SIEVING VERY THIN SETS OF PRIMES, AND PRATT TREES WITH MISSING PRIMES

KEVIN FORD

Dedicated to the memory of Paul T. Bateman

ABSTRACT. Suppose $\mathcal{P}$ is a set of primes, such that for every $p \in \mathcal{P}$, every prime factor of $p-1$ is also in $\mathcal{P}$. We apply a new sieve method to show that either $\mathcal{P}$ contains all of the primes or the counting function of $\mathcal{P}$ is $O(x^{1-c})$ for some $c > 0$, where c depends only on the smallest prime not in $\mathcal{P}$. Our proof makes use of results connected with Artin's primitive root conjecture.

1 Introduction

Consider a set $\mathcal{P}$ of primes satisfying the condition:

$$p \in \mathcal{P} \implies \forall q | (p-1), q \in \mathcal{P}. \tag{1.1}$$

Here and throughout, the letters p, q and r denote primes. Trivial examples of sets $\mathcal{P}$ are the empty set and the set of all primes.

We are concerned in this note with nontrivial examples, that is, nonempty $\mathcal{P}$ omitting at least one prime (since $2 \notin \mathcal{P}$ implies that $\mathcal{P}$ is empty, the smallest omitted prime must be odd). Let p_0 denote the smallest prime *not* in $\mathcal{P}$ and let $P(x) = \#\{p \in \mathcal{P} : p \leqslant x\}$ be the associated counting function. Our main result is the following.

Theorem 1. *Let $\mathcal{P}$ be a set of primes satisfying* (1.1) *that does not contain the prime p_0. There are constants $\delta > 0$ and $c > 0$, depending only on p_0, such that $P(x) \leqslant cx^{1-\delta}$.*

Theorem 1 implies that either $\mathcal{P}$ is the set of all primes or $\mathcal{P}$ is a very "thin" set of primes. The elements of $\mathcal{P}$ have the property that for every prime $p \notin \mathcal{P}$, $\mathcal{P}$ omits the residue classes $0, 1 \mod p$. Standard application of sieve methods produce only the much weaker bound $P(x) \ll x/\log^2 x$ (see Proposition 1 below). The weakness stems from the fact that sieve methods ignore congruential restrictions for "large" primes (i.e., those primes $> \sqrt{x}$, when bounding the number of elements of a set that are $\leqslant x$). With our new method, we are able exploit these large prime restrictions.

To the author's knowledge, sets of primes satisfying (1.1) were first considered by R. D. Carmichael [2, 3] in his work on the conjecture that now bears his name. Here ϕ is Euler's "totient" function.

Conjecture 1 (Carmichael's Conjecture)**.** *For every positive integer a, there is a positive integer $b \neq a$ such that $\phi(b) = \phi(a)$.*

The conjecture remains open, although the smallest counterexample a, if there is one, is known to exceed $10^{10^{10}}$ [6]. Assuming a counterexample a exists, Carmichael [3] attacked the problem with the following simple result.

$$\text{If } d\prod_{p|d} p \text{ divides } a \text{ and } p = 1 + d \text{ is prime, then } p^2 | a. \tag{1.2}$$

Date: February 21, 2013.

Applying (1.2) successively with $d = 1, 2, 6$ and 42, it follows immediately that $2^2 3^2 7^2 43^2 | a$. From here, Carmichael considers two cases: (i) $3^2 \| a$, which easily implies $13^2 | a$, and (ii) $3^3 | a$, which implies by (1.2) that $19^2 | a$. In each case, one can use (1.2) to produce many more primes which divide a. More precisely, in case (i), a must be divisible by all primes in $\mathcal{P}'$, where $\mathcal{P}'$ contains $2, 3, 7, 13, 43$ and for other primes p, $p \in \mathcal{P}'$ if and only if $p-1$ is squarefree and for every $q|(p-1)$, $q \in \mathcal{P}'$. Then $\mathcal{P}' = \{2, 3, 7, 13, 43, 79, 547, 3319, 6163, \dots\}$. Similarly, in case (ii), a is divisible by every prime in $\mathcal{P}''$, where $2, 3, 7, 19, 43$ are in $\mathcal{P}''$ and for other primes p, $p \in \mathcal{P}''$ if and only if (a) $p-1$ is either squarefree or $3^2 | (p-1)$ and $\frac{p-1}{9}$ is squarefree and (b) for every $q|(p-1)$, $q \in \mathcal{P}''$. Then $\mathcal{P}'' = \{2, 3, 7, 19, 43, 127, 2287, 4903, 5419, \dots\}$. Thus, the sets $\mathcal{P}'$ and $\mathcal{P}''$ each satisfy (1.1) and omit the prime 5. By Theorem 1, each of $\mathcal{P}'$ and $\mathcal{P}''$ has counting function satisfying $P(x) \ll x^{1-c}$ for some $c > 0$. Carmichael's conjecture follows if both $\mathcal{P}'$ and $\mathcal{P}''$ are infinite.

In a similar spirit, Pomerance [15] showed that if x satisfies $p^2 | x$ whenever $(p-1) | \phi(x)$, then there is no number $b \neq x$ with $\phi(b) = \phi(x)$. However, Pomerance argued heuristically that no x with this property exists.

Sets satisfying (1.1) also arise in the distribution of iterates of Euler's function. Let $\phi_k(n)$ denote the k-th iterate of ϕ (e.g., $\phi_2(n) = \phi(\phi(n))$), and let $F(n) = \prod_{k \geqslant 1} \phi_k(n)$ (the product is finite, since $\phi_k(n) = 1$ for large k). Divisibility properties of $F(n)$ were considered by Luca and Pomerance [13] in connection with construction of irreducible, radical extensions of $\mathbb{Q}$. The prime factors of $F(p)$, where p runs over the primes, were considered by Bayless [1]. Further results on $\phi_k(n)$ may be found in [4].

