ACTA ARITHMETICA
XCII.1 (2000)

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

by

Harald Niederreiter (Vienna) and
Igor E. Shparlinski (Sydney)

1. Introduction. Let $p \ge 3$ be a prime and $m \ge 1$ an integer. We write $\mathcal{U}_m = (\mathbb{Z}/p^m\mathbb{Z})^*$ 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 $|\mathcal{U}_m| = (p-1)p^{m-1}$. 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 $\psi : \mathcal{U}_m \to \mathbb{Z}/p^m\mathbb{Z}$ of the form

$$\psi(w) = aw^{-1} + b \quad \text{for } w \in \mathcal{U}_m. \tag{1}$$

It is easy to see that ψ is a permutation of $\mathcal{U}_m$ 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 $u_0 \in \mathcal{U}_m$, then the recurrence relation

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

generates a sequence $u_0, u_1, \ldots$ of elements of $\mathcal{U}_m$. It is obvious that this sequence is purely periodic with least period length $\tau \le (p-1)p^{m-1}$. Detailed studies of the possible values of τ 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

$$\sum_{n=0}^{N-1} \chi(u_n), \tag{3}$$

where χ is a nontrivial additive character of $\mathbb{Z}/p^m\mathbb{Z}$ and $1 \le N \le \tau$. In the case $m = 1$, and with a slight change of formula (1) to arrive at more

1991 *Mathematics Subject Classification*: 11K38, 11K45, 11L07, 11T23, 65C10.

interesting permutations ψ of $\mathcal{U}_1$, 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 $\mathcal{U}_m$ as above, then the numbers $u_0/p^m, u_1/p^m, \ldots$ in the interval $[0,1)$ form a sequence of *inversive 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 inversive 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 inversive 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 inversive 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 ψ is the permutation of $\mathcal{U}_m, m \geq 1$, given by (1) and r is an arbitrary integer, then let ψ^r denote the rth power of ψ in the group of permutations of $\mathcal{U}_m$. 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*

$$\psi^r(w) = \frac{(bc_r - e_r)w + ac_r}{c_r w - e_r} \quad \text{for all } w \in \mathcal{U}_m.$$

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 τ_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* τ_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 $w \in \mathcal{U}_m$. Then r is a period length of the sequence $u_0, u_1, \ldots$ considered modulo p^k, and so τ_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*

$$\sum_{z=0}^{p^m-1} \exp\left(\frac{2\pi i(fz^2 + gz)}{p^m}\right) = 0 \qquad \text{if } g \not\equiv 0 \pmod{p^l}$$

and

$$\left|\sum_{z=0}^{p^m-1} \exp\left(\frac{2\pi i(fz^2 + gz)}{p^m}\right)\right| = p^{(m+l)/2} \qquad \text{if } g \equiv 0 \pmod{p^l}.$$

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

For $1 \leq r \leq \tau - 1$ and a nontrivial additive character χ of $\mathbb{Z}/p^m\mathbb{Z}$ we introduce the exponential sum

$$\sigma_r = \sum_{w \in \mathcal{U}_m} \chi(\psi^r(w) - w). \tag{4}$$

Note that χ is determined by an integer $h \not\equiv 0 \pmod{p^m}$, in the sense that

$$\chi(v) = \exp\left(\frac{2\pi i h v}{p^m}\right) \qquad \text{for all } v \in \mathbb{Z}/p^m\mathbb{Z}. \tag{5}$$

Put $\gcd(h, p^m) = p^d$ with $0 \leq d < m$, so that we can write $h = p^d h_0$ with an integer $h_0 \not\equiv 0 \pmod{p}$. By Lemma 1 we have

$$\sigma_r = \sum_{w \in \mathcal{U}_m} \chi\left(\frac{c_r(a + bw - w^2)}{c_r w - e_r}\right).$$

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

$$\sigma_r = \sum_{w \in \mathcal{U}_m} \exp\left(\frac{2\pi i p^{d+k}}{p^m} \cdot \frac{ch_0(a + bw - w^2)}{p^k cw - e_r}\right). \tag{6}$$

It is trivial that

$$\sigma_r = |\mathcal{U}_m| = (p-1)p^{m-1} \qquad \text{if } d + k \geq m. \tag{7}$$

