Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus

by

HARALD NIETZER (Vienna) and IGOR E. SHPARLINSKI (Sydney)

1. Introduction. Let \( p \geq 3 \) be a prime and \( m \geq 1 \) an integer. We write \( \mathbb{U}_m = (\mathbb{Z}/p^m\mathbb{Z})^* \) for the group of reduced residue classes modulo \( p^m \), where we drop the dependence on \( p \) in the notation for simplicity (we may think of \( p \) as a fixed prime). Then \( |\mathbb{U}_m| = (p - 1)p^{m-1} \). It will often be convenient to identify elements of \( \mathbb{Z}/p^m\mathbb{Z} \) with the corresponding elements of the least residue system modulo \( p^m \).

For given \( a, b \in \mathbb{Z}/p^m\mathbb{Z} \) we consider a map \( \psi : \mathbb{U}_m \to \mathbb{Z}/p^m\mathbb{Z} \) of the form

\[
(1) \quad \psi(w) = aw^{-1} + b \quad \text{for} \quad w \in \mathbb{U}_m.
\]

It is easy to see that \( \psi \) is a permutation of \( \mathbb{U}_m \) if and only if \( \gcd(a, p) = 1 \) and \( b \equiv 0 \pmod{p} \). These conditions will be assumed from now on.

If we start from an initial value \( u_0 \in \mathbb{U}_m \), then the recurrence relation

\[
(2) \quad u_{n+1} = \psi(u_n) \quad \text{for} \quad n = 0, 1, \ldots
\]

generates a sequence \( u_0, u_1, \ldots \) of elements of \( \mathbb{U}_m \). It is obvious that this sequence is purely periodic with least period length \( \tau \leq (p - 1)p^{m-1} \). Detailed studies of the possible values of \( \tau \) can be found in [1] and [4].

If \( u_0, u_1, \ldots \) is a sequence generated by (1) and (2), then it is of interest for the application mentioned below to establish upper bounds for the exponential sums

\[
(3) \quad \sum_{n=0}^{N-1} \chi(u_n),
\]

where \( \chi \) is a nontrivial additive character of \( \mathbb{Z}/p^m\mathbb{Z} \) and \( 1 \leq N \leq \tau \). In the case \( m = 1 \), and with a slight change of formula (1) to arrive at more
interesting permutations $\psi$ of $U_1$, a nontrivial upper bound for the corresponding exponential sums was first proved in [10] (see also [12]). In the present paper we treat the case $m \geq 2$ in which the details of the method are quite different.

The exponential sums (3) are relevant in the analysis of a well-known family of pseudorandom numbers. If $u_0, u_1, \ldots$ is a sequence of elements of $U_m$ as above, then the numbers $u_0/p^m, u_1/p^m, \ldots$ in the interval $[0,1)$ form a sequence of inverse congruential pseudorandom numbers with modulus $p^m$. For $p \geq 3$ and $m \geq 2$, the case we are concerned with here, this method of pseudorandom number generation was introduced in [4]. In practice, one works with a large power $p^m$ of a small prime $p$. For surveys of results on inverse congruential pseudorandom numbers we refer to [2], [8, Chapter 8], [9].

It is clear that upper bounds on the exponential sums (3) yield results on the distribution of the inverse congruential pseudorandom numbers $u_0/p^m, u_1/p^m, \ldots$ A quantitative version of such a result in the form of a discrepancy bound will be given in Section 4. This is the first nontrivial discrepancy bound for parts of the period of inverse congruential pseudorandom numbers with prime-power modulus. An analogous result for prime moduli was first established in [10]. Related results on the distribution in parts of the period for pseudorandom numbers generated by nonlinear methods can be found in [5], [6], [11], [12].

2. Auxiliary results. If $\psi$ is the permutation of $U_m, m \geq 1$, given by (1) and $r$ is an arbitrary integer, then let $\psi^r$ denote the $r$th power of $\psi$ in the group of permutations of $U_m$. We have the explicit formula in Lemma 1 below. Here and in the following, it will often be convenient to write $u/v$ for an expression $uv^{-1}$ in a multiplicative abelian group.