Corollary 1. *For every prime $r \geqslant 3$, there is a constant $s < 1$ so that $\#\{n \leqslant x : r \nmid F(n)\} \ll x^s$.*

Proof. Let $\mathcal{P}_r$ be the largest set satisfying (1.1) such that $r \notin \mathcal{P}_r$; i.e., $\mathcal{P}_r$ contains all primes less than r, $r \notin \mathcal{P}_r$ and a prime $p > r$ lies in $\mathcal{P}_r$ if and only if for all $q|(p-1)$, $q \in \mathcal{P}_r$. For example,

$$\mathcal{P}_3 = \{2, 5, 11, 17, 23, 41, 43, 83, 89, 101, 137, 167, 179, 251, 257, \dots\},$$
$$\mathcal{P}_5 = \{2, 3, 7, 13, 17, 19, 29, 37, 43, 53, 59, 73, 79, 97, 103, \dots\}.$$

Since $\phi(p^a) = p^{a-1}(p-1)$, for each n the (finite) set $\mathcal{P}$ of prime factors of $F(n)$ satisfies (1.1). Hence, if $r \nmid F(n)$, then all the prime factors of n belong to $\mathcal{P}_r$. By Theorem 1, for some $c > 0$, depending on r, there are $\ll x^{1-c}$ primes in $\mathcal{P}_r$ that are less than x. For any $s > 1 - c$, it follows by partial summation that the number of $n \leqslant x$ with $r \nmid F(n)$ is at most

$$\sum_{p|n \Longrightarrow p \in \mathcal{P}_r} \left(\frac{x}{n}\right)^s = x^s \prod_{p \in \mathcal{P}_r} \left(1 - p^{-s}\right)^{-1} \leqslant x^s \exp\Big\{ \sum_{p \in \mathcal{P}_r} \frac{1}{p^s - 1} \Big\} \ll_{r,s} x^s. \qquad \square$$

The set $\mathcal{P}_r$ is also the set of all primes p for which the *Pratt tree* for p has no node labeled r. The Pratt tree for a prime p is recursively defined as the tree with root labeled p, and below p are links to the Pratt trees of each $q|(p-1)$. Properties of Pratt trees (e.g. the distribution of the height $H(p)$, number of nodes, etc.) were extensively studied in [7]. In alternative terminology, $\mathcal{P}_r$ is the set of primes p for which there is no *prime chain* $r \prec p_0 \prec \cdots \prec p_k \prec p$, where $a \prec b$ means $b \equiv 1 \pmod{a}$, and $p_0, \dots, p_k$ are primes.

A finite group G is said to have Perfect Order Subsets (POS) if the *number* of elements of G of any given order divides $|G|$. This notion was introduced by Finch and Jones [5] in 2002. In the case of Abelian groups, Finch and Jones reduced the problem of determining which groups have POS to studying those of the form $G = (\mathbb{Z}/p_1\mathbb{Z})^{a_1} \times \cdots \times (\mathbb{Z}/p_j\mathbb{Z})^{a_j}$, where $p_1, \dots, p_j$ are distinct primes. This group has POS if and only if $f(n)|n$, where $n = p_1^{a_1} \cdots p_j^{a_j} = |G|$ and $f(n) = \prod_{p^a \| n}(p^a - 1)$. Suppose that $3 \nmid n$. It follows quickly that the primes dividing n must lie in $\mathcal{P}_3$. Developing explicit estimates for the counting function of $\mathcal{P}_3$, it was shown in [8] that an Abelian group with POS is either $\mathbb{Z}/2\mathbb{Z}$ or has order divisible by 3. This answered a question posed in [5].

It is intractible with existing methods to prove nontrivial lower bounds for $P(x)$ even in the "easiest" cases when $\mathcal{P} = \mathcal{P}_r$. The difficulty, now evident from Theorem 1, is to show that many primes exist with the prime factors of $p-1$ restricted to a very thin set.

Conjecture 2. *Each set $\mathcal{P}_r$ is infinite.*

This conjecture follows, for instance, if there are infinitely many primes of the form $2^a 3^b + 1$ and infinitely many primes of the form $2^a 5^b + 1$. Each of these latter statements appears to be plausible, based on computations.

The author computed the elements of $\mathcal{P}_3$ up to 2^{44} ($\approx 1.7 \times 10^{13}$) for use in [8], and $P(x) \approx x^{0.62}$ in this range. The recursive nature of the sets $\mathcal{P}$, however, does not lead to any natural heuristic argument for the size of $P(x)$. The growth appears to be highly dependent on which small primes are omitted from the set. For an extreme example, consider $\mathcal{P}$ to be the "largest " set omitting the primes $3, 5, 17, 257, 65537$ (the list of known Fermat primes – primes that are 1 more than a power of 2). It is a famous unsolved problem whether or not there are additional Fermat primes. If there are no further Fermat primes then $\mathcal{P} = \{2\}$, while if another Fermat prime exists then $\mathcal{P}$ could potentially be infinite.

Based partly on the computations for $\mathcal{P}_3$, we make an educated guess for the growth of $P(x)$.

Conjecture 3. *For each r, there is a number $\delta_r > 0$ such that $P(x) = x^{1-\delta_r+o(1)}$ as $x \to \infty$.*

We further guess that $\delta_r \to 0$ as $r \to \infty$.

Outline of the paper. The next section contains relatively simple estimates for $P(x)$ which are needed to bootstrap the more complicated iterative method in Sections 3 and 4. Basically, we find recursive inequalities for the density of primes whose Pratt tree has height $\leqslant j$, for $j = 0, 1, 2, \ldots$. The main iteration inequalities are proved in Section 3, together with a conditional result that implies Theorem 1 under the assumption that a certain matrix has eigenvalues all inside the unit circle. Section 4 concludes the proof of Theorem 1 by showing that indeed the matrix has this property. Our method uses results from the circle of ideas used to attack Artin's primitive root conjecture.

2 Simple sieve estimates

From now on, we always assume that $\mathcal{P}$ is a set of primes satisfying (1.1) and that there is some prime not in $\mathcal{P}$, the smallest such we denote by p_0. All estimates using the Landau $O-$symbol and Vinogradov $\ll$ $-$symbol may depend on p_0, but not on any other quantity. The symbols p an q, with or without subscripts, always denote primes.

