

TWO PROBLEMS ON THE DISTRIBUTION OF CARMICHAEL'S LAMBDA FUNCTION

PAUL POLLACK

ABSTRACT. Let $\lambda(n)$ denote the exponent of the multiplicative group modulo n . We show that when q is odd, each coprime residue class modulo q is hit equally often by $\lambda(n)$ as n varies. Under the stronger assumption that $\gcd(q, 6) = 1$, we prove that equidistribution persists throughout a Siegel–Walfisz-type range of uniformity. By similar methods we show that $\lambda(n)$ obeys Benford's leading digit law with respect to natural density. Moreover, if we assume GRH, then Benford's law holds for the order of $a \bmod n$, for any fixed integer $a \notin \{0, \pm 1\}$.

1. INTRODUCTION

If f is a naturally-occurring integer-valued arithmetic function, it is reasonable to ask how the values of f are distributed in arithmetic progressions. Several results of this nature are collected in Narkiewicz's monograph [Nar84]. In particular, Chapter IV of that reference describes in detail an easily-applicable criterion of Delange (appearing originally as [Del69, Theorem 1]) deciding, for each additive function f and each modulus q , whether f is uniformly distributed (UD) modulo q .

The situation for multiplicative functions is more subtle. Here Euler's φ -function is a convenient reference point. It has long been known that for each fixed positive integer q , the relation $q \mid \varphi(n)$ holds for almost all n , meaning for all but $o(x)$ values of $n \leq x$ as $x \rightarrow \infty$. (This, and much more, follows from arguments given below.) That is, the class of 0 modulo q 'hogs' almost all the values of $\varphi(n)$, ruling out uniform distribution mod q except in the trivial case $q = 1$. This phenomenon prompted Narkiewicz in [Nar67] to introduce a weaker notion of equidistribution: f is **weakly uniformly distributed mod q** (or **WUD mod q**) if (a) $\gcd(f(n), q) = 1$ for infinitely many n , and (b) for each coprime residue class $a \bmod q$,

$$(1.1) \quad \#\{n \leq x : f(n) \equiv a \pmod{q}\} \sim \frac{1}{\varphi(q)} \#\{n \leq x : \gcd(f(n), q) = 1\}, \quad \text{as } x \rightarrow \infty.$$

In the same paper, Narkiewicz gives a criterion for weak uniform distribution that may be applied to multiplicative functions that are 'polynomial-like' (in a sense we will not describe here). As applications, he classifies the moduli q for which $d(n)$ (the divisor function), and $\varphi(n)$, are WUD mod q . For instance, $\varphi(n)$ is WUD mod q precisely when $\gcd(q, 6) = 1$. For a full development of the theory of weak uniform distribution of polynomial-like multiplicative functions (incorporating later refinements by Narkiewicz and collaborators), see Chapters V and VI of the previously mentioned monograph [Nar84].

The central object of study in this paper is Carmichael's λ -function [Car19], which is a close cognate of Euler's function. Whereas $\varphi(n)$ gives the *order* of the unit group $U(\mathbb{Z}/n\mathbb{Z})$, Carmichael's function $\lambda(n)$ describes its *exponent*; that is, $\lambda(n)$ is the smallest positive integer for which

2020 *Mathematics Subject Classification*. Primary 11N64; Secondary 11A25, 11B50.

$a^{\lambda(n)} \equiv 1 \pmod{n}$ for each a coprime to n . The λ function is not multiplicative but is what might be called **lcm-multiplicative**:

$$(1.2) \quad \lambda(\text{lcm}[m, n]) = \text{lcm}[\lambda(m), \lambda(n)], \quad \text{for all positive integers } m, n.$$

As known already to Gauss, $\lambda(p^k) = \varphi(p^k)$ whenever p^k is an odd prime power, $\lambda(1) = \lambda(2) = 1$, $\lambda(4) = 2$, and $\lambda(2^k) = 2^{k-2}$ for all $k \geq 3$; these values, along with the relation (1.2), determine $\lambda(n)$ for all inputs n .

Several statistical properties of λ , such as its average, typical, and lower order, are investigated by Erdős, Pomerance, and Schmutz in [EPS91]. One takeaway from their study is that despite having similar definitions, φ and λ can behave quite differently. To give just one example: It is classical that $\varphi(n) \gg n/\log \log(3n)$ for all n , whereas it is shown in [EPS91] that there is a sequence of n tending to infinity along which $\lambda(n) \leq (\log n)^{O(\log \log \log n)}$. As far as we are aware, there have not been prior investigations into the distribution of $\lambda(n)$ in residue classes. It is easy to prove that $\lambda(n)$ is even whenever $n \geq 3$, and so $\lambda(n)$ cannot be WUD mod q if $2 \mid q$. In our first theorem we prove that this is the only obstruction.

Theorem 1.1. *λ is WUD mod q for all odd q . In fact, as $x \rightarrow \infty$,*

$$(1.3) \quad \#\{n \leq x : \lambda(n) \equiv a \pmod{q}\} \sim \frac{1}{\varphi(q)} \#\{n \leq x : \gcd(\lambda(n), q) = 1\},$$

uniformly for coprime residue classes $a \pmod{q}$ with q odd and $q \leq \log \log \log x$.

The range of uniformity in Theorem 1.1 is rather modest (to put it mildly). If we assume that $3 \nmid q$, we can do much better.

Theorem 1.2. *Fix $A > 0$. As $x \rightarrow \infty$, the relation (1.3) holds uniformly for moduli $q \leq (\log x)^A$ with $\gcd(q, 6) = 1$.*

Our next two theorems are of a slightly different nature. To set the stage, fix an integer $b \geq 2$. Let D be a positive integer, and let x be a positive real number. We say that x **begins with D in base b** if the most significant digits of x in base b are the base b digits of D . For example, 357 and 0.03512 both begin with $D = 35$ in base 10. A sequence $\{a_n\}$ of positive real numbers is said to obey **Benford's law** in base b if, for every positive integer D , the asymptotic density of n for which a_n begins with D is $\log(1 + D^{-1})/\log b$.

Diaconis observed in [Dia77] that $\{a_n\}$ is Benford in base b precisely when the sequence $\{\frac{\log a_n}{\log b}\}$ is uniformly distributed modulo 1. It is useful to rephrase this conclusion using Weyl's criterion. For each integer k , let $\theta_k = 2\pi k/\log b$. Then $\{a_n\}$ is Benford in base b precisely when $a_n^{i\theta_k}$ has limiting mean value 0, for each $k = 1, 2, 3, \dots$. This criterion was recently used in [CLPSR] to study Benford behavior of sequences described by multiplicative functions. For example, it was shown there that the sequences $\{\varphi(n)\}$ and $\{\sigma(n)\}$ (with σ the sum-of-divisors function) are not Benford in any base b .¹ On the other hand, the sequence $\{\tau_k(n)\}$ (with τ_k the k -fold divisor function) is Benford in base b if and only if $\log k/\log b$ is irrational. (Actually the work in [CLPSR] is carried out in base 10, but the arguments generalize to arbitrary bases.)

Our next theorem implies that $\{\lambda(n)\}$ is Benford in every base.

¹Here it is important that we use asymptotic density in our definition. If we were to use logarithmic density instead, $\{\varphi(n)\}$ and $\{\sigma(n)\}$ could be shown to obey Benford's law in every base.

Theorem 1.3. *Fix a nonzero real number θ . Then $\sum_{n \leq x} \lambda(n)^{i\theta} = o(x)$, as $x \rightarrow \infty$.*

Let a be an integer with $|a| > 1$. For each positive integer n coprime to a , let $\ell_a(n)$ denote the multiplicative order of $a \bmod n$. In our final theorem we show that, under the assumption of the Generalized Riemann Hypothesis² (GRH), we can replace $\lambda(n)$ with $\ell_a(n)$ in this last result.

Theorem 1.4 (conditional on GRH). *Fix an integer a with $|a| > 1$. For each fixed nonzero real number θ ,*

$$\sum_{\substack{n \leq x \\ \gcd(n, a) = 1}} \ell_a(n)^{i\theta} = o(x), \quad \text{as } x \rightarrow \infty.$$

Thus, Benford's law holds for the orders $\ell_a(n)$ (where now the relevant densities are to be computed relative to the set of n with $\gcd(n, a) = 1$).

We conclude this introduction with a word about the proofs. The UD and WUD criteria of Delange and Narkiewicz alluded to in the introduction are proved by recasting the respective problems in terms of mean values of multiplicative functions of modulus not exceeding 1. (For additive functions, this involves composing with an additive character, while for multiplicative functions one uses Dirichlet characters.) The authors of [CLPSR] adopt a similar perspective in their work on Benford's law (note that if f is positive-valued and multiplicative, then $f^{i\theta}$ is a multiplicative function of modulus 1, for every real θ). Such an approach allows one to bring to bear powerful tools such as Halász's theorem.

Since λ is not multiplicative, we must take a different tack. In recent work with Singha Roy [PSR], we proposed an alternative method of proving UD and WUD theorems. This was used to show (among other things) that for $f = \varphi$, the relation (1.1) holds uniformly for $q \leq (\log x)^A$ with $\gcd(q, 6) = 1$. Theorem 1.2 is proved in §3 using these same ideas. Here it is important that the contribution of large primes to $\lambda(n)$ can usually be computed as if λ were multiplicative; see the discussion following (3.8).

The arguments for Theorem 1.2 fail to establish weak uniform distribution when $3 \mid q$ but do show (as described in §4) that a failure of (1.3) in this case entails the nonuniform distribution of $\lambda(n) \bmod 3$ (among n with $\gcd(\lambda(n), q) = 1$). In §5, we rule out this pathology in the range $q \leq \log \log \log x$, thus proving Theorem 1.1. This requires bringing in certain anatomical facts of the kind that frequently arise when studying Euler's φ -function. For instance, it may be instructive to compare the proof of our Lemma 5.3 with that of Theorem 8 in [ELP08].

Theorems 1.3 and 1.4 are proved in §6. The proof of Theorem 1.3 is a fairly straightforward adaptation of the arguments in §5. The proof of Theorem 1.4 has the same basic structure but also requires results on the distribution of the numbers $\ell_a(p)$, which we extract from work of Li–Pomerance [LP03], Moree [Mor05], and Pappalardi [Pap15].

Notation and conventions. We use (a, b) to denote the greatest common divisor of a and b . The letters ℓ, p , and P should always be read as being restricted to primes values. We write \log_k for the k -fold iterate of the natural logarithm. Implied constants are usually absolute but are allowed depend on parameters described explicitly as ‘fixed’; concretely, this means that constants appearing in the proof of Theorem 1.2 may depend on A , that those appearing in the

²here we mean the Riemann Hypothesis for Dedekind zeta functions

proof of Theorem 1.3 may depend on θ , and that those appearing in the proof of Theorem 1.4 may depend on both θ and a .

We write $P^+(n)$ for the largest prime factor of the positive integer n and adopt the convention that $P^+(1) = 1$. If $P^+(n) \leq y$, we say that n is *y-smooth*. The *y-smooth part* of n refers to the largest *y-smooth* divisor of n ; we denote this by $s_y(n)$, so that

$$s_y(n) = \prod_{\substack{p^k \parallel n \\ p \leq y}} p^k.$$

We let $P_1(n) = P^+(n)$ and define, inductively, $P_{k+1}(n) = P^+(n/P_k(n))$; thus, $P_k(n)$ is the k th largest prime factor of n with multiplicity taken into account.