**Lemma 1.** For any integer $r \geq 0$ there exist $c_r, e_r \in \mathbb{Z}/p^m\mathbb{Z}$ such that

$$\psi^r(w) = \frac{(bc_r - e_r)w + ac_r}{c_rw - e_r} \quad \text{for all } w \in U_m.$$  
Moreover, for even $r$ we have $c_r \equiv 0 \pmod{p}$ and $e_r \not\equiv 0 \pmod{p}$ and for odd $r$ we have $c_r \not\equiv 0 \pmod{p}$ and $e_r \equiv 0 \pmod{p}$.

**Proof.** For $r = 0$ we can take $c_0 = 0$ and $e_0 = 1$. The general case follows by straightforward induction on $r$ and the additional properties of $c_r$ and $e_r$ are obtained along the way. 

If $u_0, u_1, \ldots$ is a sequence generated by (1) and (2), then for $1 \leq k \leq m$ we let $\tau_k$ be the least period length of the sequence $u_0, u_1, \ldots$ considered modulo $p^k$ (so that $\tau = \tau_m$).
Lemma 2. If $c_r \equiv 0 \pmod{p^k}$ for some $r \geq 1$ and $1 \leq k \leq m$, then $\tau_k$ divides $r$.

Proof. From $c_r \equiv 0 \pmod{p^k}$ it follows by Lemma 1 that $e_r \not\equiv 0 \pmod{p}$ and hence $\psi^r(w) \equiv w \pmod{p^k}$ for all $w \in U_m$. Then $r$ is a period length of the sequence $u_0, u_1, \ldots$ considered modulo $p^k$, and so $\tau_k$ divides $r$. □

Lemma 3. Let $p \geq 3$ be a prime, let $m$ be a positive integer, and let $f$ and $g$ be arbitrary integers. Put $\gcd(f, p^m) = p^l$. Then
\[
\sum_{z=0}^{p^m-1} \exp \left( \frac{2\pi i (fz^2 + gz^2)}{p^m} \right) = 0 \quad \text{if } g \not\equiv 0 \pmod{p^l}
\]
and
\[
\left| \sum_{z=0}^{p^m-1} \exp \left( \frac{2\pi i (fz^2 + gz^2)}{p^m} \right) \right| = p^{(m+l)/2} \quad \text{if } g \equiv 0 \pmod{p^l}.
\]

Proof. This follows from Lemma 6 in [3]. □

For $1 \leq r \leq \tau - 1$ and a nontrivial additive character $\chi$ of $\mathbb{Z}/p^m\mathbb{Z}$ we introduce the exponential sum
\[
\sigma_r = \sum_{w \in U_m} \chi(\psi^r(w) - w).
\]

Note that $\chi$ is determined by an integer $h \not\equiv 0 \pmod{p^m}$, in the sense that
\[
\chi(v) = \exp \left( \frac{2\pi i hv}{p^m} \right) \quad \text{for all } v \in \mathbb{Z}/p^m\mathbb{Z}.
\]

Put $\gcd(h, p^m) = p^d$ with $0 \leq d < m$, so that we can write $h = p^dh_0$ with an integer $h_0 \not\equiv 0 \pmod{p}$. By Lemma 1 we have
\[
\sigma_r = \sum_{w \in U_m} \chi \left( \frac{c_r(a + bw - w^2)}{c_r w + e_r} \right).
\]

Let $\gcd(c_r, p^m) = p^k$ with $k \geq 0$, then Lemma 2 shows that $k < m$. Thus, we can write $c_r = p^k c$ with an integer $c \not\equiv 0 \pmod{p}$. Then
\[
\sigma_r = \sum_{w \in U_m} \exp \left( \frac{2\pi ip^{d+k}}{p^m} \cdot \frac{c_0(a + bw - w^2)}{p^k e_r} \right).
\]

It is trivial that
\[
\sigma_r = |U_m| = (p-1)p^{m-1} \quad \text{if } d + k \geq m.
\]

For $d + k < m$ we obtain the following bound.

