MATHEMATICS OF COMPUTATION
Volume 70, Number 236, Pages 1569–1574
S 0025-5718(00)01273-4
Article electronically published on June 12, 2000

# ON THE DISTRIBUTION OF INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS IN PARTS OF THE PERIOD

HARALD NIEDERREITER AND IGOR E. SHPARLINSKI

ABSTRACT. The inversive congruential method is an attractive alternative to the classical linear congruential method for pseudorandom number generation. In this paper we present the first nontrivial bounds on the discrepancy of individual sequences of inversive congruential pseudorandom numbers in parts of the period. The proof is based on a new bound for certain incomplete exponential sums.

## 1. INTRODUCTION

Let $p$ be a (large) prime and let $\mathbb{F}_p$ be the field of $p$ elements which we identify with the least residue system modulo $p$. For given $a \in \mathbb{F}_p^*$, $b \in \mathbb{F}_p$, let $\psi$ be the permutation of $\mathbb{F}_p$ defined by

$$\psi(w) = \begin{cases} aw^{-1} + b, & \text{if } w \neq 0, \\ b, & \text{if } w = 0. \end{cases} \tag{1}$$

Let $u_0, u_1, \ldots$ be the sequence of elements of $\mathbb{F}_p$ obtained by the recurrence relation

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

where $u_0$ is the *initial value*. Then the numbers $u_0/p, u_1/p, \ldots$ in the interval $[0, 1)$ form a sequence of *inversive congruential pseudorandom numbers*. It is obvious that the sequence (2) is purely periodic with some period $t \leq p$.

The inversive congruential generator provides a very attractive alternative to linear congruential generators and has been extensively studied in the literature. In particular, several results about the period of this generator have been obtained. For example, it is known when such sequences achieve the largest possible period, which is obviously $t = p$ (see [5]). For such sequences of period $t = p$, a number of results about the distribution and statistical almost-independence of the points $u_n/p$ over the full period have been established, starting with the paper [9]. Many of these results are essentially best possible. We refer to [4, 7, 9, 10, 11, 12] for more detail and references to original papers. On the other hand, it has been an important open question to obtain nontrivial results about the distribution of the above fractions in parts of the period. The results obtained so far for parts of

Received by the editor November 17, 1998 and, in revised form, November 19, 1999.
2000 *Mathematics Subject Classification.* Primary 11K45, 65C10; Secondary 11K38, 11L07, 11T23.
*Key words and phrases.* Pseudorandom numbers, inversive congruential method, discrepancy, exponential sums.

the period refer only to an average-case analysis for a certain set of parameters (see [2, 3]), but not to individual sequences of inversive congruential pseudorandom numbers. The case of periods $t < p$ is of interest as well.

Here we describe a method which allows us to give the first nontrivial bounds on the discrepancy of an individual sequence of inversive congruential pseudorandom numbers in parts of the period. In [13] similar results have been obtained for sequences satisfying the relation $u_{n+1} = f(u_n)$ with a polynomial $f(X) \in \mathbb{F}_p[X]$. In the very special but important case when $f(X) = X^e$, that is, for the *power generator*, an alternative approach has been proposed in [6]. This approach, although it has produced quite strong results for the power generator, cannot be extended to other nonlinear generators.

We thank the referee for suggesting improvements to the constants in the original versions of Theorems 1 and 2 of this paper.

## 2. Discrepancy bound

Let $u_0/p, u_1/p, \ldots, u_{N-1}/p$ be inversive congruential pseudorandom numbers with $1 \le N \le t$, where the period $t$ is arbitrary. The *discrepancy* $D_N$ of these numbers is defined by

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

where the supremum is extended over all subintervals $J$ of $[0,1)$, $A(J,N)$ is the number of points $u_n/p$ in $J$ for $0 \le n \le N-1$, and $\lambda(J)$ is the length of $J$. According to a standard principle, we can bound the discrepancy $D_N$ by bounding the corresponding exponential sums

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

for integers $h \not\equiv 0 \pmod p$.