Proposition 1. *We have $P(x) \ll x/\log^2 x$ and $\displaystyle\sum_{p\in\mathcal{P}} \frac{1}{p} \ll 1$.*

Proof. By (1.1) and standard application of sieve methods [10, Theorem 4.2],

$$P(x) \ll \frac{x}{\log x} \prod_{\substack{q\leqslant x^{1/4}\\ q\notin\mathcal{P}}} \left(1 - \frac{1}{q}\right). \tag{2.1}$$

Since $\mathcal{P}$ omits all primes $q \equiv 1 \pmod{p_0}$, (2.1) and Mertens' estimate for primes in arithmetic progressions imply that

$$P(x) \ll \frac{x}{(\log x)^{1+1/(p_0-1)}}.$$

By partial summation, $\sum_{p\in\mathcal{P}} 1/p \ll 1$ and thus $\prod_{p\in\mathcal{P}}(1-1/p) \gg 1$. Applying (2.1) again and Mertens' bound, we find that $P(x) \ll x/\log^2 x$. □

Our proof of Theorem 1 requires a slight improvement to Proposition 1 to bootstrap the method.

Lemma 2.1. *We have* $P(x) \ll x(\log x)^{-5/2}$.

Proof. For $p \in \mathcal{P}$ with $p \leqslant x$, let q be the largest prime factor of $p-1$, write $p = 1+qm$ and define $y = x^{1/(10\log\log x)}$. By standard counts of smooth numbers (see e.g., Theorem 1 in §III.5 of [16]), the number of p with $q \leqslant y$ is $\ll x/\log^5 x$. Next, fix $m \leqslant x/y$, and observe that $q \not\equiv 1 \pmod r$ for each prime $r \notin \mathcal{P}$. By sieve methods [10, Theorem 4.2] and Proposition 1, the number of $p \leqslant x$ is bounded above by

$$\begin{aligned}\#\{n \leqslant x/m : \forall r \notin \mathcal{P}, r \nmid n(n+1)(mn+1)\} &\ll \frac{x/m}{\log^3(x/m)} \prod_{p \mid m(m+1)} \left(1-\frac{1}{p}\right)^{-1} \\ &\leqslant \frac{x/m}{\log^3(x/y)} \frac{m^2+m}{\phi(m^2+m)} \\ &\ll \frac{x(\log\log x)^4}{m\log^3 x}.\end{aligned}$$

Since m is composed of prime factors in $\mathcal{P}$, Proposition 1 implies

$$\sum_m \frac{1}{m} \leqslant \prod_{p\in\mathcal{P}} \left(1-\frac{1}{p}\right)^{-1} \ll 1.$$

The claimed bound follows. □

3 The main iteration

The proof of Theorem 1 is based on recursive inequalities for sums over subsets of $\mathcal{P}$. We partition the primes $p \in \mathcal{P}$ according to the height $H(p)$ of their Pratt trees. The height may be defined iteratively by

$$H(2) = 1, \qquad H(p) = 1 + \max_{q \mid (p-1)} H(q).$$

We denote

$$\mathcal{P}_h = \{p \in \mathcal{P} : H(p) \leqslant h\} \qquad (h \in \mathbb{N})$$

and also define, for $h \in \mathbb{N}$ and real $s > 0$,

$$V_h(s) = \sum_{p\in\mathcal{P}_h} \frac{1}{(p-1)^s}, \qquad T_h = \{n \in \mathbb{N} : p \mid n \implies p \in \mathcal{P}_h\}.$$

We also allow $h = \infty$ in the above notations. In particular, $\mathcal{P}_1 = \{2\}$ and $\mathcal{P}_\infty = \mathcal{P}$. A trivial, but very useful observation, is that

$$p \in \mathcal{P}_h \implies p-1 \in T_{h-1}. \tag{3.1}$$

Our goal is to show that $V_\infty(s)$ is finite for some $s < 1$, which is clearly equivalent to Theorem 1.

A trivial bound which we will use often is

$$\sum_{a=1}^\infty \frac{1}{q^{as}} = \frac{1}{q^s-1} \leqslant \frac{\lambda(s)}{(q-1)^s}, \quad \lambda(s) = \frac{1}{2^s-1} \qquad (0 < s \leqslant 1). \tag{3.2}$$

Lemma 3.1. *For every* $h \geqslant 1$, $V_h(s)$ *is continuous for* $0 < s \leqslant 1$.

Proof. It suffices to show that $V_h(s)$ is finite. This follows by induction on h, starting from $V_1(s) = 1$ for all s, and using (3.1) and (3.2) to obtain the iterative bound

$$\begin{aligned} V_h(s) &\leqslant \sum_{m\in T_{h-1}} \frac{1}{m^s} = \prod_{p\in\mathcal{P}_{h-1}} \frac{1}{1-p^{-s}} = \prod_{p\in\mathcal{P}_{h-1}} \left(1+\frac{1}{p^s-1}\right) \\ &\leqslant \prod_{p\in\mathcal{P}_{h-1}} \left(1+\frac{\lambda(s)}{(p-1)^s}\right) \leqslant \mathrm{e}^{\lambda(s)V_{h-1}(s)}. \end{aligned} \tag{3.3}$$

We next develop more sophisticated bounds for $V_h(s)$ in terms of $V_{h-1}(s)$. It turns out that when s is close to 1, $V_h(s)$ is dominated by primes $p \in \mathcal{P}_h$ for which $p-1$ has only a single "large" prime factor (meaning a prime q with large height $H(q)$). For $k > j \geqslant 1$, denote

$$\begin{aligned} \widetilde{T}_{j,k} &= \{n \in T_k \setminus T_j : p^2|n \text{ for some } p \in \mathcal{P}_k \setminus \mathcal{P}_j, \text{ or } n \text{ has at least 2 prime factors in } \mathcal{P}_k \setminus \mathcal{P}_j\}, \\ \overline{T}_{j,k} &= (T_k \setminus T_j) \setminus \widetilde{T}_{j,k}. \end{aligned}$$

Lemma 3.2. *For $k > j \geqslant 1$ and $s > 0$, we have*

$$\sum_{n\in\widetilde{T}_{j,k}} \frac{1}{n^s} \leqslant 2\lambda(s)^2 \left(V_k(s) - V_j(s)\right)^2 e^{\lambda(s)V_k(s)}.$$