Lemma 4. With the notation above we have
\[
|\sigma_r| \leq 2p^{(m+d+k)/2} \quad \text{if } d + k < m.
\]
Proof. In (6) we put \( w = sp^{m-d-k} + t \) with \( 0 \leq s < p^{d+k} \) and \( t \in \mathcal{U}_{m-d-k} \). Then

\[
\sigma_r = \sum_{t \in \mathcal{U}_{m-d-k}} \exp\left(\frac{2\pi ich_0}{p^{m-d-k}} \cdot \frac{a + bt - t^2}{p^kct - er}\right). \tag{8}
\]

If \( k = 0 \), then \( t \mapsto ct - er \) is a permutation of \( \mathcal{U}_{m-d} \) by Lemma 1, hence carrying out this substitution in the sum above yields

\[ |\sigma_r| = p^d \left| \sum_{v \in \mathcal{U}_{m-d}} \exp\left(\frac{2\pi ich_0}{p^{m-d}} \cdot \frac{(a + bc^{-1}er - c^{-2}er^2)v^{-1} - c^{-2}v}{p^kcu - er}\right) \right|. \]

The last exponential sum is always bounded by \( 2p^{(m-d)/2} \), namely by a result in [13, p. 97] for \( d \leq m - 2 \) and by the Weil bound for Kloosterman sums (see [7, Theorem 5.45]) for \( d = m - 1 \). Therefore the result of the lemma follows for \( k = 0 \).

Next we consider the case \( k \geq m - d - k \). Then from (8) we get

\[ |\sigma_r| = p^{d+k} \left| \sum_{t \in \mathcal{U}_{m-d-k}} \exp\left(\frac{2\pi ich_0}{p^{m-d-k}} \cdot \frac{t^2 - bt}{e_r}\right) \right|. \]

Furthermore,

\[
\sum_{t \in \mathcal{U}_{m-d-k}} \exp\left(\frac{2\pi ich_0}{p^{m-d-k}} \cdot \frac{t^2 - bt}{e_r}\right) = \sum_{z=0}^{p^{m-d-k} - 1} \exp\left(\frac{2\pi ich_0}{p^{m-d-k}} \cdot \frac{z^2 - bz}{e_r}\right) - \sum_{z=0}^{p^{m-d-k-1} - 1} \exp\left(\frac{2\pi ich_0}{p^{m-d-k-1}} \cdot \frac{pz^2 - bz}{e_r}\right). \]

Now Lemma 3 applied to the last two sums shows that the first sum has absolute value \( p^{(m-d-k)/2} \) and the second sum has absolute value at most \( p^{(m-d-k)/2} \), and so the lemma is again established.

Finally, we consider the case \( 1 \leq k < m - d - k \). In (8) we put \( t = zp^m - d - 2k + u \), \( 0 \leq z < p^k \), \( u \in \mathcal{U}_{m-d-2k} \). Then

\[
p^{-d-k} \sigma_r = \sum_{u \in \mathcal{U}_{m-d-2k}} \exp\left(\frac{2\pi ich_0}{p^{m-d-k}} \cdot \frac{a + bu - u^2}{p^kcu - er}\right) \times \sum_{z=0}^{p^{k-1}-1} \exp\left(\frac{2\pi ich_0}{p^{m-d-k}} \cdot \frac{(b - 2u)p^{m-d-2k}z - p^{2m-2d-4k}z^2}{p^kcu - er}\right) \times \sum_{z=0}^{p^{k-1}-1} \exp\left(\frac{2\pi ich_0}{p^k} \cdot \frac{p^{m-d-2k}z^2 + (2u - b)z}{e_r}\right). \]
By Lemma 3, each inner sum is 0 since \( m - d - 2k > 0 \) and \( 2u - b \equiv 2u \not\equiv 0 \pmod{p} \) for all \( u \in U_{m-d-2k} \). Thus, we have \( \sigma_r = 0 \). ■

