COMMON VALUES OF THE ARITHMETIC FUNCTIONS ϕ AND σ

KEVIN FORD, FLORIAN LUCA, AND CARL POMERANCE

ABSTRACT. We show that the equation $\phi(a) = \sigma(b)$ has infinitely many solutions, where ϕ is Euler's totient function and σ is the sum-of-divisors function. This proves a 50-year old conjecture of Erdős. Moreover, we show that there are infinitely many integers n such that $\phi(a) = n$ and $\sigma(b) = n$ each have more than n^c solutions, for some $c > 0$. The proofs rely on the recent work of the first two authors and Konyagin on the distribution of primes p for which a given prime divides some iterate of ϕ at p, and on a result of Heath-Brown connecting the possible existence of Siegel zeros with the distribution of twin primes.

1. INTRODUCTION

Two of the oldest and most studied functions in the theory of numbers are the sum-of-divisors function σ and Euler's totient function ϕ. Over 50 years ago, Paul Erdős conjectured that the ranges of ϕ and σ have an infinite intersection ([8, p. 172], [28, p. 198]). This conjecture follows easily from some famous unsolved problems. For example, if there are infinitely many pairs of twin primes p, $p + 2$, then $\phi(p + 2) = p + 1 = \sigma(p)$, and if there are infinitely many Mersenne primes $2^p - 1$, then $\sigma(2^p - 1) = 2^p = \phi(2^{p+1})$. Results from [11] indicate that typical values taken by ϕ and by σ have a similar multiplicative structure; hence, common values should be plentiful. A short calculation reveals that there are 95145 common values of ϕ and σ between 1 and 10^6. This is to be compared with a total of 180184 ϕ-values and 189511 σ-values in the same interval. In [9], the authors write that "it is very annoying that we cannot show that $\phi(a) = \sigma(b)$ has infinitely many solutions. . . ." Annoying of course, since it is so obviously correct! Erdős knew (see [18, sec. B38]) that $\phi(a) = k!$ is solvable for every positive integer k, so all one would have to do is show that $\sigma(b) = k!$ is solvable for infinitely many choices for k. In fact, this equation seems to be solvable for every $k \neq 2$, but proving it seems difficult.

The heart of the problem is to understand well the multiplicative structure of shifted primes $p - 1$ and $p + 1$.

In this note, we give an unconditional proof of the Erdős conjecture. Key ingredients in the proof are a very recent bound on counts of prime chains from [14] (see §3 for a definition) and estimates for primes in arithmetic progressions. The possible existence of Siegel zeros (see §2 for

a definition) creates a major obstacle for the success of our argument. Fortunately, Heath-Brown [20] showed that if Siegel zeros exist, then there are infinitely many pairs of twin primes. However, despite the influence of possible Siegel zeros, our methods are completely effective.

Theorem 1. *The equation $\phi(a) = \sigma(b)$ has infinitely many solutions. Moreover, for some positive a and large x, there are at least $\exp\left((\log\log x)^a\right)$ integers $n \leqslant x$ which are common values of ϕ and σ.*

We also show that there are infinitely many integers n which are common values of ϕ and σ in many ways. Let $A(n)$ be the number of solutions of $\phi(x) = n$, and let $B(n)$ be the number of solutions of $\sigma(x) = n$. Pillai [25] showed in 1929 that the function $A(n)$ is unbounded, and in 1935, Erdős [5] showed that the inequality $A(n) > n^c$ holds infinitely often for some positive constant c. The proofs give analogous results for $B(n)$. Numerical values of c have been given by a number of people ([2], [15], [26] and [29]), the largest so far being $c = 0.7039$ which is due to Baker and Harman [1]. The key to these results is to show that there are many primes p for which $p-1$ has only small prime factors. Erdős [6] conjectured that for any constant $c < 1$ the inequality $A(n) > n^c$ holds infinitely often.

