LOWER BOUNDS ON THE PERIOD OF SOME PSEUDORANDOM NUMBER GENERATORS

PÄR KURLBERG AND CARL POMERANCE

1. Introduction

We are interested in obtaining lower bounds on the periods of two standard pseudorandom number generators from number theory—the linear congruential generator, first introduced by D. H. Lehmer, and the so called power generator. For the former, given integers e, b, n (with $e, n > 1$) and a seed $u = u_0$, we compute the sequence

$$u_{i+1} \;=\; eu_i + b \pmod{n}.$$

For the power generator, given integers $e, n > 1$ and a seed $u = u_0 > 1$, we compute the sequence

$$u_{i+1} \;=\; u_i^e \pmod{n}$$

so that $u_i = u^{e^i} \pmod{n}$. The particular case $e = 2$ is known as the Blum–Blum–Shub (BBS) generator [1]. This generator is not only simple to compute, but it has certain attractive aspects from a cryptographic perspective, especially when n is the product of two large primes that are both congruent to 3 modulo 4.

These two generators give rise to (ultimately) periodic sequences, and it is of interest to compute the periods—a useful pseudorandom number generator should have a long period. Further, to show that the sequence satisfies various equidistribution properties, exponential sum techniques are often applicable provided that the period is sufficiently large. Moreover, if the period is very short when n is a product of two primes, certain cycling attacks on the RSA public key system apply.

In this note[1] we consider the problem of the period statistically as n varies, either over all integers, or over certain subsets of the integers that are used in practice, namely the set of primes and the set of "RSA moduli," that is, numbers which are the product of two primes of the same magnitude.

Date: August 21, 2007.

1991 *Mathematics Subject Classification.* Primary 11K45, Secondary 11B50, 11N56, 11T71, 11R45.

[1]The results presented here summarise results obtained by the authors in [11].

If $(e,n)=1$, then the sequence $e^i \pmod n$ is purely periodic and its period is the least positive integer k with $e^k \equiv 1 \pmod n$. We denote this order as $\ell_e(n)$. If $(e,n)>1$, the sequence $e^i \pmod n$ is still (ultimately) periodic, with the period given by $\ell_e(n_{(e)})$ where $n_{(e)}$ is the largest divisor of n that is coprime to e. In what follows we shall denote $\ell_e(n_{(e)})$ by $\ell_e^*(n)$. The periods of both the linear congruential and power generators may be described in terms of this function. For the linear congruential generator we have $u_i = e^i(u+b(e-1)^{-1}) - b(e-1)^{-1} \pmod n$ when $e-1$ is coprime to n, so that if we additionally have $u+b(e-1)^{-1}$ coprime to n, the period is exactly $\ell_e^*(n)$. In general, the period is always a divisor of $\ell_e^*(n)(e-1,n)$.

For the power generator, the period is exactly $\ell_e^*(\ell_u^*(n))$. For most of this note we shall assume that u is chosen so that $\ell_u^*(n)$ is as large as possible for a given modulus n. This maximum, following Carmichael, is denoted $\lambda(n)$ and equals the order of the largest cyclic subgroup of $(\mathbf{Z}/n\mathbf{Z})^\times$. For the power generator, we thus will study $\ell_e^*(\lambda(n))$. Note that it is especially important to use the function ℓ_e^* rather than ℓ_e when considering the modulus $\lambda(n)$, since for $n>2$, $\lambda(n)$ is always even, and in general, $\lambda(n)$ is divisible by the fixed number e for a set of numbers n of asymptotic density 1.

