ON THE PERIOD OF THE LINEAR CONGRUENTIAL AND POWER GENERATORS

PÄR KURLBERG AND CARL POMERANCE

1. Introduction

We consider two standard pseudorandom number generators from number theory: the linear congruential generator and the power generator. For the former, we are given integers e, b, n (with $e, n > 1$) and a seed $u = u_0$, and we compute the sequence

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

This sequence was first considered as a pseudorandom number generator by D. H. Lehmer. For the power generator we are given integers $e, n > 1$ and a seed $u = u_0 > 1$, and we compute the sequence

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

so that $u_i = u^{e^i} \pmod{n}$. A popular case is $e = 2$, which is called the Blum–Blum–Shub (BBS) generator.

Both of these generators are periodic sequences, and it is of interest to compute the periods. To be useful, a pseudorandom number generator should have a long period. In this paper 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.

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 $\mathrm{ord}(e, n)$. If $(e, n) > 1$, the sequence $e^i \pmod{n}$ is still (ultimately) periodic, with the period given by $\mathrm{ord}(e, n_{(e)})$ where $n_{(e)}$ is the largest divisor of n that is coprime to e. (The aperiodic lead-in to such a sequence has length bounded by the binary logarithm of n.) In this paper we shall denote $\mathrm{ord}(e, n_{(e)})$ by $\mathrm{ord}^*(e, n)$. The periods of both the linear congruential and

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

P.K. supported in part by the National Science Foundation (DMS 0071503), the Royal Swedish Academy of Sciences and the Swedish Research Council. C.P. supported in part by the National Science Foundation.

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 $\mathrm{ord}^*(e,n)$. In general, the period is always a divisor of $\mathrm{ord}^*(e,n)(e-1,n)$.

For the power generator, the period is exactly $\mathrm{ord}^*(e, \mathrm{ord}^*(u,n))$. We shall assume that u is chosen so that $\mathrm{ord}^*(u,n)$ is as large as possible for a given modulus n.[1] This maximum is denoted $\lambda(n)$, following Carmichael. First described by Gauss, $\lambda(n)$ is the order of the largest cyclic subgroup of $(\mathbf{Z}/n\mathbf{Z})^\times$. It satisfies $\lambda([a,b]) = [\lambda(a), \lambda(b)]$, where $[\ ,\ ]$ denotes the least common multiple. Further, for a prime power p^α we have $\lambda(p^\alpha) = \phi(p^\alpha) = (p-1)p^{\alpha-1}$, except when $p = 2, \alpha \geq 3$ in which case $\lambda(2^\alpha) = 2^{\alpha-2}$. For the power generator, we thus will study $\mathrm{ord}^*(e, \lambda(n))$. Note that it is especially important to use the function ord^* rather than ord 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.

We begin by reviewing some of the literature on statistical properties of $\mathrm{ord}^*(e,n)$. In [16] Pappalardi showed that there exist $\alpha, \delta > 0$ such that $\mathrm{ord}(e,p) \geq p^{1/2}\exp((\log p)^\delta)$ for all but $O(x/\log^{1+\alpha} x)$ primes $p \leq x$. 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, then $\mathrm{ord}(e,p) > p/\psi(p)$ for all but $O(\pi(x)\log(\psi(x))/\psi(\sqrt{x}))$ primes $p \leq x$, where as usual, $\pi(x)$ is the total number of all primes $p \leq x$. (Although stated for any unbounded monotone function $\psi(x)$, it appears that the proof only supports the case when $\psi(x)$ is increasing rather slowly. A similar result with $\psi(x) \leq (\log x)^{1-\epsilon}$ is proved in the first author's paper [11]. In Theorem 23 we obtain a small, yet for our purposes crucial, strengthening of this result.) In [4], Erdős and Murty showed that if $\epsilon(x)$ is any decreasing function tending to zero as x tends to infinity, then $\mathrm{ord}(e,p) \geq p^{1/2+\epsilon(p)}$ for all but $o(\pi(x))$ primes $p \leq x$, and in [10] Indlekofer and Timofeev gave a similar lower bound with an explicit estimate on the number of exceptional primes. Further, it follows immediately from work of Goldfeld, Fouvry, and Baker–Harman that there is a positive constant γ such that $\mathrm{ord}(e,p) > p^{1/2+\gamma}$ for a positive proportion of the primes p.

The period of the power generator $u^{e^i} \pmod{pl}$ was studied in Friedlander, Pomerance and Shparlinski [7], where p, l are primes of the same magnitude.

[1] At the end of the paper we briefly consider the general case where this assumption is not made.

[2] More precisely, that the Riemann hypothesis holds for L-functions associated with certain Kummer extensions

One of the results there is that this period is $> (pl)^{1-\epsilon}$ for most choices of u, e, p, l. However, once the exponent e is fixed, say at 2, the results of [7] are noticeably weaker.

As for $\mathrm{ord}(e, n)$ for n a positive integer, in [12] Kurlberg and Rudnick proved that there exists $\delta > 0$ such that $\mathrm{ord}(e, n) \gg n^{1/2} \exp((\log n)^{\delta}))$ for all but $o(x)$ integers $n \leq x$ that are coprime to e. Further, in [11], Kurlberg showed that the GRH implies that for each $\epsilon > 0$, we have $\mathrm{ord}(e, n) \gg n^{1-\epsilon}$ for all but $o(x)$ integers $n \leq x$ that are coprime to n, and in [13] Li and Pomerance improved the lower bound to $\mathrm{ord}(e, n) \geq n(\log n)^{-(1+o(1)) \log\log\log n}$, a result that is best possible.

To complement these theorems we give some new results on $\mathrm{ord}(e, n)$ and $\mathrm{ord}^*(e, n)$.

Theorem 1. *Results on* $\mathrm{ord}^*(e, n)$*:*

(1) *Suppose* $\epsilon(x)$ *tends to zero arbitrarily slowly as* $x \to \infty$*. Then* $\mathrm{ord}^*(e, n) \geq n^{1/2+\epsilon(n)}$ *for all but* $o_\epsilon(x)$ *integers* $n \leq x$*.*
(2) *There is a positive constant* γ_1 *such that* $\mathrm{ord}(e, n) \geq n^{1/2+\gamma_1}$ *for a positive proportion of the integers* n*.*

These relatively easy results, together with the GRH-conditional results mentioned above, become the model for the principal results of this paper. We consider the power generator for 3 classes of moduli: primes, the products of two primes of the same magnitude, and general moduli.

Theorem 2. *Results on* $\mathrm{ord}^*(e, p-1)$*:*

(1) *Suppose* $\epsilon(x)$ *tends to zero arbitrarily slowly as* $x \to \infty$*. Then* $\mathrm{ord}^*(e, p-1) \geq p^{1/2+\epsilon(p)}$ *for all but* $o_\epsilon(\pi(x))$ *primes* $p \leq x$*.*
(2) *There is a positive constant* γ_2 *such that* $\mathrm{ord}^*(e, p-1) \geq p^{1/2+\gamma_2}$ *for a positive proportion of the primes* p*.*
(3) *(GRH) For each fixed* $\epsilon > 0$ *we have* $\mathrm{ord}^*(e, p-1) > p^{1-\epsilon}$ *for all but* $o_\epsilon(\pi(x))$ *primes* $p \leq x$*.*

Consider moduli pl where p, l are primes with $p, l \leq Q$ (where Q is an arbitrary bound). Using our results on $\mathrm{ord}^*(e, p-1)$, we can prove the following theorem.