Theorem 2. *For some positive constant c there are infinitely many n such that both inequalities $A(n) > n^c$ and $B(n) > n^c$ hold. Moreover, for some constant $a > 0$, there are at least $(\log\log x)^a$ such numbers $n \leqslant x$, for large x.*

Necessary results on the distribution of primes in progressions, twin primes, and prime chains are given in Sections 2 and 3. In Section 3, we prove Theorem 1. In Section 4, we present the additional arguments needed to deduce the conclusion of Theorem 2. Theorem 2 resolves another conjecture of Erdős (stated as Conjecture C_8 in [28, p. 193]): for each number k, there is some number n with $A(n) > k$ and $B(n) > k$. Later, in Section 5, we pose some additional problems concerning common values of ϕ and σ.

We consider $n = \sigma\left(\prod_{p \in \mathcal{S}} p\right) = \prod_{p \in \mathcal{S}}(p + 1)$, where $\mathcal{S}$ is a set of primes $p \leqslant x$ for which all prime factors of $p + 1$ are small, say $\leqslant z$. In this way, n should be the product of some of the primes $\leqslant z$, each to a possibly large power. We deduce that n is in the range of ϕ by exploiting the general implication

$$(1.1) \qquad \phi(\mathrm{rad}(m)) \mid m \implies m = \phi\left(\frac{m \cdot \mathrm{rad}(m)}{\phi(\mathrm{rad}(m))}\right),$$

where $\mathrm{rad}(m)$ is the product of the distinct prime factors of m. Let $v_q(m)$ denote the exponent of q in the factorization of m. We expect for $n = \sigma\left(\prod_{p \in \mathcal{S}} p\right)$ that $v_q(\phi(\mathrm{rad}(n))) \leqslant v_q(n)$ for $q \leqslant z$; hence, the hypothesis in (1.1) should hold. Turning this into a proof requires lower bounds of the expected order for the number of $p \in \mathcal{S}$ for which $q \mid p + 1$.

2. PRIMES IN PROGRESSIONS

Throughout, constants implied by O, $\ll$, $\gg$, and $\asymp$ notation are absolute unless otherwise noted. Bounds for implied constants, as well as positive quantities introduced later, are effectively computable. Symbols p, q, r always denote primes, and $P(m)$ is the largest prime factor of an integer $m > 1$. Let $\pi(x; m, a)$ be the number of primes $p \leqslant x$ with $p \equiv a \pmod{m}$, and let

$$\psi(x; m, a) = \sum_{\substack{n \leqslant x \\ n \equiv a \pmod{m}}} \Lambda(n),$$

where Λ is the von Mangoldt function. The behavior of $\pi(x; m, a)$ and $\psi(x; m, a)$ are intimately connected to the distribution of zeros of Dirichlet L-functions. Of particular importance are possible zeros near the point 1. Let $\mathcal{C}(m)$ denote the set of primitive characters modulo m. It is known (cf. [4, Ch. 14]) that for some constant $c_0 > 0$ and every $m \geqslant 3$, there is at most one zero of $\prod_{\chi \in C(m)} L(s, \chi)$ in the region

$$(2.1) \qquad \Re s \geqslant 1 - \frac{c_0}{\log(m(|\Im s| + 1))}.$$

Furthermore, if this "exceptional zero" β exists, it is real, it is a zero of $L(s, \chi)$ for a real character $\chi \in \mathcal{C}(m)$, and

$$(2.2) \qquad \beta \leqslant 1 - \frac{c_1}{m^{1/2} \log^2 m}$$

for some positive constant c_1. Better upper bounds on β are known (Siegel's Theorem, [4, Ch. 21]), but these are ineffective. The "exceptional moduli" m, for which an exceptional β exists, must be quite sparse, as the following classical results show ([4, Ch. 14]).

Lemma 2.1 (Landau). *For some constant $c_2 > 0$, if $3 \leqslant m_1 < m_2$, $\chi_1 \in \mathcal{C}(m_1)$ and $\chi_2 \in \mathcal{C}(m_2)$, then there is at most one zero β of $L(s, \chi_1)L(s, \chi_2)$ with $\beta > 1 - c_2/\log(m_1 m_2)$.*

We immediately obtain

Lemma 2.2 (Page). *For any $M \geqslant 3$,*

$$\prod_{m \leqslant M} \prod_{\chi \in \mathcal{C}(m)} L(s, \chi)$$

has at most one zero in the interval $[1 - (c_2/2)/\log M, 1]$.