Proof. For $n \in \widetilde{T}_{j,k}$, let $q_1, \ldots, q_d$ be the prime factors of n that are in $\mathcal{P}_k \setminus \mathcal{P}_j$ ("large" prime factors). Then $n = q_1^{a_1} \cdots q_d^{a_d} m$, where $m \in T_j$ and $a_1, \ldots, a_d$ are positive integers. Also, either (i) $d \geqslant 2$ or (ii) $d = 1$ and $q_1^2|n$. We deduce that

$$\sum_{n\in\widetilde{T}_{j,k}} \frac{1}{n^s} \leqslant \left[\sum_{q\in\mathcal{P}_k\setminus\mathcal{P}_j} \sum_{a=2}^{\infty} \frac{1}{q^{as}} + \sum_{d=2}^{\infty} \frac{1}{d!} \left(\sum_{q\in\mathcal{P}_k\setminus\mathcal{P}_j} \sum_{a=1}^{\infty} \frac{1}{q^{as}}\right)^d\right] \sum_{m\in T_j} \frac{1}{m^s}.$$

Using (3.2) multiple times, we see that the first double sum on the right side is at most

$$\sum_{q\in\mathcal{P}_k\setminus\mathcal{P}_j} \frac{1}{q^s(q^s-1)} \leqslant \sum_{q\in\mathcal{P}_k\setminus\mathcal{P}_j} \frac{\lambda(s)}{(q-1)^{2s}} \leqslant \lambda(s)\left(V_k(s) - V_j(s)\right)^2,$$

the second double sum over q and a is at most

$$\sum_{q\in\mathcal{P}_k\setminus\mathcal{P}_j} \frac{\lambda(s)}{(q-1)^s} = \lambda(s)\left(V_k(s) - V_j(s)\right),$$

and the sum on m is bounded above by

$$\prod_{p\in\mathcal{P}_j} (1-1/p^s)^{-1} \leqslant \mathrm{e}^{\lambda(s)V_j(s)}.$$

Thus,

$$\sum_{n\in\widetilde{T}_{j,k}} \frac{1}{n^s} \leqslant \mathrm{e}^{\lambda(s)V_j(s)} \left(V_k(s) - V_j(s)\right)^2 \left[\lambda(s) + \lambda(s)^2 \sum_{d=2}^{\infty} \frac{\left(V_k(s) - V_j(s)\right)^{d-2} \lambda(s)^{d-2}}{d!}\right].$$

Finally, $d! > (d-2)!$ and so the sum on d is less than $\mathrm{e}^{\lambda(s)(V_k(s)-V_j(s))}$. □

We now come to the main iteration inequality. Instead of descending just one level as in the proof of Lemma 3.1 (that is, examining the prime factors of $p-1$), we descend a finite (and bounded) number of levels, examining the prime factors q_1 of $p-1$, the prime factors q_2 of each q_1-1, etc. To state our result, we introduce a family of matrices $M_{s,j,Q}$. Let

$$U_Q = \{1 \leqslant n \leqslant Q : (n,Q)=1 \text{ and } \forall p|Q \text{ such that } p \notin \mathcal{P}, n \not\equiv 1 \pmod p\}. \tag{3.4}$$

By (1.1), for any Q and $p \in \mathcal{P}$ with $p \nmid Q$, we have $p \mod Q \in U_Q$. For $j \geqslant 1$, $s>0$ and $Q \in \mathbb{N}$, let $M_{s,j,Q}$ be the $Q \times Q$ matrix whose entries are given by

$$M_{s,j,Q}(a,b) = \sum_{\substack{m \in T_j \\ am \equiv b \pmod Q}} m^{-s} \tag{3.5}$$

if $a \in U_Q$ and $b \in U_Q$, and $M_{s,j,Q}(a,b)=0$ otherwise. For a generic square matrix M with non-negative entries, we introduce notation for row sums and column sums:

$$R_a(M) = \sum_b M(a,b), \quad R(M) = \max_a R_a(M), \qquad C_b(M) = \sum_a M(a,b), \quad C(M) = \max_b C_b(M).$$

Lemma 3.3. *Suppose that $n \in \mathbb{N}$, $h > j \geqslant n$, $Q \in \mathbb{N}$ and $\mathcal{P}_{j-n}$ contains every prime in $\mathcal{P}$ which divides Q. Then, for $M = M_{s,j,Q}$,*

$$V_h(s) \leqslant V_j(s) + \sum_{q \in \mathcal{P}_{h-n} \setminus \mathcal{P}_{j-n}} \frac{R_{q \bmod Q}(M^n)}{q^s} + 2n\lambda(s)^2 e^{n\lambda(s)V_{h-1}(s)} \left(V_{h-1}(s) - V_{j-n}(s)\right)^2.$$

Proof. We'll first show, by induction on n, that for any integers h and j satisfying $h > j \geqslant n$,

$$\begin{aligned} V_h(s) \leqslant V_j(s) &+ 2n\lambda(s)^2 \mathrm{e}^{n\lambda(s)V_{h-1}(s)} \left(V_{h-1}(s) - V_{j-n}(s)\right)^2 \\ &+ \sum_{q_n \in \mathcal{P}_{h-n} \setminus \mathcal{P}_{j-n}} \frac{1}{q_n^s} \sum_{\substack{m_n \in T_{j-n} \\ m_n q_n + 1 = q_{n-1} \\ q_{n-1} \text{ prime}}} \frac{1}{m_n^s} \sum_{\substack{m_{n-1} \in T_{j-n+1} \\ m_{n-1} q_{n-1} + 1 = q_{n-2} \\ q_{n-2} \text{ prime}}} \frac{1}{m_{n-1}^s} \cdots \sum_{\substack{m_1 \in T_{j-1} \\ m_1 q_1 + 1 = q_0 \\ q_0 \text{ prime}}} \frac{1}{m_1^s}. \end{aligned} \tag{3.6}$$

To begin the induction, we use (3.1) and Lemma 3.2 to obtain

$$\begin{aligned} V_h(s) &= V_j(s) + \sum_{q_0 - 1 \in T_{h-1} \setminus T_{j-1}} \frac{1}{(q_0-1)^s} \\ &\leqslant V_j(s) + 2\lambda(s)^2 \mathrm{e}^{\lambda(s)V_{h-1}(s)} \left(V_{h-1}(s) - V_{j-1}(s)\right)^2 + \sum_{q_0 - 1 \in \overline{T}_{j-1,h-1}} \frac{1}{(q_0-1)^s}. \end{aligned}$$

In the final sum, we may write $q_0 = 1 + m_1 q_1$, where $m_1 \in T_{j-1}$ and $q_1 \in \mathcal{P}_{h-1} \setminus \mathcal{P}_{j-1}$. This proves (3.6) when $n=1$.