Theorem 3. *Results on* $\mathrm{ord}^*(e, \lambda(pl))$*:*

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

Instead of considering specifically RSA moduli $n = pl$, one may consider the general case where no restriction is made on the modulus n. As we have seen, the length of the period for the sequence (u_i) is bounded by $\mathrm{ord}^*(e, \lambda(n))$. In our last theorem we establish similar results as above for this order.

Theorem 4. *Results on* $\mathrm{ord}^*(e, \lambda(n))$*:*

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

We actually achieve a best-possible result in part 3 of Theorem 4, showing that, on assumption of the GRH, that

$$\mathrm{ord}^*(e, n) \;=\; n \cdot \exp\big(-(1 + o(1))(\log\log n)^2 \log\log\log n\big)$$

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

Acknowledgement. We would like to thank Igor Shparlinski for several helpful conversations.

2. Preliminary ideas

In this section we present an argument that shows that $\mathrm{ord}^*(e, n) > n^{1/2+\epsilon(n)}$ on a set of asymptotic density 1; that is, we prove the first item in Theorem 1. This argument will then be a model for the analogous item in each of Theorems 2, 3, 4.

We begin with a useful lemma. The proof appeared in [12], section 5.1, but for completeness we give a somewhat shorter argument here.

Lemma 5. *For any natural number* n *we have*

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

Proof. The equality is trivial. For the inequality, note that for positive integers a_i, b_i we have

$$\mathrm{lcm}\{a_1 b_1, \ldots, a_k b_k\} \mid b_1 \cdots b_k \cdot \mathrm{lcm}\{a_1, \ldots, a_k\},$$

as each $a_i b_i$ divides $b_1 \cdots b_k \cdot \mathrm{lcm}\{a_1, \ldots, a_k\}$. We apply this with the a_i's being the various $\mathrm{ord}^*(e, p)$ for $p|n$ and the corresponding b_i's being

$\lambda(p^\beta)/\operatorname{ord}^*(e,p)$, where $p^\beta \| n$. Then $\operatorname{lcm}\{a_1b_1,\dots,a_kb_k\} = \lambda(n)$. Further, $\operatorname{ord}^*(e,n)$ is divisible by $\operatorname{lcm}\{a_1,\dots,a_k\}$, so that

$$\frac{\lambda(n)}{n} \;\le\; \frac{\operatorname{ord}^*(e,n)}{n} \prod_{p^\beta \| n} \frac{\lambda(p^\beta)}{\operatorname{ord}^*(e,p)} \;\le\; \frac{\operatorname{ord}^*(e,n)}{\prod_{p|n} \operatorname{ord}^*(e,p)}.$$

□

Suppose $\mathcal{P}$ is a subset of the prime numbers. We let $\pi_{\mathcal{P}}(x)$ denote the number of primes $p \le x$ 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 $\mathcal{P}$.

Let e be an integer with $e > 1$. Let $\epsilon(x)$ be an arbitrary monotonic function with

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

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

$$\begin{aligned} \mathcal{L} &= \{p \text{ prime } :\ \operatorname{ord}^*(e,p) \le p^{1/2}/\log p\} \\ \mathcal{M} &= \{p \text{ prime } :\ p^{1/2}/\log p < \operatorname{ord}(e,p) \le p^{1/2+2\epsilon(p)}\} \\ \mathcal{H} &= \{p \text{ prime } :\ \operatorname{ord}(e,p) > p^{1/2+2\epsilon(p)}\}, \end{aligned}$$

where we use the mnemonic low, medium, high for $\mathcal{L}, \mathcal{M}, \mathcal{H}$. Note that $\mathcal{L}$ contains the prime factors of e.

Let $\omega(n)$ denote the number of prime number divisors of n.

Lemma 6. *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*

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

and

$$\sum_{n_{\mathcal{L}}=n,\ n\le x} 1 \;\ll\; x/\log^3 x. \tag{3}$$

Proof. To see the first assertion, let $y = x^{1/2}/\log x$ and note that if $p \in \mathcal{L}$ and $p \le x$, then $\operatorname{ord}^*(e,p) \le y$. That is, p divides e or some $e^j - 1$ with $1 \le j \le y$. Using the estimate $\omega(m) \ll \log m/\log\log m$, we have

$$\pi_{\mathcal{L}}(x) \;\le\; \omega\left(e \prod_{1\le j\le y} (e^j - 1)\right) \;\ll\; y^2/\log y \;\ll\; x/\log^3 x.$$

The result about $\sum_{p\in\mathcal{L}} 1/p$ then follows by partial summation, and (2) follows trivially as a consequence.

We now prove (3). Let $L_k(x)$ denote the number of integers $n \le x$ with $n = n_{\mathcal{L}}$ and $\omega(n) = k$. We show by induction that there is a positive constant c such that

$$L_k(x) \ \le \ c\frac{x}{(k-1)!\log^3 x}\left(8\sum_{p\in\mathcal{L}}\frac{1}{p-1}\right)^{k-1}, \tag{4}$$

from which (3) directly follows by summing on k getting

$$\sum_{n_{\mathcal{L}}=n,\ n\le x} 1 \ \le \ c\frac{x}{\log^3 x}\exp\left(8\sum_{p\in\mathcal{L}}\frac{1}{p-1}\right) \ \ll \ \frac{x}{\log^3 x}.$$

To see (4) note that we have already verified it in the case $k = 1$. Assume it is true at k. Since no number can have two coprime prime-power divisors bigger than the squareroot, we have

$$\begin{aligned} L_{k+1}(x) \ &\le \ \frac{1}{k}\sum_{p\in\mathcal{L},\ p^a\le x^{1/2}} L_k(x/p^a) \\ &\le \ c\frac{1}{k!}\left(8\sum_{p\in\mathcal{L}}\frac{1}{p-1}\right)^{k-1}\sum_{p\in\mathcal{L},\ p^a\le x^{1/2}}\frac{x/p^a}{\log^3(x/p^a)} \\ &\le \ c\frac{1}{k!}\left(8\sum_{p\in\mathcal{L}}\frac{1}{p-1}\right)^{k}\frac{x}{\log^3 x}. \end{aligned}$$

This completes the proof of the lemma. □

Note that (2) is all we shall need in this section, but we need the stronger result (3) for our later results.

For a positive integer n, let $\gamma(n)$ denote the largest squarefree divisor of n, sometimes called the "core" of n.

