\psi(x))$ one can check that the h_{k+1} constructed satisfies properties 1. and 2..

4. Proof of Theorem 4

For $A, B \in Mat_{d\times d}(\{0,1\})$ we will write $A \preceq B$ if $A_{i,j} = 1$ implies $B_{i,j} = 1$.

Lemma 9. *Let A_n be the adjacency matrix of $\Gamma^{+r}_{p,n,q}$. Then*
(1)

$$A_1 \preceq \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix};$$

(2) for $n > 1$ one has

$$A_n \preceq \begin{pmatrix} B_1^n & B_2^n & \dots & B_p^n \\ B_1^n & B_2^n & \dots & B_p^n \\ \vdots & \vdots & \dots & \vdots \\ B_1^n & B_2^n & \dots & B_p^n \end{pmatrix} + X, \text{ where } B_j^n \in \underset{p^{n-1}\times p^{n-1}}{Mat}(\{0,1\}),$$

$B_1^n + B_2^n + ... + B_p^n = A_{n-1}$ and $X \in Mat_{p^n\times p^n}(\{0,1\})$ with less then $2rp$ non-zero columns;
(3) The number of 1s in a row of A_n is less than $2r(p-1)$.

Proof. Item (1) is trivial. The proof of Item (2) proceeds in the same way as the one of Lemma 7. As in Lemma 7 the block structure corresponds to the representation $x = y + bp^{n-1}$ with $0 \le y < p^{n-1}$ and $b \in \{0, 1, \dots, p-1\}$. The neighborhood of a vertex x in $\Gamma^r_{p,n,q}$ is easy to construct using the neighborhood of x in $\Gamma_{p,n,q}$. So, let $O^n(x) = \{y \in \mathbb{Z}_{p^n} \mid (x, y) \in E(\Gamma_{p,n,q})\}$ and $O^n_r(x) = \{y \in \mathbb{Z}_{p^n} \mid (x, y) \in E(\Gamma^r_{p,n,q})\}$. By definition of $\Gamma^r_{p,n,q}$ one has that $y + bp^{n-1} \in O^n_r(x)$ if and only if $(y + bp^{n-1} + j \mod p^n) \in O^n(x)$ for some $j = -r, \dots, r$. Observe that $y + j = (y + j \mod p^{n-1})$ for $r \le y < p^{n-1} - r$. So, $(y + j \mod p^{n-1}) + bp^{n-1} = (y + j + bp^{n-1} \mod p^n)$ for such y. It implies that

$$(B_0^n + B_1^n + \cdots + B_{p-1}^n)_{jy} = (A_{n-1})_{jy}$$

for $r \le y < p^{n-1} - r$. (Recall that $O^n(x)$ satisfies items **(i)** and **(ii)** of the proof of Lemma 7.) So, there exist no more than $2r$ columns in each block where the equality does not hold. Item (2) of the lemma follows. Item (3) holds since the number of 1s in a row x is $|O_r^n(x)|$ but $|O_r^n(x)| \le (2r+1)|O^n(x)| = (2r+1)(p-1)$. □

Now we are ready to prove Theorem 4. We have

$$C_{p,n,q}^r(k) = c_n = trace(A_n^k) \le trace(A_{n-1}^k) + \Delta = c_{n-1} + \Delta,$$

where Δ is the sum of the traces of $2^k - 1$ matrices P_s, each of them being a product of k matrices containing X. Observe that $trace(P_s) \le 2krp((2r+1)(p-1))^{k-1}$. Indeed, this is the number of k-periodic paths such that at least one edge of a path corresponds to the matrix X (X-edge). We have no more than $2rp$ ends of X-edges. Starting counting from these vertices we get no more than $2rp((2r+1)(p-1))^{k-1}$ cycles. Counting cycles with initial points we get our estimate. Observe that $c_1 \le p$ and, by induction, $c_n \le p + 4krp(2(2r+1)(p-1))^{k-1}(n-1)$.

Acknowledgments. The author thanks Igor Shparlinski, Edgardo Ugalde and Alexander Pyshchev for useful suggestions. The work was partially supported by PROMEP grant UASLP-CA21 and by CONACyT grant 50312.

References

[1] Lev Glebsky, Cycles in Repeated Exponentiation Modulo p^n, *Preprint* arXiv:1006.2500v1.

[2] Lev Glebsky and Igor E. Shparlinski, Short cycles in repeated exponentiation modulo a prime, *Des. Codes Cryptogr.* **56** (2010), no. 1, 35-42.

[3] Joshua Holden and Margaret M. Robinson, Counting fixed points, two-cycles, and collisions of the discrete exponential functions using p-adic methods, *J. Aust. Math. Soc.* **92** (2012), 163-178.