3. The bound for exponential sums. For a sequence \( u_0, u_1, \ldots \) generated by (1) and (2) with least period length \( \tau \) and for integers \( h \) and \( N \) with \( 1 \leq N \leq \tau \) we consider the exponential sum

\[
S_N(h) = \sum_{n=0}^{N-1} \exp \left( \frac{2\pi ihu_n}{p^m} \right).
\]

**Theorem 1.** Let \( p \geq 3 \) be a prime, let \( m \geq 2 \) be an integer, and let \( h \) be an integer with \( \gcd(h, p^m) = p^d, 0 \leq d < m \). Then

\[
|S_N(h)| < \frac{49}{16} \left( \frac{p^m}{\tau} \right)^{1/2} N^{1/2} p^{(m+d)/4} \quad \text{for } 1 \leq N \leq \tau.
\]

**Proof.** With the notation in (5) we can write

\[
S_N(h) = \sum_{n=0}^{N-1} \chi(u_n).
\]

Note that \( u_n = \psi^n(u_0) \) for all integers \( n \geq 0 \), and we use this identity to define \( u_n \) for all negative integers \( n \). It is easy to see that for any integer \( k \) we have

(9) \[ |S_N(h) - \sum_{n=0}^{N-1} \chi(u_{n+k})| \leq 2|k|. \]

For an integer \( K \geq 1 \) put

\[
\mathcal{R}(K) = \begin{cases} 
\{ k \in \mathbb{Z} : -(K-1)/2 \leq k \leq (K-1)/2 \} & \text{if } K \text{ is odd}, \\
\{ k \in \mathbb{Z} : -K/2 + 1 \leq k \leq K/2 \} & \text{if } K \text{ is even}.
\end{cases}
\]

Then

\[
\sum_{k \in \mathcal{R}(K)} |k| \leq K^2/4.
\]

If we use (9) for all \( k \in \mathcal{R}(K) \), then we get

(10) \[ K|S_N(h)| \leq W + K^2/2 \]

with

\[
W = \left| \sum_{n=0}^{N-1} \sum_{k \in \mathcal{R}(K)} \chi(u_{n+k}) \right| \leq \sum_{n=0}^{N-1} \left| \sum_{k \in \mathcal{R}(K)} \chi(u_{n+k}) \right|
\]

\[
= \sum_{n=0}^{N-1} \left| \sum_{k \in \mathcal{R}(K)} \chi(\psi^k(u_n)) \right|.
\]
By the Cauchy–Schwarz inequality we obtain
\[
W^2 \leq N \sum_{n=0}^{N-1} \left| \sum_{k \in \mathcal{R}(K)} \chi(\psi^k(u_n)) \right|^2 \\
\leq N \sum_{w \in \mathcal{U}_m} \left| \sum_{k \in \mathcal{R}(K)} \chi(\psi^k(w)) \right|^2 \\
\leq N \sum_{k,l \in \mathcal{R}(K)} \left| \sum_{w \in \mathcal{U}_m} \chi(\psi^k(w) - \psi^l(w)) \right| \\
\leq KNp^m + 2N \sum_{k \in \mathcal{R}(K)} \left| \sum_{w \in \mathcal{U}_m} \chi(\psi^k(w) - \psi^l(w)) \right|.
\]