Lemma 7. *But for a set of natural numbers n of asymptotic density 0 we have*

$$\begin{aligned} n_{\mathcal{L}} \ &< \ \log n \\ n/\gamma(n) \ &< \ \log n \\ \omega(n) \ &< \ 2\log\log n. \end{aligned}$$

Proof. The first assertion follows directly from (2). The assertion about $n/\gamma(n)$ follows from the fact that the number of $n \le x$ with $n/\gamma(n) > T$ is $O(x/\sqrt{T})$. Indeed, if $u = n/\gamma(n)$, then $u\gamma(u)|n$ and $u\gamma(u)$ is squareful (divisible by the square of each of its prime factors). The assertion then follows from partial summation and the fact that the number of squareful numbers up to x is $O(\sqrt{x})$. The final assertion about $\omega(n)$ follows from the

theorem of Hardy and Ramanujan that the normal number of prime factors of n is $\log\log n$. □

One 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. Erdős and Murty used this idea to show that $\pi_{\mathcal{M}}(x) = o(\pi(x))$ and Pappalardi and Indlekofer–Katai got more quantitative versions of this result. We state a consequence from the latter paper.

Lemma 8 ([10], Cor. 6)**.** *With $\epsilon(x)$ as specified in* (1)*, we have $\pi_{\mathcal{M}}(x) = O(\epsilon(x)^{1/12}\pi(x))$.*

We now show that as a consequence of Lemma 8 not many integers n have a large divisor composed of primes from $\mathcal{M}$. Let Λ denote the von Mangoldt function.

Lemma 9. *With $\epsilon(x)$ as specified in* (1)*, the number of integers $n \le x$ with $n_{\mathcal{M}} > n^{1/3}$ is $O(\epsilon(x)^{1/12}x)$.*

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 8 and (1),

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

Thus,

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

so that the result follows readily. □

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

This result follows from Theorem 5 of [7].

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

Theorem 11. *Suppose $\epsilon(n)$ satisfies (1). But for a set of integers n of asymptotic density 0 we have*

$$\mathrm{ord}^*(e,n) \;>\; n^{1/2+\epsilon(n)}.$$

Proof. By Lemma 10 we may assume that $\lambda(n) > n\exp(-(\log\log n)^3)$. Thus, from Lemma 5 and Lemma 7 we have

$$\begin{aligned}\mathrm{ord}^*(e,n) \;&>\; \exp(-(\log\log n)^3)\prod_{p\mid n/n_{\mathcal{L}}}\mathrm{ord}(e,n)\\ &\geq\; \exp(-(\log\log n)^3)\prod_{p\mid n_{\mathcal{M}}}(p^{1/2}/\log p)\prod_{p\mid n_{\mathcal{H}}}p^{1/2+2\epsilon(p)}\\ &\geq\; \exp(-(\log\log n)^3-\omega(n)\log\log n)\gamma(n_{\mathcal{M}})^{1/2}\gamma(n_{\mathcal{H}})^{1/2+2\epsilon(n)}\\ &\geq\; \exp(-2(\log\log n)^3)n^{1/2}n_{\mathcal{H}}^{2\epsilon(n)}.\end{aligned}$$

By Lemmas 7 and 9 we may also assume that $n_{\mathcal{H}} > n^{3/5}$. Thus, our result follows from (1). □

3. The $1/2+\epsilon$ results

We now consider analogs of Theorem 11 in certain interesting cases. Say an infinite subset $\mathcal{S}$ of the natural numbers has property P "almost always" if

$$\sum_{\substack{s\in\mathcal{S},\ s\leq x\\ s \text{ has property P}}} 1 \;\sim\; \sum_{s\in\mathcal{S},\ s\leq x} 1 \;\text{ as } x\to\infty.$$

In this section P will be the property that $\mathrm{ord}^*(e,\lambda(n)) > n^{1/2+\epsilon(n)}$. That is, for $\epsilon(x)$ satisfying (1),

$$n \text{ has property } \mathrm{P}_\epsilon\colon\quad \mathrm{ord}^*(e,\lambda(n)) > n^{1/2+\epsilon(n)}.$$

Our goal of this section is to prove the following theorem, which comprises the union of the first items of Theorems 2, 3, and 4.

Theorem 12. *If $\epsilon(x)$ satisfies (1) then the following sets have property P_ϵ almost always: the set of prime numbers, the set of integers $n = pl$ where p, l are primes with $p < l < 2p$, and the set of all natural numbers.*

We will need the following form of the Brun–Titchmarsh inequality (see [8], Theorem 3.8):

Lemma 13. *Suppose k, l are coprime integers with $k > 0$ and let $\pi(x,k,l)$ be the number of primes $p \leq x$ such that $p \equiv l \pmod k$. Then $\pi(x,k,l) \ll \dfrac{x}{\phi(k)\log(x/k)}$ uniformly for $x > k$.*

We begin with an analog of Lemma 7 for shifted primes.

Lemma 14. *But for a set of prime numbers p of relative density 0 within the set of all primes, we have*

$$\begin{aligned} (p-1)_{\mathcal{L}} &< \log p \\ (p-1)/\gamma(p-1) &< \log p \\ \omega(p-1) &< 2\log\log p \end{aligned}$$

Proof. Using (3) we have that

$$\sum_{n=n_{\mathcal{L}},\ n>T} \frac{1}{n} \ll \frac{1}{\log^2 T}.$$

Thus, by a trivial argument we may assume that $(p-1)_{\mathcal{L}} < p^{1/2}$. The Brun–Titchmarsh inequality and (3) allow one to handle the remaining cases where $(p-1)_{\mathcal{L}}$ is between $\log p$ and $p^{1/2}$ as follows. It suffices to show that

$$\sum_{n\geq \frac{1}{2}\log x,\ n=n_{\mathcal{L}}} \pi(x,n,1) = o(\pi(x)),$$

but the sum is $\ll \pi(x)\sum_{n\geq \frac{1}{2}\log x,\ n=n_{\mathcal{L}}} 1/\phi(n)$. Using the well-known estimate $1/\phi(n) \ll (\log\log n)/n$, we have our result from (3). The argument for $(p-1)/\gamma(p-1)$ is similar, namely that a trivial argument is used when $(p-1)/\gamma(p-1)$ is large and the Brun–Titchmarsh inequality when it is small. The final assertion follows from the main result of [3] that the normal number of prime factors of $p-1$ is $\log\log p$. □

We now turn our attention to an analog of Lemma 9 for shifted primes.

