April 5, 2011

ON A PROBLEM OF ARNOLD: THE AVERAGE MULTIPLICATIVE ORDER OF A GIVEN INTEGER

PÄR KURLBERG AND CARL POMERANCE

Time-stamp: "2011-03-28 20:35:06 kurlberg"

1. Introduction

Given coprime integers g, n with $n > 0$, let $l_g(n)$ denote the multiplicative order of g modulo n, i.e., the smallest integer $k \geq 1$ such that $g^k \equiv 1 \mod n$. For $x \geq 1$ an integer let

$$T_g(x) := \frac{1}{x} \sum_{\substack{n \leq x \\ (n,g)=1}} l_g(n)$$

denote the average multiplicative order of g. In [1], Arnold conjectured that if $|g| > 1$, then

$$T_g(x) \sim c(g) \frac{x}{\log x},$$

as $x \to \infty$, for some constant $c(g) > 0$. However, in [9] Shparlinski showed that if the Generalized Riemann Hypothesis[1] (GRH) is true, then

$$T_g(x) \gg \frac{x}{\log x} \exp\left(C(g)(\log\log\log x)^{3/2}\right),$$

where $C(g) > 0$. He also suggested that it should be possible to obtain, again assuming GRH, a lower bound of the form

$$T_g(x) \geq \frac{x}{\log x} \exp\left(C(g)(\log\log\log x)^{2+o(1)}.\right)$$

Let

$$B = e^{-\gamma} \prod_p \left(1 - \frac{1}{(p-1)^2(p+1)}\right) = 0.3453720641\ldots, \tag{1}$$

the product being over primes, and where γ is the Euler–Mascheroni constant. The aim of this note is to prove the following result.

P.K. was partially supported by grants from the Göran Gustafsson Foundation, the Knut and Alice Wallenberg foundation, the Royal Swedish Academy of Sciences, and the Swedish Research Council. C.P. was supported by NSF grant numbers DMS-0703850, DMS-1001180. The authors gratefully acknowldege Michel Balazard for suggesting the problem.

[1]What is needed is that the Riemann hypothesis holds for Dedekind zeta functions $\zeta_{K_n}(s)$ for all $n > 1$, where K_n is the Kummer extension $\mathbb{Q}(e^{2\pi i/n}, g^{1/n})$.

Theorem 1. *Assuming GRH,*

$$T_g(x) = \frac{x}{\log x} \exp\left(\frac{B \log\log x}{\log\log\log x}(1+o(1))\right)$$

as $x \to \infty$, uniformly in g with $1 < |g| \le x$. The upper bound implicit in this result holds unconditionally.

Since $l_g(n) \le \lambda(n)$, where $\lambda(n)$, commonly known as Carmichael's function, denotes the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$, we immediately obtain that

$$T_g(x) \le \frac{1}{x}\sum_{n=1}^{x} \lambda(n),$$

and it is via this inequality that we are able to unconditionally establish the upper bound implicit in Theorem 1. Indeed, in [2], Erdős, Pomerance and Schmutz determined the average order of $\lambda(n)$ showing that, as $x \to \infty$,

$$\frac{1}{x}\sum_{n=1}^{x} \lambda(n) = \frac{x}{\log x} \exp\left(\frac{B \log\log x}{\log\log\log x}(1+o(1))\right). \tag{2}$$

Theorem 1 thus shows under assumption of the GRH that the mean values of $\lambda(n)$ and $l_g(n)$ are of a similar order of magnitude. We know, on assuming GRH, that $\lambda(n)/l_g(n)$ is very small for almost all n (e.g., see [4, 6]; in the latter Li and Pomerance in fact showed that $\lambda(n)/l_g(n) \le (\log n)^{o(\log\log\log n)}$ as $n \to \infty$ on a set of asymptotic density 1), so perhaps Theorem 1 is not very surprising. *However*, in [2] it was also shown that the normal order of $\lambda(n)$ is quite a bit smaller than the average order: there exists a subset S of the positive integers, of asymptotic density 1, such that for $n \in S$ and $n \to \infty$,

$$\lambda(n) = \frac{n}{(\log n)^{\log\log\log n + A + (\log\log\log n)^{-1+o(1)}}},$$

where $A > 0$ is an explicit constant. Thus the main contribution to the average of $\lambda(n)$ comes from a *density-zero subset* of the integers, and to obtain our result on the average multiplicative order, we must show that $l_g(n)$ is large for most n such that $\lambda(n)$ is large. To do this we follow the proof of the lower bound implicit in (2) found in [2], making the changes necessary to deal with $l_g(n)$.

We remark that if one averages over g as well, then a result like our Theorem 1 holds unconditionally. In particular, it follows from Luca and Shparlinski [8] and (2) that

$$\frac{1}{x^2}\sum_{n\le x}\sum_{\substack{1<g<n\\(g,n)=1}} l_g(n) = \frac{x}{\log x}\exp\left(\frac{B\log\log x}{\log\log\log x}(1+o(1))\right)$$

as $x\to\infty$.

1.1. **Averaging over prime moduli.** Given a rational number $g\neq 0,\pm 1$ and a prime p not dividing the numerator or denominator og g, let $\ell_g(p)$ denote the order of g modulo p. For simplicity, when p does divide the numerator or denominator of g, we let $\ell_g(p)=1$. Further, given $k\in\mathbb{Z}^+$, let

$$D_g(k) := [\mathbb{Q}(g^{1/k}, e^{2\pi i/k}) : \mathbb{Q}]$$

denote the degree of the Kummer extension obtained by taking the splitting field of $X^k - g$. Let $\mathrm{rad}(k)$ denote the largest squarefree divisor of k and let $\omega(k)$ be the number of primes dividing $\mathrm{rad}(k)$.