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

LEMMA 4. *With the notation above we have*

$$|\sigma_r| \leq 2p^{(m+d+k)/2} \qquad \text{if } d + k < m.$$

Proof. In (6) we put $w = sp^{m-d-k} + t$ with $0 \le s < p^{d+k}$ and $t \in \mathcal{U}_{m-d-k}$. Then

$$\sigma_r = p^{d+k} \sum_{t \in \mathcal{U}_{m-d-k}} \exp\left(\frac{2\pi i c h_0}{p^{m-d-k}} \cdot \frac{a + bt - t^2}{p^k ct - e_r}\right). \tag{8}$$

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

$$|\sigma_r| = p^d \left| \sum_{v \in \mathcal{U}_{m-d}} \exp\left(\frac{2\pi i c h_0}{p^{m-d}}((a + bc^{-1}e_r - c^{-2}e_r^2)v^{-1} - c^{-2}v)\right)\right|.$$

The last exponential sum is always bounded by $2p^{(m-d)/2}$, namely by a result in [13, p. 97] for $d \le m - 2$ 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 $k \ge m - d - k$. Then from (8) we get

$$|\sigma_r| = p^{d+k} \left| \sum_{t \in \mathcal{U}_{m-d-k}} \exp\left(\frac{2\pi i c h_0}{p^{m-d-k}} \cdot \frac{t^2 - bt}{e_r}\right)\right|.$$

Furthermore,

$$\sum_{t \in \mathcal{U}_{m-d-k}} \exp\left(\frac{2\pi i c h_0}{p^{m-d-k}} \cdot \frac{t^2 - bt}{e_r}\right)$$
$$= \sum_{z=0}^{p^{m-d-k}-1} \exp\left(\frac{2\pi i c h_0}{p^{m-d-k}} \cdot \frac{z^2 - bz}{e_r}\right) - \sum_{z=0}^{p^{m-d-k-1}-1} \exp\left(\frac{2\pi i c h_0}{p^{m-d-k-1}} \cdot \frac{pz^2 - bz}{e_r}\right).$$

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

$$\begin{aligned}
p^{-d-k}\sigma_r = {} & \sum_{u \in \mathcal{U}_{m-d-2k}} \exp\left(\frac{2\pi i c h_0}{p^{m-d-k}} \cdot \frac{a + bu - u^2}{p^k cu - e_r}\right) \\
& \times \sum_{z=0}^{p^k-1} \exp\left(\frac{2\pi i c h_0}{p^{m-d-k}} \cdot \frac{(b - 2u)p^{m-d-2k}z - p^{2m-2d-4k}z^2}{p^k cu - e_r}\right) \\
= {} & \sum_{u \in \mathcal{U}_{m-d-2k}} \exp\left(\frac{2\pi i c h_0}{p^{m-d-k}} \cdot \frac{a + bu - u^2}{p^k cu - e_r}\right) \\
& \times \sum_{z=0}^{p^k-1} \exp\left(\frac{2\pi i c h_0}{p^k} \cdot \frac{p^{m-d-2k}z^2 + (2u - b)z}{e_r}\right).
\end{aligned}$$

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 $u\in\mathcal{U}_{m-d-2k}$. 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 τ and for integers h and N with $1\le N\le\tau$ we consider the exponential sum

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

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

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

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 $n\ge 0$, 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

$$\Big|S_N(h)-\sum_{n=0}^{N-1}\chi(u_{n+k})\Big|\le 2|k|. \tag{9}$$

For an integer $K\ge 1$ put

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

Then

$$\sum_{k\in\mathcal{R}(K)}|k|\le K^2/4.$$

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

$$K|S_N(h)|\le W+K^2/2 \tag{10}$$

with

$$\begin{aligned}W&=\Big|\sum_{n=0}^{N-1}\sum_{k\in\mathcal{R}(K)}\chi(u_{n+k})\Big|\le\sum_{n=0}^{N-1}\Big|\sum_{k\in\mathcal{R}(K)}\chi(u_{n+k})\Big|\\&=\sum_{n=0}^{N-1}\Big|\sum_{k\in\mathcal{R}(K)}\chi(\psi^k(u_n))\Big|.\end{aligned}$$

