MATHEMATICS OF COMPUTATION
Volume 70, Number 236, Pages 1591–1605
S 0025-5718(00)01282-5
Article electronically published on July 13, 2000

PERIOD OF THE POWER GENERATOR AND SMALL VALUES OF CARMICHAEL'S FUNCTION

JOHN B. FRIEDLANDER, CARL POMERANCE, AND IGOR E. SHPARLINSKI

Abstract. Consider the pseudorandom number generator

$$u_n \equiv u_{n-1}^e \pmod m, \quad 0 \le u_n \le m-1, \quad n = 1, 2, \dots,$$

where we are given the modulus m, the initial value $u_0 = \vartheta$ and the exponent e. One case of particular interest is when the modulus m is of the form pl, where p, l are different primes of the same magnitude. It is known from work of the first and third authors that for moduli $m = pl$, if the period of the sequence (u_n) exceeds $m^{3/4+\varepsilon}$, then the sequence is uniformly distributed. We show rigorously that for almost all choices of p, l it is the case that for almost all choices of ϑ, e, the period of the power generator exceeds $(pl)^{1-\varepsilon}$. And so, in this case, the power generator is uniformly distributed.

We also give some other cryptographic applications, namely, to ruling-out the cycling attack on the RSA cryptosystem and to so-called time-release crypto.

The principal tool is an estimate related to the Carmichael function $\lambda(m)$, the size of the largest cyclic subgroup of the multiplicative group of residues modulo m. In particular, we show that for any $\Delta \ge (\log\log N)^3$, we have $\lambda(m) \ge N \exp(-\Delta)$ for all integers m with $1 \le m \le N$, apart from at most $N \exp\left(-0.69\,(\Delta \log \Delta)^{1/3}\right)$ exceptions.

1. Introduction

For an integer $n \ge 1$ we define the *Carmichael function* $\lambda(n)$ as the largest possible order of elements of the unit group in the residue ring modulo n. More explicitly, for a prime power p^k we define

$$\lambda\left(p^k\right) = \begin{cases} p^{k-1}(p-1), & \text{if } p \ge 3 \text{ or } k \le 2; \\ 2^{k-2}, & \text{if } p = 2 \text{ and } k \ge 3; \end{cases}$$

and finally,

$$\lambda(n) = \operatorname{lcm}\left(\lambda(p_1^{k_1}), \dots, \lambda\big(p_\nu^{k_\nu}\big)\right),$$

where

$$n = p_1^{k_1} \cdots p_\nu^{k_\nu}$$

is the prime number factorization of n.

Received by the editor September 8, 1999.

2000 *Mathematics Subject Classification.* Primary 11B50, 11N56, 11T71; Secondary 11Y55, 94A60.

Key words and phrases. Carmichael's function, RSA generator, Blum–Blum–Shub generator.

The first author was supported in part by NSERC grant A5123 and by an NEC grant to the Institute for Advanced Study.

The third author was supported in part by ARC grant A69700294.

Various upper and lower bounds for $\lambda(n)$ have been obtained in [9]. In particular, it follows from Theorem 2 of [9] that for all except $o(N)$ positive integers $n \le N$

$$\lambda(n) = n \exp\left(-\log\log n \log\log\log n - C \log\log n + o(\log\log n)\right)$$

for some explicitly given constant C. Here we obtain a modification of this result. We are interested in the lower bound implicit in the above result but, with an application in mind, we wish to be able to say a little more about the size of the exceptional set. In order to do this we need to allow smaller values of $\lambda(n)$ but then can obtain an explicit and more precise upper bound on the cardinality of the set of positive integers $n \le N$ for which that bound is false.

We apply this estimate to study the largest possible period of the *power generator*

$$u_n \equiv u_{n-1}^e \pmod m, \quad 0 \le u_n \le m-1, \qquad n = 1, 2, \dots, \tag{1}$$

with the *initial value* $u_0 = \vartheta$ (an integer coprime to m) and *exponent* e (an integer at least 2).

In the two special cases $\gcd(e, \varphi(m)) = 1$, where $\varphi(m)$ is the Euler function, and $e = 2$, this sequence is known as the *RSA generator* and as the *Blum–Blum–Shub generator*, respectively.

For integers g and $M \ge 2$ with $\gcd(g, M) = 1$, denote by $\mathrm{ord}_M g$ the multiplicative order of g modulo M.

It is easy to see that if $\gcd(e, \lambda(m)) = 1$, then the sequence (1) is purely periodic with some period t. Moreover, this period is given by $t = \mathrm{ord}_s e$, where $s = \mathrm{ord}_m \vartheta$, and the largest possible value of t, over all possible choices of ϑ and e, is $\lambda(\lambda(m))$.

This generator has numerous cryptographic applications and has been extensively studied in the literature, see [4, 5, 7, 8, 10, 11, 12, 13, 15, 17, 19, 25, 26]. In particular, it is quite important to provide sequences of large period. Because of the aforementioned cryptographic applications this generator is mainly studied in the case $m = pl$, where p and l are two distinct primes. In this case, the results of [12] imply the uniformity of distribution of this generator provided the period $t \ge m^{3/4+\varepsilon}$. Moreover, the result becomes stronger as t gets closer to m.

Nevertheless, despite quite active studies of this generator, no lower bounds for the values of its largest period $\lambda(\lambda(m))$ are known. Here we apply the above-mentioned lower bound for $\lambda(n)$ to show that, for almost all pairs of primes p, l, $\lambda(\lambda(pl))$ is nearly of order pl. We then use it to prove that for almost all inputs of pairs of primes, initial values ϑ, and exponents e, the period of the corresponding sequence (u_n) given by (1) is close to its largest possible value. In particular, for almost all values of the above parameters it exceeds $m^{1-\varepsilon}$ for any ε and sufficiently large m.

We may remark that if one is willing to request large values of $\lambda(\lambda(pl))$ for many pairs but not for almost all, then one can get very large values indeed. If one is willing also to accept heuristic results, then, as a simple consequence of the well known conjecture about prime k-tuplets (see [3]), there are in every interval $(x, 2x)$ with large x, at least $c_1 x/(\log x)^3$ primes p such that $q = (p-1)/2$ and $r = (q-1)/2$ are both also prime. That is, we request that r, $q = 2r + 1$, and $p = 4r + 3$ are prime. It follows on pairing such primes p that there are at least $c_2 Q^2/(\log Q)^6$ pairs of primes (p, l) with $Q/2 < p < l \le Q$ for which $\lambda(\lambda(pl)) = pl/8 + O(Q)$. Here the constant $1/8$ is best possible. As we shall see below it is possible using sieve methods to unconditionally prove a result of the same strength (and even for a larger number of pairs (p, l)) apart from that constant.