Now suppose that (3.6) holds for some n, and assume that $h > j \geqslant n+1$. In the multiple sum in (3.6), replace q_n^{-s} with $(q_n-1)^{-s}$ and observe that $q_n - 1 \in T_{h-n-1} \setminus T_{j-n-1}$. The contribution to the multiple sum from those summands with $q_n - 1 \in \widetilde{T}_{j-n-1,h-n-1}$ is, by Lemma 3.2 and (3.3), at most

$$\begin{aligned} &2\lambda(s)^2 \mathrm{e}^{\lambda(s)V_{h-n-1}(s)} \left(V_{h-n-1}(s) - V_{j-n-1}(s)\right)^2 \sum_{m_n \in T_{j-n}} m_n^{-s} \cdots \sum_{m_1 \in T_{j-1}} m_1^{-s} \\ &\leqslant 2\lambda(s)^2 \mathrm{e}^{\lambda(s)V_{h-1}(s)} \left(V_{h-1}(s) - V_{j-n-1}(s)\right)^2 \mathrm{e}^{\lambda(s)(V_{j-n}(s) + \cdots + V_{j-1}(s))} \\ &\leqslant 2\lambda(s)^2 \mathrm{e}^{\lambda(s)(n+1)V_{h-1}(s)} \left(V_{h-1}(s) - V_{j-n-1}(s)\right)^2. \end{aligned}$$

If $q_n - 1 \in \overline{T}_{j-n-1,h-n-1}$, then $q_n = 1 + q_{n+1}m_{n+1}$, where $q_{n+1} \in \mathcal{P}_{h-n-1} \setminus \mathcal{P}_{j-n-1}$ and $m_{n+1} \in T_{j-n-1}$. This proves (3.6) with n replaced by $n+1$. By induction, (3.6) follows for all n.

In (3.6), we enlarge the range of all sums on m_i to $m_i \in T_{j-1}$. Also, for $0 \leqslant i \leqslant n-1$, we relax the condition that q_i is prime to $q_i \equiv a_i \pmod{Q}$, where $a_i \in U_Q$. Recalling (3.5), we find that the multiple sum in (3.6) is at most

$$\begin{aligned}
&\sum_{q_n \in \mathcal{P}_{h-n} \setminus \mathcal{P}_{j-n}} q_n^{-s} \sum_{a_{n-1} \in U_Q} \sum_{\substack{m_n \in T_{j-1} \\ m_n q_n + 1 \equiv a_{n-1} \pmod{Q}}} m_n^{-s} \cdots \sum_{a_0 \in U_Q} \sum_{\substack{m_1 \in T_{j-1} \\ m_1 a_1 + 1 \equiv a_0 \pmod{Q}}} m_1^{-s} \\
&= \sum_{q_n \in \mathcal{P}_{h-n} \setminus \mathcal{P}_{j-n}} q_n^{-s} \sum_{a_{n-1}, \ldots, a_0 \in U_Q} M(q_n \bmod Q, a_{n-1}) M(a_{n-1}, a_{n-2}) \cdots M(a_1, a_0) \\
&= \sum_{q_n \in \mathcal{P}_{h-n} \setminus \mathcal{P}_{j-n}} q_n^{-s} R_{q_n \bmod Q}(M^n).
\end{aligned}$$

This completes the proof of the lemma. □

Assuming $V_\infty(s)$ exists and h and j are large, $V_{h-1}(s) - V_{j-n}(s)$ will be very small if j is large. Consequently, of the three terms on the right side of the inequality in Lemma 3.3, the third may be regarded as "small", since it is quadratic in $V_{h-1}(s) - V_{j-n}(s)$. The second term is at most $(V_{h-1}(s) - V_{j-n}(s))R(M^n)$, and can be regarded as larger than the third term. It can also be made very small, provided that M is a contracting matrix (all eigenvalues lie inside the unit circle) and n is large enough. Under this assumption on M, it follows that

$$V_h(s) \leqslant V_j(s) + (V_{h-1}(s) - V_{j-n}(s))\varepsilon,$$

where ε is small. Iteration of this inequality, with j and n fixed, then shows that the sequence $V_0(s), V_1(s), \ldots$ is bounded. The next lemma makes this heuristic precise.

Lemma 3.4. *Suppose that for some y and for $Q = \prod_{p \leqslant y} p$, $M_{1,\infty,Q}$ is a contracting matrix. Then for some $s < 1$, $V_\infty(s)$ is finite.*

Proof. By assumption, $R(M_{1,\infty,Q}^n) \leqslant \frac{1}{4}$ for some n. Let $D = V_\infty(1)$ (D exists by Proposition 1) and let

$$\varepsilon = \frac{1}{100n\mathrm{e}^{2n(D+2)}}.$$

Fix j large enough so that $j > n$, $\mathcal{P}_{j-n}$ contains all primes in $\mathcal{P}$ which are $\leqslant y$, and $V_j(1) - V_{j-n}(1) \leqslant \varepsilon/2$. By Lemma 3.1, $V_j(s)$ and $V_{j-n}(s)$ are continuous for $0 < s \leqslant 1$, as are all entries of $M_{s,j,Q}$. Note that $R(M_{1,j,Q}^n) \leqslant R(M_{1,\infty,Q}^n) \leqslant \frac{1}{4}$. Therefore, there is an $s \in [0.9, 1)$ such that

(a) $V_j(s) \leqslant D + 1$,
(b) $V_j(s) - V_{j-n}(s) \leqslant \varepsilon$,
(c) $R(M_{s,j,Q}^n) \leqslant \frac{1}{3}$.