We will also need the **Schemmel totient** function $\varphi_2(n)$, defined as the count of residue classes $a \bmod n$ with $\gcd(a(a-1), n) = 1$. Familiar arguments show that $\varphi_2(n) = n \prod_{p|n} (1 - 2/p)$.

2. PRELIMINARIES

In this section we record some results needed for the proofs of Theorems 1.1–1.3. They are all closely related to lemmas appearing in [PSR].

For each positive integer q , we let $\alpha(q) = \prod_{p|q} (1 - 1/(p-1))$. It will be important for the sequel that when q is odd,

$$(2.1) \quad \alpha(q) \gg 1/\log_2(3q).$$

We will very often abbreviate $\alpha(q)$ to α .

The following proposition is a special case of [PSR, Proposition 2.1]. A more precise estimate could be extracted from work of Scourfield [Sco84], but we shall not need that.

Proposition 2.1. *Fix $A > 0$. For x tending to infinity and all odd integers $q \leq (\log x)^A$,*

$$(2.2) \quad \#\{n \leq x : (\lambda(n), q) = 1\} = \frac{x}{(\log x)^{1-\alpha}} \exp(O((\log_2(3q))^2)).$$

Actually, Proposition 2.1 of [PSR] estimates the frequency with which a general “polynomial-like” multiplicative function f is coprime to a given integer q . Taking $f = \varphi$ gives Proposition 2.1, after observing that the conditions $(\lambda(n), q) = 1$ and $(\varphi(n), q) = 1$ are equivalent. (For any finite abelian group, the exponent and order share the same set of prime factors.) We note that in [PSR], the exponent of $\log_2(3q)$ is given as $O(1)$, but inspecting the proof reveals that this exponent can be taken as 2 for $f = \varphi$.

Proposition 2.1 is established by a combination of sieve methods and mean value theorems. The key arithmetic input is an estimate for $\sum_{p \leq x, (p-1, q)=1} 1/p$ (see [PSR, Lemma 2.4]). We now restate this estimate alongside a slight extension that will be needed later.

Proposition 2.2. *For each positive integer q , and all $x \geq 3$,*

$$\sum_{\substack{p \leq x \\ (p-1, q)=1}} \frac{1}{p} = \alpha(q) \log_2 x + O((\log_2(3q))^2).$$

If additionally s is a positive integer coprime to q , then

$$\sum_{\substack{p \leq x \\ (p-1, q)=1 \\ s \nmid p-1}} \frac{1}{p} = \alpha(q) \left(1 - \frac{1}{\varphi(s)}\right) \log_2 x + O((\log_2(3q))^2).$$

For completeness, we sketch the proof of Proposition 2.2. We need a lemma due independently to Norton [Nor76, Lemma, p. 669] and Pomerance [Pom77, Remark 1].

Lemma 2.3. *Let q be a positive integer and let x be a real number with $x \geq \max\{3, q\}$. For each coprime residue class $a \pmod q$,*

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod q}} \frac{1}{p} = \frac{\log_2 x}{\varphi(q)} + \frac{1}{p_{q,a}} + O\left(\frac{\log(3q)}{\varphi(q)}\right),$$

where $p_{q,a}$ denotes the least prime congruent to a modulo q .

In particular: For all positive integers q and all $x \geq 3$, we have $\sum_{p \leq x, p \equiv 1 \pmod q} 1/p = \log_2 x / \varphi(q) + O(\log(3q)/\varphi(q))$ (this estimate being trivial when $q > x$).

Proof of Proposition 2.2 (sketch). We write

$$\sum_{\substack{p \leq x \\ (p-1, q)=1 \\ s \nmid p-1}} \frac{1}{p} = \sum_{\substack{p \leq x \\ (p-1, q)=1}} \frac{1}{p} - \sum_{\substack{p \leq x \\ (p-1, q)=1 \\ s \mid p-1}} \frac{1}{p}$$

and proceed to estimate the two right-hand sums. By inclusion-exclusion and Lemma 2.3,

$$\sum_{\substack{p \leq x \\ (p-1, q)=1}} \frac{1}{p} = \sum_{d|q} \mu(d) \sum_{\substack{p \leq x \\ p \equiv 1 \pmod d}} \frac{1}{p} = \log_2 x \sum_{d|q} \frac{\mu(d)}{\varphi(d)} + O\left(\sum_{d|q} |\mu(d)| \frac{\log(3d)}{\varphi(d)}\right).$$

Similarly,

$$\sum_{\substack{p \leq x \\ (p-1, q)=1 \\ s \nmid p-1}} \frac{1}{p} = \sum_{d|q} \mu(d) \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{sd}}} \frac{1}{p} = \frac{\log_2 x}{\varphi(s)} \sum_{d|q} \frac{\mu(d)}{\varphi(d)} + O\left(\sum_{d|q} |\mu(d)| \frac{\log(3ds)}{\varphi(sd)}\right).$$

Since $\sum_{d|q} \mu(d)/\varphi(d) = \alpha(q)$, we have the main terms claimed in the proposition. As far as the errors, notice that $\log(3ds)/\varphi(sd) \leq (\log(3d)/\varphi(d)) \cdot (\log(3s)/\varphi(s)) \ll \log(3d)/\varphi(d)$. Thus, the proof will be completed once it is shown that $\sum_{d|q} |\mu(d)| \log(3d)/\varphi(d) \ll (\log_2(3q))^2$. But this elementary estimate is already worked out (in greater generality) at the end of the proof of [PSR, Lemma 2.4]. (In the notation of that argument, we have $F(T) = T - 1$, $D = 1$, and $\nu(d) = 1$ for all d .) \square

The last result we need can be found, in slightly different form, near the start of [PSR, §4]. For convenience of the reader, we include a simple proof (a variant of the “Remark” in [PSR]).

Lemma 2.4. *Let q be a positive integer coprime to 6. For each integer $J \geq 2$ and each integer r prime to q ,*

$$\begin{aligned} \#\{(a_1, \dots, a_J) \bmod q : \gcd\left(\prod_{j=1}^J a_j(a_j - 1), q\right) = 1, \prod_{j=1}^J (a_j - 1) \equiv r \pmod{q}\} \\ = \frac{\varphi_2(q)^J}{\varphi(q)} \exp\left(O\left(\sum_{p|q} (p-2)^{1-J}\right)\right). \end{aligned}$$

Proof. By the Chinese remainder theorem, we can assume $q = p^k$ is a prime power with $p \geq 5$. Orthogonality of Dirichlet characters implies that the cardinality in question is

$$\frac{1}{\varphi(p^k)} \sum_{\chi \bmod p^k} \left(\sum_{a \bmod p^k} \chi_0(a) \chi(a-1) \right)^J \bar{\chi}(r).$$

Here the principal character $\chi = \chi_0$ contributes $\varphi_2(p^k)^J / \varphi(p^k)$. For $\chi \neq \chi_0$, the complete sum $\sum_{a \bmod p^k} \chi(a-1) = 0$, so that

$$\sum_{a \bmod p^k} \chi_0(a) \chi(a-1) = - \sum_{\substack{a \bmod p^k \\ a \equiv 0 \pmod{p}}} \chi(a-1) = -\chi(-1) \sum_{\substack{b \bmod p^k \\ b \equiv 1 \pmod{p}}} \chi(b).$$

The residue classes $b \bmod p^k$ with $b \equiv 1 \pmod{p}$ form an index $p-1$ subgroup of the multiplicative group $\bmod p^k$. Thus, the sum on b vanishes unless the restriction of χ to this subgroup is trivial. This happens for precisely $(p-1) - 1 = p-2$ nontrivial characters, and in these cases $\sum_{a \bmod p^k} \chi_0(a) \chi(a-1)$ has absolute value p^{k-1} . The triangle inequality thus implies that

$$\frac{1}{\varphi(p^k)} \left| \sum_{\substack{\chi \bmod p^k \\ \chi \neq \chi_0}} \left(\sum_{a \bmod p^k} \chi_0(a) \chi(a-1) \right)^J \bar{\chi}(r) \right| \leq \frac{1}{\varphi(p^k)} (p-2) p^{(k-1)J}.$$

Putting this estimate back above, our tuple count is $\frac{\varphi_2(p^k)^J}{\varphi(p^k)} (1 + \theta(p-2)^{1-J})$, for some real number θ with $|\theta| < 1$. As $1 + \theta(p-2)^{1-J} = \exp(O((p-2)^{1-J}))$, the lemma follows. \square

In our application of Lemma 2.4 we will have that $J \rightarrow \infty$. Thus, $\sum_{p|q} (p-2)^{1-J} = o(1)$, leading to a tuple count that is $\sim \varphi_2(q)^J / \varphi(q)$.

3. UNIFORMITY UP TO $(\log x)^A$ WHEN $(q, 6) = 1$: PROOF OF THEOREM 1.2

In what follows, x is assumed to be a large real number, q is an odd positive integer with $q \leq (\log x)^A$, where $A > 0$ is fixed, and $a \bmod q$ is a coprime residue class. Unless otherwise stated, asymptotic estimates refer to behavior as $x \rightarrow \infty$ and are to be read as uniform in the choice of $a \bmod q$. Implied constants may depend on A but on no other parameters unless explicitly noted.

We begin the proof of Theorem 1.1 by restricting our attention to inputs n whose large prime factors are suitably well-behaved. We let

$$J := \lfloor \log \log \log x \rfloor.$$

(Any integer-valued function of x tending to infinity sufficiently slowly would do just as well.) We also set

$$y := \exp(\sqrt{\log x}).$$

Following [PSR, §3] (choosing $\delta := 1$ in the notation of that paper), a positive integer $n \leq x$ is called **convenient** if $P_J(n) > y$ and none of the primes $P_1(n), P_2(n), \dots, P_J(n)$ have squares dividing n . That is, n is convenient when n admits a decomposition

$$(3.1) \quad n = mP_J \cdots P_1, \quad \text{with} \quad L_m := \max\{P^+(m), y\} < P_J < \cdots < P_1.$$

Write $N = N(x, q)$ for the total count of $n \leq x$ with $(\lambda(n), q) = 1$. The following lemma, proved as Lemma 3.1 in [PSR], shows that this count does not change very much if we restrict to convenient n .

Lemma 3.1. *The number of inconvenient $n \leq x$ with $(\lambda(n), q) = 1$ is $o(N)$.*

Our next lemma asserts that there are few inconvenient solutions to $\lambda(n) \equiv a \pmod{q}$.

Lemma 3.2. *The number of inconvenient $n \leq x$ with $\lambda(n) \equiv a \pmod{q}$ is $o(N/\varphi(q))$.*

For the proof of Lemma 3.2 (and subsequently), it is useful to note that (2.1) and (2.2) imply (crudely) that $N \gg x/\log x$ in our range of q .