Lemma 15. *With $\epsilon(x)$ as specified in (1), the number of primes $p \leq x$ with $(p-1)_{\mathcal{M}} > p^{1/3}$ is $O(\epsilon(x)^{1/24}\pi(x))$.*

Proof. Using Brun's or Selberg's sieve (see [8], Theorem 2.4 or Theorem 3.12) we have that the number of primes $p \leq x$ with $p-1$ divisible by a prime $q > x^{1-\epsilon(x)^{1/24}}$ is

$$\leq \sum_{a\leq x^{\epsilon(x)^{1/24}}} \sum_{\substack{q\leq x/a \\ aq+1 \text{ prime}}} 1 \ll \frac{x}{\log^2 x} \sum_{a\leq x^{\epsilon(x)^{1/24}}} \frac{1}{\phi(a)} \ll \epsilon(x)^{1/24}\pi(x),$$

where we have used the well-known result that $\sum_{a\leq T} 1/\phi(a) \sim c\log T$ for an appropriate constant c. Thus, we may assume that $p-1$ has no prime factor larger than $x^{1-\epsilon(x)^{1/24}}$. Trivially we may also assume that $p-1$ has no prime-power factor this large as well. Letting $\sum'$ denoting a sum over

primes with these conditions, we have

$$\begin{aligned}\sum_{p\le x}{}' \log(p-1)_{\mathcal{M}} &= \sum_{p\le x}{}' \sum_{\substack{d\mid p-1\\ d_{\mathcal{M}}=d}} \Lambda(d)\\ &= \sum_{\substack{d_{\mathcal{M}}=d\\ d\le x^{1-\epsilon(x)^{1/24}}}} \Lambda(d)\pi(x,d,1)\\ &\ll \sum_{\substack{d_{\mathcal{M}}=d\\ d\le x^{1-\epsilon(x)^{1/24}}}} \Lambda(d)\frac{x}{\phi(d)\log(x/d)}\\ &\le \sum_{\substack{d_{\mathcal{M}}=d\\ d\le x^{1-\epsilon(x)^{1/24}}}} \Lambda(d)\frac{x}{d\epsilon(x)^{1/24}\log x},\end{aligned}$$

the penultimate estimate coming from the Brun–Titchmarsh inequality. Using the first two displays in the proof of Lemma 9, we have

$$\sum_{\substack{d_{\mathcal{M}}=d\\ d\le x}} \frac{\Lambda(d)}{d} \ll \epsilon(x)^{1/12}\log x,$$

so that with the above estimate, we get that

$$\sum_{p\le x}{}' \log(p-1)_{\mathcal{M}} \ll \epsilon(x)^{1/24}x.$$

The lemma follows readily. □

The proof of Theorem 12 for the set of prime numbers now follows directly from the proof of Theorem 11 where we replace Lemmas 7 and 9 with Lemmas 14 and 15, respectively. Note that we may continue to use Lemma 10 since the estimate for the exceptional set in that lemma is $o(\pi(x))$.

We next turn our attention to the set of numbers pl where p, l are primes with $p < l < 2p$. Proving Theorem 12 for this set is equivalent to showing that

$$\operatorname{ord}^*(e,\lambda(pl)) > Q^{1+\epsilon(Q)} \tag{5}$$

for all but $o(\pi(Q)^2)$ pairs of primes $p, l \le Q$.

We have from [7], Theorem 6, the following result in analogy to Lemma 10: But for $o(\pi(Q)^2)$ pairs of primes $p, l \le Q$ we have

$$\lambda(\lambda(pl)) > pl/\exp(2(\log\log Q)^3). \tag{6}$$

Note that

$$\operatorname{ord}^*(e,[a,b]) \ge \operatorname{ord}^*(e,a)\operatorname{ord}^*(e,b)\frac{\lambda([a,b])}{\lambda(a)\lambda(b)}. \tag{7}$$

Indeed, letting $A = \mathrm{ord}^*(e,a), B = \mathrm{ord}^*(e,b)$ we have

$$\mathrm{ord}^*(e,[a,b]) \;=\; [A,B] \;=\; \frac{AB}{(A,B)} \;\geq\; \frac{AB}{(\lambda(a),\lambda(b))},$$

so that using $\lambda([a,b]) = [\lambda(a),\lambda(b)]$, (7) follows. We Apply (7) with $a = p-1, b = l-1$, where p, l are distinct primes. As $\lambda([p-1,l-1]) = \lambda(\lambda(pl))$, we get

$$\mathrm{ord}^*(e,\lambda(pl)) \;>\; \mathrm{ord}^*(e,p-1)\,\mathrm{ord}^*(e,l-1)\frac{\lambda(\lambda(pl))}{pl}. \tag{8}$$

So, to show (5), we assume that (6) holds and we apply (8). The result follows from the fact that the set of primes has property P_ϵ almost always. (To be perfectly precise, we use that the set of primes has property $\mathrm{P}_{2\epsilon}$ almost always.)

The third class of numbers in Theorem 12, namely, the set of all numbers n, is more difficult. We begin with a new result:

Theorem 16 (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.

We now give the analog result to Lemmas 7 and 14.

Lemma 17. *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.

Proof. We have

$$\sum_{n\leq x} \log \lambda(n)_{\mathcal{L}} \;\leq\; \sum_{n\leq x} \sum_{\substack{p^a \| \lambda(n) \\ p\in\mathcal{L}}} \log p^a \;\leq\; \sum_{\substack{p^a \leq x \\ p\in\mathcal{L}}} \log p^a \sum_{\substack{n\leq x \\ p^a \mid \lambda(n)}} 1.$$

If a prime power p^a divides $\lambda(n)$ it must be the case that either n is divisible by some prime $q \equiv 1 \pmod{p^a}$ or $p^{a+1} | n$. As

$$\sum_{\substack{q\leq x \\ q \text{ prime} \\ q\equiv 1 \,(\mathrm{mod}\ d)}} \frac{1}{q} \;=\; \frac{\log\log x + O(\log d)}{\phi(d)}$$

uniformly for all integers $d \ge 2$ (see [17], Theorem 1 and Remark 1, or Norton [15]), we have

$$\sum_{\substack{n\le x\\ p^a\mid\lambda(n)}} 1 \;\le\; \frac{x}{p^{a+1}} + \sum_{\substack{q\le x\\ q \text{ prime}\\ q\equiv 1 \,(\mathrm{mod}\ p^a)}} \frac{x}{q} \;=\; \frac{x\log\log x}{\phi(p^a)} + O\left(\frac{x\log p^a}{p^a}\right).$$

Hence

$$\begin{aligned}\sum_{n\le x}\log\lambda(n)_{\mathcal{L}} &\ll x\log\log x\sum_{\substack{p^a\le x\\ p\in\mathcal{L}}}\frac{\log p^a}{p^a} + x\sum_{\substack{p^a\le x\\ p\in\mathcal{L}}}\frac{(\log p^a)^2}{p^a}\\ &\ll x\log\log x,\end{aligned}$$

the last inequality coming from the estimate for $\pi_{\mathcal{L}}(x)$ in Lemma 6. Thus we immediately get the first assertion in the lemma.

For the second assertion note that from (6) and (7) in [6] we have

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

for all but $o(x)$ choices of $n \le x$. Thus we have the second assertion.

The third assertion follows from the fact that the normal order of $\omega(\lambda(n))$ is $\frac{1}{2}(\log\log n)^2$, see [5]. □

Now we give the analog result to Lemmas 9 and 15.