Theorem 2. *Given $g\in\mathbb{Q}$, $g\neq 0,\pm1$, define*

$$c_g := \sum_{k=1}^{\infty}\frac{\phi(k)\mathrm{rad}(k)(-1)^{\omega(k)}}{k^2 D_g(k)}.$$

The series for c_g converges absolutely. Further, assuming GRH,

$$\frac{1}{\pi(x)}\sum_{p\le x}\ell(p) = \frac{1}{2}c_g\cdot x + O\left(\frac{x}{(\log x)^{1/2-1/\log\log\log x}}\right).$$

where the error term holds uniformly for $|g|<x$.[2]

Though perhaps not obvious from the definition, $c_g>0$ for all $g\neq 0,\pm1$. In order to determine c_g, define

$$c := \prod_p\left(1-\frac{p}{p^3-1}\right) = 0.5759599689\ldots,$$

the product being over primes; c_g turns out to be a positive *rational* multiple of c. Theorem 2 should be contrasted with the unconditional result of Luca [7] that

$$\frac{1}{\pi(x)}\sum_{p\le x}\frac{1}{(p-1)^2}\sum_{g=1}^{p-1} l_g(p) = c + O(1/(\log x)^A)$$

[2]Fixme: Here we basically use the bound $\tau(h)\ll 2^{\log_2 x/\log_3 x}$ where $g=g_0^h$. Leave h-dependency explicit??

for any fixed $A > 0$. By partial summation one can then obtain

$$\frac{1}{\pi(x)} \sum_{p \le x} \frac{1}{p-1} \sum_{g=1}^{p-1} l_g(p) \sim \frac{1}{2} c \cdot x \text{ as } x \to \infty,$$

a result that is more comparable to Theorem 2.

To describe c_g we will need some further notation. Write $g = \pm g_0^h$ where h is a positive integer and $g_0 > 0$ is not an exact power of a rational number, and write $g_0 = g_1 g_2^2$ where g_1 is a squarefree integer and g_2 is a rational. Define $\Delta(g) = \Delta(g_0) = g_1$ if $g_1 \equiv 1 \mod 4$, and $\Delta(g) = \Delta(g_0) = 4g_1$ if $g_1 \equiv 2$ or $3 \mod 4$. Let $e = v_2(h)$ (that is, $2^e \| h$). For $g > 0$, define $n = \text{lcm}[2^{e+1}, \Delta(g)]$. For $g < 0$, define $n = 2g_1$ if $e = 0$ and $g_1 \equiv 3 \mod 4$, or $e = 1$ and $g_1 \equiv 2 \mod 4$; let $n = \text{lcm}[2^{e+2}, Delta(g)]$ otherwise.

Consider the multiplicative function $f(k) := (-1)^{\omega(k)} \text{rad}(k)(h,k)/k^3$. We note that for p prime and $l \ge 1$,

$$f(p^l) = \begin{cases} -p/p^{3l} & \text{if } p \nmid h, \\ -p^{1+\min(l, v_p(h))}/p^{3l} & \text{if } p | h. \end{cases}$$

Given an integer $t \ge 0$, define $F(p,t)$ and $F(p)$ by

$$F(p,t) := \sum_{l=0}^{t-1} f(p^l), \quad F(p) := \sum_{l=0}^{\infty} f(p^l)$$

In particular, we note that if $p \nmid h$, then

$$F(p) = 1 - \sum_{l=1}^{\infty} p^{1-3l} = 1 - \frac{p}{p^3 - 1} \tag{3}$$

Proposition 3. *With notation as above, if $g < 0$ and $e > 0$, we have*

$$c_g = c \cdot \prod_{p|h} \frac{F(p)}{1 - \frac{p}{p^3-1}} \cdot \left(1 - \frac{F(2, e+1) - 1}{2F(2)} + \prod_{p|n} \left(1 - \frac{F(p, v_p(n))}{F(p)} \right) \right),$$

otherwise

$$c_g = c \cdot \prod_{p|h} \frac{F(p)}{1 - \frac{p}{p^3-1}} \cdot \left(1 + \prod_{p|n} \left(1 - \frac{F(p, v_p(n))}{F(p)} \right) \right).$$

For example, if $g = 2$, then $h = 1$, $e = 0$, and $n = 8$. Thus

$$c_2 = c \cdot \left(1 + 1 - \frac{F(2,3)}{F(2)} \right) = c \cdot \left(2 - \frac{1 - 2/(2^1)^3 - 2/(2^2)^3}{1 - 2/(8-1)} \right) = c \cdot \frac{159}{160}.$$

2. Proof of Theorem 1

WARNING: g-uniformity part not quite done!!

2.1. Some preliminary results. Given a rational number $g \neq 0, \pm 1$, we recall the notation h, e, n described in the introduction, and for a positive integer k, we recall that $D_g(k)$ is the degree of the splitting field of $X^k - g$ over $\mathbb{Q}$. We record a result of Wagstaff on $D_g(k)$, see [10], Proposition 4.1 and the second paragraph in the proof of Theorem 2.2.

Proposition 4. *With notations as above,*

$$D_g(k) = \frac{\phi(k) \cdot k}{(k,h) \cdot \epsilon_g(k)} \tag{4}$$

where $\epsilon_g(k)$ is defined as follows: If $g > 0$, then

$$\epsilon_g(k) := \begin{cases} 2 & \text{if } n | k, \\ 1 & \text{if } n \nmid k. \end{cases}$$

If $g < 0$, then

$$\epsilon_g(k) := \begin{cases} 2 & \text{if } n | k, \\ 1/2 & \text{if } 2 | k \text{ and } 2^{e+1} \nmid k, \\ 1 & \text{if } n \nmid k. \end{cases}$$

We will need the following *uniform* version of [5, Theorem 23].