It is known after McCurley [24] that $c_0 = 1/9.645908801$ holds in (2.1), while Kadiri [22] has shown we may take $c_0 = 1/6.397$, and in Lemmas 2.1, 2.2 we may take $c_2 = 1/2.0452$.

The Riemann hypothesis for Dirichlet L-functions implies that no exceptional zeros can exist. If there is an infinite sequence of integers m and associated zeros β satisfying $(1 - \beta) \log m \to 0$, such zeros are known as Siegel zeros, and their existence would have profound implications on the distribution of primes in arithmetic progressions ([4, (9) in Ch. 20]). As mentioned before, Heath-Brown showed that the existence of Siegel zeros implies that there are infinitely many prime twins.

Lemma 2.3 ([20, Corollary 2]). *If $\chi \in \mathcal{C}(m)$ and $L(\beta, \chi) = 0$ for $\beta = 1 - \lambda(\log m)^{-1}$, then for $m^{300} < z \leqslant m^{500}$, the number of primes $p \leqslant z$ with $p + 2$ prime is*

$$C\frac{z}{\log^2 z} + O\left(\frac{\lambda z}{\log^2 z}\right), \quad \text{where } C = 2\prod_{p>2}(1 - (p-1)^{-2}) = 1.32\ldots.$$

If Siegel zeros do not exist, there still may be some Dirichlet L-function zeros with real part $> 1/2$, which would create irregularities in the distribution of primes in some progressions. Such progressions, however, would have moduli larger than a small power of x. We state here a character sum version of this result, due to Gallagher (see the proof of [16, Theorem 7]). Let

$$\psi(x, \chi) = \sum_{n \leqslant x} \Lambda(n)\chi(n), \quad \text{and} \quad \Psi(x, m) = \sum_{\chi \in \mathcal{C}(m)} |\psi(x, \chi)|.$$

Lemma 2.4. *If c_2 is as in Lemma 2.1, then for every $\lambda \in (0, c_2/2]$ and $\varepsilon > 0$, there are constants $1 \geqslant \alpha > 0$ and x_0 so that for $x \geqslant x_0$,*

$$\sum_{\substack{3 \leqslant m \leqslant x^\alpha \\ m \neq m_0}} \Psi(x, m) \leqslant \varepsilon x.$$

Here m_0 corresponds to the conductor of a Dirichlet character χ for which $L(\beta, \chi) = 0$ for some $\beta > 1 - \lambda/\log(x^\alpha)$. If there is no such zero, set $m_0 = 0$.

We remark that m_0, if it exists, is unique by Lemma 2.2.

We also know that $\Psi(x, m)$ is small for most $m \in (x^\alpha, x^{1/2-\delta}]$ if $\delta > 0$ is fixed. This follows from the next lemma which is a key ingredient in the proof of the Bombieri-Vinogradov theorem.

Lemma 2.5. *For $1 \leqslant M \leqslant x$,*

$$\sum_{m \leqslant M} \Psi(x, m) \ll \left(x + x^{5/6}M + x^{1/2}M^2\right)\log^4 x.$$

Proof. This is [4, Ch. 28, (2)]. $\qquad\qquad\square$

For positive reals δ, γ, y, x, with $1 \leqslant y \leqslant x^{1/2-\delta}$, and a nonzero integer a, define

$$S_q(x; \delta, a) = \#\{p \leqslant x : P(p + a) \leqslant x^{1/2-\delta}, q \mid p + a\},$$

$$\mathcal{E}(x, y; \delta, \gamma) = \left\{q \leqslant y : S_q(x; \delta, 1) \leqslant \frac{\gamma x}{q \log x} \text{ or } S_q(x; \delta, -1) \leqslant \frac{\gamma x}{q \log x}\right\}.$$

We say that a real number x is (α, ε)-good if $\Psi(x; m) \leqslant \varepsilon x$ for $3 \leqslant m \leqslant x^\alpha$. Roughly speaking, this means that the exceptional modulus in Lemma 2.4 doesn't exist (for appropriate λ).

