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
June 15, 2010

Abstract
Given a number $r$, we consider the dynamical system generated by repeated exponentiations modulo $r$, that is, by the map $u \mapsto f_q(u)$, where $f_q(u) \equiv q^u \mod r$ and $0 \leq f_q(u) \leq r - 1$. The number of cycles of the defined above dynamical system is considered for $r = p^n$.

1 Introduction and formulation of results
Given a number $r$, we consider the dynamical system generated by repeated exponentiations modulo $r$, that is, by the map $u \mapsto f_q(u)$, where $f_q(u) \equiv q^u \mod r$ and $0 \leq f_q(u) \leq r - 1$. In [1] the author with Igor Shparlinski considered the case where $r$ is a prime. We gave some estimates on number of $1$--, $2$-, $3$-periodic points of $f$. We believe that our estimates are very far from being strict (but it seems that the better estimates are not known). Maybe one of the difficulties of the problem is that $f$ is not an algebraic factor of $q^x$: if, for example, $\gcd(r, \phi(r)) = 1$ then one can choose representative $y \equiv x \mod r$ such that $q^y$ has any possible value $\mod r$. The situation where $\gcd(r, \phi(r))$ is large may be more easy to deal with. In that case, instead of considering the function $f$, one may consider the graph with edges from $x \in \mathbb{Z}_r$ to all $q^y \mod r$, $y \equiv x \mod r$. I will show that it works very well at list for $r = p^n$ with a prime $p$. In what follows we will suppose that $\gcd(q, p) = 1$.

Let $\Gamma_{p,n,q}$ be a directed graph defined as follows: the set of vertexes is $V(\Gamma) = \mathbb{Z}_{p^n}$ and the set of edges is $E = \{(x, q^y \mod p^n) \mid x \in \mathbb{Z}_{p^n}, y \equiv x \mod p^n\}$. Suppose for a moment that $q$ is primitive $\mod p^n$. Then $p - 1$ is the out degree of any edge of the graph $\Gamma$. Let $C_{p,n,q}(k)$ be the number of $k$-cycles (with initial vertex marked) in $\Gamma_{p,n,q}$.
Theorem 1. \( C_{p,n,q} \leq (p-1)^k \). If \( q \) is primitive \( \mod p \) then \( C_{p,n,q} = (p-1)^k \).

Corollary 2. The number of \( k \)-periodic points for \( f(x) \equiv q^x \mod p^n \), \( 0 \leq f(x) < p^n \) is less than \( (p-1)^k \).

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

Theorem 3. \( C_{p,n,q}^+(k) \leq p + rp[2p(2r + 1)]^k(n - 1) \)

So, \( C \) grows no more than linearly in \( n \) (but the number of all vertexes grows exponentially).

2 Proof of Theorem 1

Lemma 4. Let \( A_1, A_2, \ldots, A_r \) be elements of an associative (not necessarily commutative) algebra \( A \). Let \( M \in \text{Mat}_{n \times n}(A) \),

\[
M = \begin{pmatrix}
A_1 & A_2 & \cdots & A_n \\
A_1 & A_2 & \cdots & A_n \\
\vdots & \vdots & \ddots & \vdots \\
A_1 & A_2 & \cdots & A_n
\end{pmatrix}
\]

Then \( \text{trace}(M^k) = (A_1 + A_2 + \cdots + A_r)^k \).

Proof.

\[
M^k = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix} \begin{pmatrix} A_1 & A_2 & \cdots & A_r \\ A_1 & A_2 & \cdots & A_r \\ \vdots & \vdots & \ddots & \vdots \\ A_1 & A_2 & \cdots & A_r \end{pmatrix}^{(k-1)}
\]

\[
= (A_1 + A_2 + \cdots + A_r)^{k-1} \begin{pmatrix} A_1 & A_2 & \cdots & A_n \\ A_1 & A_2 & \cdots & A_n \\ \vdots & \vdots & \ddots & \vdots \\ A_1 & A_2 & \cdots & A_n \end{pmatrix}
\]

\[\square\]

Lemma 5. Let \( A_n \) be the adjacency matrix of \( \Gamma_{p,n,q} \). Then

1. \( A_1 = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 1 & \cdots & 1 \end{pmatrix} \), if \( q \) is primitive \( \mod p \). If \( q \) is not primitive then \( A_1 \) has the same form with some 1 changed to 0.
2. for \( n > 1 \) \( A_n = \begin{pmatrix} B_1^n & B_2^n & \ldots & B_p^n \\ B_1^n & B_2^n & \ldots & B_p^n \\ \vdots & \vdots & \ddots & \vdots \\ B_1^n & B_2^n & \ldots & B_p^n \end{pmatrix} \), where \( B_j^n \in \text{Mat}_{p^n-1 \times p^n-1}(\mathbb{Z}) \)

and \( B_1^n + B_2^n + \ldots + B_p^n = A_{n-1} \).

Proof. Item 1 is trivial. Let us prove Item 2. First of all we represent \( \{0,1,2,\ldots,p^n-1\} \) as \( x = y + bp^{n-1} \), where \( y \in \{0,1,\ldots,p^n-1\} \) and \( b \in \{0,1,\ldots,p-1\} \). The block structure of \( A_n \) corresponds to the described above representation, such that \( b \)'s are numbering our blocks and \( y \)'s are numbering the elements inside the blocks. The item 2 follows from the next facts

i) \( O^n(x) = O^n(y) \) if \( x \equiv y \mod p^{n-1} \). Where \( O^n(x) = \{ y \in \mathbb{Z}_{p^n} \mid (x, y) \in E(\Gamma_{n,p,q}) \} \).

ii) Let \( \phi: \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n-1} \) be defined as \( \phi(x) \equiv x \mod p^{n-1} \).