Theorem 5. *If the GRH is true, then for x, y with $1 \leq y \leq \log x$, $g = a/b \neq 0, \pm 1$ where a, b are integers with $|a|, |b| \leq x$, and h the largest integer such that $g = \pm g_0^h$ for some positive rational g_0, we have*

$$\left| \left\{ p \leq x : \ell_g(p) \leq \frac{p-1}{y} \right\} \right| \ll \frac{\pi(x)}{y} \cdot \frac{h\tau(h)}{\phi(h)} + \frac{x \log\log x}{\log^2 x}.$$

where $\tau(h)$ is the number of divisors of h.

Proof. Since the proof is rather similar to the proof of the main theorem in [3], [4, Theorem 2], and [5, Theorem 23] we only give a brief outline. With $i_g(p) = (p-1)/\ell_g(p)$, we see that $\ell_g(p) \leq (p-1)/y$ implies that $i_g(p) \geq y$. Further, in the case that $p \mid ab$, so that we are defining $\ell_g(p) = 1$ and hence $i_g(p) = p - 1$, the number of primes p satisfying this is $O(\log x)$. So we assume that $p \nmid ab$.

First step: We first consider primes $p \leq x$ such that $i_g(p) \geq x^{1/2} \log^2 x$. Such a prime p divides $a^k - b^k$ for some positive integer $k < x^{1/2}/\log^2 x$. Since $\omega(|a^k - b^k|) \ll k \log x$, it follows that the number of primes p in this case is $O((x^{1/2}/\log^2 x)^2 \log x) = O(x/\log^3 x)$.

Second step: Consider primes p such that $q|i_p$ for some prime q in the interval $[\frac{x^{1/2}}{\log^2 x}, x^{1/2}\log^2 x]$. We may bound this by considering primes $p \le x$ such that $p \equiv 1 \pmod q$ for some prime $q \in [\frac{x^{1/2}}{\log^2 x}, x^{1/2}\log^2 x]$. The Brun–Titchmarsh inequality then gives that the number of such primes p is at most

$$\sum_{q\in[\frac{x^{1/2}}{\log^2 x}, x^{1/2}\log^2 x]} \frac{x}{\phi(q)\log(x/q)} \ll \frac{x}{\log x} \sum_{q\in[\frac{x^{1/2}}{\log^2 x}, x^{1/2}\log^2 x]} \frac{1}{q} \ll \frac{x\log\log x}{\log^2 x}.$$

Third step: Now consider primes p such that $q|i_g(p)$ for some prime q in the interval $[y, \frac{x^{1/2}}{\log^3 x}]$. In this range the GRH gives useful bounds; by (28) in [3] or Corollary 6 and Lemma 9 of [4], we have

$$|\{p \le x : q \mid i_g(p)\}| \ll \frac{\pi(x)(q,h)}{q\phi(q)} + O(x^{1/2}\log(xq^2)).$$

since $D_g(q) \gg q\phi(q)/(q,h)$ (see (4)). Summing over primes q, we find that the number of such p is bounded by a constant times

$$\sum_{q\in[y,\frac{x^{1/2}}{\log^2 x}]} \left(\frac{\pi(x)(q,h)}{q^2} + O(x^{1/2}\log(xq^2))\right) \ll \frac{\pi(x)\omega(h)}{y} + \frac{x}{\log^2 x}.$$

Fourth step: For the remaining primes p, any prime divisor $q|i_g(p)$ is smaller than y. Hence $i_g(p)$ must be divisible by some integer d in the interval $[y, y^2]$. The analog of (28) in [3] for not-necessarily-squarefree integers, or more directly, Corollary 6 and Lemma 9 of [4], together with 4, gives

$$|\{p \le x : d \mid i_g(p)\}| \ll \frac{\pi(x)(d,h)}{d\phi(d)} + O(x^{1/2}\log(xd^2)). \tag{5}$$

Hence the total number of such p is bounded by

$$\sum_{d\in[y,y^2]} \left(\frac{\pi(x)(d,h)}{d\phi(d)} + O(x^{1/2}\log(xd^2))\right) \ll \frac{\pi(x)}{y}\frac{\tau(h)h}{\phi(h)},$$

where the last estimate follows from

$$\sum_{d\in[y,y^2]} \frac{(d,h)}{d\phi(d)} \le \sum_{m|h} \sum_{\substack{d\in[y,y^2] \\ m|d}} \frac{m}{d\phi(d)} \le \sum_{m|h} \sum_{k\ge y/m} \frac{1}{\phi(m)k\phi(k)}$$

$$\ll \sum_{m|h} \frac{m}{y\phi(m)} = \frac{h}{y\phi(h)} \sum_{m|h} \frac{m}{\phi(m)} \cdot \frac{\phi(h)}{h} \le \frac{h\tau(h)}{y\phi(h)}.$$

Here we used the bound $\sum_{k\geq T}\frac{1}{k\phi(k)}\ll 1/T$ for $T>0$, which follows by an elementary argument from the bound $\sum_{k\geq T}\frac{1}{k^2}\ll 1/T$ and the identity $k/\phi(k)=\sum_{j|k}\frac{\mu^2(j)}{\phi(j)}$. □

2.2. **Some notation.** In what follows, p and q will always denote primes. Let x be large and let g be an integer with $1<|g|\leq x$. Define

$$y=\log\log x,\quad l=[\log y],\quad m=[y/\log^3 y],\quad D=m!,$$

and let

$$S_k=\{p\leq x\,:\,(p-1,D)=2k\}.$$

Then $S_1,S_2,\ldots,S_{D/2}$ are disjoint sets of primes whose union equals $\{2<p\leq x\}$. Let

$$\tilde{S}_k=\left\{p\in S_k\,:\,p\nmid g,\ \frac{p-1}{2k}\ \Big|\ l_g(p)\right\} \tag{6}$$

be the subset of S_k where $l_g(p)$ is "large." Note that if $p\in S_k\setminus\tilde{S}_k$ and $p\nmid g$, there is some prime[3] $q>m$ with $q\mid(p-1)/l_g(p)$, so that $l_g(p)<p/m$.