1.1. **Previous work.** For $n=p$ and p a prime number, the order of e modulo p has been studied extensively. In [15] Pappalardi showed that there exist $\alpha,\delta>0$ such that $\ell_e(p) \ge p^{1/2}\exp((\log p)^\delta)$ for all but $O(x/\log^{1+\alpha} x)$ primes $p \le x$. He also asserted, assuming the Generalized Riemann Hypothesis[2] (GRH), that if $\psi(x)$ is any increasing function tending to infinity as x tends to infinity (but not too quickly), then $\ell_e(p) > p/\psi(p)$ for all but $O(\pi(x)\log(\psi(x))/\psi(\sqrt{x}))$ primes $p \le x$, where as usual, $\pi(x)$ is the total number of all primes $p \le x$. A similar result is given by Erdős and Murty in [2]. Also in [2], it is shown that if $\varepsilon(x)$ is any decreasing function tending to zero as x tends to infinity, then $\ell_e(p) \ge p^{1/2+\varepsilon(p)}$ for all but $o(\pi(x))$ primes $p \le x$, and in [8] Indlekofer and Timofeev give a similar lower bound with an explicit estimate on the number of exceptional primes. A further strengthening of this result has recently been shown by Ford [5]. Note that it follows immediately from work of Goldfeld, Motohashi, Fouvry, and Baker–Harman that there is a positive constant γ such that $\ell_e(p) > p^{1/2+\gamma}$ for a positive proportion of the primes p, with the current record being $\gamma = 0.677$.

A somewhat related new result is found in [9] where the authors show that the geometric mean for $\ell_e(p)$ for primes $p \le x$ is at least $x^{0.58}$ for x sufficiently large. This gives a small improvement on the essentially trivial result with exponent 0.5.

[2]When we refer to the Generalized Riemann Hypothesis in this note we shall mean the Riemann Hypothesis for zeta functions ζ_K, where K runs over the Kummer extensions $K=\mathbf{Q}(\sqrt[q]{e},\exp(2\pi i/q))$, $e\ge 2$, q prime.

The period of the power generator $u^{e^i} \pmod{pl}$ was studied in Friedlander, Pomerance and Shparlinski [6], where p, l are primes of the same magnitude. One of the results there is that this period is $> (pl)^{1-\varepsilon}$ for most choices of u, e, p, l. However, once the exponent e is fixed, say at 2, their results are weaker.

As for $\ell_e(n)$ for n a positive integer, in [12] Kurlberg and Rudnick proved that there exists $\delta > 0$ such that $\ell_e(n) \gg n^{1/2} \exp((\log n)^\delta))$ for all but $o(x)$ integers $n \le x$ that are coprime to e. Further, in [10], Kurlberg showed that the GRH implies that for each $\varepsilon > 0$, we have $\ell_e(n) \gg n^{1-\varepsilon}$ for all but $o(x)$ integers $n \le x$ that are coprime to n, and in [13] Li and Pomerance improved the lower bound to $\ell_e(n) \ge n(\log n)^{-(1+o(1))\log\log\log n}$, a result that is best possible.

Acknowledgement. P.K. supported in part by the Göran Gustafsson Foundation, the Royal Swedish Academy of Sciences, and the Swedish Research Council. C.P. supported in part by the National Science Foundation (DMS-0401422). P.K. would also like to thank the organizers of ANT for their kind invitation to speak.

2. The results

2.1. **The linear congruential generator.** By the previous remarks, the period of the linear congruential generator, for e, b fixed and n taking values among the integers, is essentially the same as $\ell_e^*(n)$, and thus the next Theorem shows that the period is larger than $n^{1/2+\varepsilon(n)}$, respectively $n^{1/2+\gamma_1}$, for all n in a full, respectively positive, density subset of the integers.

Theorem 1. *Results on $\ell_e^*(n)$:*

1. *Suppose $\varepsilon(x)$ tends to zero arbitrarily slowly as $x \to \infty$. Then $\ell_e^*(n) \ge n^{1/2+\varepsilon(n)}$ for all but $o_\varepsilon(x)$ integers $n \le x$.*
2. *There is a positive constant γ_1 such that $\ell_e(n) \ge n^{1/2+\gamma_1}$ for a positive proportion of the integers n.*

2.2. **The power generator.** As we have seen, the length of the period for the sequence (u_i) equals $\ell_e^*(\lambda(n))$ if u is chosen apropriately. We thus begin by considering $\ell_e^*(\lambda(n))$ for 3 natural classes of moduli, namely primes, the products of two primes of the same magnitude, and general integer moduli. (Note that $\lambda(p) = p - 1$.)