Lemma 18. *Let $\epsilon(x)$ satisfy (1). Almost all numbers n have the property that $\lambda(n)_{\mathcal{M}} < n^{2/5}$.*

Proof. Let

$$\mathcal{M}' \;=\; \{p \text{ prime} : (p-1)_{\mathcal{M}} > p^{1/3}\}.$$

Lemma 15 tells us that $\pi_{\mathcal{M}'}(x) \ll \epsilon(x)^{1/24}\pi(x)$. We apply the proof of Lemma 9 with $\mathcal{M}$ replaced by $\mathcal{M}'$ and with $\epsilon(x)^{1/12}$ replaced by $\epsilon(x)^{1/24}$. Thus, by the final display of Lemma 9 we have that

$$\sum_{n\le x}\log n_{\mathcal{M}'} \;\ll\; \epsilon(x)^{1/24}x\log x.$$

We thus get that $n_{\mathcal{M}'} \le n^{1/12}$ almost always. Assume that n has this property. By Lemma 7, we may also assume that $n/\gamma(n) < n^{1/90}$. Thus,

$$\begin{aligned}\lambda(n)_{\mathcal{M}} &\le (n/\gamma(n))\lambda(\gamma(n))_{\mathcal{M}} \;<\; n^{1/90}\prod_{p\mid n}(p-1)_{\mathcal{M}}\\ &= n^{1/90}\prod_{p\mid n_{\mathcal{M}'}}(p-1)_{\mathcal{M}}\prod_{p\mid n/n_{\mathcal{M}'}}(p-1)_{\mathcal{M}}\\ &\le n^{1/90}\gamma(n_{\mathcal{M}'})\gamma(n/n_{\mathcal{M}'})^{1/3} \;\le\; n^{1/90}\,n_{\mathcal{M}'}^{2/3}\,n^{1/3} \;\le\; n^{2/5}.\end{aligned}$$

This completes the proof of the lemma. □

We are in a position now to complete the proof of Theorem 12. Assume that n satisfies the properties in Theorem 16 and Lemmas 17, 18. By Lemma 10 we may also assume that $\lambda(n) > n\exp(-(\log\log n)^3)$. Thus, $\lambda(n)_{\mathcal{H}} > n^{3/5}/\exp(2(\log\log n)^3)$. Using Lemma 5 and assuming that n is large, we have

$$\begin{aligned}
\operatorname{ord}^*(e,\lambda(n)) &\geq \frac{\lambda(\lambda(n))}{\lambda(n)} \prod_{p|\lambda(n)} \operatorname{ord}^*(e,p) \\
&> \exp(-(\log\log n)^3) \prod_{p|\lambda(n)_{\mathcal{M}}} (p^{1/2}/\log p) \prod_{p|\lambda(n)_{\mathcal{H}}} p^{1/2+2\epsilon(p)} \\
&> \exp(-2(\log\log n)^3)\gamma(\lambda(n)_{\mathcal{M}})^{1/2}\gamma(\lambda(n)_{\mathcal{H}})^{1/2+2\epsilon(n)} \\
&> \exp(-3(\log\log n)^3)\lambda(n)^{1/2}\lambda(n)_{\mathcal{H}}^{2\epsilon(n)} \\
&> \exp(-4(\log\log n)^3)n^{1/2+(6/5)\epsilon(n)} \\
&> n^{1/2+\epsilon(n)}.
\end{aligned}$$

This completes the proof of Theorem 12.

4. The $1/2 + c$ results

The spirit of Theorems 11 and 12 concerns the best that can be said for almost all cases. In this section we relax the "almost all" to "a positive proportion" and so prove somewhat stronger results. One could relax further to "infinitely often," but then it occurs that quite cheap results can be had. For example, if p is a prime that does not divide e, then $\operatorname{ord}(e,p^j) = p^{j-O(1)}$, so that $\operatorname{ord}(e,n) \gg n$ infinitely often.

We begin with the case of $\operatorname{ord}(e,p)$ for p prime. As mentioned in the Introduction, one way of getting a fairly decent result here is to have a very large prime factor of $p-1$ as afforded by a series of papers culminating in the recent paper [2].

Lemma 19 (Baker–Harman)**.** *For a positive proportion of the primes p, there is a prime $q|p-1$ with $q > p^{0.677}$.*

Note that this result follows from (7.1) in [2].

We use this result to immediately get the following:

Lemma 20. *We have $\operatorname{ord}(e,p) > p^{0.677}$ for a positive proportion of the primes p.*

Proof. Among the primes p for which $p-1$ is divisible by a prime $q > p^{0.677}$, consider those for which $\operatorname{ord}(e,p)$ is not divisible by q. Then if $p \leq x$, we have $\operatorname{ord}(e,p) < x^{0.323}$. As in the argument for $\pi_{\mathcal{L}}(x)$ in the proof of Lemma 7, the number of such primes is $O(x^{0.646}/\log x) = o(\pi(x))$. Thus,

only a negligible number of primes which satisfy the previous lemma do not satisfy the present lemma. □

Our basic strategy in this section to make $\mathrm{ord}^*(e,m)$ large, is to manage to place in m a large prime p for which $\mathrm{ord}(e,p)$ is large, and then use the ideas of the previous sections to show that the remainder of m cannot do too much damage most of the time. For $\mathrm{ord}^*(e,n)$ the idea is especially transparent.

Theorem 21. *We have* $\mathrm{ord}^*(e,n) > n^{0.677}$ *for a positive proportion of integers* n.

Proof. The only subtlety here is that we need to extend Lemma 19 slightly. By the Brun–Titchmarsh inequality, the proportion of primes p with a prime factor q of $p-1$ in the interval $[p^{0.677}, p^{0.677+2\epsilon}]$ is $O(\epsilon)$. So if ϵ is small enough compared to the positive proportion produced in Lemma 19, then there must be a positive proportion left over with $q > p^{0.677+2\epsilon}$. And, for all but a negligible proportion of these numbers, as in Lemma 20, we have $\mathrm{ord}(e,p) > p^{0.677+2\epsilon}$. Now consider for such primes p, integers of the form $ap \le x$, where $a \le x^\epsilon$. For such primes $p \le x$ the number of integers a that may be taken is $\gg x/p$, and letting p run from $x^{1-\epsilon}$ to x there is never any double counting of any ap. Thus, the number of such numbers ap is $\gg \sum x/p \gg x$. Further,

$$\mathrm{ord}^*(e,ap) \ge \mathrm{ord}(e,p) > p^{0.677+2\epsilon} > (ap)^{0.677}.$$

This completes the proof of the theorem. □

We say n has property P_c if $\mathrm{ord}^*(e,\lambda(n)) > n^{1/2+c}$. In the rest of this section we take $c = 0.092$.

Theorem 22. *Positive proportions of the set of primes and the set of all natural numbers have property* P_c. *Further, there are* $\gg \pi(Q)^2$ *pairs of primes* $p, l \le Q$ *such that* pl *has property* P_c.