Since $s \geqslant 0.9$, we have $\lambda(s) \leqslant 2$. By Lemma 3.3 and (c), for any $h > j$, it follows that

$$V_h(s) \leqslant V_j(s) + \frac{1}{3}\left(V_{h-1}(s) - V_{j-n}(s)\right) + 8n\mathrm{e}^{2nV_{h-1}(s)}\left(V_{h-1}(s) - V_{j-n}(s)\right)^2.$$

For $k \geqslant 0$, let $x_k = V_{j+k}(s) - V_j(s)$. Then $x_0 = 0$ and, by (a) and (b), for $k \geqslant 1$ we have

$$\begin{aligned}
x_k &\leqslant \frac{1}{3}(x_{k-1} + V_j(s) - V_{j-n}(s)) + 8n\mathrm{e}^{2n(x_{k-1}+V_j(s))}\left(x_{k-1} + V_j(s) - V_{j-n}(s)\right)^2 \\
&\leqslant \frac{1}{3}(x_{k-1} + \varepsilon) + 8n\mathrm{e}^{2n(D+1+x_{k-1})}(x_{k-1} + \varepsilon)^2 =: f(x_{k-1}).
\end{aligned}$$

We have $f(0) > 0$, $f''(x) > 0$ for $x > 0$ and

$$f(\varepsilon) = \frac{2}{3}\varepsilon + 8n\mathrm{e}^{2n(D+1+\varepsilon)}(2\varepsilon)^2 < \frac{2}{3}\varepsilon + \frac{32}{100}\varepsilon < \varepsilon.$$

Therefore, $f(x) = x$ has a unique root $\tilde{x} \in (0, \varepsilon)$ and it follows that $\lim_{k\to\infty} x_k \leqslant \tilde{x}$. Consequently,

$$V_\infty(s) \leqslant V_j(s) + \tilde{x} \leqslant D + 1 + \varepsilon. \qquad \square$$

4 Matrix eigenvalues and the proof of Theorem 1

Throughout this section, we assume that $Q = \prod_{p\leqslant y} p$ and $M = M_{1,\infty,Q}$. Observe that by Proposition 1,

$$K = \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{p}\right) \gg 1. \tag{4.1}$$

Because all entries of M are nonnegative, the Perron-Frobenius theorem implies that there is an eigenvalue of largest modulus which is real and positive. The matrices M are similar to the matrices studied in [7, §2], and we will likewise focus on bounding column sums of M. However, the estimation problem is much more complicated than the analogous problem in [7].

Lemma 4.1. *For any $b \in U_Q$, let $d = (b-1, Q)$ and $b' = \frac{b-1}{d}$. Then*

$$C_b(M) = \frac{\phi(d)}{d} \sum_{\substack{k\in T_\infty \\ (k,Q/d)=1 \\ \text{(4.3)}}} \frac{1}{k}, \tag{4.2}$$

where

$$\forall p \leqslant y \text{ with } p \notin \mathcal{P}, k \not\equiv b' \pmod{p}. \tag{4.3}$$

Proof. By the definition of U_Q in (3.4), $2|d$ and for all $p|d$, $p \in \mathcal{P}$. In (3.5), therefore, $am+1 \equiv b \pmod{Q}$ implies that $d|m$. Writing $m = dk$, we have $(k, Q/d) = 1$ and $ak \equiv b' \pmod{Q/d}$. Since $a \in U_Q$, $a \not\equiv 1 \pmod{p}$ for any $p \leqslant y$ with $p \notin \mathcal{P}$. Hence, (4.3) holds. Therefore, by (3.5),

$$C_b(M) = \sum_{a\in U_Q} \sum_{\substack{k\in T_\infty \\ ak\equiv b' \pmod{Q/d} \\ \text{(4.3)}}} \frac{1}{dk} = \frac{1}{d} \sum_{\substack{k\in T_\infty \\ (k,Q/d)=1 \\ \text{(4.3)}}} \frac{1}{k} \#\{a \in U_Q : ak \equiv b' \pmod{Q/d}\}.$$

For every $k \in T_\infty$ satisfying $(k, Q/d) = 1$ and (4.3), there is a unique solution $a \mod Q/d$ of the congruence $ak \equiv b' \pmod{Q/d}$ and moreover this solutions satisfies $a \in U_Q$. Thus, there are $\phi(d)$ solutions $a \in U_Q$, and this completes the proof. $\square$

Notice that if we ignore condition (4.3), then we obtain from (4.2) the upper bound

$$C_b(M) \leqslant \frac{\phi(d)}{d} \sum_{\substack{k\in T_\infty \\ (k,Q/d)=1}} \frac{1}{k} = \frac{\phi(d)}{d} \prod_{\substack{p\in\mathcal{P} \\ p|d \text{ or } p>y}} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p\in\mathcal{P}, p>y} \left(1 - \frac{1}{p}\right)^{-1}. \tag{4.4}$$

The product on the far right side of (4.4) is always greater than 1, however it tends to 1 as $y \to \infty$ by Proposition 1. In order to obtain a bound $C(M) < 1$, it is necessary to use (4.3) to eliminate some numbers k from the sum in (4.4). However, if $k \in T_\infty$ with $(k, Q/d) = 1$ and $k < y$, then only primes dividing d may divide k. In the worst case $d = 2$, the only numbers $k < y$ that are available to eliminate are powers of 2. If there is a prime $p \notin \mathcal{P}$ for which 2 is a primitive root (generator of $(\mathbb{Z}/p\mathbb{Z})^*$), then we will succeed.

Lemma 4.2. *Suppose $p \notin \mathcal{P}$ and 2 is a primitive root of p. Then, for large enough y depending on p,*

$$C(M) \leqslant 1 - 2^{1-p}K,$$

where K is defined in (4.1).