Recalling that \(\psi\) is a permutation of \(\mathcal{U}_m\), we can now write
\[
\sum_{w \in \mathcal{U}_m} \chi(\psi^k(w) - \psi^l(w)) = \sum_{w \in \mathcal{U}_m} \chi(\psi^{k-l}(w) - \psi^l(w)) = \sum_{w \in \mathcal{U}_m} \chi(\psi^{k-l}(w) - w),
\]
and so
\[
W^2 \leq KNp^m + 2KN \sum_{r=1}^{K-1} |\sigma_r|,
\]
where \(\sigma_r\) is as in (4) and we assume \(K \leq \tau\). From Lemma 2, equation (7), and Lemma 4 we derive
\[
\sum_{r=1}^{K-1} |\sigma_r| \leq 2p^{(m+d)/2} \sum_{k=0}^{m-d-1} p^{k/2} N_k + (p-1)p^{m-1} \sum_{r=1}^{K-1} 1 \\
\leq 2p^{(m+d)/2} \sum_{k=0}^{m-d-1} p^{k/2}(M_k - M_{k+1}) + (p-1)p^{m-1} \frac{K}{\tau_{m-d}},
\]
where \(N_k\), resp. \(M_k\), is the number of \(r, 1 \leq r \leq K - 1\), with \(\gcd(c_r, p^m) = p^k\), resp. \(c_r \equiv 0 \pmod{p^k}\). For \(1 \leq k \leq m\) and each \(r\) counted by \(M_k\) we have \(\tau_k \mid r\) by Lemma 2. By using either [4, Lemma 6] or noting that every value modulo \(p^k\) gives rise to \(p^{m-k}\) distinct values modulo \(p^m\), we see that
\[
\tau \leq p^{m-k}\tau_k \quad \text{for } 1 \leq k \leq m.
\]
Therefore
\[
M_k \leq K/\tau_k \leq Kp^{m-k}/\tau \quad \text{for } 1 \leq k \leq m.
\]
It follows that
\[
\sum_{k=0}^{m-d-1} p^{k/2}(M_k - M_{k+1}) = M_0 + \sum_{k=1}^{m-d-1} \left( p^{k/2} - p^{(k-1)/2} \right) M_k - p^{(m-d-1)/2} M_{m-d}
\]
\[
\leq K + \left( 1 - \frac{1}{p^{1/2}} \right)^{m-d-1} \sum_{k=1}^{m-d-1} p^{k/2} M_k < K + \left( 1 - \frac{1}{p^{1/2}} \right) \frac{K p^m}{\tau} \sum_{k=1}^{\infty} p^{-k/2}
\]
\[
< \left( 1 + \frac{1}{p^{1/2}} \right) \frac{K p^m}{\tau}.
\]
Together with (12) and (13) this yields
\[
\sum_{r=1}^{K-1} |\sigma_r| < 2 \left( 1 + \frac{1}{p^{1/2}} \right) \frac{p^m}{\tau} K p^{(m+d)/2} + \frac{p - 1}{p} \frac{p^m}{\tau} K p^d
\]
\[
\leq \left( 2 + \frac{2}{p^{1/2}} + \frac{p - 1}{p^{3/2}} \right) \frac{p^m}{\tau} K p^{(m+d)/2}
\]
\[
< 3.54 \frac{p^m}{\tau} K p^{(m+d)/2}.
\]
Substituting this bound in (11), we obtain
\[
W^2 < K N p^m + 7.08 \frac{p^m}{\tau} K^2 N p^{(m+d)/2}.
\]
We put
\[
K = \lceil p^{m/2} \rceil.
\]
Then
\[
W^2 < 8.08 \frac{p^m}{\tau} K^2 N p^{(m+d)/2}.
\]
We remark that if \( \tau < K \), then the bound in Theorem 1 is trivial because
\[
|S_N(h)| \leq N \leq \tau < p^{m/2} < \frac{49}{16} \left( \frac{p^m}{p^{m/2}} \right)^{1/2} p^{m/4}
\]
\[
< \frac{49}{16} \left( \frac{p^m}{\tau} \right)^{1/2} N^{1/2} p^{(m+d)/4}.
\]
So we can assume \( K \leq \tau \), and similarly we can assume
\[
N^{1/2} \geq \frac{49}{16} p^{m/4}.
\]
because otherwise

$$|S_N(h)| \leq N < \frac{49}{16} \left(\frac{p^m}{\tau}\right)^{1/2} N^{1/2} p^{(m+d)/4}.$$