Lemma 2.6. *There are absolute constants $\delta > 0$ and $\gamma > 0$ so that the following holds. For every $\alpha > 0$, there are constants $\eta > 0$ and $x_1 > 0$ so that if $x \geqslant x_1$ and x is $(\alpha, \frac{1}{10})$-good, then for all $y \leqslant x^{1/2-\delta}$,*

$$\#\mathcal{E}(x, y; \delta, \gamma) \leqslant yx^{-\eta}.$$

Proof. We may assume that $0 < \delta < 1/6$. Let k be a positive integer such that $Q = 2^{-k}x^{1/2-\delta} \geqslant 1$. Let $R_1 = \max\{Q^{-1}x^{1/2-\delta}, x^{\delta/2}\}$, and let $R_2 = R_1 x^{\delta/6}$. By standard estimates ([4, (3) in Ch. 20]), if $q \in (Q, 2Q]$ and $r \in (R_1, R_2]$, then for $a = \pm 1$,

$$(2.3) \qquad \left| \psi(x; qr, a) - \frac{x}{\phi(qr)} \right| \leqslant \frac{1}{\phi(qr)} \left(\Psi(x, q) + \Psi(x, r) + \Psi(x, qr) + O(x/\log x) \right).$$

Let $\mathcal{E}_1(Q) = \{q \in (Q, 2Q] : \Psi(x, q) > x/10\}$. Since x is $(\alpha, \frac{1}{10})$-good, we have $\mathcal{E}_1(Q) = \emptyset$ when $Q \leqslant \frac{1}{2}x^\alpha$. Otherwise, by Lemma 2.5,

$$\#\mathcal{E}_1(Q) \ll \left(1 + Qx^{-1/6} + Q^2 x^{-1/2} \right) \log^4 x \ll Q(x^{-\delta} + x^{-\alpha}) \log^4 x.$$

Let $\mathcal{E}_2(Q) = \{q \in (Q, 2Q] : \Psi(x, qr) > x/10 \text{ for at least } R_1 x^{-\delta/12} \text{ primes } r \in (R_1, R_2]\}$. By Lemma 2.5 and the inequality $R_2 Q \leqslant x^{1/2-\delta/3}$,

$$\#\mathcal{E}_2(Q) \ll \frac{(x + x^{5/6} R_2 Q + x^{1/2}(R_2 Q)^2) \log^4 x}{R_1 x^{1-\delta/4}} \ll Q x^{-\delta/12} \log^4 x.$$

Also, by Lemma 2.5,

$$\#\{r \in (R_1, R_2] : \Psi(x, r) \geqslant x/10\} \ll \left(1 + x^{-1/6} R_2 + x^{-1/2} R_2^2 \right) \log^4 x \ll R_1 x^{-\delta/2} \log^4 x.$$

For each $q \in (Q, 2Q]$ with $q \notin \mathcal{E}_1(Q) \cup \mathcal{E}_2(Q)$, let

$$\mathcal{R}(q) = \{r \in (R_1, R_2] : \Psi(x, qr) \leqslant x/10, \ \Psi(x, r) \leqslant x/10\}.$$

By (2.3), for $r \in \mathcal{R}(q)$ and $a = \pm 1$,

$$(2.4) \qquad \pi(x; qr, a) \geqslant \frac{\psi(x; qr, a) - O(\sqrt{x})}{\log x} \geqslant \frac{x}{2qr \log x}.$$

Also, by the above estimates and Mertens' formula,

$$(2.5) \qquad \sum_{r \in \mathcal{R}(q)} \frac{1}{r} \geqslant \sum_{R_1 < r \leqslant R_2} \frac{1}{r} - O(x^{-\delta/12} \log^4 x) \geqslant \frac{\delta}{3}.$$