In addition, it will be helpful to have at hand certain basic estimates from the theory of smooth numbers. Let $\Psi(X, Y)$ denote the count of Y -smooth numbers in $[1, X]$. Canfield, Erdős, and Pomerance have shown [CEP83] that if X, Y , and $U := \frac{\log X}{\log Y}$ all tend to infinity, with $X \geq Y \geq (\log X)^2$, then

$$(3.2) \quad \Psi(X, Y) = X \exp(-(1 + o(1))U \log U).$$

Also, it is known (see [Ten15, Theorem 5.1, p. 512]) that for all $X \geq Y \geq 2$,

$$(3.3) \quad \Psi(X, Y) \ll X \exp(-U/2).$$

Proof of Lemma 3.2. We may assume that

- (i) n has no repeated prime factor exceeding $(\log x)^{A+1}$,

since the number of $n \leq x$ failing (i) is $o(x/(\log x)^{A+1})$, which is $o(N/\varphi(q))$ in our range of q . We may also assume that, with $y' := x^{1/\log_2 x}$,

- (ii) $P^+(n) > y'$.

Indeed, (3.2) shows that (ii) holds for all but $x/(\log x)^{(1+o(1))\log_3 x} = o(N/\varphi(q))$ values of $n \leq x$. We write each remaining inconvenient solution $n \leq x$ to $\lambda(n) \equiv a \pmod{q}$ in the form $n = rP$, where $P = P^+(n)$. By (i) and (ii), we know that $P \nmid r$, and so

$$(3.4) \quad \lambda(n) = \text{lcm}[\lambda(r), P - 1] = \frac{\lambda(r) \cdot (P - 1)}{(\lambda(r), P - 1)}.$$

Continuing, let $y'' = \exp((\log_2 x)^2)$. We may further suppose that

(iii) $(\lambda(r), P - 1)$ is y'' -smooth.

Indeed, if (iii) fails choose a prime $\ell > y''$ for which ℓ divides $(\lambda(r), P - 1)$. By (i), $\ell^2 \nmid r$, and so there must be a prime p dividing r with $p \equiv 1 \pmod{\ell}$. There are at most x/pP values of n corresponding to a given pair of p, P . Summing x/pP on *all* primes $p, P \equiv 1 \pmod{\ell}$ with $p, P \leq x$ bounds the count of n corresponding to a given ℓ as $O(x(\log_2 x)^2/\ell^2)$. (We have bounded the sums on p, P by partial summation and the Brun–Titchmarsh inequality.) Now summing on $\ell > y''$ shows that the number of exceptions to (iii) is $O(x(\log_2 x)^2/y'')$, which is $o(N/\varphi(q))$.

Continuing, we may suppose that

(iv) $(\lambda(r), P - 1) \leq y^{1/3}$.

When (iv) fails, we use (iii) to decompose $P - 1 = dh$, where d is y'' -smooth and $d > y^{1/3}$. Since the number of possibilities for n given P is at most $x/P < x/dh$, summing on h and d bounds the number of exceptions to (iv) as

$$\ll x \log x \sum_{\substack{d > y^{1/3} \\ d \text{ } y''\text{-smooth}}} \frac{1}{d}.$$

Summing by parts, (3.3) gives that the sum on d is $O(\log y'' \cdot \exp(-\frac{1}{6} \frac{\log y'}{\log y''}))$. Thus, the number of n where (iv) fails is $O(x \exp(-(\log x)^{0.9}))$ (say), which is $o(N/\varphi(q))$.

We now fix $d := (\lambda(r), P - 1)$ and count possibilities for P given r and d . We must have $(\lambda(r), q) = 1$ (otherwise $(\lambda(n), q) > 1$, contradicting $\lambda(n) \equiv a \pmod{q}$) and hence also $(d, q) = 1$. Furthermore,

$$P \equiv 1 \pmod{d}$$

and, from (3.4),

$$P - 1 \equiv \frac{ad}{\lambda(r)} \pmod{q}.$$

(The right-hand side of the congruence makes sense mod q , since $(\lambda(r), q) = 1$.) These two congruences put P in a unique residue class mod dq . Since $y' < P \leq x/r$ while $d, q < y^{1/3}$, the Brun–Titchmarsh inequality gives that the number of possibilities for P given r, d is

$$\ll \frac{x}{\varphi(dq)r \log(x/rdq)} \ll \frac{x \log_2 x}{\varphi(d)\varphi(q)r \log x} \ll \frac{x(\log_2 x)^2}{d\varphi(q)r \log x},$$

using in the last step that $d/\varphi(d) \ll \log_2 d \ll \log_2 x$. Since d is y'' -smooth, it follows that the number of P given r is

$$(3.5) \quad \ll \frac{x(\log_2 x)^2}{\varphi(q)r \log x} \prod_{p \leq y''} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) \ll \frac{x(\log_2 x)^4}{\varphi(q)r \log x}.$$

Finally we sum on r . Write $r = r_1 r_2$, where r_1 is the y -smooth part of r . We bound $\sum 1/r$ by summing on all possibilities for r_1 and r_2 . Since $n = r_1 r_2 P$ is inconvenient, it must be that

$\Omega(r_2) < J$. Thus,

$$\begin{aligned} \sum_r \frac{1}{r} &\leq \left(1 + \sum_{p \leq x} (1/p + 1/p^2 + 1/p^3 + \dots)\right)^J \sum_{r_1} \frac{1}{r_1} \\ &\leq \exp(O((\log_3 x)^2)) \cdot \sum_{r_1} \frac{1}{r_1}. \end{aligned}$$

Since r_1 is divisible only by primes $p \leq y$ with $(p-1, q) = 1$,

$$\sum_{r_1} \frac{1}{r_1} \leq \prod_{\substack{p \leq y \\ (p-1, q) = 1}} \left(\sum_{j \geq 0} p^{-j} \right) \ll \exp \left(\sum_{\substack{p \leq y \\ (p-1, q) = 1}} \frac{1}{p} \right) \ll (\log x)^{\frac{1}{2}\alpha} \exp(O((\log_2(3q))^2)),$$

using Proposition 2.2 to estimate the final sum on p . Plugging these estimates back into (3.5), we conclude that the number of inconvenient $n \leq x$ with $\lambda(n) \equiv a \pmod{q}$ and all of (i)–(iv) being satisfied is

$$\ll \frac{x}{\varphi(q)(\log x)^{1-\frac{1}{2}\alpha}} \exp(O((\log_2(3q))^2 + (\log_3 x)^2)).$$

Comparing with the estimate for N from Proposition 2.1, and keeping in mind the lower bound (2.1) on α , this is seen to be $o(N/\varphi(q))$ (in fact, it is $O(N/\varphi(q) \exp((\log_2 x)^{0.9}))$, say). \square

By Lemmas 3.1 and 3.2, Theorem 1.2 will follow if it is shown that

$$\begin{aligned} (3.6) \quad &\#\{\text{convenient } n \leq x : \lambda(n) \equiv a \pmod{q}\} \\ &= \frac{1}{\varphi(q)} \#\{\text{convenient } n \leq x : (\lambda(n), q) = 1\} + o(N/\varphi(q)). \end{aligned}$$

Referring back to the description of convenient numbers appearing as (3.1), the left-hand side of (3.6) can be rewritten as

$$(3.7) \quad \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \sum_{\substack{P_j, \dots, P_1 \\ L_m < P_J < P_{J-1} < \dots < P_1 \\ P_J \cdots P_1 \leq x/m \\ \text{lcm}[\lambda(m), P_1-1, \dots, P_J-1] \equiv a \pmod{q}}} 1.$$

Proceeding further requires that we tame the ornery-seeming lcm condition. To this end, we let

$$w := \exp((\log x)^{1/8})$$

and we show that most of the time

$$(3.8) \quad \lambda(m), P_1 - 1, \dots, P_J - 1 \quad \text{are pairwise coprime at primes } > w,$$

meaning that no prime $\ell > w$ divides two terms from the list. Suppose there is such an ℓ . Then ℓ divides at least one of $P_1 - 1, \dots, P_J - 1$ and divides two of these unless $\ell \mid \lambda(m)$. If $\ell \mid \lambda(m)$, then either $\ell^2 \mid m$ or $\ell \mid p - 1$ for some prime p dividing m . In any case, we find that $n = mP_1 \cdots P_J$ is either divisible by ℓ^2 or there are primes p_1, p_2 dividing n with $p_1, p_2 \equiv 1 \pmod{\ell}$. The number of $n \leq x$ satisfying the first condition is $O(x/\ell^2)$, while the count of $n \leq x$ satisfying the second is $O(x(\log_2 x)^2/\ell^2)$ (cf. the handling of condition (iii) in the proof of Lemma 3.2). Summing on $\ell > w$, we see that our coprimality condition excludes only $o(x/w)$ values of n , which is acceptable as $x/w = o(N/\varphi(q))$.

Recall our notation $s_w(\cdot)$ for the w -smooth part. When our coprimality condition (3.8) holds,

$$(3.9) \quad \text{lcm}[\lambda(m), P_1 - 1, \dots, P_J - 1] \\ = \text{lcm}[s_w(\lambda(m)), s_w(P_1 - 1), \dots, s_w(P_J - 1)] \frac{\lambda(m)}{s_w(\lambda(m))} \prod_{j=1}^J \frac{P_j - 1}{s_w(P_j - 1)}.$$

So at the cost of an error of $o(N/\varphi(q))$, we may swap out the lcm congruence condition in (3.7) for the condition that the right-hand side of (3.9) be congruent to a modulo q . We then remove the ordering on the P_j , which introduces a factor of $1/J!$, and we partition the inner sum on P_1, \dots, P_J according to the values of $d_j := s_w(P_j - 1)$. The upshot is as follows: Let $\mathbf{d} = (d_1, \dots, d_J)$ and define rational numbers $r_{m,\mathbf{d}}$ and $a_{m,\mathbf{d}}$ by

$$(3.10) \quad r_{m,\mathbf{d}} = \text{lcm}[s_w(\lambda(m)), d_1, \dots, d_J] \frac{\lambda(m)}{s_w(\lambda(m))} \prod_{j=1}^J \frac{1}{d_j}, \quad a_{m,\mathbf{d}} = a/r_{m,\mathbf{d}}.$$

Then the count described by (3.7) is equal — up to an error of $o(N/\varphi(q))$ — to

$$(3.11) \quad \frac{1}{J!} \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \sum_{\substack{d_J, \dots, d_1 \text{ } w\text{-smooth} \\ (d_j, q) = 1 \ \forall j \\ 2|d_j \ \forall j}} \sum_{\substack{P_J, \dots, P_1 \text{ distinct} \\ L_m < P_j \ \forall j \\ P_J \cdots P_1 \leq x/m \\ s_w(P_j - 1) = d_j \ \forall j \\ \prod_{j=1}^J (P_j - 1) \equiv a_{m,\mathbf{d}} \pmod{q}}} 1.$$

(The subscripted condition $2 \mid d_j$ could be omitted at this stage but will prove useful later.) Note that $a_{m,\mathbf{d}}$ determines a well-defined coprime residue class mod q , since $a_{m,\mathbf{d}}$ is a rational number with numerator and denominator prime to q .