**Theorem 1.** *For any prime $p$ and any integer $h \not\equiv 0 \pmod p$ we have*

$$|S_h(N)| < \left(\left(\frac{8}{3}\right)^{1/2} + 2\right)^{1/2} N^{1/2} p^{1/4} + \left(\frac{3}{8}\right)^{1/2} p^{1/2}, \qquad 1 \le N \le t.$$

*Proof.* The theorem is trivial for $N \le 2p^{1/2}$ since in this case the upper bound for $|S_h(N)|$ in the theorem is greater than $N$. Thus, we can assume that $N > 2p^{1/2}$. By the way, this implies that $p \ge t \ge N > 2p^{1/2}$, and so $p \ge 5$. Fix the prime $p \ge 5$ and the integer $h \not\equiv 0 \pmod p$, and write

$$\chi(w) = \exp\left(\frac{2\pi i h w}{p}\right), \qquad w \in \mathbb{F}_p.$$

Then

$$S_h(N) = \sum_{n=0}^{N-1} \chi(u_n).$$

For any integer $m$ let $\psi^m$ denote the $m$th power of the permutation $\psi$ given by (1) in the symmetric group on $p$ symbols. Then $u_n = \psi^n(u_0)$ 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

$$\left| S_h(N) - \sum_{n=0}^{N-1} \chi\left(u_{n+k}\right) \right| \le 2|k|. \tag{3}$$

For an integer $K \ge 1$ put

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

thus,

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

Therefore, if we use (3) for all $k \in \mathcal{R}(K)$, then we get

$$K|S_h(N)| \le W + K^2/2, \tag{4}$$

with

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

By the Cauchy–Schwarz inequality we obtain

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

Recalling that $\psi$ is a permutation, we can now write

$$\begin{aligned} \sum_{w \in \mathbb{F}_p} \chi\left(\psi^k\left(w\right) - \psi^l\left(w\right)\right) &= \sum_{w \in \mathbb{F}_p} \chi\left(\psi^{k-l}\left(\psi^l\left(w\right)\right) - \psi^l\left(w\right)\right) \\ &= \sum_{w \in \mathbb{F}_p} \chi\left(\psi^{k-l}\left(w\right) - w\right), \end{aligned}$$

and so

$$W^2 \le KNp + 2N \sum_{m=1}^{K-1} (K-m) \left| \sum_{w \in \mathbb{F}_p} \chi\left(\psi^m\left(w\right) - w\right) \right|. \tag{5}$$

Now we assume that $K \le t$. Then it follows by straightforward induction that for $1 \le m \le K-1$ there exist nonzero constant or linear polynomials $f_m, g_m \in \mathbb{F}_p[X]$ such that

$$\psi^m(w) = \frac{f_m(w)}{g_m(w)}$$

for all $w \in \mathbb{F}_p \backslash \mathcal{E}_m$, where $\mathcal{E}_m$ consists of the roots of all polynomials $g_j$, $1 \le j \le m$. Thus $|\mathcal{E}_m| \le m$ and

$$\left| \sum_{w \in \mathbb{F}_p} \chi\left(\psi^m(w) - w\right) - \sum_{\substack{w \in \mathbb{F}_p \\ g_m(w) \ne 0}} \chi\left(\frac{f_m(w)}{g_m(w)} - w\right) \right| \le 2m - 1$$

for $1 \le m \le K-1$. Indeed, it is easy to see that the first sum may contain at most $m$ terms which do not occur in the second sum, and the second sum may contain at most $m-1$ terms which do not occur in the first sum.

A closer inspection of the polynomials $f_m$ and $g_m$ shows that if $g_m$ is a nonzero constant polynomial, then $\psi^m(w) = w$ for all $w \in \mathbb{F}_p \backslash \mathcal{E}_m$. But since $|\mathcal{E}_m| \le m < t$, there exists $u_n \notin \mathcal{E}_m$, and then $\psi^m(u_n) = u_{m+n} \ne u_n$. Hence the case where $g_m$ is a nonzero constant polynomial need not be considered here. If $g_m$ is a linear polynomial, then

$$\left| \sum_{\substack{w \in \mathbb{F}_p \\ g_m(w) \ne 0}} \chi\left(\frac{f_m(w)}{g_m(w)} - w\right) \right| = \left| \sum_{w \in \mathbb{F}_p^*} \chi\left(dw^{-1} + ew\right) \right|$$

for some $d \in \mathbb{F}_p$ and $e \in \mathbb{F}_p^*$. The last sum is a Kloosterman sum over $\mathbb{F}_p$, and since such a sum is bounded in absolute value by $2p^{1/2}$ (see Theorem 5.45 of [8]), we obtain

$$\left| \sum_{w \in \mathbb{F}_p} \chi\left(\psi^m(w) - w\right) \right| \le 2p^{1/2} + 2m - 1, \qquad 1 \le m \le K-1.$$