Theorem 2. *Results on $\ell_e^*(p-1)$:*

1. *Suppose $\varepsilon(x)$ tends to zero arbitrarily slowly as $x \to \infty$. Then $\ell_e^*(p-1) \ge p^{1/2+\varepsilon(p)}$ for all but $o_\varepsilon(\pi(x))$ primes $p \le x$.*
2. *There is a positive constant γ_2 such that $\ell_e^*(p-1) \ge p^{1/2+\gamma_2}$ for a positive proportion of the primes p.*

(3) *(GRH) For each fixed $\varepsilon > 0$ we have $\ell_e^*(p-1) > p^{1-\varepsilon}$ for all but $o_\varepsilon(\pi(x))$ primes $p \le x$.*

Now consider RSA moduli, namely integers of the form pl where p, l are primes with $p, l \le Q$ (where Q is an arbitrary bound). Using our results on $\ell_e^*(p-1)$, we can prove the following theorem.

Theorem 3. *Results on $\ell_e^*(\lambda(pl))$:*

(1) *Suppose $\varepsilon(x)$ tends to zero arbitrarily slowly as $x \to \infty$. Then $\ell_e^*(\lambda(pl)) \ge (pl)^{1/2+\varepsilon(pl)}$ for all but $o_\varepsilon(\pi(Q)^2)$ pairs of primes $p, l \le Q$.*
(2) *There is a positive constant γ_3 such that for a positive proportion of the pairs of primes $p, l \le Q$, we have $\ell_e^*(\lambda(pl)) \ge (pl)^{1/2+\gamma_3}$.*
(3) *(GRH) For each fixed $\varepsilon > 0$ we have $\ell_e^*(\lambda(pl)) > (pl)^{1-\varepsilon}$ for all but $o_\varepsilon(\pi(Q)^2)$ pairs of primes $p, l \le Q$.*

Instead of considering specifically RSA moduli $n = pl$, one may consider the general case where no restriction is made on the modulus n. In our next theorem we establish similar results as above for this order.

Theorem 4. *Results on $\ell_e^*(\lambda(n))$:*

(1) *Suppose $\varepsilon(x)$ tends to zero arbitrarily slowly as $x \to \infty$. Then $\ell_e^*(\lambda(n)) \ge n^{1/2+\varepsilon(n)}$ for all but $o_\varepsilon(x)$ integers $n \le x$.*
(2) *There is a positive constant γ_4 such that $\ell_e^*(\lambda(n)) \ge n^{1/2+\gamma_4}$ for a positive proportion of the integers n.*
(3) *(GRH) For each fixed $\varepsilon > 0$ we have $\ell_e^*(\lambda(n)) > n^{1-\varepsilon}$ for all but $o_\varepsilon(x)$ integers $n \le x$.*

In fact, we can actually achieve a best possible result in part 3 of Theorem 4, namely:

Theorem 5. *If the GRH is true, then for each fixed integer $e \ge 2$,*

$$\ell_e^*(\lambda(n)) \;=\; n \cdot \exp(-(1+o(1))(\log\log n)^2 \log\log\log n)$$

as $n \to \infty$ through a set of asymptotic density 1.

We may also handle the situation for a general modulus n and u fixed, i.e., we do not need to make the assumption that u is chosen in an optimal way.

Theorem 6. *Assuming the GRH, for any fixed integers $e, u \ge 2$, the period of the sequence $u^{e^i} \pmod n$ is equal to*

$$n \cdot \exp(-(1+o(1))(\log\log n)^2 \log\log\log n)$$

as $n \to \infty$ through a certain set of integers of asymptotic density 1.

3. A brief outline of the arguments

We give a brief outline of the ideas used to prove the first cases of Theorems 1 and 4, namely unconditional proofs of the periods of the two generators both being slightly larger than $\sqrt{n}$ for full density subsets of the integers. For full details and proofs of the other statements we refer the reader to [11].

3.1. **On the order of e modulo n.** We begin by outlining the argument that $\ell_e^*(n) > n^{1/2+\varepsilon(n)}$ on a set of asymptotic density 1; that is, we prove the first item in Theorem 1.

We begin with a Lemma that allows us to replace $\ell_e^*(n)$ by $\prod_{p|n} \ell_e^*(p)$, at the price of losing a factor of at most $\lambda(n)/n$.