Following [PSR], we view the condition on $\prod_{j=1}^J (P_j - 1)$ in (3.11) as cutting out a collection of possible tuples $(P_1, \dots, P_J) \pmod{q}$. Let

$$(3.12) \quad \mathcal{V}_{m,\mathbf{d}}(q) = \{(a_1, \dots, a_J) \pmod{q} : \gcd\left(\prod_{i=1}^J a_i(a_i - 1), q\right) = 1, \prod_{j=1}^J (a_j - 1) \equiv a_{m,\mathbf{d}} \pmod{q}\}.$$

Then (3.11) can be rewritten as

$$(3.13) \quad \frac{1}{J!} \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \sum_{\substack{d_J, \dots, d_1 \text{ } w\text{-smooth} \\ (d_j, q) = 1 \ \forall j \\ 2|d_j \ \forall j}} \sum_{\mathbf{v} \in \mathcal{V}_{m,\mathbf{d}}(q)} \sum_{\substack{P_J, \dots, P_1 \text{ distinct} \\ L_m < P_j \ \forall j \\ P_J \cdots P_1 \leq x/m \\ s_w(P_j - 1) = d_j \ \forall j \\ P_j \equiv a_j \pmod{q} \ \forall j}} 1;$$

this expression (3.13) will serve as our basic approximation to the left-hand side of (3.6).

Analogous manipulations reveal that the count of convenient $n \leq x$ with $(\lambda(n), q) = 1$ is (precisely) equal to

$$(3.14) \quad \frac{1}{J!} \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \sum_{\substack{d_J, \dots, d_1 \text{ } w\text{-smooth} \\ (d_j, q) = 1 \ \forall j \\ 2|d_j \ \forall j}} \sum_{\substack{P_J, \dots, P_1 \text{ distinct} \\ L_m < P_j \ \forall j \\ P_J \cdots P_1 \leq x/m \\ s_w(P_j - 1) = d_j \ \forall j}} 1.$$

Rather than estimate (3.13) or (3.14) directly, our strategy to prove (3.6) is to directly compare (3.13) and (3.14).

View (3.13) as having the sum on P_1 innermost. We now argue that (in a precise sense) on average over the $m, \mathbf{d}, \mathbf{v}$, and P_J, \dots, P_2 from (3.13),

$$(3.15) \quad \sum_{\substack{L_m < P_1 \leq x/mP_2 \cdots P_J \\ P_1 \neq P_2, \dots, P_J \\ P_1 \equiv a_1 \pmod{q} \\ s_w(P_1-1)=d_1}} 1 \approx \frac{1}{\varphi_2(q)} \sum_{\substack{L_m < P_1 \leq x/mP_2 \cdots P_J \\ P_1 \neq P_2, \dots, P_J \\ s_w(P_1-1)=d_1}} 1.$$

The left-hand side of (3.15) is the sum on P_1 in (3.13); thus, we are asserting with this approximation that the mod q congruence condition on P_1 in (3.13) can essentially be removed by insertion of a factor of $1/\varphi_2(q)$. To argue this will assume that

$$(3.16) \quad L_m < x/mP_2 \cdots P_j;$$

otherwise (3.15) is (trivially) an equality.

To save on notation, write d for d_1 and a for a_1 . We start by estimating for each $T \geq y$ the count of $p \leq T$ with $p \equiv a \pmod{q}$ and $s_w(p-1) = d$. This is a sieve problem: We start with the set \mathcal{P} of primes $p \leq T$ with $p \equiv a \pmod{q}$ and $p \equiv 1 \pmod{d}$, which we view as having approximate size $\mathcal{X} := \text{Li}(T)/\varphi(d)\varphi(q)$. To enforce the condition $s_w(p-1) = d$, we remove (sieve out) those $p \in \mathcal{P}$ for which $\frac{p-1}{d}$ is divisible by a prime at most w . By the definition of $\mathcal{V}_{m,\mathbf{d}}(q)$, the integer $a-1$ is coprime to q , and so any prime divisor of $\frac{p-1}{d}$ must be coprime to q . Thus, we need only sieve by those primes up to w not dividing q .

Let e be a squarefree, w -smooth number with $(e, q) = 1$. The count of $p \in \mathcal{P}$ for which $e \mid \frac{p-1}{d}$ is precisely the count of primes up to T belonging to a certain coprime progression mod deq ; it is therefore

$$(3.17) \quad \frac{\text{Li}(T)}{\varphi(de)\varphi(q)} + O(E(T; qde)),$$

where (anticipating an application of the Bombieri–Vinogradov theorem) we have set

$$E(X; M) := \max_{2 \leq Y \leq X} \max_{\substack{A \bmod M \\ (A, M)=1}} \left| \pi(Y; M, A) - \frac{\text{Li}(Y)}{\varphi(M)} \right|.$$

Setting $g(e) := \varphi(d)/\varphi(de)$, the main term in (3.17) is $\mathcal{X}g(e)$. Now g is multiplicative in e , and g satisfies the Iwaniec condition (with $\kappa = 1$): If $\frac{3}{2} \leq w_1 \leq w_2 \leq w$, then $\prod_{w_1 < p \leq w_2, p \nmid q} (1-g(p))^{-1} \leq (1 + O(1/\log w_1))^{\frac{\log w_2}{\log w_1}}$, where the implied constant is absolute. So we are set up to apply the Fundamental Lemma of the Sieve (see, e.g., [Kou19, Theorem 18.11, p. 190]), which yields

$$(3.18) \quad \#\{p \leq T : p \equiv a \pmod{q}, s_w(p-1) = d\} \\ = \left(\frac{\text{Li}(T)}{\varphi(d)\varphi(q)} \prod_{\substack{p \leq w \\ p \nmid q}} (1 - g(p)) \right) (1 + O(u^{-u/2})) + O\left(\sum_{e \leq w^u} E(T; qde) \right),$$

where $u \geq 1$ is a parameter at our disposal. Letting

$$z := \exp((\log x)^{1/4}),$$

we choose u so that $w^u = z$ (i.e., $u = (\log x)^{1/8}$). Inserting this choice of u and simplifying, the right-hand side of (3.18) becomes

$$(3.19) \quad \left(\frac{1}{2} \prod_{2 < p \leq w} \frac{p-2}{p-1} \right) \frac{\text{Li}(T)}{\varphi(d)\varphi_2(q)} \cdot \frac{\varphi(d_{\text{odd}})^2}{d_{\text{odd}}\varphi_2(d_{\text{odd}})} \\ + O\left(\frac{T}{\varphi(d)\varphi(q)} \exp(-(\log x)^{1/8}) + \sum_{e \leq z} E(T; qde) \right),$$

where d_{odd} denotes the largest odd divisor of d .

If we forget the mod q congruence condition on p and estimate the total number of $p \leq T$ with $s_w(p-1) = d$, we obtain an identical estimate to (3.19), but with all occurrences of q replaced by 1. Thus, writing $\Delta = \Delta(m, \mathbf{d}, \mathbf{v}, P_J, \dots, P_2)$ for the magnitude of the difference between the two sides of (3.15),

$$(3.20) \quad \Delta \ll \Delta_1 + \Delta_2 + \Delta_3,$$

where

$$\Delta_1 = J + \frac{x \exp(-(\log x)^{1/8})}{mP_2 \cdots P_J \varphi(d)\varphi_2(q)}, \quad \Delta_2 = \sum_{e \leq z} E\left(\frac{x}{mP_2 \cdots P_J}; qde \right), \quad \text{and} \\ \Delta_3 = \frac{1}{\varphi_2(q)} \sum_{e \leq z} E\left(\frac{x}{mP_2 \cdots P_J}; de \right).$$

When d is large, the bound

$$(3.21) \quad \Delta \ll x/mdP_2 \cdots P_J$$

will be more useful than (3.20); (3.21) is obvious, since the count of primes $1 \bmod d$ to $x/mP_2 \cdots P_J$ is smaller than $x/mdP_2 \cdots P_J$.

Let us show, using (3.20) and (3.21), that

$$(3.22) \quad \sum_{m, \mathbf{d}, \mathbf{v}, P_J, \dots, P_2} \Delta(m, \mathbf{d}, \mathbf{v}, P_J, \dots, P_2) \ll x/(\log x)^{A+2},$$

where $m, \mathbf{d}, \mathbf{v}, P_J, \dots, P_2$ are restricted by the conditions of summation in (3.13) and by (3.16).

We take first the cases when $d \leq z$. Here we appeal to (3.20), considering separately the contributions from $\Delta_1, \Delta_2, \Delta_3$. It is easy to handle Δ_1 : Since $x/mP_2 \cdots P_J > L_m \geq y$, we have $J \ll \frac{x \exp(-(\log x)^{1/8})}{mP_2 \cdots P_J \varphi(d)\varphi_2(q)}$. Summing $\frac{x \exp(-(\log x)^{1/8})}{mP_2 \cdots P_J \varphi(d)\varphi_2(q)}$ on all $m \leq x$, all primes $P_2, \dots, P_J \leq x$ and all $d \leq z$ gives a quantity of size $O(\frac{x}{\varphi_2(q)} \exp(-(\log x)^{1/9}))$. Since P_2, \dots, P_J and d together determine \mathbf{d} and the components a_2, \dots, a_J of \mathbf{v} , and since there are at most $\varphi_2(q)$ choices for $a_1 \bmod q$, we conclude that Δ_1 contributes only $O(x \exp(-(\log x)^{1/9}))$ to the left-hand side of (3.22).

Since $\varphi_2(q) \leq q \leq (\log x)^A$, the Δ_2 piece will be satisfactorily handled if

$$(3.23) \quad \sum_{m \leq x} \sum_{\substack{P_2, \dots, P_J \\ P_2 \cdots P_J \leq x/my}} \sum_{d \leq z} \sum_{e \leq z} E\left(\frac{x}{mP_2 \cdots P_J}; qde \right) = O(x/(\log x)^{2A+2}).$$

(We use again that P_2, \dots, P_J and d determine \mathbf{d} and a_2, \dots, a_J . Note that the restrictions in (3.23) on m, P_2, \dots, P_J , and d are implied by the conditions of summation in (3.13), the assumption (3.16), and our present stipulation that $d \leq z$.) Trivially, $E(x/mP_2 \cdots P_J; M) \ll x/\varphi(M)mP_2 \cdots P_J$ whenever $M \leq x/mP_2 \cdots P_J$. So by Cauchy–Schwarz and the Bombieri–Vinogradov theorem (bearing in mind that $qz^2 < y^{1/3} \leq (x/mP_2 \cdots P_J)^{1/3}$),

$$\begin{aligned} \sum_{d, e \leq z} E\left(\frac{x}{mP_2 \cdots P_J}; qde\right) &\leq \sum_{M \leq qz^2} \tau(M) \cdot E\left(\frac{x}{mP_2 \cdots P_J}; M\right) \\ &\ll \left(\frac{x}{mP_2 \cdots P_J} \sum_{M \leq qz^2} \frac{\tau(M)^2}{\varphi(M)}\right)^{1/2} \left(\sum_{M \leq qz^2} E\left(\frac{x}{mP_2 \cdots P_J}; M\right)\right)^{1/2} \\ &\ll \left(\frac{x(\log x)^4}{mP_2 \cdots P_J}\right)^{1/2} \left(\frac{x}{mP_2 \cdots P_J(\log x)^{4A+12}}\right)^{1/2}, \end{aligned}$$

which is $O((x/mP_2 \cdots P_J)(\log x)^{-2A-4})$. Summing on $m \leq x$ and $P_2, \dots, P_J \leq x$, this is $O(x/(\log x)^{2A+2})$, which is acceptable for (3.23). The errors induced by Δ_3 can be treated entirely analogously; we leave the tedious but inglorious details to the reader.