Proof. For any $b \in U_Q$, let $d = (b-1, Q)$ and $b' = \frac{b-1}{d}$ as before. Since $b \not\equiv 1 \pmod p$, we have $(b', p) = 1$. Hence, there is an exponent $\theta \in \{0, 1, \dots, p-2\}$ such that $2^\theta \equiv b' \pmod p$. By Lemma 4.1 and (4.4),

$$C_b(M) \leqslant \frac{\phi(d)}{d}\left[\sum_{\substack{k\in T_\infty\\(k,Q/d)=1}} \frac{1}{k} - \frac{1}{2^\theta}\right] \leqslant \prod_{\substack{p\in\mathcal{P}\\p>y}}\left(1-\frac{1}{p}\right)^{-1} - 2^{2-p}\frac{\phi(d)}{d}.$$

The lemma follows upon observing that

$$\inf_{d\in T_\infty} \frac{\phi(d)}{d} = K$$

and that if y is large then

$$\prod_{\substack{p\in\mathcal{P}\\p>y}}\left(1-\frac{1}{p}\right)^{-1} \leqslant 1 + 2^{1-p}K. \qquad \square$$

Remarks. It is conjectured that there are infinitely many primes that have 2 as a primitive root, but this is an open problem. Hooley [12] showed that the Riemann Hypothesis for the Dedekind zeta functions $\zeta_{K_r}(s)$ for the number fields $K_r = \mathbb{Q}(2^{1/r}, \mathrm{e}^{2\pi i/r})$, where r runs over the primes, implies that the number of primes $p \leqslant x$ which have 2 as a primitive root is $\sim cx/\log x$, where $c = \prod_r(1 - \frac{1}{r(r-1)}) = 0.3739\ldots$. This asymptotic formula is known as Artin's primitive root conjecture for the base 2. If true, then by Proposition 1, most of these primes are not in $\mathcal{P}$, and we obtain Theorem 1 upon invoking Lemma 4.2. For more about Artin's conjecture, the reader may consult the comprehensive survey article [14].

Unconditionally, Lemmas 3.4 and 4.2 imply Theorem 1 in the case that 2 is a primitive root of p_0 ($p_0 \in \{3, 5, 11, 13, 19, \ldots\}$), or if there is a prime $q \equiv 1 \pmod{p_0}$ with 2 as a primitive root; for example if $p_0 = 7$ then we may take $q = 29$.

There is a way around invoking Artin's conjecture: by examining column sums of small powers of M, we succeed if there is a prime $p \notin \mathcal{P}$ with $(\mathbb{Z}/p\mathbb{Z})^*$ generated by a bounded set of small primes. The following result of Gupta and Murty [9] supplies us with the necessary prime p.

Lemma 4.3. *For $\gg x/\log^2 x$ primes $p \leqslant x$, $(\mathbb{Z}/p\mathbb{Z})^*$ is generated by 2, 3 and 5.*

Remarks. Heath-Brown [11] proved the stronger statement that for $\gg x/\log^2 x$ primes $p \leqslant x$, either 2, 3 or 5 is a primitive root of p. Our argument below, in fact, requires only the weaker statement that for some k and primes $p_1, \ldots, p_k$, each with 2 as a primitive root, there are $\gg x/\log^2 x$ primes $p \leqslant x$ for which $(\mathbb{Z}/p\mathbb{Z})^*$ is generated by $2, p_1, \ldots, p_k$. We would then iterate Lemma 4.4 below k times instead of twice.

Utilizing Lemma 4.3, we will show that $C(M^3) < 1$ for large y. Our main tool is the following, which roughly says that if $C_b(M^k) < 1$ for every b lying in some arithmetic progression, then $C_b(M^{k+1}) < 1$ for all b lying in a larger arithmetic progression.

Lemma 4.4. *Let p be a prime in $\mathcal{P}$ with 2 as a primitive root, and let $n \in T_\infty$ satisfy $n|Q$ and $p \nmid n$. Let $u \in \mathbb{N}$. Suppose that for large y and for all $b \equiv 1 \pmod{pn}$, $C_b(M^u) \leqslant 1 - \delta$ where $\delta > 0$. Then, for large enough y (depending on p, n, δ, p_0, u) and all $b \equiv 1 \pmod n$, $C_b(M^{u+1}) \leqslant 1 - \delta'$, where*

$$\delta' = \frac{\delta K}{2^p n}.$$

Proof. Suppose that $b \in U_Q$ with $b \equiv 1 \pmod n$. If $p|(b-1)$, we apply (4.4) and the general inequality $C_b(AB) \leqslant C(A)C_b(B)$ to obtain

$$C_b(M^{u+1}) \leqslant C_b(M^u)C(M) \leqslant (1-\delta) \prod_{p\in\mathcal{P}, p>y} \left(1-\frac{1}{p}\right)^{-1} \leqslant 1 - \frac{\delta}{2} \leqslant 1-\delta'$$

if y is large enough. Now assume $p \nmid (b-1)$. As in Lemma 4.1, put $d=(b-1,Q)$ and $b' = \frac{b-1}{d}$. We have

$$\begin{aligned} C_b(M^{u+1}) &= \sum_{a\in U_Q} C_a(M^u) M(a,b) \\ &= \sum_{a\in U_Q} C_a(M^u) \sum_{\substack{m\in T_\infty \\ am+1\equiv b \pmod Q}} \frac{1}{m} \\ &= \frac{1}{d} \sum_{\substack{k\in T_\infty \\ (k,Q/d)=1}} \frac{1}{k} \sum_{\substack{a\in U_Q \\ ak\equiv b' \pmod{Q/d}}} C_a(M^u). \end{aligned} \tag{4.5}$$

(4.3)

For each k, the congruence $ak \equiv b' \pmod{Q/d}$ has a unique solution $a \mod Q/d$, hence there are $\phi(d)$ solutions $a \in U_Q$. By assumption, there is a $\theta \in \{0,1,\dots,p-2\}$ with $2^\theta \equiv b' \pmod p$. In (4.5), we use the crude bound $C_a(M^u) \leqslant C(M^u) \leqslant C(M)^u$ for all pairs a,k except when both $k=2^\theta$ and $a \equiv 1 \pmod n$. In the latter case, $a \equiv 1 \pmod p$ as well, hence $a \equiv 1 \pmod{pn}$ and $C_a(M^u) \leqslant 1-\delta$. Also, since $n|Q$ and $b \equiv 1 \pmod n$, we have $n|d$. By (4.4) and (4.5),

$$\begin{aligned} C_b(M^{u+1}) &\leqslant C(M)^u \left[\frac{\phi(d)}{d} \sum_{\substack{k\in T_\infty \\ (k,Q/d)=1}} \frac{1}{k} - \frac{1}{2^\theta d} \sum_{\substack{a\in U_Q \\ a\equiv 1 \pmod{nQ/d}}} 1 \right] + \frac{1}{2^\theta d} \sum_{\substack{a\in U_Q \\ a\equiv 1 \pmod{nQ/d}}} (1-\delta) \\ &\leqslant \max(1, C(M)^u) \frac{\phi(d)}{d} \sum_{\substack{k\in T_\infty \\ (k,Q/d)=1}} \frac{1}{k} - \frac{\delta}{2^\theta d} \phi\left(\frac{d}{n}\right) \\ &\leqslant \prod_{p\in\mathcal{P}, p>y} \left(1-\frac{1}{p}\right)^{-(u+1)} - \frac{\delta}{2^{p-2}d} \phi\left(\frac{d}{n}\right). \end{aligned}$$