Since $R_1 \geqslant x^{\delta/2}$, a shifted prime $p + a$ is divisible by at most $\lfloor \frac{2}{\delta} \rfloor$ primes in $\mathcal{R}(q)$. Hence,

$$S_q(x; \delta, a) \geqslant \frac{\delta}{2} \sum_{r \in \mathcal{R}(q)} \left(\pi(x; qr, a) - \#\mathcal{U}(q, r) \right), \qquad \text{where}$$

$$\mathcal{U}(q, r) = \{p \leqslant x : qr | p + a, P(p + a) > x^{1/2-\delta}\}.$$

For $p \in \mathcal{U}(q, r)$, we have $p + a = qrsb$, where $s > x^{1/2-\delta}$ is prime and $b \leqslant x^{2\delta}$. For fixed b, q, r, a, we estimate the number of possible choices for s using the sieve ([19], Theorem 3.12). We get

$$\#\mathcal{U}(q, r) \ll \sum_{b \leqslant x^{2\delta}} \frac{x}{bqr \log^2(x/bqr)} \frac{b}{\phi(b)} \ll \frac{x}{qr \log^2 x} \sum_{b \leqslant x^{2\delta}} \frac{1}{\phi(b)} \ll \frac{\delta x}{qr \log x}.$$

For small enough δ, we then have $\#\mathcal{U}(q,r) \leqslant \frac{x}{4qr\log x}$, and we conclude from (2.4), (2.5) that

$$S_q(x;\delta,a) \geqslant \frac{\delta x}{8q\log x} \sum_{r\in\mathcal{R}(q)} \frac{1}{r} \geqslant \frac{\delta^2 x}{24q\log x}.$$

Finally, $\#\mathcal{E}_1(Q)+\#\mathcal{E}_2(Q) \leqslant \frac{1}{4}Qx^{-\eta}$ for $\eta = \min\{\alpha/2, \delta/13\}$ and large x. Summing over choices of the dyadic interval $(Q, 2Q]$ with $Q \leqslant y$ and $a \in \{-1, 1\}$ finishes the proof. $\square$

3. PRIME CHAINS AND THE PROOF OF THEOREM 1

Suppose that n is a positive integer with $\phi(\mathrm{rad}(n)) \mid n$ and that q is a prime with $q \nmid n$. Then n is not divisible by any prime $t \equiv 1 \pmod q$, since otherwise $q \mid \phi(\mathrm{rad}(n))$, which would imply that $q \mid n$. Iterating, n is not divisible by any prime $t' \equiv 1 \pmod t$, where t is a prime with $t \equiv 1 \pmod q$. And so on. Thus, the single nondivisibility assumption that $q \nmid n$, plus the assumption that $\phi(\mathrm{rad}(n)) \mid n$, forces any prime t in any *prime chain* for q to also not divide n. We define a prime chain as a sequence of primes $q = t_0, t_1, t_2, \ldots$, where each $t_{j+1} \equiv 1 \pmod{t_j}$. Alternatively, if ϕ_j is the j-fold iterate of ϕ, then a prime t is in a prime chain for q if $t = q$ or $q \mid \phi_j(t)$ for some j.

Let $\mathcal{T}(y, q)$ be the set of primes $t \leqslant y$ which are in a prime chain for q. Crucial to our proof is the following estimate.

Lemma 3.1 ([14, Theorem 5]). *For every $\varepsilon > 0$ there is a constant $C(\varepsilon)$ so that if q is prime and $y > q$, then $\#\mathcal{T}(y, q) \leqslant C(\varepsilon)(y/q)^{1+\varepsilon}$.*

More estimates for counts of prime chains with various properties may be found in [3, 10, 14, 23].

We now proceed to prove Theorem 1. There is an absolute constant $\lambda_0 > 0$ so that if $\lambda \leqslant \lambda_0$, then the error term in the conclusion of Lemma 2.3 is at most $0.1z/\log^2 z$ in absolute value. Let $\alpha > 0$ and x_0 be the constants from Lemma 2.4 corresponding to $\varepsilon = \frac{1}{10}$ and $\lambda = \lambda_0$, and let δ, γ, η and x_1 be the constants from Lemma 2.6.