By the Cauchy–Schwarz inequality we obtain

$$\begin{aligned}W^2 &\le N \sum_{n=0}^{N-1} \Big| \sum_{k\in\mathcal{R}(K)} \chi(\psi^k(u_n))\Big|^2 \\ &\le N \sum_{w\in\mathcal{U}_m} \Big| \sum_{k\in\mathcal{R}(K)} \chi(\psi^k(w))\Big|^2 \\ &\le N \sum_{k,l\in\mathcal{R}(K)} \Big| \sum_{w\in\mathcal{U}_m} \chi(\psi^k(w)-\psi^l(w))\Big| \\ &\le KNp^m + 2N \sum_{\substack{k,l\in\mathcal{R}(K)\\ k>l}} \Big| \sum_{w\in\mathcal{U}_m} \chi(\psi^k(w)-\psi^l(w))\Big|.\end{aligned}$$

Recalling that ψ is a permutation of $\mathcal{U}_m$, we can now write

$$\begin{aligned}\sum_{w\in\mathcal{U}_m} \chi(\psi^k(w)-\psi^l(w)) &= \sum_{w\in\mathcal{U}_m} \chi(\psi^{k-l}(\psi^l(w))-\psi^l(w)) \\ &= \sum_{w\in\mathcal{U}_m} \chi(\psi^{k-l}(w)-w),\end{aligned}$$

and so

$$W^2 \le KNp^m + 2KN \sum_{r=1}^{K-1} |\sigma_r|, \tag{11}$$

where σ_r is as in (4) and we assume $K \le \tau$. From Lemma 2, equation (7), and Lemma 4 we derive

$$\begin{aligned}\sum_{r=1}^{K-1} |\sigma_r| &\le 2p^{(m+d)/2} \sum_{k=0}^{m-d-1} p^{k/2} N_k + (p-1)p^{m-1} \sum_{\substack{r=1\\ \tau_{m-d}\mid r}}^{K-1} 1 \\ &\le 2p^{(m+d)/2} \sum_{k=0}^{m-d-1} p^{k/2}(M_k - M_{k+1}) + (p-1)p^{m-1}\frac{K}{\tau_{m-d}},\end{aligned} \tag{12}$$

where N_k, resp. M_k, is the number of $r, 1 \le r \le K-1$, with $\gcd(c_r, p^m) = p^k$, resp. $c_r \equiv 0 \pmod{p^k}$. For $1 \le k \le m$ 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

$$\tau \le p^{m-k}\tau_k \quad \text{for } 1 \le k \le m. \tag{13}$$

Therefore

$$M_k \le K/\tau_k \le Kp^{m-k}/\tau \quad \text{for } 1 \le k \le m.$$

It follows that

$$\begin{aligned}
&\sum_{k=0}^{m-d-1} p^{k/2}(M_k - M_{k+1})\\
&= M_0 + \sum_{k=1}^{m-d-1} (p^{k/2} - p^{(k-1)/2})M_k - p^{(m-d-1)/2}M_{m-d}\\
&\le K + \left(1 - \frac{1}{p^{1/2}}\right)\sum_{k=1}^{m-d-1} p^{k/2}M_k < K + \left(1 - \frac{1}{p^{1/2}}\right)\frac{Kp^m}{\tau}\sum_{k=1}^{\infty} p^{-k/2}\\
&< \left(1 + \frac{1}{p^{1/2}}\right)\frac{Kp^m}{\tau}.
\end{aligned}$$

Together with (12) and (13) this yields

$$\begin{aligned}
\sum_{r=1}^{K-1} |\sigma_r| &< 2\left(1 + \frac{1}{p^{1/2}}\right)\frac{p^m}{\tau}Kp^{(m+d)/2} + \frac{p-1}{p}\cdot\frac{p^m}{\tau}Kp^d\\
&\le \left(2 + \frac{2}{p^{1/2}} + \frac{p-1}{p^{3/2}}\right)\frac{p^m}{\tau}Kp^{(m+d)/2}\\
&< 3.54\frac{p^m}{\tau}Kp^{(m+d)/2}.
\end{aligned}$$

Substituting this bound in (11), we obtain

$$W^2 < KNp^m + 7.08\frac{p^m}{\tau}K^2Np^{(m+d)/2}.$$

We put

$$K = \lceil p^{m/2}\rceil.$$

Then

$$W^2 < 8.08\frac{p^m}{\tau}K^2Np^{(m+d)/2}.$$

We remark that if $\tau < K$, then the bound in Theorem 1 is trivial because

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

So we can assume $K \le \tau$, and similarly we can assume

$$N^{1/2} \ge \frac{49}{16}p^{m/4}$$

because otherwise

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

Then

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

From (10) we conclude

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

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 $1 \le N \le \tau$. 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 $0 \le n \le N-1$, and $|J|$ is the length of J.