To handle the contributions to (3.22) from cases where $d > z$, it is enough (appealing now to (3.21)) to show that

$$(3.24) \quad \sum_{m \leq x} \sum_{P_2, \dots, P_J \leq x} \sum_{\substack{d > z \\ P^+(d) \leq w}} \frac{x}{mdP_2 \cdots P_J} = O(x/(\log x)^{2A+2}).$$

By (3.3), $\sum_{d > z, P^+(d) \leq w} 1/d \ll (\log w) \exp(-\frac{1}{2}(\log x)^{1/8})$. This yields (3.24) after crudely bounding the sums on m, P_2, \dots, P_J . Thus, we have (3.22).

We conclude from (3.22) that

$$\begin{aligned} &\frac{1}{J!} \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \sum_{\substack{d_J, \dots, d_1 \text{ } w\text{-smooth} \\ (d_j, q) = 1 \ \forall j \\ 2|d_j \ \forall j}} \sum_{\mathbf{v} \in \mathcal{V}_{m, \mathbf{d}}(q)} \sum_{\substack{P_J, \dots, P_1 \text{ distinct} \\ L_m < P_j \ \forall j \\ P_J \cdots P_1 \leq x/m \\ s_w(P_j - 1) = d_j \ \forall j \\ P_j \equiv a_j \pmod{q} \ \forall j}} 1 \\ &= \frac{1}{\varphi_2(q)} \frac{1}{J!} \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \sum_{\substack{d_J, \dots, d_1 \text{ } w\text{-smooth} \\ (d_j, q) = 1 \ \forall j \\ 2|d_j \ \forall j}} \sum_{\mathbf{v} \in \mathcal{V}_{m, \mathbf{d}}(q)} \sum_{\substack{P_J, \dots, P_1 \text{ distinct} \\ L_m < P_j \ \forall j \\ P_J \cdots P_1 \leq x/m \\ s_w(P_j - 1) = d_j \ \forall j \\ P_j \equiv a_j \pmod{q} \ \forall j \geq 2}} 1 + O(x/(\log x)^{A+2}). \end{aligned}$$

In fact, our arguments justify an error term of $O(x/J!(\log x)^{A+2})$, but the extra factor of $J!$ is otiose here.

Proceeding in exactly the same manner, we can successively remove the mod q congruence conditions on P_2, P_3, \dots, P_J . At each step, we introduce a new factor of $1/\varphi_2(q)$ and a new error of size $O(x/(\log x)^{A+2})$. (Actually the error introduced after the j th step could be estimated as $O(x/J!\varphi_2(q)^{j-1}(\log x)^{A+2})$, but $O(x/(\log x)^{A+2})$ is all we need.) Since $Jx/(\log x)^{A+2} =$

$o(N/\varphi(q))$, we make the following deduction: Up to an error of $o(N/\varphi(q))$, the count of convenient $n \leq x$ with $\lambda(n) \equiv a \pmod{q}$ is

$$(3.25) \quad \frac{1}{\varphi_2(q)^J} \frac{1}{J!} \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \sum_{\substack{d_J, \dots, d_1 \text{ } w\text{-smooth} \\ (d_j, q) = 1 \quad \forall j \\ 2|d_j \quad \forall j}} \sum_{\substack{P_J, \dots, P_1 \text{ distinct} \\ L_m < P_j \quad \forall j \\ P_J \cdots P_1 \leq x/m \\ s_w(P_j - 1) = d_j \quad \forall j}} \#\mathcal{V}_{m, \mathbf{d}}(q).$$

Up to this point, it was only necessary to assume that q is odd. We now tack on the hypothesis that $3 \nmid q$. Lemma 2.4 then implies that $\#\mathcal{V}_{m, \mathbf{d}}(q) = (1 + o(1)) \frac{\varphi_2(q)^J}{\varphi(q)}$, uniformly in the values of m and \mathbf{d} from (3.25). Hence, the size of (3.25) is $(1 + o(1))/\varphi(q)$ times that of (3.14). Since (3.14) counts convenient $n \leq x$ with $(\lambda(n), q) = 1$, the relation (3.6) follows. This completes the proof of Theorem 1.2.

4. INTERLUDE

Our proof of Theorem 1.2 does not yield weak uniform distribution when $3 \mid q$. However, one can show by these methods that the only obstruction to weak uniform distribution mod q arises from an obstruction modulo 3. The following proposition makes this precise.

Proposition 4.1. *Fix $A > 0$. As $x \rightarrow \infty$,*

$$(4.1) \quad \#\{n \leq x : \lambda(n) \equiv a \pmod{q}\} = \frac{2 + o(1)}{\varphi(q)} \#\{n \leq x : \lambda(n) \equiv a \pmod{3}\} + o(N/\varphi(q)),$$

uniformly in the choice of coprime residue class $a \pmod{q}$, where q is odd, $3 \mid q$, and $q \leq (\log x)^A$.

In the remainder of this section we describe how to adapt the proof of Theorem 1.2 to obtain Proposition 4.1. Note that by Lemmas 3.1 and 3.2, to prove Proposition 4.1 it suffices to establish the “convenient version” of (4.1), where n is restricted to convenient values in both sets.

We start from (3.25), which (as we know already) counts convenient solutions $n \leq x$ to $\lambda(n) \equiv a \pmod{q}$, up to an error of $o(N/\varphi(q))$. The new twist is that when $3 \mid q$, the sets $\mathcal{V}_{m, \mathbf{d}}(q)$ are no longer uniformly of size $\sim \varphi_2(q)^J/\varphi(q)$. In fact, since each a with $a(a-1)$ coprime to q has $a-1 \equiv 1 \pmod{3}$, the set $\mathcal{V}_{m, \mathbf{d}}(q)$ is empty unless $a_{m, \mathbf{d}} \equiv 1 \pmod{3}$.

Suppose we are in the case that $a_{m, \mathbf{d}} \equiv 1 \pmod{3}$; here we say that m and \mathbf{d} are **compatible**. Then $\#\mathcal{V}_{m, \mathbf{d}}(q) = \#\mathcal{V}_{m, \mathbf{d}}(q_0) \cdot \#\mathcal{V}'$, where

$$\mathcal{V}' = \{(a_1, \dots, a_J) \pmod{3^k} : \text{each } a_j \equiv 2 \pmod{3}, \prod_{j=1}^J (a_j - 1) \equiv a_{m, \mathbf{d}} \pmod{3^k}\}.$$

By Lemma 2.4, $\#\mathcal{V}_{m, \mathbf{d}}(q_0) = (1 + o(1))\varphi_2(q_0)^J/\varphi(q_0)$. Also, $\#\mathcal{V}' = (3^{k-1})^{J-1}$: every choice of $a_1, \dots, a_{J-1} \equiv 2 \pmod{3}$ determines a unique a_J . As $(3^{k-1})^{J-1} = 2\varphi_2(3^k)^J/\varphi(3^k)$, we deduce that $\#\mathcal{V}_{m, \mathbf{d}}(q) = (2 + o(1))\varphi(q)^J/\varphi(q)$ for compatible m and \mathbf{d} .

We can recast the compatibility condition by referring back to (3.9) and the definition (3.10) of $a_{m, \mathbf{d}}$: For m, \mathbf{d} , and P_1, \dots, P_J as in (3.25),

$$m \text{ and } \mathbf{d} \text{ are compatible} \iff \lambda(mP_J \cdots P_1) \equiv a \pmod{3}.$$

Here we have used that each $P_j - 1 \equiv 1 \pmod{3}$.

Combining the observations of the previous two paragraphs, we find that (3.25) has size

$$\frac{(2 + o(1))}{\varphi(q)} \left[\frac{1}{J!} \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \sum_{\substack{d_J, \dots, d_1 \text{ } y\text{-smooth} \\ (d_j, q) = 1 \quad \forall j \\ 2 \mid d_j \quad \forall j}} \sum_{\substack{P_J, \dots, P_1 \text{ distinct} \\ L_m < P_j \quad \forall j \\ P_J \cdots P_1 \leq x/m \\ s_w(P_j - 1) = d_j \quad \forall j \\ \lambda(m P_J \cdots P_1) \equiv a \pmod{3}}} 1 \right].$$

The bracketed expression is precisely analogous to (3.14); it counts convenient $n \leq x$ with $(\lambda(n), q) = 1$ and $\lambda(n) \equiv a \pmod{3}$. We have therefore shown the ‘convenient version’ of (4.1) and completed the proof of Proposition 4.1.

5. UNIFORMITY TO $\log_3 x$ WHEN $3 \mid q$: PROOF OF THEOREM 1.1

In view of Proposition 4.1, Theorem 1.1 follows from our next result.

Theorem 5.1. *Let $a \in \{\pm 1\}$. As $x \rightarrow \infty$,*

$$(5.1) \quad \#\{n \leq x : (\lambda(n), q) = 1, \lambda(n) \equiv a \pmod{3}\} \sim \frac{1}{2} \#\{n \leq x : (\lambda(n), q) = 1\},$$

uniformly for integers $q \leq \log_3 x$ where q is odd and $3 \mid q$.

Our strategy for proving Theorem 5.1 shares many features with the proof of Theorem 1.1 but we must select certain parameters rather differently. In particular, the reader should be warned that y, w , and L_m will be (re)used with different (but related) meanings.

We start by refreshing our notion of convenient. We will now call $n \leq x$ **convenient** if $P^+(n) > y := x^{1/\sqrt{\log_3 x}}$ and $P^+(n)^2 \nmid n$. Thus, n is convenient precisely when we can write

$$(5.2) \quad n = mP, \quad \text{where} \quad L_m := \max\{P^+(m), y\} < P.$$

We continue to use N to denote the count of $n \leq x$ with $(\lambda(n), q) = 1$. The following statement is the analogue of Lemma 3.1 for our new definition of inconvenient.

Lemma 5.2. *The number of inconvenient $n \leq x$ with $(\lambda(n), q) = 1$ is $o(N)$.*

Proof. The number of $n \leq x$ divisible by the square of a prime exceeding y is $o(x/y)$ and thus also $o(N)$. All other inconvenient $n \leq x$ with $(\lambda(n), q) = 1$ are y -smooth and divisible only by p with $(p-1, q) = 1$. The sieve bounds the number of such $n \leq x$ as

$$\begin{aligned} &\ll x \prod_{\substack{p \leq y \\ (p-1, q) > 1}} \left(1 - \frac{1}{p}\right) \prod_{y < p \leq x} \left(1 - \frac{1}{p}\right) \ll \frac{x}{\log x} \prod_{\substack{p \leq y \\ (p-1, q) = 1}} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll \frac{x}{\log x} \exp\left(\sum_{\substack{p \leq y \\ (p-1, q) = 1}} \frac{1}{p}\right) = \frac{x}{(\log x)^{1-\alpha}} \exp(O((\log_2(3q))^2)) \cdot \frac{1}{(\log_3 x)^{\alpha/2}}, \end{aligned}$$

where we used Proposition 2.2 to estimate on the sum on p . Comparing with (2.2), keeping in mind the lower bound (2.1) and the upper bound $q \leq \log_3 x$, this is seen to be $o(N)$. (In fact, it is $o(N/\exp(\sqrt{\log_4 x}))$.) \square

In view of Lemma 5.2, Theorem 5.1 will be established once it is shown that

$$(5.3) \quad \#\{\text{convenient } n \leq x : (\lambda(n), q) = 1, \lambda(n) \equiv a \pmod{3}\} \\ = \frac{1}{2} \#\{\text{convenient } n \leq x : (\lambda(n), q) = 1\} + o(N).$$

For convenient n with $n = mP$ as in (5.2),

$$(5.4) \quad \lambda(n) = \frac{\lambda(m)(P-1)}{(\lambda(m), P-1)}.$$

The following “near-identity” for $(\lambda(m), P-1)$ is the linchpin of our proof. Let

$$w := \log_2 x.$$

Lemma 5.3. *Among all convenient $n \leq x$ with $(\lambda(n), q) = 1$, all but $o(N)$ satisfy*

$$(\lambda(m), P-1) = s_w(P-1).$$

Proof. First, we may restrict attention to convenient $n = mP \leq x$ for which

- (i) m is not divisible by the square of a prime exceeding $\log_3 x$.