We shall use Theorem 23 of [5], which implies on GRH that

$$|\{p\leq x: l_g(p)<p/z\}|\ll\frac{\pi(x)}{z}+O\left(\frac{x\log\log x}{\log^2 x}\right), \tag{7}$$

uniformly in g,x,z, with $1<|g|\leq x$. In particular,

$$|S_k\setminus\tilde{S}_k|\leq|\{p\leq x: l_g(p)<p/m\}|+\sum_{p|g}1\ll\pi(x)/m.$$

Using this it is easy to see that S_k and $\tilde{S}_k$ are of similar size when k is small. However, we shall essentially measure the "size" of S_k or $\tilde{S}_k$ by the sum of the reciprocals of its members. We define

$$E_k:=\sum_{\substack{p\in S_k\\ p^\alpha\leq x}}\frac{1}{p^\alpha}$$

and

$$\tilde{E}_k:=\sum_{\substack{p\in\tilde{S}_k\\ p^\alpha\leq x}}\frac{1}{p^\alpha}.$$

[3]Fixme: This seems fishy!! What about small prime divisors, say if $2^e||D$, but $2^{e+1}|(p-1)$?? I think these can be taken care of fairly easily, but some argument needed. Or!?

By Lemma 1 of [2], uniformly for $k \le \log^2 y$,

$$E_k = \frac{y}{\log y} \cdot P_k \cdot (1 + o(1)) \tag{8}$$

where

$$P_k = \frac{e^{-\gamma}}{k} \prod_{q>2} \left(1 - \frac{1}{(q-1)^2}\right) \prod_{q|k,\, q>2} \frac{q-1}{q-2}. \tag{9}$$

Note that

$$\sum_{k=1}^{\infty} \frac{P_k}{2k} = B. \tag{10}$$

The following lemma shows that not much is lost when restricting to primes $p \in \tilde{S}_k$.

Lemma 6. *For $k \le \log y$, we uniformly have*

$$\tilde{E}_k = E_k \cdot \left(1 + O\left(\frac{\log^5 y}{y}\right).\right)$$

Proof. By (8) and (9), we have

$$E_k \gg \frac{y}{k \log y} \ge \frac{y}{\log^2 y}, \tag{11}$$

and it is thus sufficient to show that $\sum_{p \in E_k \setminus \tilde{E}_k} 1/p \ll \log^3 y$ since the contribution from prime powers p^α for $\alpha \ge 2$ is $O(1)$. Now, if $p \in E_k \setminus \tilde{E}_k$ then[4] $l_g(p) < p/m$, and hence (7), together with partial summation, gives that

$$\sum_{p \in E_k \setminus \tilde{E}_k} \frac{1}{p} \ll \frac{\log\log x}{m} = \frac{y}{[y/\log^3 y]} \ll \log^3 y.$$

This completes the proof. □

Lemma 7. *We have*

$$\sum_{k=1}^{l} \frac{E_k}{2k} = \frac{By}{\log y}(1 + o(1))$$

where B is given by (1).

Proof. This follows immediately from (8), (9), and (10). □

[4]Fixme: care required if we want a g-uniform version! But: can use $q > m$ property as on page 5.

Given a vector $\mathbf{j} = (j_1, j_2, \ldots, j_{D/2})$ with each $j_i \in \mathbb{Z}_{\geq 0}$, let

$$\|\mathbf{j}\| := j_1 + j_2 + \ldots + j_{D/2}.$$

Paralleling the notation $\Omega_i(x; \mathbf{j})$ from [2], let:

- $\tilde{\Omega}_1(x; \mathbf{j})$ be the set of integers that can be formed by taking products of $v = \|\mathbf{j}\|$ distinct primes $p_1, p_2, \ldots, p_v$ in such a way that:
  - for each i, $p_i < x^{1/y^3}$, and
  - the first j_1 primes are in $\tilde{S}_1$, the next j_2 are in $\tilde{S}_2$, etc.;
- $\tilde{\Omega}_2(x; \mathbf{j})$ be the set of integers $u = p_1 p_2 \cdots p_v \in \tilde{\Omega}_1(x; \mathbf{j})$ such that $(p_i - 1, p_j - 1)$ divides D for all $i \neq j$;
- $\tilde{\Omega}_3(x; \mathbf{j})$ be the set of integers of the form $n = up$ where $u \in \tilde{\Omega}_2(x; \mathbf{j})$ and p satisfies $(p-1, D) = 2$, $\max(x/2u, x^{1/y}) < p \leq x/u$ and $l_g(p) > p/y^2$;
- $\tilde{\Omega}_4(x; \mathbf{j})$ be the set of integers $n = (p_1 p_2 \cdots p_v)p$ in $\tilde{\Omega}_3(x; \mathbf{j})$ with the additional property that $(p - 1, p_i - 1) = 2$ for all i.