Although studying the power generator (1) has been our primary motivation, we mention two further applications of our results.

The first of these is the conclusion that the so-called *cycling attack* on the RSA cryptosystem has a negligible chance to be efficient. Despite the common belief that this should be the case, no rigorous proof of the statement has been given. The attack is based on the observation that the power generator (1) can be considered as a sequence of consecutive RSA encryptions starting with the "message" u_0. Thus, if the period is t, then after $t-1$ iterations of the encrypted message u_1 we obtain $u_t \equiv u_0 \pmod m$, and if t is small, then this is an efficient procedure. Even more, if t is small, then, because it is very likely that the periods t_p and t_l of this sequence modulo p and l are distinct, after at most $\min\{t_p, t_l\} - 1$ iterations this attack may produce a complete factorization of m. This attack, as well as various ways of protecting against it, have been discussed in the literature, see [5, 18, 22, 24]. In particular, the so-called *safe primes* have been introduced. Rivest and Silverman [24] present arguments which show that randomly selected primes p and l are likely to be strong against this attack. Our results imply a more precise statement which basically means that for a random selection of parameters the expected complexity of this attack is about $m^{1/2}$, that is, of the same magnitude as the trial-division factorization algorithm. Indeed, obviously $t_p(l-1) \geq t$ and $t_l(p-1) \geq t$; thus when t is of order m and $p \sim l \sim m^{1/2}$ we obtain that $\min\{t_p, t_l\}$ is of order $m^{1/2}$.

Our second application is related to the recently introduced notion of *timed-release crypto*, see [23]. For example, for the construction of [23] it is essential to guarantee that the power generator (1) has a large period; see the discussion at the end of Section 2.1 of [23]. Our results provide rigorous support for this assumption.

Throughout the paper the implied constants in symbols "O", "$\gg$" and "$\ll$" are absolute. (The notations $U \ll V$ and $V \gg U$ are equivalent to $U = O(V)$ for positive functions U, V.)

We use $\log x$ to denote the natural logarithm of x and we let $\mathcal{P}$ denote the set of primes.

Acknowledgement. We thank Ron Rivest for his interest and for helpful references.

2. Preparations

Here we collect some known number-theoretic estimates, which we use in the sequel.

First of all we recall that

$$\varphi(k) \gg \frac{k}{\log\log(k+2)}, \tag{2}$$

where $\varphi(k)$ is the Euler function of $k \geq 1$; see Theorem 5.1 of Chapter 1 of [21].

In estimating various sums over primes, we use that the nth prime p_n satisfies $n \log n \ll p_n \ll n \log n$, for $n \geq 2$.

Let $\pi(X; k, a)$ denote the number of primes $p \leq X$ with $p \equiv a \pmod k$. We need the following relaxed version of the *Brun–Titchmarsh* theorem. For any integers $k, a \geq 1$ with $1 \leq k \leq X^{1/2}$ and $\gcd(a, k) = 1$, the bound

$$\pi(X; k, a) \ll \frac{X}{\varphi(k) \log X} \tag{3}$$

holds; see Theorem 4.1 of Chapter 2 of [21].

We need the following estimate. For any integers $X \ge 3$ and $k \ge \log X$,

$$\sum_{\substack{q \in \mathcal{P},\ q \le X \\ q \equiv 1 \pmod k}} \frac{1}{q} \ll \frac{\log k}{\varphi(k)}. \tag{4}$$

Indeed, for $k \ge X^{1/2}$ we have

$$\sum_{\substack{q \in \mathcal{P},\ q \le X \\ q \equiv 1 \pmod k}} \frac{1}{q} \le \sum_{\substack{k \le n \le X \\ n \equiv 1 \pmod k}} \frac{1}{n} \ll \frac{\log X}{k} \ll \frac{\log k}{k}.$$

For $k < X^{1/2}$ we use the same bound, but also the Brun–Titchmarsh estimate (3), to deduce that

$$\begin{aligned} \sum_{\substack{q \in \mathcal{P},\ q \le X \\ q \equiv 1 \pmod k}} \frac{1}{q} &\ll \sum_{s=\lceil \log k \rceil}^{\lceil \log X \rceil} \frac{\pi(\exp(s); k, 1)}{\exp(s)} \ll \frac{\log k}{k} + \sum_{s=\lfloor 2 \log k \rfloor}^{\lceil \log X \rceil} \frac{\pi(\exp(s); k, 1)}{\exp(s)} \\ &\ll \frac{\log k}{k} + \frac{1}{\varphi(k)} \sum_{s=1}^{\lceil \log X \rceil} \frac{1}{s} \ll \frac{\log k}{k} + \frac{\log \log X}{\varphi(k)} \ll \frac{\log k}{\varphi(k)}. \end{aligned}$$

We shall also require a bound for smaller k. For any fixed $\alpha > 0$, there exists $X_0(\alpha)$ such that the following holds. For all $X \ge X_0(\alpha)$ and all $k \le \log X$,

$$\sum_{\substack{q \in \mathcal{P},\ X^\alpha \le q \le X \\ q \equiv 1 \pmod k}} \frac{1}{q} \ll \frac{\log(1/\alpha)}{\varphi(k)}\ . \tag{5}$$

This follows from the above Brun–Titchmarsh bound (3) by partial summation.

Let $\tau(k)$ denote the number of positive integer divisors of an integer $k \ge 1$. The following bounds are well known and hold for any $X \ge 2$:

$$\sum_{k \le X} \tau(k) \ll X \log X \qquad \text{and} \qquad \sum_{k \le X} \tau^2(k) \ll X (\log X)^3\,; \tag{6}$$

see Theorems 5.3 and 5.4 of Chapter 1 of [21].

Finally, we recall that an integer $k \ge 1$ is called Y-smooth if it is divisible only by primes $p \le Y$. Let $\Psi(X, Y)$ denote the total number of Y-smooth numbers $k \le X$. The following estimate is a substantially relaxed and simplified version of (for example) Corollary 1.3 of [16], see also [6]. Let $X = Y^u$; then for any $u \to \infty$ with $u \le Y^{1/2}$ we have the bound

$$\Psi(X, Y) \ll X u^{-u + o(u)}. \tag{7}$$

We remark that all the above results are presented in very elementary and simplified forms which nevertheless are sufficient to prove our main results. Much stronger versions are known. For example, a much more precise version of (4) is given in [20]. Unfortunately these more sophisticated results do not seem to improve our estimates.