Lemma 7. *For any natural number n we have*

$$\ell_e^*(n) \;\geq\; \frac{\lambda(n)}{n} \prod_{p|n} \ell_e^*(p) \;=\; \frac{\lambda(n)}{n} \prod_{p|n,\ p\nmid e} \ell_e(p).$$

Now, although $\lambda(n)$ can be as small as $(\log n)^{c_1 \log\log\log n}$ for some $c_1 > 0$, as shown by Erdős, Pomerance, and Schmutz in [4], it readily follows from Theorem 5 of [6] that $\lambda(n)$ is quite large for most integers[3].

Lemma 8. *For x sufficiently large, the number of integers $n \leq x$ with $\lambda(n) \leq n \exp(-(\log\log n)^3)$ is at most $x/(\log x)^{10}$.*

As mentioned in the introduction, if $\varepsilon(x) \to 0$ as $x \to \infty$, then $\ell_e^*(p) > p^{1/2+\varepsilon(p)}$ for almost all prime p. In other words, $\ell_e^*(p)$ is fairly large for "typical" primes p. Thus, if the product of the "typical" prime divisors of a generic integer n is of size comparable with n, we find that $\ell_e^*(n) > n^{1/2+\varepsilon(n)}$ for most n. We can make this more precise as follows.

Suppose $\mathcal{P}$ is a subset of the prime numbers. We let $\pi_{\mathcal{P}}(x)$ denote the number of primes $p \leq x$ with $p \in \mathcal{P}$. For a positive integer n we let $n_{\mathcal{P}}$ denote the largest divisor of n that is free of prime factors outside of $\mathcal{P}$.

Assume $\varepsilon(x)$ is an arbitrary monotonic function with

$$\varepsilon(x) = o(1),\ \varepsilon(x) > 1/\log\log x,\ \varepsilon(x^{1/\log\log x}) < 2\varepsilon(x), \tag{1}$$

where the last two conditions hold for x sufficiently large. We now partition the primes into 3 sets:

$$\begin{aligned} \mathcal{L} &= \{p \text{ prime } :\ \ell_e^*(p) \leq p^{1/2}/\log p\} \\ \mathcal{M} &= \{p \text{ prime } :\ p^{1/2}/\log p < \ell_e(p) \leq p^{1/2+2\varepsilon(p)}\} \\ \mathcal{H} &= \{p \text{ prime } :\ \ell_e(p) > p^{1/2+2\varepsilon(p)}\}, \end{aligned}$$

[3]In fact, in [4] it was also shown that $\lambda(n) = n/(\log n)^{\log\log\log n + A + o(1)}$, where $A \simeq 0.227$, for most integers.

where we use the mnemonic low, medium, and high (order) for $\mathcal{L}, \mathcal{M}, \mathcal{H}$. Note that $\mathcal{L}$ contains the prime factors of e. Further, let $\omega(n)$ denote the number of prime number divisors of n.

By an argument due to Hooley [7], we can show that the "low order" primes are rare enough that the sum of their reciprocals converge.

Lemma 9. *We have $\pi_{\mathcal{L}}(x) = O(x/\log^3 x)$ so that $\sum_{p\in\mathcal{L}} 1/p = O(1)$. In addition, we have*

$$\sum_{n_{\mathcal{L}}=n} \frac{1}{n} \;=\; \prod_{p\in\mathcal{L}} (1-1/p)^{-1} \;=\; O(1). \tag{2}$$

For a positive integer n, let $\gamma(n)$ denote the largest squarefree divisor of n, sometimes called the "core" or "radical" of n. Using Lemma 9, together with the Erdős-Kac theorem (or the Hardy-Ramanujan theorem on the normal number of prime divisors of integers), we can show that a generic integer n has the following properties: the low order part $n_{\mathcal{L}}$ of n is quite small, the core of n is quite large, and n does not have too many prime divisors. More precisely, we have:

Lemma 10. *But for a set of natural numbers n of asymptotic density 0 we have: $n_{\mathcal{L}} < \log n$, $n/\gamma(n) < \log n$, and $\omega(n) < 2\log\log n$.*

Our next question of interest is how large can we expect $n_{\mathcal{M}}$ to be for most numbers n. Since most numbers do not have a divisor very near their square root, there is hope that this ingredient can be used. In fact, Erdős and Murty used this idea to show that $\pi_{\mathcal{M}}(x) = o(\pi(x))$, and Pappalardi and Indlekofer–Timofeev got more quantitative versions of this result. We state a consequence from the latter paper.