2.3. **Preliminary lemmas.** We shall also need the following analogues of Lemmas 2-4 of [2]. Recall that $l = [\log y]$, and let

$$\mathbf{J} := \{\mathbf{j} : 0 \leq j_k \leq E_k/k \text{ for } k \leq l, \text{ and } j_k = 0 \text{ for } k > l\}.$$

Lemma 8. *If $\mathbf{j} \in \mathbf{J}$ and $n \in \tilde{\Omega}_4(x; \mathbf{j})$ and x is large, then*

$$l_g(n) \geq c_1 \frac{x}{y^3} \prod_{k=1}^{l} (2k)^{-j_k},$$

where $c_1 > 0$ is an absolute constant.

Proof. Suppose that $n = (p_1 p_2 \cdots p_v)p \in \tilde{\Omega}_4(x; \mathbf{j})$. Let $d_i = (p_i - 1, D)$, and let $u_i := (p_i - 1)/d_i$. By (6), u_i divides $l_g(p_i)$ for all i, and by the definition of $\tilde{\Omega}_3(x; \mathbf{j})$ we also have $l_g(p) > p/y^2$. Since $(p-1)/2$ is coprime to $(p_i - 1)/2$ for each i and each $(p_i - 1, p_j - 1) \mid D$ for $i \neq j$, we have $u_1, \ldots, u_v, p - 1$ pairwise coprime. But

$$l_g(n) = \operatorname{lcm}(l_g(p_1), l_g(p_2), \ldots, l_g(p_v), l_g(p)),$$

so we find that, using the minimal order of Euler's function and $l_g(p) > p/y^2$,

$$\begin{aligned} l_g(n) \geq u_1 u_2 \cdots u_v l_g(p) &\geq \frac{\phi(n)}{y^2 \cdot \prod_{i=1}^{v} d_i} \\ &\gg \frac{n}{y^2 \cdot \log\log n \cdot \prod_{k=1}^{l} (2k)^{j_k}} \gg \frac{x}{y^3 \cdot \prod_{k=1}^{l} (2k)^{j_k}} \end{aligned}$$

(recalling that $d_i = (p_i - 1, D) = 2k$ if $p_i \in \tilde{S}_k$, and that $n \in \tilde{\Omega}_4(x; \mathbf{j})$ implies that $n > x/2$). $\square$

Lemma 9. *If $\mathbf{j} \in \mathbf{J}$ and $u \in \tilde{\Omega}_2(x; \mathbf{j})$ and x is large, then*

$$|\{p : up \in \tilde{\Omega}_4(x; \mathbf{j})\}| > c_2 x/(uy \log x)$$

where $c_2 > 0$ is an absolute constant.

Proof. Note that for $\mathbf{j} \in \mathbf{J}$, $\|\mathbf{j}\| \le \sum_{k=1}^{l} E_k/k \ll y/\log y$ by (8) and (9). For such vectors $\mathbf{j}$, Lemma 3 of [2] implies that the number of primes p with $\max(x/2u, x^{1/y}) < p \le x/u$, $(p-1, D) = 2$, and $(p-1, p_i - 1) = 2$ for all $p_i \mid u$ is $\gg x/(uy \log x)$. Thus it suffices to show that

$$|\{p \le x/u : (p-1, D) = 2,\ l_g(p) \le p/y^2\}| = o(x/(uy \log x)).$$

By (7), this count is[5]

$$\ll \frac{\pi(x/u)}{y^2} \ll \frac{x}{uy^2 \log x} = o\left(\frac{x}{uy \log x}\right).$$

The result follows. $\square$

Lemma 10. *If $\mathbf{j} \in \mathbf{J}$, then for all sufficiently large x,*

$$\sum_{u \in \tilde{\Omega}_2(x; \mathbf{j})} \frac{1}{u} > \exp\left(\frac{-c_3 y \log\log y}{\log^2 y}\right) \prod_{k=1}^{l} \frac{E_k^{j_k}}{j_k!}$$

where $c_3 > 0$ is an absolute constant.

Proof. The sum in the lemma is equal to

$$\frac{1}{j_1! j_2! \cdots j_l!} \sum_{\langle p_1, p_2, \ldots, p_v \rangle} \frac{1}{p_1 p_2 \cdots p_v}$$

where the sum is over sequences of distinct primes where the first j_1 are in $\tilde{S}_1$, the next j_2 are in $\tilde{S}_2$, and so on, and also each $(p_i - 1, p_j - 1) \mid D$ for $i \ne j$. Such a sum is estimated from below in Lemma 4 of [2] but without the extra conditions that differentiate $\tilde{S}_k$ from S_k. The key prime reciprocal sum there is estimated on pages 381–383 to be

$$E_k \left(1 + O\left(\frac{\log\log y}{\log y}\right)\right).$$

In our case we have the extra conditions that $p \nmid g$ and $(p-1)/2k \mid l_g(p)$, which alters the sum by a factor of $1 + O(\log^6 y/y)$ by Lemma 6. But the factor $1 + O(\log^5 y/y)$ is negligible compared with the factor $1 + O(\log\log y/\log y)$, so we have exactly the same expression in our current case. The proof is complete. $\square$

[5]Fixme: Careful, g-uniformity problems here!