We need the following simple statement about the proportion of numbers whose multiplicative order modulo $M \ge 2$ is much smaller than $\lambda(M)$. Some results of this kind have been known [5] but they apply only to special moduli M.

Lemma 1. *Let M be a positive integer and j a divisor of $\lambda(M)$. Let $N_j(M)$ be the number of integers g with $1 \le g \le M$, $\gcd(g, M) = 1$ and $\operatorname{ord}_M g$ dividing $\lambda(M)/j$. Then*

$$N_j(M) \le \varphi(M)/j.$$

Moreover, for any real $K \ge 1$ the number $S_K(M)$ of integers g, $1 \le g \le M$, with $\gcd(g, M) = 1$ and $\operatorname{ord}_M g \le \lambda(M)/K$ satisfies

$$S_K(M) \le \varphi(M)\tau(\lambda(M))/K.$$

Proof. Let

$$M = p_1^{m_1} \dots p_\nu^{m_\nu} \qquad \text{and} \qquad \lambda(M) = q_1^{l_1} \dots q_\mu^{l_\mu}$$

be the prime number factorizations of M and $\lambda(M)$. For a divisor j of $\lambda(M)$, let $j = q_1^{j_1} \cdots q_\mu^{j_\mu}$ be its prime factorization, where each exponent j_t satisfies $0 \le j_t \le l_t$. For each $p_i^{m_i}$ in the prime factorization of M, let d_i be the product of those $q_t^{j_t}$ in the prime factorization of j for which $q_t^{l_t}$ (in the prime factorization of $\lambda(M)$) divides $\lambda(p_i^{m_i})$. Note that for each $q_t^{j_t}$ there is at least one d_i divisible by $q_t^{j_t}$, so that $j | d_1 \cdots d_\nu$.

For $\operatorname{ord}_M g$ to divide $\lambda(M)/j$, it is necessary that for each $p_i^{m_i}$ we have that g is a d_i-power modulo $p_i^{m_i}$. The number of residues g modulo $p_i^{m_i}$ which are coprime to p_i and are a d_i-power is at most $\varphi(p_i^{m_i})/d_i$. (It is equal to this bound except when $d_i = 2^s$, $s \ge 1$, $p_i = 2$, $m_i \ge 3$, in which case it is half of this bound.) Thus, by the Chinese remainder theorem, we have

$$N_j(M) \le \varphi(M)/d_1 \cdots d_\nu \le \varphi(M)/j,$$

as required. The second statement follows from the first simply by summing over $j | \lambda(M)$, $j \ge K$ (certainly this last part could be sharpened). □

We also need the following elementary statement.

Lemma 2. *Assume $d \ge 1$ is a divisor of an integer $n > 1$. Then for any integer g with $gcd(g, n) = 1$ we have that $\varphi(d)/\operatorname{ord}_d g$ divides $\varphi(n)/\operatorname{ord}_n g$. We also have $\varphi(d)/\lambda(d)$ divides $\varphi(n)/\lambda(n)$ and, as a consequence,*

$$\frac{\lambda(d)}{d} \ge \frac{\lambda(n)}{n}.$$

Proof. The natural projection of multiplicative groups $(\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*$ gives rise to the projection

$$(\mathbb{Z}/n\mathbb{Z})^* / \langle g \rangle \to (\mathbb{Z}/d\mathbb{Z})^* / \langle g \rangle,$$

and so $\varphi(d)/\operatorname{ord}_d g$ divides $\varphi(n)/\operatorname{ord}_n g$ as claimed. Next, taking any g satisfying $\operatorname{ord}_n g = \lambda(n)$, we deduce that, for this g, $\varphi(d)/\operatorname{ord}_d g$ divides $\varphi(n)/\lambda(n)$. But since $\varphi(d)/\lambda(d)$ divides $\varphi(d)/\operatorname{ord}_d g$, the second statement follows. Finally, using the inequality $d/\varphi(d) \le n/\varphi(n)$, we obtain the third statement from the second one. □

As we mentioned above, the largest possible period for the power generator given by (1) for a given modulus m is $\lambda(\lambda(m))$. The next result shows that many pairs ϑ, e lead to a period that is not much smaller than the maximum.

Lemma 3. *For any positive integer m and any numbers $K_1, K_2 \ge 1$, let W denote the number of pairs of integers ϑ, e with $1 \le \vartheta \le m$, $1 \le e \le \lambda(m)$ and $\gcd(\vartheta, m) = \gcd(e, \lambda(m)) = 1$, such that the period of the power generator given by (1) is at most $\lambda(\lambda(m))/K_1K_2$. Then*

$$W \le \varphi(m)\varphi(\lambda(m)) \left(\frac{\tau(\lambda(m))}{K_1} + \frac{\tau(\lambda(\lambda(m)))}{K_2} \right).$$

Proof. We apply Lemma 1 first with $M = m$ and $K = K_1$. So the number of values of ϑ in $[1, m]$ with $s := \operatorname{ord}_m \vartheta > \lambda(m)/K_1$ is at least $\varphi(m)(1 - \tau(\lambda(m))/K_1)$. For each such ϑ we again apply Lemma 1 now with $M = s$ and $K = K_2$. We deduce that the number of choices for e in $[1, s]$ with $\operatorname{ord}_s e > \lambda(s)/K_2$ is at least $\varphi(s)(1 - \tau(\lambda(s))/K_2)$. Thus, there are at least $\varphi(\lambda(m))(1 - \tau(\lambda(s))/K_2)$ choices of $e \in [1, \lambda(m)]$ that are coprime to $\lambda(m)$ and such that $\operatorname{ord}_s e > \lambda(s)/K_2$.

