

**CORRIGENDUM TO “PERIOD OF THE POWER GENERATOR
 AND SMALL VALUES OF CARMICHAEL’S FUNCTION”**

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

We are indebted to Kelly Postelmans whose question drew our attention to a slip in the proof of Theorem 8 of [1]. In particular, we asserted that for a fixed number n , the number of pairs of primes p, l with $\gcd(p-1, l-1) < D$ and $\lambda(\lambda(pl)) = n$ is at most $D\tau(n)$, an assertion which now seems unjustified. (The notation is defined below.) In this note we give a corrected proof of Theorem 8.

As in [1] we consider the *power generator*

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

with the *initial value* $u_0 = \vartheta$ (an integer coprime to m) and *exponent* e (an integer at least 2). We recall that for an integer $n \geq 1$ the *Carmichael function* $\lambda(n)$ is the largest order occurring amongst elements of the unit group in the residue ring modulo n . As usual, φ denotes Euler’s function. We let $\tau(n)$ denote the number of natural divisors of n , we let $\omega(n)$ denote the number of divisors of n that are prime, and we let $\Omega(n)$ denote the number of divisors of n that are (either a prime or) a prime power. An integer n is said to be *squarefull* if for each prime $p|n$ we have $p^2|n$. If p^a is the largest power of the prime p which divides n , and a is at least 1, we write $p^a||n$. The letters p, q, l always denote prime numbers.

The following is a slightly stronger form of Theorem 8 of [1].

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

$$1 \leq \vartheta \leq m-1, \quad 1 \leq e \leq \lambda(m), \quad \gcd(\vartheta, m) = \gcd(e, \lambda(m)) = 1,$$

where $m = pl$, except at most $m\lambda(m)\exp(-\Delta/4)$ of them, the period t of the sequence (u_n) given by (1) satisfies

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

Proof. Let \mathcal{S} be the set of pairs (p, l) of primes with $1 < p < l \leq Q$ and let \mathcal{R} be the set of pairs $(p, l) \in \mathcal{S}$ for which all of the following hold:

- (i) $\lambda(\lambda(pl)) \geq Q^2 \exp(-\Delta/3)$,
- (ii) $\tau(p-1), \tau(l-1) < 2\Delta^{2/5}$ (so that $\omega(p-1), \omega(l-1) < \Delta^{2/5}$),
- (iii) for each prime $q|\lambda(pl)$, $\tau(q-1) < \exp(\Delta^{2/5})$.

Received by the editor April 19, 2002.

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

By Theorem 6 of [1] we have that the number of pairs $(p, l) \in \mathcal{S}$ that do not satisfy (i) is

$$E_1 \ll Q^2 \exp\left(-0.11 (\Delta \log \Delta)^{1/3}\right).$$

From the well-known bound

$$\sum_{n \leq x} \tau^2(n) \ll x \log^3 x,$$

it follows that the number of pairs $(p, l) \in \mathcal{S}$ that do not satisfy (ii) is

$$E_2 \ll Q^2 \exp\left(-\Delta^{2/5}\right).$$

We now consider pairs $(p, l) \in \mathcal{S}$ that do not satisfy (iii). Suppose $\omega(q-1) \geq \Delta^{2/5}$ for some prime $q | \lambda(pl)$. We have

$$\begin{aligned} \sum_{n \leq Q, \omega(n) \geq \Delta^{2/5}} \frac{1}{n} &\leq \sum_{j \geq \Delta^{2/5}} \frac{1}{j!} \left(\sum_{q \leq Q} \left(\frac{1}{q} + \frac{1}{q^2} + \dots \right) \right)^j \\ &= \sum_{j \geq \Delta^{2/5}} \frac{1}{j!} \left(\sum_{q \leq Q} \frac{1}{q-1} \right)^j \\ &\leq \sum_{j \geq \Delta^{2/5}} \frac{1}{j!} (c + \log \log Q)^j, \end{aligned}$$

where c is an absolute constant. Since $\Delta \geq 6(\log \log Q)^3$, it follows that if Q is sufficiently large, the terms in the above series decay at least geometrically, so that

$$\sum_{n \leq Q, \omega(n) \geq \Delta^{2/5}} \frac{1}{n} \leq \exp\left(-\frac{1}{3} \Delta^{2/5} \log \Delta\right).$$

Thus, the number of primes $p \leq Q$ such that $p-1$ is divisible by a prime q with $\omega(q-1) \geq \Delta^{2/5}$ is at most

$$(2) \quad \sum_{n \leq Q, \omega(n) \geq \Delta^{2/5}} \frac{Q}{n+1} \leq Q \exp\left(-\frac{1}{3} \Delta^{2/5} \log \Delta\right),$$