2.4. **Conclusion.** We clearly have

$$T_g(x) \geq \frac{1}{x} \sum_{\mathbf{j} \in \mathbf{J}} \sum_{n \in \tilde{\Omega}_4(x;\mathbf{j})} l_g(n).$$

By Lemma 8, we have

$$T_g(x) \gg \frac{1}{y^3} \sum_{\mathbf{j} \in \mathbf{J}} \prod_{k=1}^{l} (2k)^{-j_k} \sum_{n \in \tilde{\Omega}_4(x;\mathbf{j})} 1.$$

Now,

$$\sum_{n \in \tilde{\Omega}_4(x;\mathbf{j})} 1 = \sum_{u \in \tilde{\Omega}_2(x;\mathbf{j})} \sum_{up \in \tilde{\Omega}_4(x;\mathbf{j})} 1,$$

and by Lemma 9, this is

$$\gg \sum_{u \in \tilde{\Omega}_2(x;\mathbf{j})} \frac{x}{uy \log x},$$

which in turn by Lemma 10 is

$$\gg \frac{x}{y \log x} \exp\left(\frac{-c_3 y \log\log y}{\log^2 y}\right) \prod_{k=1}^{l} \frac{E_k^{j_k}}{j_k!}.$$

Hence

$$T_g(x) \gg \frac{x}{y^4 \log x} \exp\left(\frac{-c_3 y \log\log y}{\log^2 y}\right) \sum_{\mathbf{j} \in \mathbf{J}} \prod_{k=1}^{l} (2k)^{-j_k} \frac{E_k^{j_k}}{j_k!}.$$

Now,

$$\sum_{\mathbf{j} \in \mathbf{J}} \prod_{k=1}^{l} (2k)^{-j_k} \frac{E_k^{j_k}}{j_k!} = \prod_{k=1}^{l} \left(\sum_{j_k=0}^{[E_k/k]} \frac{(E_k/2k)^{j_k}}{j_k!} \right).$$

Note that $\sum_{j=0}^{2w} w^j/j! > e^w/2$ for $w \geq 1$ and also that $E_k/2k \geq 1$ for x sufficiently large, as $E_k \gg y/(k \log y)$ by (11). Thus,

$$\sum_{\mathbf{j} \in \mathbf{J}} \prod_{k=1}^{l} (2k)^{-j_k} \frac{E_k^{j_k}}{j_k!} > 2^{-l} \exp\left(\sum_{k=1}^{l} \frac{E_k}{2k} \right).$$

Hence

$$T_g(x) \gg \frac{x}{y^4 \log x} \exp\left(\frac{-c_3 y \log\log y}{\log^2 y}\right) 2^{-l} \exp\left(\sum_{k=1}^{l} \frac{E_k}{2k} \right).$$

By Lemma 7 we thus have the lower bound in the theorem. The proof is concluded.

3. Averaging over prime moduli — the proofs

3.1. **Proof of Theorem 2.** Let $z = (\log x / \log\log x)^{1/2}$, and let $i(p) = (p-1)/l(p)$. We have

$$\sum_{p \le x} l(p) = \sum_{\substack{p \le x \\ i(p) \le z}} l(p) + \sum_{\substack{p \le x \\ i(p) > z}} l(p) = A + B,$$

say. Note that

$$\begin{aligned} A &= \sum_{\substack{p \le x \\ i(p) \le z}} (p-1) \sum_{uv \mid i(p)} \frac{\mu(v)}{u} \\ &= \sum_{p \le x} (p-1) \sum_{\substack{uv \mid i(p) \\ uv \le z}} \frac{\mu(v)}{u} - \sum_{\substack{p \le x \\ i(p) > z}} (p-1) \sum_{\substack{uv \mid i(p) \\ uv \le z}} \frac{\mu(v)}{u} \\ &= C - D, \end{aligned}$$

say. The main term C is

$$C = \sum_{uv \le z} \frac{\mu(v)}{u} \sum_{\substack{p \le x \\ uv \mid i(p)}} (p-1).$$

Following Hooley[6], the inner sum here[7] is

$$\frac{1}{2} x \frac{\pi(x)}{D_g(uv)} + O\left(\frac{x^2}{\log^2 x}\right).$$

Thus,

$$C = \frac{1}{2} x \pi(x) \left(\sum_{uv \le z} \frac{\mu(v)}{u D_g(uv)} \right) + O\left(\frac{x^2}{\log^2 x} \sum_{n \le z} \left| \sum_{uv = n} \frac{\mu(v)}{u} \right| \right).$$

The inner sum in the O-term is $\phi(n)/n$, so the O-term is $O(x^2 z / \log^2 x)$. Recalling that $\mathrm{rad}(n)$ denotes the largest squarefree divisor of n, we note that $\sum_{v \mid k} \mu(v) v = \prod_{p \mid k} (1-p) = (-1)^{\omega(k)} \phi(\mathrm{rad}(k))$, and hence

$$\sum_{u,v} \frac{\mu(v)}{u D_g(uv)} = \sum_{k \ge 1} \sum_{v \mid k} \frac{\mu(v) v}{D_g(k) k} = \sum_{k \ge 1} \frac{(-1)^{\omega(k)} \phi(\mathrm{rad}(k))}{D_g(k) k}$$

---

[6] Fixme: Make more precise.

[7] Fixme: Switch to $Li(x^2)$? Also, explain error?

which, on noting that $\phi(\mathrm{rad}(k)) = \phi(k)\cdot\phi(\mathrm{rad}(k))/\phi(k) = \phi(k)\mathrm{rad}(k)/k$, equals

$$\sum_{k\geq 1} \frac{(-1)^{\omega(k)}\mathrm{rad}(k)\phi(k)}{D_g(k)k^2} = c_g$$