Proof. We begin with the case of primes, from which the other two cases will follow easily. We actually show a slightly stronger result: there is some $\delta > 0$ such that a positive proportion of the primes have property $\mathrm{P}_{c+\delta}$. Let $\mathcal{P}$ be the set of primes q for which $\mathrm{ord}(e,q) > q^{0.677}$. Lemma 20 tells us that this set of primes comprises a positive proportion of all primes. Consider primes $p \le x$ where $q|p-1$ for some $q \in \mathcal{P}$ and with $x^{0.52-\epsilon} < q \le x^{0.52}$. Here, $\epsilon > 0$ is arbitrarily small but fixed. It follows from [1], Theorem 1, that a positive proportion of primes p are so representable. Further, it follows from Lemma 14 that by neglecting only a relative density 0 of such

primes p, we have

$$\begin{aligned}\operatorname{ord}^*(e,p-1) &> (p/q)^{1/2-o(1)}q^{0.677} = p^{1/2-o(1)}q^{0.177+o(1)}\\ &> p^{1/2+(0.52-\epsilon)(0.177)-o(1)}.\end{aligned}$$

As $(0.52)(0.177) > c$, if ϵ is taken small enough, we have $(0.52-\epsilon)(0.177) > c+\delta$ for some fixed $\delta > 0$. Thus, $\operatorname{ord}^*(e,p-1) > p^{1/2+c+\delta}$, with this holding for a positive proportion of primes p. Thus, we have the theorem for the set of primes.

Now consider the numbers pl, where p, l are primes with $p, l \le Q$. We apply (8) where p, l are primes with $p, l \le Q$ which have property $\mathrm{P}_{c+\delta}$. Assuming as we may that pl satisfies (6), we have

$$\operatorname{ord}^*(e,\lambda(pl)) > (pl)^{1/2+c+\delta}\exp(-2(\log\log Q)^3).$$

Thus, there are $\gg \pi(Q)^2$ pairs of primes $p, l \le Q$ for which pl has property P_c.

We now consider the set of all positive integers. Consider the integers $n = ap$ where $a \le p^{\delta/2}$, where p is a prime with property $\mathrm{P}_{c+\delta}$. By the first part of the proof, these numbers n comprise a positive proportion of all numbers n. Further, for such a number n we have

$$\operatorname{ord}^*(e,\lambda(n)) \ge \operatorname{ord}^*(e,p-1) > p^{1/2+c+\delta} > (ap)^{1/2+c} = n^{1/2+c}.$$

Thus, n has property P_c. This completes the proof of the theorem.

□

5. The $1-\epsilon$ results

In this section we improve the $1/2+\epsilon$ results to $1-\epsilon$, but we assume the Generalized Riemann Hypothesis (GRH). We begin with the following slight strengthening of Theorem 2 of [11]:

Theorem 23. *Let $e \ge 2$ be an integer. If the GRH is true, then for x, y with $1 \le y \le \log x$,*

$$\left|\left\{p \le x : \operatorname{ord}(e,p) \le \frac{p}{y}\right\}\right| \ll \frac{\pi(x)}{y} + \frac{x\log\log x}{\log^2 x},$$

where the implied constant depends at most on the choice of e.

Proof. Since the proof is rather similar to the proof of the main theorem in [9] and the proof of Theorem 2 in [11], we only give a brief outline. With $i_p = (p-1)/\operatorname{ord}(e,p)$, we see that $\operatorname{ord}(e,p) \le p/y$ implies that $i_p \ge y/2$.

First step: We first consider primes p such that $i_p \in ((x\log x)^{1/2}, x)$. As in the first part of the proof of Lemma 6, the number of such primes is $O(x/\log^2 x)$.

Second step: Consider primes p such that $q|i_p$ for some prime q in the interval $[\frac{x^{1/2}}{\log^3 x}, (x\log x)^{1/2}]$. We may bound this by considering primes $p \le x$ such that $p \equiv 1 \pmod q$ for some prime $q \in [\frac{x^{1/2}}{\log^3 x}, (x\log x)^{1/2}]$. The Brun–Titchmarsh inequality then gives that the number of such primes p is at most

$$\sum_{q\in[\frac{x^{1/2}}{\log^3 x},(x\log x)^{1/2}]} \frac{x}{\phi(q)\log(x/q)} \ll \frac{x}{\log x} \sum_{q\in[\frac{x^{1/2}}{\log^3 x},(x\log x)^{1/2}]} \frac{1}{q} \ll \frac{x\log\log x}{\log^2 x}.$$

Third step: Now consider primes p such that $q|i_p$ 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 [9] or Corollary 6 and Lemma 9 of [11], we have

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

Summing over q, we find that the number of such p is bounded by

$$\sum_{q\in[y,\frac{x^{1/2}}{\log^3 x}]} \left(\frac{\pi(x)}{q^2} + O(x^{1/2}\log(xq^2))\right) \ll \frac{\pi(x)}{y} + \frac{x}{\log^2 x}.$$

Fourth step: For the remaining primes p, any prime divisor $q|i_p$ is smaller than y. Hence i_p must be divisible by some integer d in the interval $[y/2, y^2]$. The analog of (28) in [9] for not-necessarily-squarefree integers, or more directly, Corollary 6 and Lemma 9 of [11], gives

$$|\{p \le x : d \mid i_p\}| \ll \frac{\pi(x)}{d\phi(d)} + O(x^{1/2}\log(xd^2)). \tag{9}$$

Hence the total number of such p is bounded by

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

where the last estimate follows from the well-known result $\sum_{a\le T} 1/\phi(a) = c\log T + O(1)$ (for an appropriate constant c) and partial summation. □

Remark. It follows easily from (9) that for $1 \le y \le x^{1/4}/\log x$ and assuming the GRH, we have

$$\left|\left\{p \le x : p^{1/2} y \log^2 x \le \operatorname{ord}(e,p) \le \frac{p}{y}\right\}\right| \ll \frac{\pi(x)}{y}.$$

Let $\delta(x) = \sqrt{\log\log x/\log x}$. By a slight abuse of notation, say an integer n has property $\mathrm{P}_{1-\delta}$ if $\operatorname{ord}^*(e,\lambda(n)) \ge n^{1-\delta(n)}$. Theorem 23 is our principal tool in the proof of the following result.