as can be seen by forgetting just for the moment that p and q are primes and using only that they are integers at least 2. Now suppose that $q | p-1$, $\omega(q-1) < \Delta^{2/5}$, and $\tau(q-1) \geq \exp(\Delta^{2/5})$. Note that if $\omega(n) < \Delta^{2/5}$ and $\tau(n) \geq \exp(\Delta^{2/5})$, then $2^{\Omega(n)} \geq \exp(\Delta^{2/5}) > \exp(\omega(n))$, so that $\Omega(n) - \omega(n) > \frac{1}{3} \Delta^{2/5}$. (The constant $\frac{1}{3}$ can be improved to $0.75679\dots$ using the inequality $\tau(n) \leq (3/2)^{\Omega(n) - \omega(n)} 2^{\omega(n)}$.) Every such number n may be factored as $n_1 n_2$, where n_1 is squarefull, $\Omega(n_1) > \frac{1}{3} \Delta^{2/5}$, and $n_2 \leq Q$. Thus the sum of reciprocals of such numbers $n \leq Q$ is at most

$$\sum_{n_1} \frac{1}{n_1} \sum_{n_2} \frac{1}{n_2} \ll 2^{-\frac{1}{6} \Delta^{2/5}} \log Q \ll \exp\left(-\frac{1}{9} \Delta^{2/5}\right),$$

where n_1 and n_2 independently run through integers of the above types. (Here we have used that the least squarefull number n with $\Omega(n) \geq k > 1$ is 2^k and that the sum of the reciprocals of the squarefull numbers that are at least B is $\ll B^{-1/2}$, the latter following from partial summation and the fact that there are $O(x^{1/2})$ squarefull numbers in $[1, x]$.) Thus, the number of primes $p \leq Q$ such that

$p - 1$ is divisible by a prime q with $\tau(q - 1) \geq \exp(\Delta^{2/5})$ and $\omega(q - 1) \leq \Delta^{2/5}$ is $\ll Q \exp(-\frac{1}{9}\Delta^{2/5})$ and, by (2), this latter condition (on ω) may be dropped. Hence, the number of pairs $(p, l) \in \mathcal{S}$ which do not satisfy (iii) is

$$E_3 \ll Q^2 \exp\left(-\frac{1}{9}\Delta^{2/5}\right).$$

We conclude that for sufficiently large Q ,

$$|\mathcal{R}| \geq \binom{\pi(Q)}{2} - E_1 - E_2 - E_3 \geq \binom{\pi(Q)}{2} - Q^2 \exp\left(-0.1(\Delta \log \Delta)^{1/3}\right).$$

We shall show that the conclusion of the theorem holds for every pair (p, l) in \mathcal{R} . Let us fix some pair $(p, l) \in \mathcal{R}$ and put $m = pl$. We have, by (ii),

$$\tau(\lambda(m)) \leq \tau(\varphi(m)) \leq \tau(p - 1)\tau(l - 1) < \exp\left(2\Delta^{2/5}\right).$$

Further, using that $\varphi(ab) | \varphi(a)\varphi(b)$ for all positive integers a, b ,

$$\tau(\lambda(\lambda(m))) \leq \tau(\varphi((p - 1)(l - 1))) \leq \tau(\varphi(p - 1))\tau(\varphi(l - 1))\tau(l - 1).$$

Here, we have $\tau(l - 1) \leq \exp(\Delta^{2/5})$, by (ii). Moreover, for $(p, l) \in \mathcal{R}$, we have, by (ii) and (iii),

$$\begin{aligned} \tau(\varphi(p - 1)) &\leq \prod_{q^a \parallel p-1} \tau(\varphi(q^a)) = \prod_{q^a \parallel p-1} a\tau(q - 1) \leq \tau(p - 1) \prod_{q|p-1} \tau(q - 1) \\ &< \exp\left(\Delta^{2/5}\right) \exp\left(\Delta^{2/5}\omega(p - 1)\right) < \exp\left(\Delta^{4/5} + \Delta^{2/5}\right), \end{aligned}$$

and the same bound holds for $\tau(\varphi(l - 1))$. We conclude that

$$\tau(\lambda(\lambda(m))) < \exp\left(2\Delta^{4/5} + 3\Delta^{2/5}\right).$$

We apply Lemma 3 of [1] with $K_1 = K_2 = \exp(\Delta/3)$. It follows that for sufficiently large Q , apart from at most

$$\varphi(m)\varphi(\lambda(m)) \left(\frac{\tau(\lambda(m))}{\exp(\Delta/3)} + \frac{\tau(\lambda(\lambda(m)))}{\exp(\Delta/3)} \right) \leq m\lambda(m) \exp(-\Delta/4)$$

exceptional pairs (ϑ, e) , the period t of the power generator satisfies

$$t \geq \lambda(\lambda(m)) \exp(-2\Delta/3) \geq Q^2 \exp(-\Delta),$$

by (i), so the result follows. □

We remark that Kelly Postelmans also pointed out to us a slip in the proof of Lemma 1 concerning reduced residues modulo a prime power p^m . This slip is easily fixed by replacing in the last paragraph of the proof our incorrect assertion that g be a d -th power modulo p^m by the condition that it be a $\lambda(p^m)/d$ -th root of unity. (In case $p = 2$, these are not quite the same.)

REFERENCES

- [1] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, *Period of the power generator and small values of Carmichael's function*, Math. Comp., **70** (2001), 1591–1605.

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`