Thus,

$$\sum_{uv\leq z} \frac{\mu(v)}{uvD_g(uv)} = c_g - \sum_{k>z} \frac{(-1)^{\omega(k)}\mathrm{rad}(k)\phi(k)}{D_g(k)k^2} = c_g + O(\tau(h)^{1+\epsilon}/z),$$

by the same argument as in the fourth step of the proof of Theorem 5. It now follows by our choice of z that

$$C = \frac{c_g}{2} x\pi(x)(1 + O(1/z)).$$

It remains to estimate the two error terms B, D. Using Theorem 23 in [KP] (or merely the Brun–Titchmarsh inequality), we have

$$B \ll \frac{x}{z} \cdot \frac{\pi(x)}{z} \ll \frac{x\pi(x)}{z^2}.$$

To estimate D, we consider separately terms with $z < i(p) \leq z^2$ and terms with $i(p) > z^2$, denoting the two sums D_1, D_2, respectively. Note that

$$\left| \sum_{\substack{uv|n \\ uv\leq z}} \frac{\mu(v)}{u} \right| \leq \sum_{u|n} \frac{1}{u} \sum_{\substack{v|n \\ v\leq z}} 1 \leq \frac{\tau(n)\sigma(n)}{n},$$

$\sigma(n) = \sum_{d|n} d$. We use this estimate for D_1, getting

$$|D_1| \leq \sum_{z<n\leq z^2} \frac{\tau(n)\sigma(n)}{n} \sum_{\substack{p\leq x \\ n|i(p)}} (p-1) \ll x\pi(x) \sum_{z<n\leq z^2} \frac{\tau(n)\sigma(n)}{nD_g(n)},$$

using Hooley. An elementary calculation then shows that

$$|D_1| \ll \frac{x\pi(x)\tau(h)^{1+\epsilon}\log z}{z}.$$

For D_2 we use

$$\left| \sum_{\substack{uv|n \\ uv\leq z}} \frac{\mu(v)}{u} \right| \leq \sum_{u\leq z} \frac{1}{u} \sum_{v\leq z/u} 1 \leq z \sum_{u\leq z} \frac{1}{u^2} \ll z.$$

Thus, using (5)

$$|D_2| \leq xz \sum_{\substack{p\leq x \\ i(p)>z^2}} 1 \ll \frac{x\pi(x)\tau(h)^{1+\epsilon}}{z}.$$

We conclude that

$$\begin{aligned}\sum_{p\leq x} l(p) &= A + B = C - D_1 - D_2 + B \\ &= \frac{c_g}{2}x\pi(x) + O\left(\frac{x^2 z}{\log^2 x} + \frac{x\pi(x)}{z^2} + \frac{x\pi(x)\log z}{z} + \frac{x\pi(x)}{z}\right) \\ &= \frac{c_g}{2}x\pi(x) + O\left(\frac{x^2(\log\log x)^{1/2}}{(\log x)^{3/2}}\right),\end{aligned}$$

and the proof is finished.

3.2. **Proof of Proposition 3.**

Proof of Proposition 3. We begin with the cases $g > 0$, or $g < 0$ and $e = 0$. Recalling that $D_g(k) = \phi(k)k/(\epsilon_g(k)(k,h))$, we find that

$$c_g = \sum_{k\geq 1} \frac{(-1)^{\omega(k)}\mathrm{rad}(k)\phi(k)}{D_g(k)k^2} = \sum_{k\geq 1} \frac{(-1)^{\omega(k)}\mathrm{rad}(k)(k,h)\epsilon_g(k)}{k^3}. \tag{12}$$

Now, since $\epsilon_g(k)$ equals 1 if $n \nmid k$, and 2 otherwise, (12) equals

$$\sum_{k\geq 1} \frac{(-1)^{\omega(k)}\mathrm{rad}(k)(h,k)}{k^3} + \sum_{n|k} \frac{(-1)^{\omega(k)}\mathrm{rad}(k)(h,k)}{k^3} = \sum_{k\geq 1}(f(k)+f(kn)) \tag{13}$$

where the function $f(k) = (-1)^{\omega(k)}\mathrm{rad}(k)(h,k)/k^3$ is multiplicative.

If $p \nmid h$ and $l \geq 1$, we have

$$f(p^l) = -p/p^{3l}.$$

On the other hand, writing $h = \prod_{p|h} p^{e_{h,p}}$ we have

$$f(p^l) = -p^{1+\min(l,e_{h,p})}/p^{3l}$$

for $p|h$ and $l \geq 1$. Since f is multiplicative,

$$\sum_{k\geq 1}(f(k) + f(kn)) = \sum_{k:\mathrm{rad}(k)|hn} (f(k) + f(kn)) \cdot \sum_{(k,hn)=1} f(k)$$

Now, for $p \nmid h$ and $l \geq 1$, we have $f(p^l) = -\mathrm{rad}(p^l)/p^{3l} = -p/p^{3l}$, hence $\sum_{l\geq 0} f(p^l) = 1 - \frac{p}{p^3(1-1/p^3)} = 1 - \frac{p}{p^3-1}$ and thus

$$\sum_{(k,hn)=1} f(k) = \prod_{p\nmid hn} F(p) = \prod_{p\nmid hn}(1 - \frac{p}{p^3-1}) = \frac{c}{\prod_{p|hn}(1 - \frac{p}{p^3-1})}$$

Similarly, $\sum_{\mathrm{rad}(k)|hn} f(k) = \prod_{p|hn} F(p)$ and

$$\sum_{\mathrm{rad}(k)|hn} f(kn) = \prod_{p|hn} \left(\sum_{l \geq e_{n,p}} f(p^l) \right) = \prod_{p|hn} (F(p) - F(p, e_{n,p}))$$

Hence

$$\sum_{\mathrm{rad}(k)|hn} f(k) + \sum_{\mathrm{rad}(k)|hn} f(kn) = \prod_{p|hn} F(p) + \prod_{p|hn} (F(p) - F(p, e_{n,p}))$$

$$= \prod_{p|hn} F(p) \cdot \left(1 + \prod_{p|hn} \left(1 - \frac{F(p, e_{n,p})}{F(p)} \right) \right)$$