Note that Lemma 2 implies that if ϑ, e are chosen as above, then the period $\operatorname{ord}_s e$ of the power generator satisfies

$$\operatorname{ord}_s e > \frac{\lambda(s)}{K_2} \ge \frac{\lambda(\lambda(m))s}{\lambda(m)K_2} > \frac{\lambda(\lambda(m))\lambda(m)}{\lambda(m)K_1K_2} = \frac{\lambda(\lambda(m))}{K_1K_2}.$$

Since $\tau(\lambda(s)) \le \tau(\lambda(\lambda(m)))$, the result follows. □

Using the well-known bound $\tau(k) \le k^{o(1)}$ (see Theorem 5.2 of Chapter 1 of [21]), we can obtain the following corollary, which is possibly useful if $\lambda(\lambda(m))$ is not too small in comparison to $\lambda(m)$:

Corollary 4. *Let $\varepsilon > 0$ be arbitrary and let the integer m be sufficiently large depending on the choice of ε. The number of pairs of integers ϑ, e in the range $1 \le \vartheta \le m$, $1 \le e \le \lambda(m)$ with $\gcd(\vartheta, m) = \gcd(e, \lambda(m)) = 1$, and such that the period t of the power generator given by (1) satisfies $t \le \lambda(\lambda(m))/\lambda(m)^\varepsilon$ is at most $\varphi(m)\varphi(\lambda(m))/\lambda(\lambda(m))^{\varepsilon/3}$.*

3. Lower bounds for the Carmichael function

Theorem 5. *For sufficiently large numbers N and for $\Delta \ge (\log\log N)^3$, the number of positive integers $n \le N$ with*

$$\lambda(n) \le n \exp(-\Delta)$$

is at most $N \exp\left(-0.69\,(\Delta \log \Delta)^{1/3}\right)$.

Proof. Fix $\Delta \ge (\log\log N)^3$ and let us define K from the equation

$$\frac{(\log K)^3}{\log\log K} = \Delta - \Delta^{1/2};$$

thus $K = \exp\left(\left(3^{-1/3} + o(1)\right)(\Delta \log \Delta)^{1/3}\right)$. Note that $K \ge (\log N)^{\alpha(N)}$ for some $\alpha(N) \to \infty$ as $N \to \infty$.

Let $\mathcal{S}_1$ denote the set of $n \le N$ with $p^2 | \varphi(n)$ for some prime $p > K$. There are four possibilities for $n \in \mathcal{S}_1$.

- There exists a prime $p > K$ with $p^3 | n$. There are at most

$$\sum_{K \le p \le N^{1/3}} \left\lfloor \frac{N}{p^3} \right\rfloor \le N \sum_{K \le k \le N} \frac{1}{k^3} \ll NK^{-2}$$

such $n \le N$. Here, and in a number of places below, we are a little inefficient by not saving all possible logarithmic factors.

- There exists a prime $p > K$ with $p^2 | n$ and also there exists a prime $q | n$ with $q \equiv 1 \pmod p$. From (4) and partial summation we derive that the number of such $n \le N$ is at most

$$\sum_{K \le p \le N^{1/3}} \sum_{\substack{q \in \mathcal{P}, \\ q \equiv 1 \pmod p}} \sum_{\substack{p < q \le N/p^2 \\ (\mathrm{mod}\ p)}} \left\lfloor \frac{N}{p^2 q} \right\rfloor \ll N \sum_{K \le p \le N} \frac{\log p}{p^3} \ll NK^{-2}.$$

- There exists a prime $p > K$ and there exists a prime $q | n$ with $q \equiv 1 \pmod{p^2}$. As before we see that the number of such $n \le N$ is bounded by

$$N \sum_{K \le p \le N^{1/3}} \frac{\log p}{p^2} \ll NK^{-1}.$$

- There exists a prime $p > K$ and there exist two distinct primes $q_1 q_2 | n$ with $q_1 \equiv q_2 \equiv 1 \pmod p$. In this, the most frequently occurring case, we see that the number of such $n \le N$ is majorized by

$$N \sum_{K \le p \le N^{1/3}} \frac{(\log p)^2}{p^2} \ll NK^{-1} \log K.$$

So the cardinality of $\mathcal{S}_1$ satisfies $|\mathcal{S}_1| \ll NK^{-1} \log K \le NK^{-1+o(1)}$.
Put

$$v = \frac{\log K}{\log \log K} \qquad \text{and} \qquad L = K^v.$$

Denote by $\mathcal{Q}$ the set of primes $p \le N$ such that the contribution to $p-1$ from primes $q < K$ is at least L. Let $\mathcal{L}$ denote the set of K-smooth integers k with $N \ge k \ge L$. Then, from (4) we see that

$$\sum_{p \in \mathcal{Q}} \frac{1}{p} \le \sum_{k \in \mathcal{L}} \sum_{\substack{p \le N \\ p \equiv 1 \pmod k}} \frac{1}{p} \ll \sum_{k \in \mathcal{L}} \frac{\log k}{\varphi(k)}.$$

For the last sum, using (2) we derive

$$\sum_{k \in \mathcal{L}} \frac{\log k}{\varphi(k)} \ll \sum_{s = \lceil \log L \rceil}^{\lceil \log N \rceil} \frac{s \log s}{\exp(s)} \Psi(\exp(s), K).$$

It is easy to verify that if for $\lceil \log L \rceil \le s \le \lceil \log N \rceil$ we define u by the equation $\exp(s) = K^u$, then $v \le u \le \log N + 1 \le K^{1/2}$, so the bound (7) applies. Therefore

$$\begin{aligned} \sum_{p \in \mathcal{Q}} \frac{1}{p} &\le v^{-v+o(v)} \sum_{s = \lceil \log L \rceil}^{\lceil \log N \rceil} s \log s \\ &\le v^{-v+o(v)} (\log N)^2 \log \log N \le K^{-1+o(1)}. \end{aligned}$$

Denote by $\mathcal{S}_2$ the set of $n \le N$ which are divisible by a prime from $\mathcal{Q}$. Then

$$|\mathcal{S}_2| \le \sum_{p \in \mathcal{Q}} \left\lfloor \frac{N}{p} \right\rfloor \le N \sum_{p \in \mathcal{Q}} \frac{1}{p} \le NK^{-1+o(1)}.$$

Similarly, the cardinality of the set $\mathcal{S}_3$ of $n \le N$, such that the contribution to n itself from primes $q < K$ is at least L, satisfies

$$|\mathcal{S}_3| \le \sum_{k \in \mathcal{L}} \left\lfloor \frac{N}{k} \right\rfloor \le N \sum_{k \in \mathcal{L}} \frac{1}{k} \ll NK^{-1+o(1)}.$$

Let $\omega(n)$ denote the number of distinct prime divisors of an integer $n \ge 1$. Denote by $\mathcal{S}_4$ the set of $n \le N$ with $\omega(n) \ge \log K - 1$. Because, for every $n \in \mathcal{S}_4$, $\tau(n) \ge 2^{\omega(n)} \ge \frac{1}{2} K^{\log 2} > K^{1/2}$, we derive from the second part of (6) that

$$|\mathcal{S}_4| \le K^{-1} \sum_{n \le N} \tau^2(n) \ll NK^{-1+o(1)}.$$

Finally, we define the set

$$\mathcal{N} = \{NK^{-1} \le n \le N\} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3 \cup \mathcal{S}_4).$$

Combining the above results, one verifies that $|\mathcal{N}| = N + O\left(NK^{-1+o(1)}\right)$.