Since $y < P \leq x/m$, the number of convenient n corresponding to a given m is bounded by $\pi(x/m)$, which is $\ll x/m \log(x/m) \ll x/m \log y = x\sqrt{\log_3 x}/m \log x$. Thus, an upper bound for the number of exceptions to (i) follows from an upper bound for $\sum 1/m$.

Assuming (i) fails, write $m = \ell^2 m_0$ where $\ell > \log_3 x$. As $(\lambda(m), q) = 1$, every p dividing m_0 has $(p-1, q) = 1$. Hence, the reciprocal sum of possible m_0 satisfies $\sum 1/m_0 \ll \exp(\sum_{p \leq x, (p-1, q)=1} 1/p) \ll (\log x)^\alpha \exp(O((\log_2(3q))^2))$. Also, $\sum_{\ell > \log_3 x} 1/\ell^2 \ll 1/\log_3 x$. It follows that the number of exceptions to (i) is .

$$\ll \frac{x}{(\log x)^{1-\alpha}} \exp(O((\log_2(3q))^2)) \cdot \frac{\sqrt{\log_3 x}}{\log_3 x}.$$

This is $o(N)$ (in fact, $o(N/(\log_3 x)^{1/3})$) and so is acceptable for us.

We may further assume that

- (ii) $\lambda(m)$ is divisible by every positive integer $s \leq w' := \log_2 x/(\log_3 x)^2$ with $(s, q) = 1$.

Let s be a positive integer with $s \leq w'$, $(s, q) = 1$, and suppose that $s \nmid \lambda(m)$. Then m is divisible only by primes p with $p-1$ coprime to q and $p-1$ not divisible by s . Invoking Proposition 2.2,

$$\sum \frac{1}{m} \ll \exp \left(\sum_{\substack{p \leq x \\ (p-1, q)=1 \\ s \nmid p-1}} \frac{1}{p} \right) \ll (\log x)^{\alpha(1-1/\varphi(s))} \exp(O((\log_2(3q))^2)).$$

Reasoning as in (i), the number of corresponding n is therefore

$$(5.5) \quad \ll \frac{x}{(\log x)^{1-\alpha}} \exp(O((\log_2(3q))^2)) \cdot \frac{\sqrt{\log_3 x}}{(\log x)^{\alpha/\varphi(s)}}.$$

As $s \leq w'$,

$$(\log x)^{\alpha/\varphi(s)} \geq (\log x)^{\alpha/s} \geq \exp(\alpha(\log_3 x)^2),$$

and so the right-hand side of (5.5) is $o(N/\exp((\log_3 x)^{3/2}))$ (say). Summing on the at most w' values of s , we obtain only $o(N)$ exceptions to (ii).

Continuing, we can assume that

$$(iii) \quad (\lambda(m), P-1) \text{ has all prime factors at most } w'' := \log_2 x (\log_3 x)^2.$$

If (iii) fails, choose a prime $\ell > w''$ dividing $\lambda(m)$ and $P-1$. Our strategy will be to count possibilities for P given m, ℓ and then sum on m, ℓ . If we assume temporarily that $\ell \leq y^{1/3}$, we can apply Brun–Titchmarsh: The number of $P \equiv 1 \pmod{\ell}$ with $y < P \leq x/m$ is

$$\ll \frac{x}{m\ell \log(x/m\ell)} \ll \frac{x\sqrt{\log_3 x}}{m\ell \log x}.$$

Since $\ell \mid \lambda(m)$ and (by (i)) $\ell^2 \nmid m$, we must be able to write $m = pm_0$, where $p \equiv 1 \pmod{\ell}$. Since $\sum 1/p \ll \log_2 x/\ell$ (taken over all $p \leq x$ with $p \equiv 1 \pmod{\ell}$) and $\sum 1/m_0 \ll (\log x)^\alpha \exp(O((\log_2(3q))^2))$ (taken over all $m_0 \leq x$ divisible only by p with $(p-1, q) = 1$), we conclude that the count of exceptional n arising from a given $\ell \leq y^{1/3}$ is

$$\ll \frac{x}{(\log x)^{1-\alpha}} \exp(O((\log_2(3q))^2)) \cdot \frac{\log_2 x \sqrt{\log_3 x}}{\ell^2}.$$

Summing on $\ell > w''$ gives a quantity that is $o(N)$, in fact $o(N/\log_3 x)$. Above, we ignored the cases when $\ell > y^{1/3}$. These are handled similarly, except that in place of Brun–Titchmarsh one bounds the number of P trivially by $x/m\ell$. We leave to the reader to check that these cases contribute $o(N)$ (in fact, $o(N/y^{1/4})$).

We can also assume that

$$(iv) \quad P-1 \text{ has no prime factors in the interval } (w', w''].$$

If (iv) fails, choose $\ell \mid P-1$ with $\ell \in (w', w'']$. Arguing with Brun–Titchmarsh as in (iii), the number of P given ℓ, m is $\ll x\sqrt{\log_3 x}/m\ell \log x$. Summing on m , the number of exceptions to (iv) arising from a given ℓ is

$$\ll \frac{x}{(\log x)^{1-\alpha}} \exp(O((\log_2(3q))^2)) \cdot \frac{\sqrt{\log_3 x}}{\ell}.$$

Since $\sum_{\ell \in (w, w'']} 1/\ell \ll \log_4 x/\log_3 x$, there are $o(N)$ exceptions to (iv) (in fact, $o(N/(\log_3 x)^{1/3}))$.

Conditions (iii) and (iv) ensure that $(\lambda(m), P-1)$ divides $s_w(P-1)$. Furthermore, if $(\lambda(m), P-1) \neq s_w(P-1)$, then there is a prime power p^k , with $p \leq w'$, $p \nmid q$, such that $p^k \mid P-1$ but $p^k \nmid \lambda(m)$. By (ii), $p^k > w'$, and so $k > 1$. Write $s = p^k$ and suppose to start with that $s \leq y^{1/3}$. Arguing as in (iv) the number of n corresponding to a given s is

$$\ll \frac{x}{(\log x)^{1-\alpha}} \exp(O((\log_2(3q))^2)) \cdot \frac{\sqrt{\log_3 x}}{s}.$$

This is $o(N)$ after being summed on proper prime powers $s > w'$; in fact, the sum on all squarefull $s > w'$ is $o(N/(\log_2 x)^{1/3})$. When $s > y^{1/3}$, we bound the count of P given m, s by x/ms . Summing on all $m \leq x$ and all squarefull $s > y^{1/3}$ gives a contribution of size $o(x/y^{1/7})$ (say), which is certainly also $o(N)$. This completes the proof of Lemma 5.3. \square

If $n \leq x$ is convenient with $(\lambda(n), q) = 1$, and n satisfies the conclusion of Lemma 5.3, then (by (5.4)) $\lambda(n) \equiv \lambda(m)(P-1)/s_w(P-1) \equiv \lambda(m)/s_w(P-1) \pmod{3}$. It follows that the count of convenient $n \leq x$ with $(\lambda(n), q) = 1$ and $\lambda(n) \equiv a \pmod{3}$ is given by

$$(5.6) \quad \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \sum_{\substack{d \text{ } w\text{-smooth} \\ d \equiv a\lambda(m) \pmod{3} \\ (d, q) = 1, 2 \nmid d}} \sum_{\substack{L_m < P \leq x/m \\ s_w(P-1) = d}} 1,$$

up to an error of $o(N)$.

This sum on P in (5.6) is reminiscent of (3.15) but (since w is now minuscule) can be estimated satisfactorily by a direct application of inclusion-exclusion. Let

$$(5.7) \quad W = \frac{1}{2} \prod_{2 < p \leq w} \frac{p-2}{p-1}, \quad \text{and define, for odd } d, \quad g(d) = \frac{\varphi(d)^2}{d\varphi_2(d)}.$$

A straightforward calculation shows that, as long as $L_m < x/m$,

$$\begin{aligned} \sum_{\substack{L_m < P \leq x/m \\ s_w(P-1) = d}} 1 &= \sum_{e \mid \prod_{p \leq w} p} \mu(e) (\pi(x/m; 1, de) - \pi(L_m; 1, de)) \\ &= (\text{Li}(x/m) - \text{Li}(L_m)) W \frac{g(d_{\text{odd}})}{\varphi(d)} + O \left(\sum_{e \mid \prod_{p \leq w} p} \tilde{E}(x/m; de) \right), \end{aligned}$$

where

$$\tilde{E}(X; M) = \max_{2 \leq Y \leq X} \left| \pi(Y; M, 1) - \frac{\text{Li}(Y)}{\varphi(M)} \right|.$$

This estimate might be compared with (3.19); note that $\varphi_2(q)$ is absent from the denominator of our new main term as there is no mod q congruence condition on P .

The contribution of the error terms when summed on the m, d from (5.6) can be estimated as in our discussion of (3.15): We use Bombieri–Vinogradov and Cauchy–Schwarz to treat cases when $d \leq y^{1/3}$; these total $O(x/(\log x)^B)$ for any fixed B . To handle $d > y^{1/3}$, we use the trivial bound $\tilde{E}(x/m; de) \ll x/m\varphi(de)$, valid for all d, e . (It is important here that we work with $\tilde{E}(x/m; de)$ rather than $E(x/m; de)$.) Since $x/m\varphi(de) \leq x/m\varphi(d)\varphi(e)$ and $d/\varphi(d) \ll \log w$ for w -smooth d ,

$$\sum_{m \leq x} \sum_{\substack{d > y^{1/3} \\ P^+(d) \leq w}} \sum_{e \mid \prod_{p \leq w} p} \frac{x}{m\varphi(de)} \ll x \log w \left(\sum_{m \leq x} \frac{1}{m} \right) \left(\sum_{e \text{ } w\text{-smooth}} \frac{1}{\varphi(e)} \right) \sum_{\substack{d > y^{1/3} \\ P^+(d) \leq w}} \frac{1}{d}.$$

By (3.3), the sum on d is $O(\exp(-(\log x)^{9/10}))$. Since the sums on m and e are $O(\log x)$ and $O(\log w)$ respectively, we see that those $d > y^{1/3}$ also contribute $O(x/(\log x)^B)$. In particular (taking $B = 1$, say), the error terms are in total $o(N)$.