Together with (5) this yields

$$\begin{aligned} W^2 &\le KNp + 2N \sum_{m=1}^{K-1} (K-m)\left(2p^{1/2} + 2m - 1\right) \\ &= KNp + (K-1)KN\left(2p^{1/2} + (2K-1)/3\right) \\ &< KNp + (K-1)KN\left(2p^{1/2} + 2K/3\right) \\ &= K^2N\left((p - 2p^{1/2})K^{-1} + 2p^{1/2} - 2/3 + 2K/3\right). \end{aligned}$$

By combining this with (4), we arrive at

$$|S_h(N)| < N^{1/2}\left((p - 2p^{1/2})K^{-1} + 2p^{1/2} - 2/3 + 2K/3\right)^{1/2} + K/2,$$

under the condition that $K \le t$. Now we put

$$K = \left\lceil \left(\frac{3}{2}\right)^{1/2} (p - 2p^{1/2})^{1/2} \right\rceil.$$

Then $t \geq N > 2p^{1/2}$ shows that the condition $K \leq t$ is satisfied. For this choice of $K$ we have

$$\begin{aligned}(p-2p^{1/2})K^{-1} &+ 2p^{1/2} - 2/3 + 2K/3 \\ &\leq \left(\frac{2}{3}\right)^{1/2}(p-2p^{1/2})^{1/2} + 2p^{1/2} + \left(\frac{2}{3}\right)^{1/2}(p-2p^{1/2})^{1/2} \\ &< \left(\frac{8}{3}\right)^{1/2} p^{1/2} + 2p^{1/2}.\end{aligned}$$

Thus we get

$$|S_h(N)| < N^{1/2}\left(\left(\frac{8}{3}\right)^{1/2} p^{1/2} + 2p^{1/2}\right)^{1/2} + \left(\frac{3}{8}\right)^{1/2}(p-2p^{1/2})^{1/2} + \frac{1}{2}.$$

Using the inequalities $(p-2p^{1/2})^{1/2} < p^{1/2} - 1$ and $(3/8)^{1/2} > 1/2$, we conclude the proof. □

**Theorem 2.** *The discrepancy $D_N$ of the inversive congruential pseudorandom numbers $u_0/p, u_1/p, \ldots, u_{N-1}/p$ satisfies*

$$D_N \leq \left(\left(\left(\frac{8}{3}\right)^{1/2} + 2\right)^{1/2} N^{-1/2}p^{1/4} + \left(\frac{3}{8}\right)^{1/2} N^{-1}p^{1/2}\right)\left(\frac{4}{\pi^2}\log p + \frac{2}{5}\right) + \frac{1}{p}$$

*for $1 \leq N \leq t$.*

*Proof.* According to a general discrepancy bound, given by Corollary 3.11 of [10] in combination with an inequality of Cochrane [1], we have

$$D_N \leq \frac{B}{N}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.608}{p} + \frac{0.116}{p^2}\right) + \frac{1}{p},$$

where $B$ is a bound on all $|S_h(N)|$ for integers $h \not\equiv 0 \pmod{p}$. For $p \geq 31$ we can take

$$B = \left(\left(\frac{8}{3}\right)^{1/2} + 2\right)^{1/2} N^{1/2}p^{1/4} + \left(\frac{3}{8}\right)^{1/2} p^{1/2}$$

by Theorem 1, and then the desired bound on $D_N$ follows. For primes $p \leq 29$ the theorem is trivial since we always have $D_N \leq 1$. □

Theorem 2 yields a nontrivial discrepancy bound only in the case where $N$, and therefore $t$, is at least of the order of magnitude $p^{1/2}\log^2 p$. In this case we get

$$D_N = O\left(N^{-1/2}p^{1/4}\log p\right), \qquad N \leq t,$$

with an absolute implied constant.