Suppose $x \geqslant \max(x_0, x_1)$. We show that there are many common values of ϕ and σ which are $\leqslant e^{2x}$ by considering two cases. First, suppose that x is not (α, ε)-good. Then for some $m \leqslant x^\alpha$ and $\chi \in \mathcal{C}(m)$, $L(\beta, \chi) = 0$ for some $\beta \geqslant 1 - \lambda_0/\log(x^\alpha)$. By (2.2),

$$m \gg \frac{\log^2 x}{(\log\log x)^4}.$$

Let $z = m^{500}$. By Lemma 2.3, the set $\mathcal{T}$ of primes $p \leqslant z-1$ for which $p+2$ is also prime satisfies $\#\mathcal{T} \geqslant 1.2z/\log^2 z$. Let $1/500 > \theta > 0$ be a sufficiently small constant and x large depending on θ. If $q = P(p+1) \leqslant z^\theta$, then $p+1 = qb$ where b is free of prime factors in $(q, z^{1/4}]$. The number of such $p \in \mathcal{T}$ is, by an application of the large sieve [4, p. 159],

$$\ll \sum_{q\leqslant z^\theta} \frac{z}{\log^3 z} \frac{\log q}{q} \ll \frac{\theta z}{\log^2 z}.$$

Let $\mathcal{S} = \{p \in \mathcal{T} : P(p + 1) > z^\theta\}$. Choose θ so small that $\#\mathcal{S} \geqslant z/\log^2 z$. For $p \in \mathcal{S}$, we have

$$\#\{p' \in \mathcal{S} : P(p + 1) \mid p' + 1\} \leqslant \frac{z}{P(p + 1)} < z^{1-\theta}.$$

Hence, there is a set $\mathcal{P}$ of primes in $\mathcal{S}$ with $\#\mathcal{P} = \lfloor z^\theta/\log^2 z \rfloor$, and such that for each $p \in \mathcal{P}$, $P(p+1) \nmid p'+1$ for all $p' \in \mathcal{P}$ different from p. For any subset $\mathcal{M}$ of $\mathcal{P}$, let $n(\mathcal{M}) = \prod_{p \in \mathcal{P}'}(p+1)$, so that $n(\mathcal{M}) = \sigma(\prod_{p \in \mathcal{M}} p) = \phi(\prod_{p \in \mathcal{M}}(p + 2))$. Furthermore, the numbers $n(\mathcal{M})$ are distinct and at most $z^{\#\mathcal{P}} \leqslant x^{500\alpha x^{500\theta\alpha}} \leqslant e^x$ for x large. Thus, there are at least $2^{\#\mathcal{P}} > \exp\{z^{\theta/2}\}$ common values of ϕ and σ which are $\leqslant e^x$. Observing that $z > (\log x)^{999}$ completes the proof in this case.

Now assume that x is (α, ε)-good. Let $\mathcal{E} = \mathcal{E}(x, x^{1/2-\delta}; \delta, \gamma)$ and let

$$(3.1) \qquad \mathcal{T} = \bigcup_{q \in \mathcal{E}} \mathcal{T}(x^{1/2-\delta}, q).$$

Put

$$(3.2) \qquad \mathcal{S} = \{p \leqslant x : P(p + 1) \leqslant x^{1/2-\delta} \text{ and } t \nmid p + 1 \text{ for all } t \in \mathcal{T}\}.$$

By partial summation and Lemmas 2.6, 3.1, we have for each $\varepsilon > 0$,

$$\sum_{t \in \mathcal{T}} \frac{1}{t} \leqslant \sum_{q \in \mathcal{E}} \sum_{t \in \mathcal{T}(x^{1/2-\delta}, q)} \frac{1}{t} \ll_\varepsilon \sum_{q \in \mathcal{E}} \frac{x^{(1/2-\delta)\varepsilon}}{q^{1+\varepsilon}} \ll_\varepsilon x^{(1/2-\delta)\varepsilon - \eta}.$$