Therefore, up to an error of $o(N)$, the count of convenient $n \leq x$ with $(\lambda(n), q) = 1$ and $\lambda(n) \equiv a \pmod{3}$ is

$$(5.8) \quad W \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1 \\ L_m < x/m}} (\text{Li}(x/m) - \text{Li}(L_m)) \sum_{\substack{d \text{ } w\text{-smooth} \\ d \equiv a\lambda(m) \pmod{3} \\ (d, q) = 1, 2 \nmid d}} \frac{g(d_{\text{odd}})}{\varphi(d)}.$$

Carrying out the same arguments, but forgetting the mod 3 constraint on $\lambda(n)$, will show that the count of convenient $n \leq x$ with $(\lambda(n), q) = 1$ is

$$(5.9) \quad W \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1 \\ L_m < x/m}} (\text{Li}(x/m) - \text{Li}(L_m)) \sum_{\substack{d \text{ } w\text{-smooth} \\ (d, q) = 1, 2 \nmid d}} \frac{g(d_{\text{odd}})}{\varphi(d)},$$

up to an error of $o(N)$. So to prove (5.3), it is enough to show that (5.8) is half of (5.9), to within $o(N)$. For this we zero in on the sums on d in (5.8) and (5.9).

It is expedient to group d sharing the same odd part d' . For each $\epsilon \in \{\pm 1\}$,

$$\begin{aligned} \sum_{\substack{d \text{ } w\text{-smooth} \\ d \equiv \epsilon \pmod{3} \\ (d, q) = 1, 2 \nmid d}} \frac{g(d_{\text{odd}})}{\varphi(d)} &= \sum_{\substack{d' \text{ } w\text{-smooth} \\ (d', 2q) = 1}} \frac{g(d')}{\varphi(d')} \sum_{\substack{k \geq 1 \\ 2^k d' \equiv \epsilon \pmod{3}}} \frac{1}{\varphi(2^k)} \\ &= \frac{2}{3} \sum_{\substack{d' \text{ } w\text{-smooth} \\ d' \equiv \epsilon \pmod{3} \\ (d', 2q) = 1}} \frac{g(d')}{\varphi(d')} + \frac{4}{3} \sum_{\substack{d' \text{ } w\text{-smooth} \\ d' \equiv -\epsilon \pmod{3} \\ (d', 2q) = 1}} \frac{g(d')}{\varphi(d')}. \end{aligned}$$

Hence, with χ denoting the nontrivial character mod 3,

$$\left| \sum_{\substack{d \text{ } w\text{-smooth} \\ d \equiv 1 \pmod{3} \\ (d, q) = 1, 2 \nmid d}} \frac{g(d_{\text{odd}})}{\varphi(d)} - \sum_{\substack{d \text{ } w\text{-smooth} \\ d \equiv -1 \pmod{3} \\ (d, q) = 1, 2 \nmid d}} \frac{g(d_{\text{odd}})}{\varphi(d)} \right| = \frac{2}{3} \left| \sum_{\substack{d' \text{ } w\text{-smooth} \\ (d', 2q) = 1}} \frac{\chi(d') g(d')}{\varphi(d')} \right|.$$

We develop the sum on d' as an Euler product, noting that $g(p) = g(p^2) = g(p^3) = \dots$:

$$\sum_{\substack{d' \text{ } w\text{-smooth} \\ (d', 2q) = 1}} \frac{\chi(d') g(d')}{\varphi(d')} = \prod_{\substack{p \leq w \\ p \nmid 2q}} \left(1 + \frac{\chi(p) g(p)}{p-1} \left(1 - \frac{\chi(p)}{p} \right)^{-1} \right).$$

The term corresponding to p in our right-hand product has size $1 + \chi(p)/p + O(1/p^2)$. Hence, the product is $\ll \exp(\sum_{p \leq w, p \nmid 2q} \chi(p)/p)$, which is $\ll \log_2(3q) \exp(\sum_{p \leq w} \chi(p)/p) \ll \log_2(3q)$, using in the last step the convergence of $\sum_p \chi(p)/p$. It follows that the difference between (5.8) and half of (5.9) is

$$\begin{aligned} &\ll \log_2(3q) \cdot W \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1 \\ L_m < x/m}} (\text{Li}(x/m) - \text{Li}(L_m)) \ll \log_2(3q) \cdot W \sum_{\substack{m \leq x \\ (\lambda(m), q) = 1}} \frac{x \sqrt{\log_3 x}}{m \log x} \\ &\ll \frac{x}{(\log x)^{1-\alpha}} \exp(O((\log_2(3q))^2)) \cdot W \log_2(3q) \sqrt{\log_3 x}. \end{aligned}$$

As $W \ll 1/\log w \ll 1/\log_3 x$ and $\log_2(3q) \ll \log_5 x$, this last expression is $o(N/(\log_3 x)^{1/3})$ and so in particular $o(N)$. This completes the proof of Theorem 1.1.

6. LEADING DIGITS OF $\lambda(n)$ AND $\ell_a(n)$

The proofs of Theorems 1.3 and 1.4 proceed along similar lines to our argument for Proposition 4.1; in particular, we keep the definition (5.2) of ‘convenient’ and continue to write w for $\log_2 x$.

6.1. Proof of Theorem 1.3. By Lemma 5.2 with $q = 1$, all but $o(x)$ values of $n \leq x$ are convenient. Furthermore, among convenient $n = mP \leq x$, all but $o(x)$ have $(\lambda(m), P-1) = s_w(P-1)$ (apply Lemma 5.3 with $q = 1$). It follows that $\sum_{n \leq x} \lambda(n)^{i\theta}$ is equal to

$$(6.1) \quad \sum_{\substack{m \leq x \\ L_m < x/m}} \lambda(m)^{i\theta} \sum_{\substack{d \text{ } w\text{-smooth} \\ 2 \nmid d}} \frac{1}{d^{i\theta}} \sum_{\substack{L_m < P \leq x/m \\ s_w(P-1)=d}} (P-1)^{i\theta},$$

up to an error of $o(x)$.

As in §5, the sum on P can be estimated using inclusion-exclusion:

$$\sum_{\substack{L_m < P \leq x/m \\ s_w(P-1)=d}} (P-1)^{i\theta} = \sum_{e \text{ } w\text{-smooth}} \mu(e) \sum_{\substack{P \equiv 1 \pmod{de} \\ L_m < P \leq x/m}} (P-1)^{i\theta}.$$

Summing by parts,

$$\sum_{\substack{P \equiv 1 \pmod{de} \\ L_m < P \leq x/m}} (P-1)^{i\theta} = I_m / \varphi(de) + O(\tilde{E}(x/m; de) \log x),$$

where

$$I_m := \int_{L_m}^{x/m} \frac{(t-1)^{i\theta}}{\log t} dt.$$

(Here and below, we allow implied constants to depend on the fixed parameter θ .) Plugging these estimates back into (6.1), the arguments of §5 will show that the accumulation of errors terms is, in total, $O(x/(\log x)^B)$, for any fixed B .

After simplifying the main terms (6.1) becomes, up to an error of $o(x)$,

$$W \sum_{\substack{m \leq x \\ L_m < x/m}} \lambda(m)^{i\theta} I_m \sum_{\substack{d \text{ } w\text{-smooth} \\ 2 \nmid d}} \frac{g(d_{\text{odd}})}{\varphi(d) d^{i\theta}},$$

with W and $g(d)$ as in (5.7). Grouping d sharing the same odd part d' transforms this last expression into

$$K_\theta W \sum_{\substack{m \leq x \\ L_m < x/m}} \lambda(m)^{i\theta} I_m \sum_{\substack{d' \text{ } w\text{-smooth} \\ 2 \nmid d'}} \frac{g(d')}{\varphi(d') d'^{i\theta}}, \quad \text{where} \quad K_\theta := \sum_{k \geq 1} \frac{1}{\varphi(2^k) \cdot 2^{ki\theta}}.$$

The sum on d' can be developed into an Euler product with the term associated to p of the form $1 + p^{-1-i\theta} + O(p^{-2})$, for each odd $p \leq w$; hence, that sum is $O(\exp(\Re \sum_{2 < p \leq w} p^{-1-i\theta}))$. By the prime number theorem with de la Vallée Poussin error and Abel summation, the series $\sum_p p^{-1-i\theta}$ converges. (A well-timed use of integration by parts is helpful in this calculation.) In particular, the partial sums of $p^{-1-i\theta}$ are $O(1)$ (cf. [CLPSR, Lemma 4.3]). Thus, our sum on d' is also $O(1)$.

Collecting estimates shows that $\sum_{n \leq x} \lambda(n)^{i\theta}$ is, up to an error of $o(x)$,

$$\ll W \sum_{\substack{m \leq x \\ L_m < x/m}} |I_m| \ll W \sum_{\substack{m \leq x \\ L_m < x/m}} \frac{x}{m \log(x/m)} \ll \frac{xW \sqrt{\log_3 x}}{\log x} \sum_{m \leq x} \frac{1}{m} \ll xW \sqrt{\log_3 x} \ll \frac{x}{\sqrt{\log_3 x}}.$$

This completes the proof of Theorem 1.3.

6.2. Proof of Theorem 1.4. We need two additional lemmas whose proofs are deferred momentarily. Throughout this section, all implied constants may depend on a .

Lemma 6.1. *Fix an integer a with $|a| > 1$. Among all convenient $n = mP \leq x$ with $(a, n) = 1$, all but $o(x)$ satisfy*

$$(\ell_a(m), \ell_a(P)) = s_w(\ell_a(P)).$$

Lemma 6.2 (conditional on GRH). *Fix an integer a with $|a| > 1$. Among all convenient $n = mP \leq x$ with $(a, n) = 1$, all but $o(x)$ are such that $(P-1)/\ell_a(P)$ is w -smooth.*

Fix $a \in \mathbb{Z}$ with $|a| > 1$. If $n \leq x$ is convenient with $(a, n) = 1$ and n satisfies the conclusions of both Lemmas 6.1 and 6.2, then

$$\ell_a(mP) = \text{lcm}[\ell_a(m), \ell_a(P)] = \ell_a(m) \cdot \frac{\ell_a(P)}{s_w(\ell_a(P))} = \ell_a(m) \cdot \frac{P-1}{s_w(P-1)}.$$

From Lemmas 5.2 (with $q = 1$), 6.1, and 6.2, we deduce that $\sum_{n \leq x, (n,a)=1} \ell_a(n)^{i\theta}$ coincides, up to an error of $o(x)$, with

$$(6.2) \quad \sum_{\substack{m \leq x \\ (m,a)=1 \\ L_m < x/m}} \ell_a(m)^{i\theta} \sum_{\substack{d \text{ } w\text{-smooth} \\ 2|d}} \frac{1}{d^{i\theta}} \sum_{\substack{L_m < P \leq x/m \\ s_w(P-1)=d}} (P-1)^{i\theta}.$$

This is nearly the same expression as (6.1); the only differences are that $\lambda(m)$ has been replaced by $\ell_a(m)$ and that m is now restricted to values coprime with a . It is straightforward to check that the method used to bound (6.1) still applies, so that (6.2) is $o(x)$ (in fact, $O(x/\sqrt{\log_3 x})$). Thus, it remains only to prove Lemmas 6.1 and 6.2.

For the proof of Lemma 6.1, we recall a result of Pappalardi on the frequency of primes p for which $\ell_a(p)$ is divisible by a given d .

