On the Distribution of the Power Generator over a Residue Ring for Parts of the Period

Edwin D. El-Mahassni

Department of Computing
Macquarie University
North Ryde, NSW, Australia, 2109
edwinelm@ics.mq.edu.au

Received: March 13, 2007
Accepted: October 11, 2007

ABSTRACT

This paper studies the distribution of the power generator of pseudorandom numbers over a residue ring for parts of the period. These results compliment some recently obtained distribution bounds of the power generator modulo an arbitrary number for the entire period. Also, the arbitrary modulus case may have some cryptography related applications and could be of interest in other settings which require quality pseudorandom numbers.

Key words: sequences, pseudorandom numbers, discrepancy, exponential sums.

2000 Mathematics Subject Classification: Primary 11L07, 11K38; Secondary 11B50, 11K45.

Introduction

Let $e \geq 2$, $M \geq 1$, and ϑ be integers such that $\gcd(\vartheta, M) = 1$. Then one can define the sequence (u_n) by the recurrence relation

$$u_n \equiv u_{n-1}^e \pmod{M}, \quad 0 \leq u_n \leq M-1, \qquad n = 1, 2, \ldots, \tag{1}$$

with the *initial value* $u_0 = \vartheta$.

This sequence is known as the *power generator* of pseudorandom numbers.

It is obvious that the sequence (1) eventually becomes periodic with some period τ. In this paper we assume that $\gcd(e, \varphi(M)) = 1$; and so it follows that the sequence (u_n) is *purely periodic*. Apart from some results such as those in [1–5, 10,

ISSN: 1139-1138
http://dx.doi.org/10.5209/rev_REMA.2008.v21.n2.16374

13, 18, 19], as well as [14, 16, 24] which deal with the power generator in more detail, very little else is known about the distribution of the sequence of numbers produced by the power generator. More specifically [7, 11] contain distribution bounds for the case when the modulus is a prime power.

Here we show that the original method of [20], and more recently also used in [8, 9], combined with bounds for exponential sums with sparse polynomials from [12] allows us to study the distribution of the power generator of pseudorandom numbers over a residue ring. In particular, in [12] a distribution result for the sequence generated by (1) has been established for the sequence over the entire period. However, no analogous results exist for segments of this sequence. In some cases, obtaining a bound for subsets of a sequence is a much more difficult problem than for the entire period, e.g., [25]. Furthermore, some publications explicitly set out to obtain results which only deal with such subsets, e.g., [17, 22] and more recently [7]. Further, the later applies to prime power moduli, whereas here we aim to establish a result for any arbitrary modulus.

Several other results about non-linear pseudorandom number generators have been obtained in [8, 9, 15]. However these apply to generators of the form $u_n \equiv f(u_{n-1}) \pmod M$ where f is a polynomial or a rational function, whilst [17, 21, 22] provide results for the inverse generator. Both of these types of generators, however, are of small degree, while in this paper we do not impose any restrictions on the size of the exponent e.

1. Preliminaries

For a sequence of N points

$$\Gamma = (\gamma_n), \qquad n = 1, \ldots, N \tag{2}$$

in the half-open interval $[0, 1)$, denote by Δ_Γ its *discrepancy*, that is,

$$\Delta_\Gamma = \sup_{B \subseteq [0,1)} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence Γ which hit the interval

$$B = [\alpha_1, \beta_1) \subseteq [0, 1)$$

and the supremum is taken over all such intervals.

Also, for an integer $a \in \mathbb{Z}$, we put $|a| = \max\{|a|, 1\}$.

This discrepancy of a sequence of points in the 1-dimensional unit cube can be estimated by the well-known *Erdös–Turán inequality* (see [6, Theorem 1.21]) which we present in the following form.

Lemma 1.1. *There exists a constant $C > 0$ such that, for any integer $L \geq 1$, for the discrepancy of a sequence of points* (2) *the bound*

$$\Delta_\Gamma < C\left(\frac{1}{L} + \frac{1}{N}\sum_{0<|a|\leq L}\frac{1}{|a|}\left|\sum_{n=1}^{N}\exp(2\pi i a\gamma_n)\right|\right)$$

holds, where the sum is taken over all integers $a \in \mathbb{Z}$ with $0 < |a| \leq L$.

Define the residue ring $\mathbb{Z}_M = \mathbb{Z}/M\mathbb{Z}$ for a positive integer M, where we identify $\mathbb{Z}_M$ with the integers $\{0, \ldots, M-1\}$.