For $n \in \mathcal{N}$ we write $\varphi(n) = mM$, where m is the contribution of primes $q < K$ and M is the contribution of primes $q \ge K$. We see that for any $n \in \mathcal{N}$

$$m \le L^{\omega(n)+1} \le L^{\log K} = \exp\left(v (\log K)^2\right) = \exp\left(\Delta - \Delta^{1/2}\right)$$

because of our choice of K and v. We also remark that M is squarefree. Therefore,

$$\begin{aligned} \lambda(n) &\ge M = \frac{\varphi(n)}{m} \gg \frac{n}{m \log\log n} \\ &\gg \frac{NK^{-1}}{\log\log N} \exp\left(-\Delta + \Delta^{1/2}\right) \gg N \exp(-\Delta) \end{aligned}$$

for sufficiently large N. Taking into account that $3^{-1/3} > 0.69$ we obtain the desired statement. □

4. Period of the power generator

Here we apply Theorem 5 to obtain a lower bound for the largest possible period of the power generator. Recall that $\mathcal{P}$ denotes the set of primes.

Theorem 6. *For Q sufficiently large and for any $\Delta \ge 2(\log\log Q)^3$, the number of pairs $(p, l) \in \mathcal{P}^2$, $1 < p < l \le Q$, with*

$$\lambda(\lambda(pl)) < Q^2 \exp(-\Delta)$$

is at most $Q^2 \exp\left(-0.16 (\Delta \log \Delta)^{1/3}\right)$.

Proof. Fix $\Delta \ge 2(\log\log Q)^3$ and put

$$D = \exp\left(0.16 (\Delta \log \Delta)^{1/3}\right).$$

The number W of pairs $(p, l) \in \mathcal{P}^2$, $1 < p < l \le Q$, with $\gcd(p-1, l-1) \ge D$ satisfies

$$W \le \sum_{d \ge D} \pi(Q; d, 1)^2.$$

We use the estimate (3) for $d < Q^{1/2}$ together with (2) and just $\pi(Q;d,1) \le Q/d$ for $d \ge Q^{1/2}$, getting

$$W \ll \sum_{Q^{1/2} \ge d \ge D} \frac{Q^2}{\varphi(d)^2 \left(\log Q\right)^2} + \sum_{d \ge Q^{1/2}} \frac{Q^2}{d^2} \ll \frac{Q^2 (\log\log D)^2}{D \left(\log Q\right)^2} + Q^{3/2}.$$

Let $R(n)$ be the number of solutions of the equation $n = \lambda(pl)$ in pairs $(p,l) \in \mathcal{P}^2$, $1 < p < l \le Q$, with $\gcd(p-1, l-1) < D$. Obviously $R(n) \le D\tau(n)$. Indeed, we have at most $\tau(n)$ possibilities for $p-1$ and at most D possibilities for $\gcd(p-1, l-1)$. These two choices determine l.

Put $N = Q^2$. We say that n is *exceptional* if $\lambda(n) \le N \exp(-\Delta)$. Because we have $\Delta \ge (\log\log N)^3$, Theorem 5 may be applied. Let $\mathcal{E}$ denote the set of exceptional $n \le N$. Applying Theorem 5 and the Cauchy inequality and (6) we obtain

$$\begin{aligned} \sum_{n \in \mathcal{E}} R(n) &\le |\mathcal{E}|^{1/2} \left(\sum_{n \in \mathcal{E}} R(n)^2 \right)^{1/2} \ll |\mathcal{E}|^{1/2} D \left(\sum_{n \le N} \tau(n)^2 \right)^{1/2} \\ &\ll ND \exp\left(-0.34 \left(\Delta \log \Delta\right)^{1/3} \right). \end{aligned}$$

Noting that the cardinality of the set $\mathcal{Q}$ of these pairs $(p,l) \in \mathcal{P}^2$, $1 < p < l \le Q$, for which $\lambda(pl)$ is exceptional is at most

$$|\mathcal{Q}| \le W + \sum_{n \in \mathcal{E}} R(n),$$

after simple calculations we derive the result. □

We now show using sieve methods that for a large number of pairs $(p,l) \in \mathcal{P}^2$ we have $\lambda(\lambda(pl)) \gg pl$. Specifically we prove the following result.

Theorem 7. *There exist positive constants c_1 and c_2 such that, for more than $c_1 Q^2/(\log Q)^4$ pairs $(p,l) \in \mathcal{P}^2$, $1 < p < l \le Q$, we have*

$$\lambda(\lambda(pl)) > c_2 Q^2.$$

Proof. This proof contains a real parameter $\alpha > 0$ which will eventually be fixed. Throughout we shall assume, as we may, that Q is chosen sufficiently large in terms of α. We shall require both upper and lower bound sieve results.

The upper bound we require is as follows. Let $\beta > 0$ and define

$$P = \prod_{p < Q^\beta} p.$$

Let $1 \le k \le Q^{1-\beta}$ be an integer satisfying $\gcd(k, P) = 1$. The number of primes $p < Q$ satisfying $\gcd((p-1)/2, P) = 1$ and also $p \equiv 1 \pmod k$ is majorized by the number of positive integers $m \le Q$, $m \equiv 1 \pmod k$ for which $\gcd(m(m-1)/2, P) = 1$. Bounding this latter set above by means of the ("two-dimensional" upper bound) sieve (for example Theorem 5.1 of the standard reference [14]), we see that this number is $O\left(Q/k\beta^2 \left(\log Q\right)^2\right)$.

Using the lower bound sieve (see for example Theorem 8.3 of [14]), and estimating the error term with the aid of the Bombieri–Vinogradov theorem, we may fix $\alpha > 0$ sufficiently small that, in every interval $(Q/2, Q)$ there are at least $cQ/\alpha \left(\log Q\right)^2$ primes p such that $(p-1)/2$ is free of primes less than Q^α where the constant $c > 0$

is absolute. We may assume, by discarding no more than $Q^{1-\alpha}$ of our primes, that $p-1$ is also squarefree. By possibly making α somewhat smaller (and using the above upper bound sieve to remove the primes and products of two primes) we can also demand that $(p-1)/2$ is the product of three or more primes, the product of any two of which is thus no more than $Q^{1-\alpha}$. To remove the primes we merely take $k=1$ and $\beta=1/2$. To remove the products of two primes, we group in accordance with the smaller of the two, calling that one k, apply the upper bound, again with $\beta=1/2$, and then sum over k. The result follows from (5) in view of the fact that as α decreases $\log(1/\alpha)$ grows more slowly than $1/\alpha$.