Since $\phi(d/n) \geqslant \phi(d)/n$ and $\phi(d)/d \geqslant K$, upon recalling the definition of δ' we conclude that

$$C_b(M^{u+1}) \leqslant \prod_{p\in\mathcal{P}, p>y} \left(1-\frac{1}{p}\right)^{-(u+1)} - \frac{\delta K}{2^{p-2}n} \leqslant 1-\delta'$$

if y is large enough. □

Proof of Theorem 1. If $p_0 \in \{3,5\}$, Lemma 4.2 (with $p=p_0$) implies that $C(M) < 1$ for large enough y. Hence, by Lemma 3.4, $V_\infty(s)$ is finite for some $s<1$.

Now assume that $3 \in \mathcal{P}$ and $5 \in \mathcal{P}$. Combining Lemmas 2.1 and 4.3, we find that there is a prime $p_1 \notin \mathcal{P}$ for which 2,3 and 5 generate $(\mathbb{Z}/p_1\mathbb{Z})^*$. Following the proof of Lemma 4.2, for any $b \in U_Q$ with $b \equiv 1 \pmod{30}$, there are exponents $a_2, a_3, a_5 \in \{0,1,\dots,p_1-2\}$ so that $2^{a_2}3^{a_3}5^{a_5} \equiv b' \pmod{p_1}$. As before,

$b' = \frac{b-1}{(b-1,Q)}$. By (4.3), $k = 2^{a_2}3^{a_3}5^{a_5}$ is excluded from the sum in (4.2). By (4.4), if y is large enough then

$$C_b(M) \leqslant \prod_{p\in\mathcal{P},p>y}\left(1-\frac{1}{p}\right)^{-1} - \frac{\phi(d)/d}{2^{a_2}3^{a_3}5^{a_5}} \leqslant \prod_{p\in\mathcal{P},p>y}\left(1-\frac{1}{p}\right)^{-1} - \frac{K}{30^{p_1-2}} < 1-\delta,$$

where $\delta = K/30^{p_1-1}$. By Lemma 4.4 with $n = 6$, $p = 5$ and $u = 1$, we find that for large enough y, $C_b(M^2) \leqslant 1-\delta'$ for every $b \equiv 1 \pmod 6$, where

$$\delta' = \frac{K\delta}{2^5\cdot 6}.$$

A second application of Lemma 4.4, with $n = 2$, $p = 3$ and $u = 2$ implies that for *every* $b \in U_Q$, $C_b(M^3) \leqslant 1-\delta''$ if y is large enough, where $\delta'' = K\delta'/16$. Thus, the dominant eigenvalue of M^3 is at most $1-\delta''$, hence the dominant eigenvalue of M is $\leqslant (1-\delta'')^{1/3} < 1$. Finally, applying Lemma 3.4, we find that $V_\infty(s)$ is finite for some $s < 1$. It follows immediately that $P(x) = O(x^s)$. □

Acknowledgements. The author thanks Paul Pollack for helpful conversations concerning Lemma 2.1, and is thankful to Paul Bateman for introducing to him Carmichael's conjecture and related problems.

The author's research was supported by National Science Foundation Grants DMS-0901339 and DMS-1201442. Much of the work was accomplished while the author attended the N.S.F. supported Workshop in Linear Analysis and Probability at Texas A&M University, July-August, 2012.

References

[1] J. Bayless, *The Lucas-Pratt primality tree*, Math. Comp. **77** (2008), 495-502.
[2] R. D. Carmichael , *On Euler's ϕ-function* , Bull. Amer. Math. Soc. **13** (1907) , 241–243.
[3] _____, *Note on Euler's ϕ-function* , Bull. Amer. Math. Soc. **28** (1922) , 109–110.
[4] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, in Analytic Number Theory, Proceedings of a conference in honor of Paul T. Bateman, Birkhäuser, Boston, 1990, 165–204.
[5] C. Finch and L. Jones, *A Curious Connection Between Fermat Numbers and Finite Groups*, Amer. Math. Monthly **109** (2002), 517–524.
[6] K. Ford, *The distribution of totients*, Ramanujan J. (Paul Erdős memorial issue) **2** (1998), 67–151.
[7] K. Ford, S. Konyagin and F. Luca, *Prime chains and Pratt trees*, Geom. Funct. Anal. **20** (2010), 1231–1258.
[8] K. Ford, S. Konyagin and F. Luca, *On groups with perfect order subsets*, Moscow J. Comb. Number Theory **2**, no. 4 (2012), to appear.
[9] R. Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Inv. Math. **78** (1984), 127–130.
[10] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London, 1974.
[11] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford (2) **37** (1986), 27–38.
[12] C. Hooley, *On Artin's conjecture*, J. reine angew. Math. **225** (1967), 209–220.
[13] F. Luca and C. Pomerance, *Irreducible radical extensions and Euler-function chains*, in "Combinatorial number theory", 351–361, de Gruyter, Berlin (2007).
[14] P. Moree, *Artin's primitive root conjecture - a survey*, INTEGERS (The electronic journal of combinatorial number theory) **12A** (2012), paper A13. See also `arXiv.math/0412262v2` (2012).
[15] C. Pomerance, *On Carmichael's conjecture*, Proc. Amer. Math. Soc. **43** (1974), 297–298.
[16] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, troisième Édition, coll. Échelles, Belin, 2008, 592 pp. English translation of the second edition: *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 1995.

DEPARTMENT OF MATHEMATICS, 1409 WEST GREEN STREET, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, URBANA, IL 61801, USA

E-mail address: `ford@math.uiuc.edu`