Then

$$K \leq p^{m/2} + 1 \leq \frac{64}{147} N^{1/2} p^{m/4}.$$

From (10) we conclude

$$|S_N(h)| \leq \frac{W}{K} + \frac{K}{2} \left(\sqrt{8.08} \left(\frac{p^m}{\tau}\right)^{1/2} N^{1/2} p^{(m+d)/4} + \frac{32}{147} N^{1/2} p^{m/4}\right),$$

and this yields the desired result. ■

4. The discrepancy bound. Let $u_0/p^m, u_1/p^m, \ldots, u_{N-1}/p^m$ be inversive congruential pseudorandom numbers with modulus $p^m$ and $1 \leq N \leq \tau$. The discrepancy $D_N$ of these numbers is defined by

$$D_N = \sup_{J \subseteq [0,1)} \left| \frac{A(J,N)}{N} - |J| \right|,$$

where the supremum is extended over all subintervals $J$ of $[0,1)$, $A(J,N)$ is the number of points $u_n/p^m$ in $J$ for $0 \leq n \leq N-1$, and $|J|$ is the length of $J$.

**Theorem 2.** Let $p \geq 3$ be a prime and $m \geq 2$ an integer. Then the discrepancy $D_N$ of inversive congruential pseudorandom numbers with modulus $p^m$ satisfies

$$D_N < \left(\frac{p^m}{\tau}\right)^{1/2} N^{-1/2} p^{m/4} (1.8 \log N + 15.1)$$

for $1 \leq N \leq \tau$.

**Proof.** By the Erdős–Turán inequality in the form given in [14, p. 214], for any integer $H \geq 1$ we have

$$D_N \leq \frac{1}{H+1} + \frac{2}{N} \sum_{h=1}^{H} \left(\frac{1}{\pi h} + \frac{1}{H+1}\right) |S_N(h)|,$$

where $S_N(h)$ is as in Theorem 1. We apply this bound with

$$H = \left\lfloor \left(\frac{3\tau}{p^m}\right)^{1/2} N^{1/2} p^{-m/4} \right\rfloor.$$

We can assume $H \geq 1$ since otherwise the discrepancy bound in the theorem
is trivial. By Theorem 1 we obtain
\[
\sum_{h=1}^{H} \frac{1}{h} |S_N(h)| < \frac{49}{16} \left( \frac{p^m}{\tau} \right)^{1/2} N^{1/2} p^{m/4} \sum_{d=0}^{m-1} p^{d/4} \sum_{h=1}^{H} \frac{1}{h}
\]
\[
\leq \frac{49}{16} \left( \frac{p^m}{\tau} \right)^{1/2} N^{1/2} p^{m/4} (1 + \log H) \sum_{d=0}^{m-1} p^{-3d/4}
\]
\[
< \frac{11}{2} \left( \frac{p^m}{\tau} \right)^{1/2} N^{1/2} p^{m/4} \left( 1 + \frac{1}{2} \log N \right).
\]
Similarly we get
\[
\sum_{h=1}^{H} |S_N(h)| < \frac{11}{2} \left( \frac{p^m}{\tau} \right)^{1/2} N^{1/2} p^{m/4} H.
\]
Using (14) and the special form of \(H\), we conclude
\[
D_N < \left( \frac{p^m}{3\tau} \right)^{1/2} N^{-1/2} p^{m/4}
\]
\[
+ 11 \left( \frac{p^m}{\tau} \right)^{1/2} N^{-1/2} p^{m/4} \left( \frac{1}{2\pi} \log N + \frac{1}{\pi} + 1 \right),
\]
and after simple calculations we derive the desired result. \( \blacksquare \)

Theorem 2 yields a nontrivial discrepancy bound in the case where \(N\) is at least of the order of magnitude \(p^{m/2} \log^2 \tau\). We note that, in principle, the method in this paper works also for the case \(p = 2\) which is convenient for practical implementations of pseudorandom number generators, but that some modifications have to be made in the details. It is also of interest to extend our results to inversive congruential pseudorandom numbers with an arbitrary composite modulus.

References


Institute of Discrete Mathematics  
Austrian Academy of Sciences  
Sonnenfelsgasse 19  
A-1010 Vienna, Austria  
E-mail: niederreiter@oeaw.ac.at

Department of Computing  
Macquarie University  
Sydney, NSW 2109  
Australia  
E-mail: igor@comp.mq.edu.au

Received on 11.6.1999