For an integer $a \in \mathbb{Z}$ we define the exponential sum

$$S_a(t, \tau; M, N) = \sum_{n=0}^{N-1} \mathbf{e}_M\big(a\vartheta^{e^n}\big).$$

where

$$\mathbf{e}_M(z) = \exp(2\pi i z/M),$$

and where t and τ are the multiplicative orders of ϑ and e respectively, with $N \leq \tau$.

In this paper, we obtain a non-trivial upper bound for the sums $S_a(t, \tau; M, N)$ and derive (see Theorem 2.2) the uniformity of distribution modulo M of the elements u_n, $n = 1, \ldots, N \leq \tau$.

To prove our main result, we also make use the following lemma from [12].

Lemma 1.2. *Let a, c be integers with $\gcd(a, M) = \delta_a < M$. Then the bound*

$$\sum_{y=1}^{t}\left|\sum_{x=1}^{t}\mathbf{e}_M(a\vartheta^x + c\vartheta^{xy})\right|^4 \ll \delta_a t^{9/4} M^{5/2+\varepsilon},$$

holds, for any $\varepsilon > 0$.

2. Discrepancy bound

Now we are ready to formulate our main estimate.

Theorem 2.1. *Let (u_n), the recurrence sequence defined by* (1)*, be of period τ, which is the multiplicative order of e modulo t. Fix $\delta_a = \gcd(a, M)$. Then, for any $\varepsilon > 0$, the bound*

$$|S_a(t, \tau; M, N)| \ll N^{4/9}\delta^{1/9}t^{1/4}M^{5/18+\varepsilon}$$

holds, where the implied bound depends at most on ϵ.

Proof. For any integer $k \geq 0$ we have

$$\left| S_a(t,\tau;M,N) - \sum_{n=0}^{N-1} \mathbf{e}_M(au_{n+k}t) \right| \leq 2k.$$

Therefore, for any integer $K \geq 1$,

$$K\,|S_a(t,\tau;M,N)| \leq W + K^2,$$

where

$$W = \left| \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \mathbf{e}_M(au_{n+k}) \right| \leq \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathbf{e}_M(au_{n+k}) \right|.$$

We then obtain

$$\begin{aligned}
W^2 &\leq N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathbf{e}_M(au_{n+k}) \right|^2 \\
&\leq N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathbf{e}_M\big(a\vartheta^{e^{n+k}}\big) \right|^2 \\
&\leq N \sum_{x\in\mathbb{Z}_t} \left| \sum_{k=0}^{K-1} \mathbf{e}_M\big(a\vartheta^{xe^k}\big) \right|^2 \\
&\leq N \sum_{k_1=0}^{K-1} \sum_{k_2=0}^{K-1} \sum_{x\in Z_t} \mathbf{e}_M\big(a\big(\vartheta^{xe^{k_1}} - \vartheta^{xe^{k_2}}\big)\big) \\
&< N \sum_{k_1=0}^{K-1} \sum_{k_2=0}^{K-1} \left| \sum_{x\in Z_t} \mathbf{e}_M\big(a\big(\vartheta^{xe^{k_1}} - \vartheta^{xe^{k_2}}\big)\big) \right| \\
&< N \sum_{k_1=0}^{K-1} \sum_{k_2=0}^{K-1} \left| \sum_{x\in Z_t} \mathbf{e}_M\big(a\big(\vartheta^{xe^{k_1}} - \vartheta^{xe^{k_2}}\big)\big) \right| \\
&= N \sum_{k_1=0}^{K} \sum_{k_2=0}^{K} \left| \sum_{v\in Z_t} \mathbf{e}_M\big(a\big(\vartheta^{v} - \vartheta^{ve^{k_2-k_1}}\big)\big) \right|,
\end{aligned}$$

after substituting $v \equiv e^{k_1}x \pmod{t}$.

Now, it is clear that $k_2 - k_1 \in [-K+1, K-1]$ for $0 \leq k_1, k_2 \leq K-1$. Further, each $k = k_2 - k_1 \in [-K+1, K-1]$ is repeated at most K times for $k_1, k_2 = 0, \ldots, K-1$. Thus,

$$W^2 \leq NK \sum_{k=-K+1}^{K-1} \left| \sum_{v\in Z_t} \mathbf{e}_M\big(a\big(\vartheta^{v} - \vartheta^{ve^k}\big)\big) \right|.$$