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

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

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

$$D_N \le \frac{1}{H+1} + \frac{2}{N} \sum_{h=1}^{H} \left(\frac{1}{\pi h} + \frac{1}{H+1}\right) |S_N(h)|, \tag{14}$$

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 $H \ge 1$ since otherwise the discrepancy bound in the theorem is trivial. By Theorem 1 we obtain

$$\begin{aligned}\sum_{h=1}^{H}\frac{1}{h}|S_N(h)| &< \frac{49}{16}\Big(\frac{p^m}{\tau}\Big)^{1/2}N^{1/2}p^{m/4}\sum_{d=0}^{m-1}p^{d/4}\sum_{\substack{h=1\\ p^d|h}}^{H}\frac{1}{h}\\ &\le \frac{49}{16}\Big(\frac{p^m}{\tau}\Big)^{1/2}N^{1/2}p^{m/4}(1+\log H)\sum_{d=0}^{m-1}p^{-3d/4}\\ &< \frac{11}{2}\Big(\frac{p^m}{\tau}\Big)^{1/2}N^{1/2}p^{m/4}\Big(1+\frac{1}{2}\log N\Big).\end{aligned}$$

Similarly we get

$$\sum_{h=1}^{H}|S_N(h)| < \frac{11}{2}\Big(\frac{p^m}{\tau}\Big)^{1/2}N^{1/2}p^{m/4}H.$$

Using (14) and the special form of H, we conclude

$$\begin{aligned}D_N &< \Big(\frac{p^m}{3\tau}\Big)^{1/2}N^{-1/2}p^{m/4}\\ &\quad + 11\Big(\frac{p^m}{\tau}\Big)^{1/2}N^{-1/2}p^{m/4}\Big(\frac{1}{2\pi}\log N+\frac{1}{\pi}+1\Big),\end{aligned}$$

and after simple calculations we derive the desired result. ■

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

[1] W.-S. Chou, *The period lengths of inversive congruential recursions*, Acta Arith. 73 (1995), 325–341.

[2] J. Eichenauer-Herrmann, E. Herrmann and S. Wegenkittl, *A survey of quadratic and inversive congruential pseudorandom numbers*, in: Monte Carlo and Quasi-Monte Carlo Methods 1996, H. Niederreiter *et al.* (eds.), Lecture Notes in Statist. 127, Springer, New York, 1998, 66–97.

[3] J. Eichenauer-Herrmann and H. Niederreiter, *On the discrepancy of quadratic congruential pseudorandom numbers*, J. Comput. Appl. Math. 34 (1991), 243–249.

[4] J. Eichenauer-Herrmann and A. Topuzoğlu, *On the period length of congruential pseudorandom number sequences generated by inversions*, ibid. 31 (1990), 87–96.

[5] F. Griffin, H. Niederreiter and I. E. Shparlinski, *On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders*, in: Proc. 13th Sympos. on Appl. Algebra, Algebraic Algorithms, and Error-Correcting Codes, Hawaii, 1999, Lecture Notes in Comput. Sci., Springer, Berlin, to appear.

[6] J. Gutierrez, H. Niederreiter and I. E. Shparlinski, *On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period*, Monatsh. Math., to appear.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983; reprint, Cambridge Univ. Press, Cambridge, 1997.

[8] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[9] —, *New developments in uniform pseudorandom number and vector generation*, in: Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, H. Niederreiter and P.J.-S. Shiue (eds.), Lecture Notes in Statist. 106, Springer, New York, 1995, 87–120.

[10] H. Niederreiter and I. E. Shparlinski, *On the distribution of inversive congruential pseudorandom numbers in parts of the period*, preprint, 1998.

[11] —, —, *On the distribution and lattice structure of nonlinear congruential pseudorandom numbers*, Finite Fields Appl. 5 (1999), 246–253.

[12] —, —, *On the distribution of pseudorandom numbers and vectors generated by inversive methods*, Appl. Algebra Engrg. Comm. Comput., to appear.

[13] H. Salié, *Über die Kloostermanschen Summen $S(u,v;q)$*, Math. Z. 34 (1932), 91–109.

[14] J. D. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc. (N.S.) 12 (1985), 183–216.

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 (3621)