Theorem 24. *Assume the GRH holds. The set of primes and the set of integers pl with p, l prime and $p < l < 2p$ have property $\mathrm{P}_{1-\delta}$ almost always.*

Proof. Let

$$\mathcal{W} \;=\; \{p \text{ prime} : \mathrm{ord}^*(e,p) < p/\log p\},$$

where we use the mnemonic $\mathcal{W}$ for weak. From Theorem 23 we have

$$\pi_{\mathcal{W}}(x) \;\ll\; x \log\log x/\log^2 x. \tag{10}$$

We now consider

$$S := \sum_{p\le x} \log(p-1)_{\mathcal{W}}\,,$$

following the lines of the proof of Lemma 15. We have

$$S \;=\; \sum_{\substack{d\le x\\ d_{\mathcal{W}}=d}} \Lambda(d)\pi(x,d,1) \;=\; \sum_{\substack{p\le x\\ p\in\mathcal{W}}} \pi(x,p,1)\log p + O\left(\frac{x}{\log x}\right). \tag{11}$$

Using Brun's or Selberg's sieve as in the proof of Lemma 15, we have $\sum_{p>x^{1-\epsilon}} \pi(x,p,1) \;\ll\; \epsilon x/\log x$, so that the contribution to the last sum in (11) from the primes $p > x^{1-\epsilon}$ is $\ll \epsilon x$. For primes $p \le x^{1-\epsilon}$ we use the Brun–Titchmarsh inequality to get $\pi(x,p,1) \ll x/(\epsilon p \log x)$, so that using (10), the contribution to the sum from these primes is $\ll x/(\epsilon \log x)$. Letting $\epsilon = 1/\sqrt{\log x}$, we get

$$\sum_{p\le x} \log(p-1)_{\mathcal{W}} \;\ll\; x/\sqrt{\log x}. \tag{12}$$

Thus, $(p-1)_{\mathcal{W}} \le p^{\delta(p)/2}$ almost always. The proof of our theorem for the set of primes now follows in exactly the same way as in Theorem 12.

The case for the numbers pl now also follows using (6) and our prior arguments. □

We now begin to examine the normal contribution to $\lambda(n)$ from primes in $\mathcal{W}$.

Lemma 25. *Assuming the GRH is true, for $x, T \ge 3$, the number of integers $n \le x$ such that $p|\lambda(n)$ for $p \in \mathcal{W}$ and $p > T$ is*

$$\ll\; x \log\log x \cdot \frac{\log\log T}{\log T}.$$

Proof. If $p|\lambda(n)$, then either $p^2|n$ or some prime $q \equiv 1 \pmod p$ divides n. The number of $n \le x$ in the first case is clearly bounded by x/T. By the Brun–Titchmarsh inequality and partial summation,

$$x \sum_{q\le x,\, q\equiv 1 \,(\mathrm{mod}\, p)} \frac{1}{q} \;\ll\; \frac{x\log\log x}{p},$$

hence the number of $n \le x$ for which the second case occurs is

$$\ll \sum_{p>T,\, p\in\mathcal{W}} \sum_{q\le x,\, q\equiv 1 \,(\mathrm{mod}\, p)} x/q \;\ll\; x\log\log x \sum_{p>T,\, p\in\mathcal{W}} 1/p$$

which, since $\pi_{\mathcal{W}}(x) \ll x\log\log x/\log^2 x$, is

$$\ll\; x\log\log x \cdot \frac{\log\log T}{\log T}$$

by partial summation. □

We now prove that for most integers n, $\lambda(n)_{\mathcal{W}}$ is fairly small in the following sense:

Lemma 26. *Let $f(n) = \sum_{p|\lambda(n),\, p\in\mathcal{W}} \log p$. Assuming the GRH is true, for almost all integers n, we have*

$$f(n) \;<\; (\log\log n)^2.$$

Proof. Take $T = \exp\left((\log\log x)^2\right)$ in Lemma 25. Then the number of $n \le x$ for which some $p \in \mathcal{W}$, $p > T$ divides $\lambda(n)$ is $o(x)$. Letting $\sum'$ denote a sum over n for which no $p \in \mathcal{W}$, $p > T$ divides $\lambda(n)$, we obtain as before that

$$\begin{aligned}\sum_{n\le x}{}' f(n) \;&=\; \sum_{p\le T,\, p\in\mathcal{W}} \log p \sum_{\substack{n\le x\\ p|\lambda(n)}}{}' 1\\ &\ll\; x\sum_{p\le T,\, p\in\mathcal{W}} \frac{\log p}{p^2} + x\log\log x \sum_{p\le T,\, p\in\mathcal{W}} \frac{\log p}{p}.\end{aligned}$$

Since $\pi_{\mathcal{W}}(x) \ll x\log\log x/\log^2 x$, partial summation gives that

$$\sum_{p\le T,\, p\in\mathcal{W}} \frac{\log p}{p} \;\ll\; (\log\log T)^2 \;\ll\; (\log\log\log x)^2.$$

Hence

$$\sum_{n\le x}{}' f(n) \;\ll\; x\log\log x\,(\log\log\log x)^2.$$

Thus, the average order of $f(n)$, after removing those integers n where $\lambda(n)$ is divisible by some $p \in \mathcal{W}$, $p > T$, is $\ll \log\log n(\log\log\log n)^2$. We conclude that $f(n) < (\log\log n)^2$ holds for almost all n. □

We are now ready to prove a result for $\mathrm{ord}^*(e, \lambda(n))$ on the assumption of the GRH.

Theorem 27. *If the GRH is true, then for each fixed integer $e \ge 2$,*

$$\mathrm{ord}^*(e, \lambda(n)) \;=\; n\cdot\exp(-(1+o(1))(\log\log n)^2\log\log\log n)$$

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

Proof. We shall show that if the GRH is true, then

$$\operatorname{ord}^*(e,\lambda(n)) \geq \lambda(\lambda(n))\exp\left(-3(\log\log n)^2(\log\log\log\log n)^2\right) \tag{13}$$

for almost all n. The theorem will then follow from the trivial inequality $\operatorname{ord}^*(e,\lambda(n)) \leq \lambda(\lambda(n))$ and Theorem 16. By Lemma 26 we may assume that $f(n) < (\log\log n)^2$. Let

$$\mathcal{W}_1 \;=\; \{p \text{ prime} : p/\log p \;\leq\; \operatorname{ord}^*(e,p) <\; p/(\log\log p\cdot\log\log\log p)\},$$

so that by Theorem 23 we have $\pi_{\mathcal{W}_1}(x) \ll \pi(x)/(\log\log x\cdot\log\log\log x)$. Let $g(n) = \sum_{p|\lambda(n),\, p\in\mathcal{W}_1} 1$. Then

$$\begin{aligned}\sum_{n\leq x} g(n) &= \sum_{p\leq x,\, p\in\mathcal{W}_1}\;\sum_{n\leq x,\, p|\lambda(n)} 1\\ &\ll x\sum_{p\leq x,\, p\in\mathcal{W}_1}\frac{1}{p^2} + x\log\log x\sum_{p\leq x,\, p\in\mathcal{W}_1}\frac{1}{p}\\ &\ll x\log\log x\cdot\log\log\log\log x,\end{aligned}$$

the last estimate coming from partial summation and our inequality for $\pi_{\mathcal{W}_1}(x)$. Thus, for almost all n, $g(n) < \log\log n\,(\log\log\log\log n)^2$.