Consider now the integers pl in the interval $\left(Q^2/4, Q^2\right)$ formed by pairing distinct primes p, l as above. There are at least $c^2Q^2/3\alpha^2\left(\log Q\right)^4$ of them.

By removing $O\left(Q^{2-\alpha}\right)$ of these pairs, we may assume that

$$\gcd\left(\frac{p-1}{2}, \frac{l-1}{2}\right) = 1$$

for all pairs under consideration. Thus, for such a pair (p,l) we may write

$$\frac{p-1}{2}\frac{l-1}{2} = q_1 \cdots q_r, \tag{8}$$

where $q_1, \dots, q_r \in \mathcal{P}$ are distinct and each satisfies $Q^\alpha \le q_j < Q^{1-2\alpha}$, $j=1,\dots,r$. In particular, $r < 2/\alpha$. Moreover we have

$$\lambda\left(\lambda(pl)\right) = \lambda\left(\operatorname{lcm}\left(p-1, l-1\right)\right) = \operatorname{lcm}\left(q_1-1, \dots, q_r-1\right),$$

and for all large Q this satisfies

$$\lambda\left(\lambda(pl)\right) \ge \frac{(q_1-1)\cdots(q_r-1)}{D(p;l)^{r^2/2}} \ge \frac{Q^2}{17D(p;l)^{r^2/2}},$$

where

$$D(p;l) = \max_{1\le i<j\le r} \gcd(q_i-1, q_j-1).$$

For given d, we next apply our upper bound sieve result to bound the number of pairs $(p,l) \in \mathcal{P}^2$, $1 < p < l \le Q$, for which $q_i \equiv q_j \equiv 1 \pmod d$ for some $1 \le i < j \le r$, where $q_1, \dots, q_r$ are defined by (8). We choose $\beta = \alpha$. To bound the number of occurrences with q_i and q_j both coming from the same member of the pair, we apply the bound once with $k = q_iq_j < Q^{1-\alpha}$. For the case where each of the two comes from a different member of the pair we apply the bound twice, once with $k=q_i$ and once with $k=q_j$. The number of pairs in question for both cases is bounded by

$$N_d \ll \frac{Q^2}{\alpha^4\left(\log Q\right)^4}\left(\sum_{\substack{q\in\mathcal{P},\ Q^\alpha\le q<Q^{1-\alpha}\\ q\equiv 1 \pmod d}} \frac{1}{q}\right)^2.$$

For $d > \log Q$ we use (4) and for smaller d we use (5). These give

$$\sum_{\substack{q\in\mathcal{P},\ Q^\alpha\le q<Q^{1-\alpha}\\ q\equiv 1 \pmod d}} \frac{1}{q} \ll \frac{\log(1/\alpha)\log d}{\varphi(d)}.$$

Thus the number of of pairs $(p,l) \in \mathcal{P}^2$, $1 < p < l \le Q$, in our set which satisfy $D(p;l) > D$ is bounded above by

$$\begin{aligned}\sum_{d>D} N_d &\ll \frac{Q^2}{\alpha^4 (\log Q)^4} \sum_{d>D} \left(\frac{\log(1/\alpha)\log d}{\varphi(d)}\right)^2 \\ &\ll \frac{Q^2}{(\log Q)^4} \frac{(\log(1/\alpha))^2}{\alpha^4} \frac{(\log D)^2}{D}.\end{aligned}$$

Provided D is chosen sufficiently large in terms of α, say $D = \alpha^{-3}$, and α is sufficiently small, this latter set makes a small contribution compared to those for which $D(p;l) \le D$ and the result follows. □

We remark that the constants c_1 and c_2 in Theorem 7 can be effectively evaluated.

Now we study the period of the sequence (u_n) given by (1) with $m = pl$ when the primes p and l, the initial value ϑ, and the exponent e are all selected at random.

Theorem 8. *For Q sufficiently large, for any $\Delta \ge 6 (\log\log Q)^3$, and for all pairs $(p,l) \in \mathcal{P}^2$, $1 < p < l \le Q$, except at most $Q^2 \exp\left(-0.1 (\Delta \log \Delta)^{1/3}\right)$ of them, the following statement holds. For all pairs (ϑ, e) with*

$$1 \le \vartheta \le m-1, \qquad 1 \le e \le \lambda(m), \qquad \gcd(\vartheta, m) = \gcd(e, \lambda(m)) = 1,$$

where $m = pl$, except at most $m\lambda(m)\exp(-0.2\Delta)$ of them, the period t of the sequence (u_n) given by (1) satisfies

$$t \ge Q^2 \exp(-\Delta).$$

Proof. First of all we recall that the above period $t = \operatorname{ord}_s e$, where $s = \operatorname{ord}_m \vartheta$.

It follows from (6) that the number of pairs $(p,l) \in \mathcal{P}^2$, $1 < p < l \le Q$, with

$$\tau((p-1)(l-1)) > \exp(\Delta/8)$$

is at most

$$\exp(-\Delta/8) \sum_{k \le Q^2} \tau^2(k) \ll Q^2 \exp(-\Delta/9).$$

We will consider only pairs p, l where $\gcd(p-1, l-1) < D$, where D is as in the proof of Theorem 6. So, as in that proof, for any number n, the number of pairs p, l with $\lambda(\lambda(pl)) = n$ is at most $D\tau(n)$. Thus, the number of pairs p, l with

$$\tau(\lambda(\lambda(pl))) > \exp(\Delta/8),$$

is at most

$$D \sum_{\substack{n \le Q^2 \\ \tau(n) > \exp(\Delta/8)}} \tau(n).$$

From the second part of (6) the number of $n \le Q^2$ with $B \le \tau(n) < 2B$ is $O\left(Q^2 (\log Q)^3 / B^2\right)$, so the sum of these values of $\tau(n)$ is $O\left(Q^2 (\log Q)^3 / B\right)$. Letting B run over powers of 2 starting just below $\exp(\Delta/8)$, we get that

$$D \sum_{\substack{n \le Q^2 \\ \tau(n) > \exp(\Delta/8)}} \tau(n) \ll DQ^2 (\log Q)^3 \exp(-\Delta/8) \ll Q^2 \exp(-\Delta/9).$$