Lemma 11 ([8], Cor. 6)**.** *With $\varepsilon(x)$ as specified in* (1)*, we have $\pi_{\mathcal{M}}(x) = O(\varepsilon(x)^{1/12}\pi(x))$.*

We now show that as a consequence of Lemma 11, not many integers n have a large divisor composed of primes from $\mathcal{M}$. Let Λ denote the von Mangoldt function.

Lemma 12. *With $\varepsilon(x)$ as specified in* (1)*, the number of integers $n \le x$ with $n_{\mathcal{M}} > n^{1/3}$ is $O(\varepsilon(x)^{1/12}x)$.*

Proof. We have

$$\sum_{n\le x} \log n_{\mathcal{M}} = \sum_{n\le x} \sum_{\substack{d\mid n\\ d_{\mathcal{M}}=d}} \Lambda(d) \;=\; \sum_{\substack{d_{\mathcal{M}}=d\\ d\le x}} \Lambda(d) \left\lfloor \frac{x}{d} \right\rfloor \;\le\; x \sum_{\substack{p\in\mathcal{M}\\ p\le x}} \frac{\log p}{p} + O(x).$$

Now, using Lemma 11 and (1),

$$\begin{aligned}\sum_{p\in\mathcal{M},\ p\le x}\frac{\log p}{p} &= \frac{\log x}{x}\pi_{\mathcal{M}}(x)+\int_2^x\frac{\log t-1}{t^2}\pi_{\mathcal{M}}(t)\,dt\\ &\ll \int_2^x\frac{\varepsilon(t)^{1/12}}{t}\,dt+o(1)\\ &= \int_2^{x^{1/\log\log x}}\frac{\varepsilon(t)^{1/12}}{t}\,dt+\int_{x^{1/\log\log x}}^x\frac{\varepsilon(t)^{1/12}}{t}\,dt+o(1)\\ &\ll \frac{\log x}{\log\log x}+\varepsilon(x)^{1/12}\log x \ \ll\ \varepsilon(x)^{1/12}\log x.\end{aligned}$$

Thus,

$$\sum_{n\le x}\log n_{\mathcal{M}} \ \ll\ \varepsilon(x)^{1/12}x\log x,$$

and the result follows readily. □

We are now ready to prove the first part of Theorem 1.

Theorem 13. *Suppose $\varepsilon(n)$ satisfies* (1). *But for a set of integers n of asymptotic density* 0 *we have*

$$\ell_e^*(n) \ >\ n^{1/2+\varepsilon(n)}.$$

Proof. By Lemma 8 we may assume that $\lambda(n) > n\exp(-(\log\log n)^3)$. Thus, from Lemma 7 and Lemma 10 we have

$$\begin{aligned}\ell_e^*(n) &> \exp(-(\log\log n)^3)\prod_{p\mid n/n_{\mathcal{L}}}\ell_e(n)\\ &\ge \exp(-(\log\log n)^3)\prod_{p\mid n_{\mathcal{M}}}(p^{1/2}/\log p)\prod_{p\mid n_{\mathcal{H}}}p^{1/2+2\varepsilon(p)}\\ &\ge \exp(-(\log\log n)^3-\omega(n)\log\log n)\gamma(n_{\mathcal{M}})^{1/2}\gamma(n_{\mathcal{H}})^{1/2+2\varepsilon(n)}\\ &\ge \exp(-2(\log\log n)^3)n^{1/2}n_{\mathcal{H}}^{2\varepsilon(n)}.\end{aligned}$$

By Lemmas 10 and 12 we may also assume that $n_{\mathcal{H}} > n^{3/5}$. Thus, our result follows from (1). □

3.2. **On the order of e modulo $\lambda(n)$.** The proof in this case is fairly similar. Using Lemma 7 we obtain the bound

$$\ell_e^*(\lambda(n)) \ge \frac{\lambda(\lambda(n))}{\lambda(n)}\prod_{p\lambda(n)}\ell_e(p)$$

Using the following result of Martin and Pomerance [14] on the normal order of $\lambda(\lambda(n))$ we may control the ratio $\lambda(\lambda(n))/\lambda(n)$.