## 3. Remarks

It would be important to study the distribution of the $s$-tuples

$$(u_n/p, \ldots, u_{n+s-1}/p), \qquad 0 \leq n \leq N-1.$$

The case $N = t = p$ has been treated in [9]. For polynomial generators it has been done in [13] (although the results are rather weak). It would be very interesting to

extend the results of this paper to the case of nonlinear generators with rational functions $f(X) \in \mathbb{F}_p(X)$.

We also believe that our method is able to produce nontrivial results about the distribution of sequences satisfying nonlinear recurrence relations of order $m \geq 2$, that is, of the form

$$u_{n+m} = f(u_{n+m-1}, \ldots, u_n), \qquad n = 0, 1, \ldots,$$

where $f(X_1, \ldots, X_m) \in \mathbb{F}_p(X_1, \ldots, X_m)$ is a rational function over $\mathbb{F}_p$.

Finally we remark that our method works for generators modulo a composite number as well. But one should expect weaker results because instead of the very powerful Weil bound one will have to use bounds on exponential sums with composite denominator which are essentially weaker (see [14]).

## References


[1] T. Cochrane, 'On a trigonometric inequality of Vinogradov', *J. Number Theory*, **27** (1987), 9–16. MR **88k:**11053

[2] J. Eichenauer-Herrmann and F. Emmerich, 'Compound inversive congruential pseudorandom numbers: an average-case analysis', *Math. Comp.*, **65** (1996), 215–225. MR **96i:**65005

[3] J. Eichenauer-Herrmann, F. Emmerich, and G. Larcher, 'Average discrepancy, hyperplanes, and compound pseudorandom numbers', *Finite Fields Appl.*, **3** (1997), 203–218. MR **98j:**11059

[4] J. Eichenauer-Herrmann, E. Herrmann, and S. Wegenkittl, 'A survey of quadratic and inversive congruential pseudorandom numbers', *Lect. Notes in Statistics*, Springer-Verlag, Berlin, **127** (1998), 66–97.

[5] M. Flahive and H. Niederreiter, 'On inversive congruential generators for pseudorandom numbers', *Finite Fields, Coding Theory, and Advances in Communications and Computing* (G.L. Mullen and P.J.-S. Shiue, eds.), Marcel Dekker, New York, 1993, 75–80. MR **94a:**11117

[6] J.B. Friedlander, D. Lieman, and I.E. Shparlinski, 'On the distribution of the RSA generator', *Sequences and Their Applications* (C. Ding, T. Helleseth, and H. Niederreiter, eds.), Springer-Verlag, London, 1999, 205–212.

[7] R. Lidl and H. Niederreiter, 'Finite fields and their applications', *Handbook of Algebra* (M. Hazewinkel, ed.), Vol. 1, Elsevier, Amsterdam, 1996, 321–363. MR **97i:**11114

[8] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997. MR **97i:**11115

[9] H. Niederreiter, 'The serial test for congruential pseudorandom numbers generated by inversions', *Math. Comp.*, **52** (1989), 135–144.

[10] H. Niederreiter, *Random number generation and quasi–Monte Carlo methods*, SIAM, Philadelphia, 1992. MR **93h:**65008

[11] H. Niederreiter, 'Finite fields, pseudorandom numbers, and quasirandom points', *Finite Fields, Coding Theory, and Advances in Communications and Computing* (G.L. Mullen and P.J.-S. Shiue, eds.), Marcel Dekker, New York, 1993, 375–394. MR **94a:**11121

[12] H. Niederreiter, 'New developments in uniform pseudorandom number and vector generation', *Lect. Notes in Statistics*, Springer-Verlag, Berlin, **106** (1995), 87–120. MR **97k:**65019

[13] H. Niederreiter and I.E. Shparlinski, 'On the distribution and lattice structure of nonlinear congruential pseudorandom numbers', *Finite Fields Appl.*, **5** (1999), 246–253. CMP 99:17

[14] S.B. Stečkin, 'An estimate of a complete rational trigonometric sum', *Trudy Mat. Inst. Steklov.*, **143** (1977), 188–207 (in Russian). MR **58:**543



Institute of Discrete Mathematics, Austrian Academy of Sciences, Sonnenfelsgasse 19, A–1010 Vienna, Austria

*E-mail address*: niederreiter@oeaw.ac.at

Department of Computing, Macquarie University, New South Wales 2109, Australia

*E-mail address*: igor@comp.mq.edu.au