Let $\mathcal{R}$ be the set of the pairs $(p,l) \in \mathcal{P}^2$, $1 < p < l \le Q$, for which

$$\lambda\left(\lambda(pl)\right) \ge Q^2 \exp\left(-\Delta/3\right)$$

and

$$\tau\left(\lambda(pl)\right) \le \exp\left(\Delta/8\right), \quad \tau(\lambda(\lambda(pl))) \le \exp\left(\Delta/8\right).$$

It follows from the above estimates and from Theorem 6 that

$$|\mathcal{R}| \ge Q^2 - Q^2 \exp\left(-0.1\left(\Delta \log \Delta\right)^{1/3}\right).$$

Let us fix some pair $(p,l) \in \mathcal{R}$ and put $m = pl$. We apply Lemma 3 with $K_1 = K_2 = \exp(\Delta/3)$. It follows that, except for at most

$$2\varphi(m)\varphi(\lambda(m)) \exp(-\Delta/5) \le m\lambda(m) \exp(-\Delta/5)$$

of them, the period t of the power generator is at least $\lambda(\lambda(m)) \exp(-2\Delta/3)$. But this bound is at least $Q^2 \exp(-\Delta)$, so the result follows. □

A similar result also holds for p and l described in Theorem 7.

It would be of great interest to be able to give a result of the strength of Theorem 8 but where now e is kept fixed while the other parameters p, l, ϑ vary. This seems a much harder question and is quite reminiscent of the Gauss–Artin problem on primitive roots. Using the same ideas as in Theorem 7, we are able to show that quite often the period is reasonably large. Because of its special interest we consider the case when $e = 2$, that is the Blum–Blum–Shub generator.

Theorem 9. *Given $\varepsilon > 0$, there exist positive constants c, γ such that for Q sufficiently large, there are more than $cQ^2/\left(\log Q\right)^4$ pairs $(p,l) \in \mathcal{P}^2$, $p < l \le Q$, such that for all integers ϑ with*

$$1 \le \vartheta \le m - 1 \qquad \text{and} \qquad \gcd(\vartheta, m) = 1,$$

where $m = pl$, except at most $m^{1-\gamma}$ of them, the period t of the sequence (u_n) given by (1) with $e = 2$ satisfies

$$t \ge cQ^{1-\varepsilon}.$$

Proof. We select the pairs $(p,l) \in \mathcal{P}^2$, $1 < p < l \le Q$, which gave us large values of $\lambda(\lambda(pl))$ as described in the proof of Theorem 7 and then eliminate those pairs for which

$$\operatorname{ord}_{q_1 \dots q_r} 2$$

is small. Here $q_1, \dots, q_r$ are given by (8) and also satisfy the condition that $\gcd(q_i - 1, q_j - 1)$ is bounded for all $i \ne j$. The number of primes q up to a bound B for which $\operatorname{ord}_q 2 < q^{1/2-\varepsilon/2}$ is at most $B^{1-\varepsilon}$, since these primes divide the product of $2^j - 1$ for j up to $B^{1/2-\varepsilon/2}$ and each factor $2^j - 1$ clearly has fewer than j prime factors. Thus, the number of primes $p \le Q$ with $p - 1$ divisible by a prime $q > Q^\alpha$ with $\operatorname{ord}_q 2 < q^{1/2-\varepsilon/2}$ is $O\left(Q^{1-\alpha\varepsilon}\right)$. Hence, we may assume that the pairs p, l

produced in Theorem 7 all have, for each i, $\operatorname{ord}_{q_i} 2 \geq q_i^{1/2-\varepsilon/2}$. Then

$$\begin{aligned}\operatorname{ord}_{q_1\cdots q_r} 2 &= \operatorname{lcm}\,(\operatorname{ord}_{q_1} 2, \ldots, \operatorname{ord}_{q_r} 2)\\ &\gg \operatorname{ord}_{q_1} 2 \cdot \cdots \cdot \operatorname{ord}_{q_r} 2\\ &\geq (q_1 \cdots q_r)^{1/2-\varepsilon/2}\\ &\gg (pl)^{1/2-\varepsilon/2}\\ &\gg Q^{1-\varepsilon}.\end{aligned}$$

But, by Lemma 1 the number of choices of ϑ up to m that are coprime to m and with $\operatorname{ord}_m \vartheta < q_1 \cdots q_r$ is $O\left(m/Q^{\alpha}\right)$. Hence, $\operatorname{ord}_m \vartheta$ is either $q_1 \cdots q_r$ or $2q_1 \cdots q_r$ (since $\lambda(m) = 2q_1 \cdots q_r$) for all ϑ up to m and coprime to m, except at most $O\left(m^{1-\alpha}\right)$ of them. For any choice of ϑ, the period t of the power generator with $e = 2$ is the order of 2 modulo the largest odd divisor of $\operatorname{ord}_m \vartheta$. So, but for few exceptional choices of ϑ, this period is $\operatorname{ord}_{q_1\ldots q_r} 2$ and, as we have already seen, $\operatorname{ord}_{q_1\ldots q_r} 2 \gg Q^{1-\varepsilon}$. This completes the proof. □

5. Remarks

Our results cover the important special case where one wishes to show that the exceptional set has cardinality $O\left(N(\log N)^{-A}\right)$ with an arbitrary A, which is more than sufficient to deal with integers of the form pl. Actually they go rather further than that. Moreover, one can take slightly smaller values of Δ in both Theorems 5 and 6. On the other hand, some heuristic arguments show that there are at least $N^{1-o(1)}$ integers $m \leq N$ with $\lambda(m) \leq m^{o(1)}$. So to get an exceptional set of size $O\left(N^{1-\varepsilon}\right)$ one may have to allow very small values of λ.

Rigorously, we can show that there are at least $N^{7/10}$ values of $m \leq N$ with $\lambda(m) < m^{1/\log\log m}$. This is done using a recent paper of Baker and Harman [2]. Here is a sketch of the proof: Let M denote the least common multiple of the integers up to $\log N/\log\log N$. Consider the primes p up to $(\log N)^{3.37}$ for which $p-1$ divides M. From [2], there are more than $(\log N)^{3.37}/(\log\log N)^{O(1)}$ such primes p. Consider now the squarefree integers m up to M composed solely of these primes p. A simple binomial coefficient calculation shows that there are more than $N^{.703}$ such numbers m. But each such m has $\lambda(m)|M$, and note that $M \leq N^{O(1/\log\log N)}$.