Thus

$$c_g = \frac{c}{\prod_{p|hn}(1 - \frac{p}{p^3-1})} \cdot \prod_{p|hn} F(p) \cdot \left(1 + \prod_{p|hn} \left(1 - \frac{F(p, e_{n,p})}{F(p)} \right) \right)$$

which, by (3), simplifies to

$$= c \cdot \prod_{p|h} \frac{F(p)}{1 - \frac{p}{p^3-1}} \cdot \left(1 + \prod_{p|hn} \left(1 - \frac{F(p, e_{n,p})}{F(p)} \right) \right)$$

The case $g < 0$ and $e > 0$ is similar: using the multiplicativity of f together with the definition of $\epsilon_g(k)$, we find that

$$c_g = \sum_{k \geq 1} (f(k) + f(kn)) - \frac{1}{2} \sum_{l=1}^{e} \sum_{(k,2)=1} f(2^l k)$$

$$= \prod_p F(p) + \prod_p (F(p) - F(p, e_{n,p})) - \frac{1}{2} \cdot (F(2, e+1) - 1) \cdot \prod_{p>2} F(p)$$

$$= \prod_p F(p) \left(1 + \prod_{p|n} \left(1 - \frac{F(p, e_{n,p})}{F(p)} \right) - \frac{F(2, e+1) - 1}{2F(2)} \right)$$

Again using the fact that

$$\prod_p F(p) = \prod_{p \nmid h} (1 - \frac{p}{p^3+1}) \prod_{p|h} F(p) = c \cdot \prod_{p|h} \frac{F(p)}{1 - p/(p^3+1)}$$

the proof is concluded.

$\square$

Still to do

- Check the proof and possibly improve the error estimate.

- The result should have some uniformity in the range of g, hopefully, $1 < |g| \leq x$. This would take a version of Theorem 23 in [KP] that has an explicit dependence on g.
- More importantly, Theorem 23 in Kurlberg–Pomerance is *not* stated as uniform in g, as asserted here. This needs to be fixed. The cheap way would be to remove assertions on uniformity in our results and prove them only for g fixed. It would be better to modify Theorem 23 so that it is uniform, if this is not too difficult. It would make it a much more useful result! (In progress.)
- It might be remarked that the theorem goes through with a still smaller value of z, and that then parts of the proof follow without GRH.
- I asked Pieter Moree about whether results on the average order of $l_g(p)$ were already known, and he didn't know any. It still seems odd to me, since the argument is essentially Hooley. I guess no one bothered. He told me of a paper of Wagstaff who considered the average of $i_g(p)$ for values of it that are $\leq T$, where T is arbitrarily large, but fixed. This is somewhat related. The paper is "Pseudoprimes and a generalization of Artin's conjecture" in Acta Arith. 41 (1982), 141–150.
- I have been checking the literature, and I found a 1995 paper of Francesco Pappalardi, "Hooley's theorem with weights" in Rend. Sem. Math. Univ. Pol. Torino **53** (1995), 375–388. In the notation of this section, he considers estimating

  $$\sum_{p \leq x} f(i(p)),$$

  where f satisfies some growth conditions. In his Theorem 2 he essentially gives an asymptotic for the above sum, on GRH, that involves the numbers δ_m, the density of primes p with $i(p) = m$. If one takes $f(x) = 1/x$, then the hypotheses of the theorem are satisfied, and I'm guessing we'd have, via partial summation, some sort of formula for the average order. At the end of the paper he gives 5 examples of his work, but this is not one of them. The densities δ_m are sort of a mess to compute, and involve Artin's constant, so I believe the approach we take above is better. Maybe it would be good to work it once the other way to see if we get the same constant! (I did this for $g = 2$, and I did get the same constant, but it would be good for some independent verification. I could have made the same mistake in both calculations.)

- Add Luca ref [7] somewhere.

4. Ideas/questions

- Consider adding some connection to dynamical systems (statistics of periodic orbit lengths, etc).

References

[1] V. Arnold. Number-theoretical turbulence in Fermat-Euler arithmetics and large Young diagrams geometry statistics. *J. Math. Fluid Mech.*, 7(suppl. 1):S4–S50, 2005.
[2] P. Erdős, C. Pomerance, and E. Schmutz. Carmichael's lambda function. *Acta Arith.*, 58(4):363–385, 1991.
[3] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.
[4] P. Kurlberg. On the order of unimodular matrices modulo integers. *Acta Arith.*, 110(2):141–151, 2003.
[5] P. Kurlberg and C. Pomerance. On the period of the linear congruential and power generators. *Acta Arith*, 119(2):149–169, 2005.
[6] S. Li and C. Pomerance. On generalizing Artin's conjecture on primitive roots to composite moduli. *J. Reine Angew. Math.*, 556:205–224, 2003.
[7] F. Luca. Some mean values related to average multiplicative orders of elements in finite fields. *Ramanujan J.*, 9(1-2):33–44, 2005.
[8] F. Luca and I. E. Shparlinski. Average multiplicative orders of elements modulo n. *Acta Arith.*, 109(4):387–411, 2003.
[9] I. E. Shparlinski. On some dynamical systems in finite fields and residue rings. *Discrete Contin. Dyn. Syst.*, 17(4):901–917, 2007.
[10] S. S. Wagstaff, Jr. Pseudoprimes and a generalization of Artin's conjecture. *Acta Arith.*, 41:141–150, 1982.

Department of Mathematics, Royal Institute of Technology, SE-100 44 Stockholm, Sweden
E-mail address: `kurlberg@math.kth.se`

Mathematics Department, Dartmouth College, Hanover, NH 03755-3551, U.S.A.
E-mail address: `carl.pomerance@dartmouth.edu`