Proposition 6.3. *Fix an integer a with $|a| > 1$. For all $x \geq 3$, and all positive integers d ,*

$$(6.3) \quad \#\{p \leq x : p \nmid a, d \mid \ell_a(p)\} = \beta_a(d) \frac{x}{\log x} + O\left(\tau(d)d \cdot x \left(\frac{(\log_2 x)^2}{\log x}\right)^{7/6}\right),$$

where $\beta_a(d)$ is a constant depending only on a and d , and

$$(6.4) \quad \beta_a(d) \asymp 1/d.$$

The estimate (6.3) is a special case of [Pap15, Theorem 1] while (6.4) is implicit in the exact expression for $\beta_a(d)$ obtained by Moree in [Mor05, Theorem 2]. We note that while the statement of Theorem 1 in [Pap15] requires that $x \rightarrow \infty$, the estimate (6.3) holds trivially for $x \geq 3$ that are bounded in terms of a .

Proposition 6.3 implies the following analogue of Lemma 2.3, which seems of independent interest.

Lemma 6.4. *Fix an integer a with $|a| > 1$. For each $x \geq 3$ and each positive integer d ,*

$$(6.5) \quad \sum_{\substack{p \leq x, p \nmid a \\ d \mid \ell_a(p)}} \frac{1}{p} = \beta_a(d) \log_2 x + O\left(\frac{\log(3d)}{\varphi(d)}\right),$$

where $\beta_a(d)$ is as in the statement of Proposition 6.3.

Lemma 6.4 is somewhat sharper than will be needed; it will suffice in our application that the O -term in (6.5) is $O(1)$.

Proof. First, observe that with $x_0 := \exp(2d^{30})$,

$$\sum_{\substack{p \leq x_0, p \nmid a \\ d \mid \ell_a(p)}} \frac{1}{p} \leq \sum_{\substack{p \leq x_0 \\ p \equiv 1 \pmod{d}}} \frac{1}{p} \ll \frac{\log_2 x_0}{\varphi(d)} \ll \frac{\log(3d)}{\varphi(d)}.$$

This implies (6.5) when $3 \leq x \leq x_0$ (keeping in mind that $\beta_a(d) \ll 1/d$). So we suppose now that $x > x_0$. Let $N(t)$ be the number of primes p up to t , not dividing a , for which $d \mid \ell_a(p)$. By Proposition 6.3,

$$\begin{aligned} \sum_{\substack{x_0 < p \leq x, p \nmid a \\ d \mid \ell_a(p)}} \frac{1}{p} &= \int_{x_0}^x \frac{1}{t} dN(t) = \beta_a(d) \int_{x_0}^x \frac{dt}{t \log t} \\ &\quad + O\left(\frac{\beta_a(d)}{\log x_0} + \tau(d)d \left(\frac{(\log_2 x_0)^2}{\log x_0}\right)^{7/6} + \tau(d)d \int_{x_0}^x \frac{1}{t} \left(\frac{(\log_2 t)^2}{\log t}\right)^{7/6} dt\right). \end{aligned}$$

The main term here has size $\beta_a(d)(\log_2 x - \log_2 x_0) = \beta_a(d) \log_2 x + O(\log(3d)/d)$. Since $\tau(d)d \leq d^2$ and $((\log_2 t)^2 / \log t)^{7/6} \ll (\log t)^{-11/10}$, the O -terms are

$$\ll \frac{1}{d \log x_0} + d^2 (\log x_0)^{-11/10} + d^2 \int_{x_0}^x t^{-1} (\log t)^{-11/10} dt \ll d^{-1}.$$

Collecting estimates gives the lemma. \square

Proof of Lemma 6.1. We claim all but $o(x)$ convenient $n \leq x$ having $(n, a) = 1$ satisfy

(ii') $\ell_a(m)$ is divisible by every positive integer $s \leq w' := \log_2 x / (\log_3 x)^2$,

(iii') $(\ell_a(m), \ell_a(P))$ has all prime factors at most $w'' := \log_2 x (\log_3 x)^2$, and

(iv') $\ell_a(P)$ has no prime factors in the interval $(w', w'']$.

Conditions (iii') and (iv') are implied by conditions (iii) and (iv) from the proof of Lemma 5.3, and so (from that proof, with $q = 1$) these two conditions admit only $o(x)$ exceptions. Turning to (ii'), fix a positive integer $s \leq w'$. If $s \nmid \ell_a(m)$, then there is no prime p dividing m for which $s \mid \ell_a(p)$. Hence,

$$\sum_m \frac{1}{m} \leq \prod_{\substack{p \leq x, p \nmid a \\ s \nmid \ell_a(p)}} \left(1 - \frac{1}{p}\right)^{-1} \ll \log x \prod_{\substack{p \leq x, p \nmid a \\ s \mid \ell_a(p)}} \left(1 - \frac{1}{p}\right) \ll (\log x) \exp(-\beta_a(s) \log_2 x).$$

Given m , the number of possible P is $O\left(\frac{x\sqrt{\log_3 x}}{m \log x}\right)$. It follows that the number of convenient $n \leq x$ with $(n, a) = 1$ and $s \nmid \ell_a(n)$ is

$$\ll (x\sqrt{\log_3 x}) \exp(-\beta_a(s) \log_2 x) \ll x \exp(-(\log_3 x)^{3/2}),$$

using in the last step that $\beta_a(s) \gg 1/s \gg 1/w'$. Summing on $s \leq w'$ shows that the number of exceptions to (ii') is $o(x)$.

We thus restrict to n satisfying all of (ii')–(iv'). By (iii') and (iv'), $(\ell_a(m), \ell_a(P))$ is a divisor of $s_w(\ell_a(P))$. If it is a proper divisor, then there is a prime power p^k with $p \leq w'$ such that $p^k \mid \ell_a(P)$ but $p^k \nmid \ell_a(m)$. By (ii'), it must be that $k > 1$. Since $s \mid \ell_a(P) \mid P - 1$, we deduce that $P - 1$ is divisible by a proper prime power $s > w'$. The number of convenient n of this kind is shown to be $o(x)$ in the paragraph concluding the proof of Lemma 5.3 (read now with $q = 1$). \square

Lemma 6.2 is very close in character to Li and Pomerance's Proposition 1 in [LP03] and admits a nearly identical proof. The next three results are taken from [LP03].

Lemma 6.5. *Fix an integer a with $|a| > 1$. For all $x \geq 100$, the number of integers $n \leq x$ divisible by a prime $p > w$ with $\ell_a(p) < p^{1/2}/\log p$ is $\ll x/\log_3 x$.*

Lemma 6.6. *Let r be a prime. For all $x \geq 3$, the number of integers $n \leq x$ divisible by a prime $p \equiv 1 \pmod{r}$ with*

$$\frac{r^2}{4(\log r)^2} < p \leq r^2(\log r)^4$$

is $\ll x(\log_2(2r))/r \log r$.

Lemma 6.7 (GRH-conditional). *Suppose that r is an odd prime and that a is not an r th power. Let A_r denote the set of primes $p \equiv 1 \pmod{r}$ with $a^{(p-1)/r} \equiv 1 \pmod{p}$. For $x \geq 3$, the number of $n \leq x$ divisible by a prime $p \in A_r$ with $p \geq r^2(\log r)^4$ is $\ll x/r \log r + x \log_2 x/r^2$.*

Lemma 6.5 is the special case of [LP03, Lemma 1] where $\psi(x) = \log_2 x$. Lemmas 6.6 and 6.7 are restatements of Lemmas 2 and 3 of [LP03], respectively.

Proof of Lemma 6.2 (following the proof of Proposition 1 in [LP03]). Suppose that $(P-1)/\ell_a(P)$ has a prime factor $r > w$. Then $P \equiv 1 \pmod{r}$ and $\ell_a(P) \mid (P-1)/r$, so that $a^{(P-1)/r} \equiv 1 \pmod{P}$. Hence, P is a prime factor of n belonging to the set A_r from Lemma 6.7.

Thus, it is enough to show that only $o(x)$ positive integers $n \leq x$ have a prime factor p from any of the sets A_r , where $r > w$ is prime. We can assume by Lemma 6.5 that $\ell_a(p) > p^{1/2}/\log p$. Since $\ell_a(p) \leq \frac{p-1}{r}$, we must have $p > \frac{r^2}{4(\log r)^2}$. Noting that a cannot be an r th power (once x is large), Lemmas 6.6 and 6.7 put the remaining n in a set of size

$$\ll x \sum_{\substack{r > w \\ r \text{ prime}}} \left(\frac{\log_2 r}{r \log r} + \frac{\log_2 x}{r^2} \right) \ll x \frac{\log_4 x}{\log_3 x},$$

which is $o(x)$. \square

ACKNOWLEDGEMENTS

The author is supported by NSF award DMS-2001581. He thanks the referee for a careful reading of the manuscript.

REFERENCES

- [Car19] R. D. Carmichael, *On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$* , Amer. Math. Monthly **26** (1919), 137–146.
- [CEP83] E. R. Canfield, P. Erdős, and C. Pomerance, *On a problem of Oppenheim concerning “factorisatio numerorum”*, J. Number Theory **17** (1983), 1–28.
- [CLPSR] V. Chandee, X. Li, P. Pollack, and A. Singha Roy, *On Benford’s law for multiplicative functions*, submitted.
- [Del69] H. Delange, *On integral-valued additive functions*, J. Number Theory **1** (1969), 419–430.
- [Dia77] P. Diaconis, *The distribution of leading digits and uniform distribution mod 1*, Ann. Probability **5** (1977), 72–81.
- [ELP08] P. Erdős, F. Luca, and C. Pomerance, *On the proportion of numbers coprime to a given integer*, Anatomy of integers, CRM Proc. Lecture Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008, pp. 47–64.
- [EPS91] P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael’s lambda function*, Acta Arith. **58** (1991), 363–385.
- [Kou19] D. Koukoulopoulos, *The distribution of prime numbers*, Graduate Studies in Mathematics, vol. 203, American Mathematical Society, Providence, RI, 2019.
- [LP03] S. Li and C. Pomerance, *On generalizing Artin’s conjecture on primitive roots to composite moduli*, J. Reine Angew. Math. **556** (2003), 205–224.
- [Mor05] P. Moree, *On primes p for which d divides $\text{ord}_p(g)$* , Funct. Approx. Comment. Math. **33** (2005), 85–95.
- [Nar84] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Mathematics, vol. 1087, Springer-Verlag, Berlin, 1984.
- [Nar67] ———, *On distribution of values of multiplicative functions in residue classes*, Acta Arith. **12** (1966/67), 269–279.
- [Nor76] K. K. Norton, *On the number of restricted prime factors of an integer. I*, Illinois J. Math. **20** (1976), 681–705.
- [Pap15] F. Pappalardi, *Divisibility of reduction in groups of rational numbers*, Math. Comp. **84** (2015), 385–407.
- [Pom77] C. Pomerance, *On the distribution of amicable numbers*, J. Reine Angew. Math. **293(294)** (1977), 217–222.
- [PSR] P. Pollack and A. Singha Roy, *Distribution in coprime residue classes of polynomially-defined multiplicative functions*, Math. Z., to appear.
- [Sco84] E. J. Scourfield, *Uniform estimates for certain multiplicative properties*, Monatsh. Math. **97** (1984), 233–247.
- [Ten15] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, third ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602

Email address: pollack@uga.edu