Thus, if ε is small enough and x large, we have

$$(3.3) \qquad \sum_{t \in \mathcal{T}} \frac{1}{t} < \frac{\gamma}{20 \log x}.$$

Using Lemma 2.6, $2 \notin \mathcal{E}$, so that $\#\{p \leqslant x : P(p + 1) \leqslant x^{1/2-\delta}\} > (\gamma/2)x/\log x$. Thus,

$$(3.4) \qquad \#\mathcal{S} > \frac{\gamma x}{2 \log x} - \sum_{t \in \mathcal{T}} \frac{x}{t} \geqslant \frac{\gamma x}{3 \log x}.$$

Let p_j be the j-th largest prime in $\mathcal{S}$, and

$$n_j = \sigma\Big(\prod_{p \in \mathcal{S} - \{p_j\}} p \Big) = \prod_{p \in \mathcal{S} - \{p_j\}} (p + 1).$$

Clearly $B(n_j) \geqslant 1$. Note that the prime factors of n_j are $\leqslant x^{1/2-\delta}$, so that

$$\phi(\mathrm{rad}(n_j)) \mid u!,$$

where $u = \lfloor x^{1/2-\delta} \rfloor$. If $q \leqslant x^{1/2-\delta}$ and $q \in \mathcal{T}$, then $q \nmid \phi(\mathrm{rad}(n_j))$. If $q \notin \mathcal{T}$, we have

$$(3.5) \qquad v_q(\phi(\mathrm{rad}(n_j))) \leqslant v_q(u!) \leqslant \frac{x^{1/2-\delta}}{q - 1}.$$

On the other hand, for such q, Lemma 2.6 and (3.3) imply

$$(3.6) \qquad v_q(n_j) \geqslant \#\{p \in \mathcal{S} - \{p_j\} : q \mid p + 1\} \geqslant \frac{\gamma x}{q \log x} - 1 - \sum_{t \in T} \frac{x}{qt} \geqslant \frac{\gamma x}{2q \log x}$$

for x sufficiently large. Therefore, comparing (3.5) with (3.6) we see that (1.1) holds with $m = n_j$ and so $A(n_j) \geqslant 1$. By the prime number theorem, $n_j \leqslant \prod_{p \leqslant x}(p+1) \leqslant e^{2x}$ if x is large. The numbers n_j are distinct, hence there are at least $\#\mathcal{S} \geqslant (\gamma/3)x/\log x$ common values of ϕ and σ less than e^{2x}. This completes the proof of Theorem 1.

4. POPULAR COMMON VALUES OF ϕ AND σ

In this section, we combine the proof of Theorem 1 with a method of Erdős [5]. A key estimate is [5, Lemma 2]:

$$(4.1) \qquad \#\{n \leqslant x : P(n) \leqslant \log x\} = x^{o(1)} \qquad (x \to \infty).$$

More results about the distribution of integers n with $P(n)$ small may be found in [21].

Define $\lambda = \lambda_0$, α, x_0, x_1 and η as in the proof of Theorem 1. Without loss of generality, suppose $\alpha \leqslant \frac{1}{500}$. Theorem 2 is proved by considering the two cases, x is not $(\alpha, \frac{1}{10})$-good and x is $(\alpha, \frac{1}{10})$-good. The next lemmas provide the necessary arguments.