Applying the Hölder inequality we now have

$$\left(\frac{W^2}{K^2}\right)^4 \le \left(\frac{N}{K}\right)^4 K^3 \sum_{k=-K+1}^{K-1} \left| \sum_{v\in\mathbb{Z}_t} \mathbf{e}_M\big(a\big(\vartheta^v - \vartheta^{ve^k}\big)\big)\right|^4.$$

Recalling that τ is the multiplicative order of e modulo t, then if $K < t/2$ this can be rewritten as

$$\begin{aligned}\left(\frac{W^2}{K^2}\right) &\le \left(\frac{N}{K}\right)^4 K^3 \sum_{k=0}^{\tau-1} \left| \sum_{v\in\mathbb{Z}_t} \mathbf{e}_M\big(a\big(\vartheta^v - \vartheta^{ve^j}\big)\big)\right|^4 \\ &= \frac{N^4}{K} \sum_{k=0}^{\tau-1} \left| \sum_{v\in\mathbb{Z}_t} \mathbf{e}_M\big(a\big(\vartheta^v - \vartheta^{ve^j}\big)\big)\right|^4.\end{aligned}$$

Using Lemma 1.2 with $c = -a$, we obtain

$$\left(\frac{W^2}{K^2}\right) \ll N^4 K^{-1} \delta t^{9/4} M^{5/2+\varepsilon}.$$

Hence,

$$|S_a(t,\tau;M,N)| \ll N^{1/2} K^{-1/8} \delta^{1/8} t^{9/32} M^{5/16+\varepsilon} + K.$$

Choosing $K = \lfloor N^{4/9}\delta^{1/9}t^{1/4}M^{5/18+\varepsilon}\rfloor$, the theorem obviously follows if

$$N^{4/9}\delta^{1/9}t^{1/4}M^{5/18+\varepsilon} < t/2,$$

else we note $|S_a(t,\tau;M,N)| \le N \le t$ and so the theorem follows again. □

Now let $D_M(t,\tau;N)$ denote the discrepancy of the points (u_n/M), $n = 1,\dots,N \le \tau$.

Theorem 2.2. *Let (u_n), the recurrence sequence defined by (1), be of order τ, which is the multiplicative order of e modulo t. Then, for any $\varepsilon > 0$, the bound*

$$D_M(t,\tau;N) \ll N^{-5/9} t^{1/4} M^{5/18+\varepsilon}$$

holds, where the implied constant depends at most on ε.

Proof. Using Lemma 1.1, with $L = M - 1$ and the bound from Theorem 2.1, we obtain

$$\begin{aligned}D_M(t,\tau;N) &\ll N^{-5/9} t^{1/4} M^{5/18+\varepsilon/2} \sum_{\delta\mid M} \delta^{1/9} \sum_{\substack{0<|a|<M\\ \gcd(a,M)=\delta}} \frac{1}{|a|} \\ &\ll N^{-5/9} t^{1/4} M^{5/18+\varepsilon/2} \log M \sum_{\delta\mid M} \delta^{-8/9}.\end{aligned}$$

Noting that $d(k)$, the number of positive divisors of an integer, $k \geq 1$, can be bounded by

$$\log d(k) \ll \frac{\log k}{\log \log 3k},$$

(see [23, Theorem 5.2, chapter 1]), we obtain the desired result. □

3. Remarks

We remark that in order to calculate the s-dimensional discrepancy we would need an upper bound for

$$\sum_{j=0}^{\tau-1} \left| \sum_{v \in \mathbb{Z}_t} \mathbf{e}_M \left(\sum_{l=0}^{s-1} a_l (v^{ve^l} - v^{ve^{j+l}}) \right) \right|^4.$$

Unfortunately, Lemma 1.2 can only be applied to the case where $s = 1$. It remains an open problem to find an analogous lemma which could then be used to establish a discrepancy bound for all other s. And, when N is a value close to t and $\delta \ll M^{\varepsilon}$, then Theorem 2.1 is non-trivial as long as $t > M^{10/11+\varepsilon}$. Lastly, we also remark that when t is of order near M the bound of Theorem 2.2 is valuable as long as $N > M^{19/20+\varepsilon}$.

Acknowledgement. The author wishes to thank Igor Shparlinski for suggesting this problem and for helpful comments, advice, and the reading of this paper.

References

[1] L. Blum, M. Blum, and M. Shub, *A simple unpredictable pseudorandom number generator*, SIAM J. Comput. **15** (1986), no. 2, 364–383.

[2] J. J. Brennan and B. Geist, *Analysis of iterated modular exponentiation: The orbits of* x^{α} mod N, Des. Codes Cryptogr. **13** (1998), no. 3, 229–245.