Theorem 14 (Martin–Pomerance [14])**.** *As $n \to \infty$ through a certain set of integers of asymptotic density* 1*, we have*

$$\lambda(\lambda(n)) = n \cdot \exp(-(1+o(1))(\log\log n)^2 \log\log\log n).$$

Thus, $\lambda(\lambda(n)) > n/\exp((\log\log n)^3)$ almost always.

Now, by using the fact (see [3]) that the normal order of $\omega(\lambda(n))$ is equal to $(\log\log n)^2/2$, together with the fact (easily deduced from (6) and (7) in [4]) that the estimate

$$\log(\lambda(n)/\gamma(\lambda(n))) \ll \log\log n/\log\log\log n$$

holds for most n, it is possible to obtain the following analog of Lemma 10.

Lemma 15. *We have*

$$\begin{aligned} \lambda(n)_{\mathcal{L}} &< \exp((\log\log n)^2) \\ \lambda(n)/\gamma(\lambda(n)) &< \log n \\ \omega(\lambda(n)) &< (\log\log n)^2 \end{aligned}$$

almost always.

A similar, but more elaborate, argument to the one used to prove Lemma 12, then gives the following result.

Lemma 16. *Let $\varepsilon(x)$ satisfy* (1)*. Almost all numbers n have the property that $\lambda(n)_{\mathcal{M}} < n^{2/5}$.*

With these results at our disposal, the argument used in Theorem 13 easily gives that

$$\ell_e^*(\lambda(n)) > n^{1/2+\varepsilon(n)}$$

for most n.

References

[1] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudorandom number generator. *SIAM J. Comput.*, 15(2):364–383, 1986.

[2] P. Erdős and M. R. Murty. On the order of $a \pmod p$. In *Number theory (Ottawa, ON, 1996)*, pages 87–97. Amer. Math. Soc., Providence, RI, 1999.

[3] P. Erdős and C. Pomerance. On the normal number of prime factors of $\phi(n)$. *Rocky Mountain J. Math.*, 15(2):343–352, 1985. Number theory (Winnipeg, Man., 1983).

[4] P. Erdős, C. Pomerance, and E. Schmutz. Carmichael's lambda function. *Acta Arith.*, 58(4):363–385, 1991.

[5] K. Ford. The distribution of integers with a divisor in a given interval. *Annals Math.*, to appear.

[6] J. B. Friedlander, C. Pomerance, and I. E. Shparlinski. Period of the power generator and small values of Carmichael's function. *Math. Comp.*, 70(236):1591–1605, 2001. Corrigendum, *op. cit.*, 71(240):1803–1806, 2002.

[7] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.
[8] K.-H. Indlekofer and N. M. Timofeev. Divisors of shifted primes. *Publ. Math. Debrecen*, 60(3-4):307–345, 2002.
[9] S. V. Konyagin, C. Pomerance, and I. E. Shparlinski. On the distribution of pseudopowers. Preprint.
[10] P. Kurlberg. On the order of unimodular matrices modulo integers. *Acta Arith.*, 110(2):141–151, 2003.
[11] P. Kurlberg and C. Pomerance. On the period of the linear congruential and power generators. *Acta Arith.*, 119(2):149–169, 2005.
[12] P. Kurlberg and Z. Rudnick. On quantum ergodicity for linear maps of the torus. *Comm. Math. Phys.*, 222(1):201–227, 2001.
[13] S. Li and C. Pomerance. On generalizing Artin's conjecture on primitive roots to composite moduli. *J. Reine Angew. Math.*, 556:205–224, 2003.
[14] G. Martin and C. Pomerance. The iterated Carmichael λ-function and the number of cycles of the power generator. *Acta Arith.*, 118(4):305–335, 2005.
[15] F. Pappalardi. On the order of finitely generated subgroups of $\mathbf{Q}^*$ (mod p) and divisors of $p-1$. *J. Number Theory*, 57(2):207–222, 1996.

E-mail address: kurlberg@math.kth.se

Department of Mathematics, KTH, SE-100 44 Stockholm, Sweden

E-mail address: carl.pomerance@dartmouth.edu

Mathematics Department, Dartmouth College, Hanover, NH 03755-3551, U.S.A.