Also, let

$$\begin{aligned}\mathcal{W}_2 \;=\; \{p \text{ prime} : p/(\log\log p\cdot\log\log\log p) \;\leq\; &\operatorname{ord}^*(e,p)\\ &<\; p/\log\log\log p\},\end{aligned}$$

so that by Theorem 23 we have $\pi_{\mathcal{W}_2}(x) \ll \pi(x)/\log\log\log x$. We let $h(n) = \sum_{p|\lambda(n),\, p\in\mathcal{W}_2} 1$. As in the calculation for $g(n)$, we get

$$\sum_{n\leq x} h(n) \;\ll\; x(\log\log x)^2/\log\log\log x,$$

so that for almost all n we have

$$h(n) < (\log\log n)^2\log\log\log\log n/\log\log\log n.$$

Now assume that $f(n), g(n), h(n)$ are bounded as above, and assume that the inequalities in Lemma 17 hold. We have by Lemma 5

$$\operatorname{ord}^*(e,\lambda(n)) \;\geq\; \frac{\lambda(\lambda(n))}{\lambda(n)}\prod_{p|\lambda(n)}\operatorname{ord}^*(e,p) \;\geq\; \frac{\lambda(\lambda(n))}{\lambda(n)}ABC, \tag{14}$$

where

$$\begin{aligned} A: &= \prod_{p|\lambda(n)_{\mathcal{W}_1}} \frac{p}{\log p}, \\ B: &= \prod_{p|\lambda(n)_{\mathcal{W}_2}} \frac{p}{\log\log p \cdot \log\log\log p}, \\ C: &= \prod_{p|\lambda(n)/\lambda(n)_{\mathcal{W}\cup\mathcal{W}_1\cup\mathcal{W}_2}} \frac{p}{\log\log\log p}. \end{aligned}$$

Now

$$ABC \ \geq \ \frac{\prod_{p|\lambda(n)/\lambda(n)_{\mathcal{W}}} p}{DEF},$$

where

$$\begin{aligned} D: &= (\log n)^{g(n)}, \\ E: &= (\log\log n \cdot \log\log\log n)^{h(n)}, \\ F: &= (\log\log\log n)^{\omega(\lambda(n))}. \end{aligned}$$

By our assumptions on n, and taking n sufficiently large, we have

$$DEF \ \leq \ \exp(2(\log\log n)^2(\log\log\log\log n)^2).$$

Further,

$$\prod_{p|\lambda(n)/\lambda(n)_{\mathcal{W}}} p \ = \ \frac{\gamma(\lambda(n))}{\exp(f(n))} \ \geq \ \frac{\lambda(n)}{\log n \cdot \exp\left((\log\log n)^2\right)}.$$

Hence by our above estimates,

$$ABC \ \geq \ \lambda(n)\exp\left(-3(\log\log n)^2(\log\log\log\log n)^2\right)$$

for almost all n. We use this estimate in (14), so that (13) and the theorem follow. □

As mentioned in the introduction, $\mathrm{ord}^*(e,\lambda(n))$ is the period of the power generator $u^{e^i} \pmod n$ if $\mathrm{ord}^*(u,n) = \lambda(n)$, that is, if $\mathrm{ord}^*(u,n)$ is as large as possible. We now briefly consider the situation for a general modulus n when we do not make this assumption about u. We have the following result.

Theorem 28. *Assuming the GRH, for any fixed integers $e, u \geq 2$, 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.

Proof. First note the elementary inequality

$$\text{for } j \mid n \text{ we have } \operatorname{ord}^*(e, n/j) \geq \frac{1}{j} \operatorname{ord}^*(e, n). \tag{15}$$

To see this, as before let $j_{(e)}, n_{(e)}$ be the largest divisors of j, n respectively that are coprime to e, so that $\operatorname{ord}^*(e, n) = \operatorname{ord}(e, n_{(e)})$ and $\operatorname{ord}^*(e, n/j) = \operatorname{ord}(e, n_{(e)}/j_{(e)})$. Let $j_{(e)} = j_1 j_2$ where j_1 is the largest divisor of $j_{(e)}$ that is coprime to $n_{(e)}/j_{(e)}$. Then

$$\operatorname{ord}(e, n_{(e)}) \;=\; \operatorname{ord}(e, j_1 j_2 n_{(e)}/j_{(e)}) \;=\; [\operatorname{ord}(e, j_1), \operatorname{ord}(e, j_2 n_{(e)}/j_{(e)})].$$

Further, $\operatorname{ord}(e, j_2 n_{(e)}/j_{(e)}) \mid j_2 \cdot \operatorname{ord}(e, n_{(e)}/j_{(e)})$, so that

$$\begin{aligned} \operatorname{ord}^*(e, n) \;=\; \operatorname{ord}(e, n_{(e)}) \;&\leq\; \operatorname{ord}(e, j_1) \cdot j_2 \cdot \operatorname{ord}(e, n_{(e)}/j_{(e)}) \\ &\leq\; j_{(e)} \cdot \operatorname{ord}(e, n_{(e)}/j_{(e)}) \;\leq j \cdot \operatorname{ord}^*(e, n/j), \end{aligned}$$

which proves (15). Recall that the period for the sequence $u^{e^i} \pmod n$ is $\operatorname{ord}^*(e, \operatorname{ord}^*(u, n))$. Thus, if $\operatorname{ord}^*(u, n) = \lambda(n)/j$, we have by (15) that the period is

$$\operatorname{ord}^*(e, \lambda(n)/j) \;\geq\; \frac{1}{j} \operatorname{ord}^*(e, \lambda(n)).$$

But, on the GRH we have $\operatorname{ord}^*(u, n) > n/(\log n)^{2 \log\log\log n}$ almost always; this follows from the proof of Cor. 2 in [13]. Thus, we may take $j < (\log n)^{2 \log\log\log n}$, so the result follows from Theorem 27. □

References

[1] R. C. Baker and G. Harman. The Brun-Titchmarsh theorem on average. In *Analytic number theory, Vol. 1 (Allerton Park, IL, 1995)*, volume 138 of *Progr. Math.*, pages 39–103. Birkhäuser Boston, Boston, MA, 1996.

[2] R. C. Baker and G. Harman. Shifted primes without large prime factors. *Acta Arith.*, 83(4):331–361, 1998.

[3] P. Erdős, On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's φ-function. *Quart. J. Math. (Oxford Ser.)* 6: 205–213, 1935.

[4] 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.

[5] P. Erdős and C. Pomerance. On the normal number of prime factors of $\varphi(n)$. *Rocky Mountain J. Math.*, 15: 343–352, 1985.

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

[7] 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. *Math. Comp.*, 71(240):1803–1806, 2002.

[8] H. Halberstam and H.-E. Richert. *Sieve methods*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974. London Mathematical Society Monographs, No. 4.
[9] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.
[10] K.-H. Indlekofer and N. M. Timofeev. Divisors of shifted primes. *Publ. Math. Debrecen*, 60(3-4):307–345, 2002.
[11] P. Kurlberg. On the order of unimodular matrices modulo integers. *Acta Arith.*, 110(2):141–151, 2003.
[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. To appear.
[15] K. Norton. On the number of restricted prime factors of an integer. I. *Illinois J. Math.*, 20(4), 681–705, 1976.
[16] 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.
[17] C. Pomerance. On the distribution of amicable numbers. *J. Reine Angew. Math.*, 293/294: 217–222, 1977.

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

Department of Mathematics, Chalmers University of Technology, SE-412 96 Gothenburg, Sweden

E-mail address: carlp@math.dartmouth.edu

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