[3] W.-S. Chou and I. E. Shparlinski, *On the cycle structure of repeated exponentiation modulo a prime*, J. Number Theory **107** (2004), no. 2, 345–356.

[4] T. W. Cusick, *Properties of the* x^2 *mod N pseudorandom number generator*, IEEE Trans. Inform. Theory **41** (1995), no. 4, 1155–1159.

[5] T. W. Cusick, C. Ding, and A. Renvall, *Stream ciphers and number theory*, North-Holland Mathematical Library, vol. 55, North-Holland Publishing Co., Amsterdam, 1998.

[6] M. Drmota and R. F. Tichy, *Sequences, discrepancies and applications*, Lecture Notes in Mathematics, vol. 1651, Springer-Verlag, Berlin, 1997.

[7] E. D. El-Mahassni, *On the distribution of the power generator modulo a prime power for parts of the period*, Bol. Soc. Mat. Mexicana (3), accepted.

[8] E. D. El-Mahassni, I. E. Shparlinski, and A. Winterhof, *Distribution of nonlinear congruential pseudorandom numbers modulo almost squarefree integers*, Monatsh. Math. **148** (2006), no. 4, 297–307.

[9] E. D. El-Mahassni and A. Winterhof, *On the distribution of nonlinear congruential pseudorandom numbers in residue rings*, Int. J. Number Theory **2** (2006), no. 1, 163–168.

[10] R. Fischlin and C. P. Schnorr, *Stronger security proofs for RSA and Rabin bits*, J. Cryptology **13** (2000), no. 2, 221–244.

[11] J. B. Friedlander, J. S. Hansen, and I. E. Shparlinski, *On the distribution of the power generator modulo a prime power*, Unusual Applications of Number Theory (New Brunswick, 2000), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 64, Amer. Math. Soc., Providence, RI, 2004, pp. 71–79.

[12] J. B. Friedlander, S. Konyagin, and I. E. Shparlinski, *Some doubly exponential sums over* $\mathbb{Z}_m$, Acta Arith. **105** (2002), no. 4, 349–370.

[13] J. B. Friedlander, D. Lieman, and I. E. Shparlinski, *On the distribution of the RSA generator*, Sequences and Their Applications (Singapore, 1998), Springer Ser. Discrete Math. Theor. Comput. Sci., Springer, London, 1999, pp. 205–212.

[14] J. B. Friedlander and I. E. Shparlinski, *On the distribution of the power generator*, Math. Comp. **70** (2001), no. 236, 1575–1589.

[15] F. Griffin, H. Niederreiter, and I. E. Shparlinski, *On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders*, 13th Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (Honolulu, 1999), Lecture Notes in Comput. Sci., vol. 1719, Springer, Berlin, 1999, pp. 87–93.

[16] F. Griffin and I. E. Shparlinski, *On the linear complexity profile of the power generator*, IEEE Trans. Inform. Theory **46** (2000), no. 6, 2159–2162.

[17] J. Gutierrez, H. Niederreiter, and I. E. Shparlinski, *On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period*, Monatsh. Math. **129** (2000), no. 1, 31–36.

[18] J. Håstad and M. Näslund, *The security of individual RSA bits*, 39th IEEE Symposium on Foundations of Computer Science (Palo Alto, CA, 1998), IEEE Computer Society, Washington, DC, 1998, pp. 510–519.

[19] J. C. Lagarias, *Pseudorandom number generators in cryptography and number theory*, Cryptology and Computational Number Theory (Boulder, CO, 1989), Proc. Sympos. Appl. Math., vol. 42, Amer. Math. Soc., Providence, RI, 1990, pp. 115–143.

[20] H. Niederreiter and I. E. Shparlinski, *On the distribution and lattice structure of nonlinear congruential pseudorandom numbers*, Finite Fields Appl. **5** (1999), no. 3, 246–253.

[21] ———, *Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus*, Acta Arith. **92** (2000), no. 1, 89–98.

[22] ———, *On the distribution of inversive congruential pseudorandom numbers in parts of the period*, Math. Comp. **70** (2001), no. 236, 1569–1574.

[23] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957.

[24] I. E. Shparlinski, *On the linear complexity of the power generator*, Des. Codes Cryptogr. **23** (2001), no. 1, 5–10.

[25] ———, *On the uniformity of distribution of the Naor-Reingold pseudo-random function*, Finite Fields Appl. **7** (2001), no. 2, 318–326.