In addition, using some ideas in [1] one can force $\lambda(m)$ to be even smaller and still have a power of N values of m. Namely, for each $\varepsilon > 0$ there is a number N_ε such that if $N \geq N_\varepsilon$, the number of $m \leq N$ with $\lambda(m) < \exp\left((\log\log m)^{5/(2\varepsilon)}\right)$ exceeds $N^{5/12-\varepsilon}$. Here is a sketch of the proof: Let $c = 5/12 - \varepsilon/2$ and $\gamma = 5/(2\varepsilon)$. Let y be large and let L be the product of the primes in the interval $[y^\gamma/\log y, y^\gamma]$. Let $x = \exp\left(y^2\right)$. Using Theorem 3.1 in [1] there is an integer $K < x^{1-c}$ such that

$$\#\{d|L\,:\, d < x^c,\ dK+1 \in \mathcal{P}\} \gg \frac{1}{\log x}\#\{d|L : d < x^c\}.$$

A simple binomial coefficient calculation shows that there are at least $x^{c(1-2/\gamma)}$ such divisors d. Now, take these primes $dK+1$ and form squarefree integers m. In fact, take them t at a time, where $t = \left\lfloor \exp\left(y^{3/2}\right)\right\rfloor$. These numbers m are all at most $N := x^t$ and each such $\lambda(m)$ is a divisor of KL, and so is at most $\exp\left((\log\log N)^\gamma\right)$. Again, a simple binomial coefficient calculation shows that there

are at least $N^{c(1-3/\gamma)}$ such integers m. Since $c(1-3/\gamma) > 5/12 - \varepsilon$, the proof is complete.

Given the results above for general integers m, it seems reasonable to expect that there are many pairs $(p, l) \in \mathcal{P}^2$, $1 < p < l \le Q$, with quite small values of $\lambda(\lambda(pl))$. On the other hand, to prove that this is the case seems quite a difficult proposition. Indeed, it is not even known that there are infinitely many values of $p-1$ which are very smooth and, for $\lambda(\lambda(pl))$ to be small, necessarily both $p-1$ and $l-1$ must be smooth.

References

[1] W. R. Alford, A. Granville and C. Pomerance, 'There are infinitely many Carmichael numbers', *Annals Math.* **140** (1994), 703–722. MR **95k:**11114

[2] R. C. Baker and G. Harman, 'Shifted primes without large prime factors', *Acta Arith.* **83** (1998), 331–361. MR **99b:**11104

[3] A. Balog, 'The prime k-tuplets conjecture on average', *Analytic Number Theory*, Progress in Mathematics **85**, Birkhäuser, Boston, 1990, 47–75. MR **92e:**11105

[4] L. Blum, M. Blum and M. Shub, 'A simple unpredictable pseudorandom number generator', *SIAM J. Comp.*, **15** (1986), 364–383. MR **87k:**65007

[5] J. J. Brennan and B. Geist, 'Analysis of iterated modular exponentiation: The orbit of x^α mod N', *Designs, Codes and Cryptography*, **13** (1998), 229–245. MR **99b:**11086

[6] E. R. Canfield, P. Erdős and C. Pomerance,'On a problem of Oppenheim concerning "Factorisatio Numerorum"', *J. Number Theory*, **17** (1983), 1–28. MR **85j:**11012

[7] T. W. Cusick, 'Properties of the x^2 mod N pseudorandom number generator', *IEEE Trans. Inform. Theory*, **41** (1995), 1155–1159. MR **96k:**65006

[8] T. W. Cusick, C. Ding and A. Renvall, *Stream Ciphers and Number Theory*, Elsevier, Amsterdam, 1998. MR **99h:**94045

[9] P. Erdős, C. Pomerance and E. Schmutz, 'Carmichael's lambda function', *Acta Arith.*, **58** (1991), 363–385. MR **92g:**11093

[10] R. Fischlin and C. P. Schnorr, 'Stronger security proofs for RSA and Rabin bits', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1233** (1997), 267–279. CMP 98:09

[11] J. B. Friedlander, D. Lieman and I. E. Shparlinski, 'On the distribution of the RSA generator', *Proc. Intern. Conf. on Sequences and their Applications (SETA'98), Singapore*, Springer-Verlag, London, 1999, 205–212.

[12] J. B. Friedlander and I. E. Shparlinski, 'On the distribution of the power generator', *Math. Comp.*, (to appear).

[13] F. Griffin and I. E. Shparlinski, 'On the linear complexity profile of the power generator', *Preprint*, 1998, 1–11.

[14] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London 1974. MR **54:**12689

[15] J. Håstad and M. Näslund, 'The security of individual RSA bits', *Proc. 39th IEEE Symp. on Foundations of Comp. Sci.*, 1998, 510–519.

[16] A. Hildebrand and G. Tenenbaum, 'Integers without large prime factors', *J. de Théorie des Nombres de Bordeaux*, **5** (1993), 411–484. MR **95d:**11116

[17] J. C. Lagarias, 'Pseudorandom number generators in cryptography and number theory', *Proc. Symp. in Appl. Math.*, Amer. Math. Soc., Providence, RI, **42** (1990), 115–143. MR **92f:**11109

[18] U. M. Maurer, 'Fast generation of prime numbers and secure public-key cryptographic parameters', *J. Cryptology*, **8** (1995), 123–155. MR **96i:**94021

[19] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1997. MR **99g:**94015

[20] C. Pomerance, 'On the distribution of amicable numbers', *J. Reine Angew. Math.*, **293/294** (1977), 217–222. MR **56:**5402

[21] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957. MR **19:**393b

[22] R. L. Rivest, 'Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem', *Cryptologia*, **2** (1978), 62–65.

[23] R. L. Rivest, A. Shamir and D. A. Wagner, 'Time-lock puzzles and timed-release crypto', *Preprint*, 1996, 1–9.
[24] R. L. Rivest and R. D. Silverman, 'Are "strong" primes needed for RSA?', *Preprint*, 1999, 1–23.
[25] I. E. Shparlinski, 'On the linear complexity of the power generator', *Designs, Codes and Cryptography*, (to appear).
[26] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, FL, 1995. MR **96k:**94015

Department of Mathematics, University of Toronto, Toronto, Ontario M5S 3G3, Canada
E-mail address: frdlndr@math.toronto.edu

Department of Fundamental Mathematics, Bell Labs, Murray Hill, New Jersey 07974-0636
E-mail address: carlp@research.bell-labs.com

Department of Computing, Macquarie University, Sydney, New South Wales 2109, Australia
E-mail address: igor@ics.mq.edu.au