Then for any \( y \in \{0,1,2,\ldots,p^n-1\} \) \( \phi \) defines a bijection \( O^n(y) \leftrightarrow O^{n-1}(y) \).

Fact i). To find \( q^x \mod p^n \) it suffices to know \( z \mod (p-1)p^{n-1} \). Let \( P_x = \{ z \in \mathbb{Z}_{(p-1)p^{n-1}} \mid \exists a \in \mathbb{Z} \ a \equiv z \mod (p-1)p^{n-1} \text{ and } a \equiv x \mod p^n \} \). One has that \( O^n(x) = \{ q^x \mod p^n \mid z \in P_x \} \). By Chinese Remainder Theorem \( P_x = P_y \) if and only if \( x \equiv y \mod p^{n-1} \). Observe that \( O^n(x) = \{ q^x q^{bp^n} \mod p^n \mid b \in \{0,1,\ldots,p-2\} \} \).

Fact ii). Recall that \( O^n(x) = \{ q^x q^{bp^n} \mod p^n \mid b \in \{0,1,\ldots,p-2\} \} \) and \( O^{n-1}(x) = \{ q^x q^{bp^{n-1}} \mod p^{n-1} \mid b \in \{0,1,\ldots,p-2\} \} \). Now, \( q^{bp^n} \equiv q^{bp^{n-1}} \mod p^n \). Indeed, \( bp^{n-1} - bp^n \equiv 0 \mod (p-1)p^{n-1} \). It proves fact ii) if \( q \) is primitive \( \mod p^{n-1} \). For non primitive \( q \) it suffices to prove that for \( b_1, b_2 \in \{0,1,\ldots,p-2\} \) the congruence

\[
q^{b_1p^{n-1}} \equiv q^{b_2p^{n-1}} \mod p^{n-1}
\]

imply the congruence

\[
q^{b_1p^{n-1}} \equiv q^{b_2p^{n-1}} \mod p^n
\]

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 it is easy to finish the proof of Theorem 4. First of all \( C_{p,n,q}(k) = \text{trace}((A_n)^k) \). Using Lemma 4 Lemma 5 and compatibility of the trace and multiplication with the block structure we get

\[
\text{trace}((A_n)^k) = \text{trace}((A_{n-1})^k) = \cdots = \text{trace}((A_1)^k) = (p-1)^k
\]
3 Proof of theorem

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

**Lemma 6.** Let $A_n$ be the adjacency matrix of $\Gamma^{+, _r}_{p, n, q}$. Then

1. $A_1 \preceq \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & 1 & 1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \ldots & 1 \end{pmatrix}$, if $q$ is primitive modulo $p$. If $q$ is not primitive then $A_1$ has the same form with some $1$ changed to $0$.

2. for $n > 1$ $A_n \preceq \begin{pmatrix} B_1^n & B_2^n & \ldots & B_p^n \\ B_1^n & B_2^n & \ldots & B_p^n \\ \vdots & \vdots & \ddots & \vdots \\ B_1^n & B_2^n & \ldots & B_p^n \end{pmatrix} + X$, where $B_j^n \in \text{Mat}_{p^n-1 \times p^n-1}(\mathbb{Z})$,

$B_1^n + B_2^n + \ldots + B_p^n = A_{n-1}$, $X \in \text{Mat}_{p^n \times p^n}((0, 1)$ with less then $2rp$ rows.

**Proof.** Item 1 is trivial. The prove of Item 2 proceeds the same way as the one of Theorem 1, but now we have to take into account that $y + s( \mod p^n)$ may be different from $y + s( \mod p^{n-1})$. Observe, that $y + s( \mod p^{n-1}) = y + s( \mod p^n)$ for $r \geq y \leq p^{n-1} - 1 - r$. So, for each $b \in \{0, 1, \ldots, p-1\}$ there exists only $2r$ of $y \in \{0, 1, \ldots, p^{n-1} - 1\}$ where the rows of $X$ are non zero.

Now we are ready to prove Theorem 3

$$C^{+, _r}_{n, p, q}(k) = c_n = \text{trace}(A_n^k) \leq \text{trace}(A_{n-1}^k) + \Delta = c_{n-1} + \Delta$$

$\Delta$ is the sum of the traces of $2^{k-1}$ matrices $P_s$, each of them is a product of $k$ matrices containing $X$. Observe, that $\text{trace}(P_s) \leq 2rp((2r + 1)p)^k$. Indeed, this is a number of $k$-periodic paths such that some steps of the path correspond to the matrix $X$ and some to the matrix $B$. The estimate follows from the number of non-zero rows of $X$, and that each row of $X$ and $B$ contains no more than $(2r + 1)p$ ones. Noting that $c_1 \leq p$ we get $c_n \leq p + rp(2r + 1)p^k(n-1)$.

**Acknowledgments** The proof of Lemma 4 was suggested by Edgardo Ugalde. The author thanks Igor Shparlinski for useful suggestions. The work were partially supported by PROMEP grant UASLP-CA21 and by CONACyT grant 50312.

**References**

[1] Lev Glebsky and Igor E. Shparlinski, Short cycles in repeated exponentiation modulo a prime, *Designs, Codes and Cryptography*, 56, N1, (2010) p.35-42