Lemma 4.1. *For some absolute constants $c > 0$ and $a > 0$, if $0 < \alpha \leqslant \frac{1}{500}$, x is large (depending on α) and not $(\alpha, \frac{1}{10})$-good then there are at least $(\log x)^a$ integers $n \leqslant e^x$ for which both $A(n) > n^c$ and $B(n) > n^c$.*

Proof. As in the proof of Theorem 1, by (2.2) there is an exceptional modulus m satisfying

$$\frac{\log^2 x}{(\log \log x)^4} \ll m \leqslant x^\alpha$$

and so that

$$(4.2) \qquad \#\{p \leqslant z : p+2 \text{ prime}\} \geqslant \frac{z}{\log^2 z}, \qquad z = m^{500}.$$

Let δ be a positive, absolute constant. Let $\mathcal{P}$ be the set of primes $p \leqslant z$ with $p+2$ prime and $P(p+1) \leqslant z^{1-\delta}$. If p and $p+2$ are both prime and $P(p+1) > z^{1-\delta}$, then $p+1 = qb$ for some prime q and some $b \leqslant z^\delta$. By sieve methods ([19, Theorem 2.4]), for small enough δ, we have

$$\#\mathcal{P} \geqslant \frac{z}{\log^2 z} - \sum_{b \leqslant z^\delta} \#\{q \leqslant z/b : q, \; qb-1, \; qb+1 \text{ prime}\}$$

$$\geqslant \frac{z}{\log^2 z} - O\left(\sum_{b \leqslant z^\delta} \frac{z}{b \log^3 z}\left(\frac{b}{\phi(b)}\right)^2\right) \geqslant \frac{z}{\log^2 z} - O\left(\frac{\delta z}{\log^2 z}\right) \geqslant \frac{z}{2\log^2 z}.$$

Let $H = \lfloor z^{1-\delta/2} \rfloor$ and $J = \lfloor \#\mathcal{P}/H \rfloor$. Define sets $\mathcal{P}_j$, $1 \leqslant j \leqslant J$, as follows: $\mathcal{P}_1$ is the set of the smallest H primes in $\mathcal{P}$, $\mathcal{P}_2$ is the set of the next H smallest primes from $\mathcal{P}$, etc. Let $K = \lceil z^{1-\delta}/\log z \rceil$. We may assume that x is large enough that $K \geqslant 2$, so that if $\mathcal{M}$ is a set of K primes from some $\mathcal{P}_j$, then

$$(4.3) \qquad n(\mathcal{M}) = \sigma\left(\prod_{p \in \mathcal{M}} p\right) = \phi\left(\prod_{p \in \mathcal{M}}(p+2)\right) \leqslant z^K, \quad P(n(\mathcal{M})) \leqslant z^{1-\delta} \leqslant \log\left(z^K\right).$$

By (4.1), the function $n(\cdot)$ maps sets $\mathcal{M}$ into a set of integers of cardinality $\leqslant z^{\delta K/6}$. But the number of K-element subsets $\mathcal{M}$ of some $\mathcal{P}_j$ is

$$\binom{H}{K} \geqslant \left(\frac{H}{K}\right)^K \geqslant z^{\delta K/2}$$

for x large. Thus, for each $j \leqslant J$ there is some n_j such that $n_j = n(\mathcal{M})$ for at least $z^{\delta K/3}$ K-element subsets $\mathcal{M}$ of $\mathcal{P}_j$. We conclude from (4.3) that both $A(n_j), B(n_j) \geqslant z^{\delta K/3} \geqslant n_j^{\delta/3}$. Since $n_1 < n_2 < \cdots < n_J \leqslant z^K < e^x$ and $J \geqslant z^{\delta/2}/(2 \log^2 z) - 1$, we conclude that the lemma holds with $c = \delta/3$, $a = 499\delta$ once x is sufficiently large. $\qquad \square$

Lemma 4.2. *There is an absolute constant $c > 0$, so that if $\alpha > 0$, x is large (depending on α) and $(\alpha, \frac{1}{10})$-good, then there are $\gg \log x$ integers $n \leqslant e^x$ satisfying $A(n) > n^c$ and $B(n) > n^c$.*

Proof. Let $\varepsilon = 1/10$. Let δ, γ, and η be the constants from Lemma 2.6. Define $\mathcal{T}$ as in (3.1), $\mathcal{S}$ as in (3.2) and put $\widetilde{\mathcal{S}} = \{p \in \mathcal{S} : p \geqslant \sqrt{x}\}$. Let $N := \#\widetilde{\mathcal{S}}$, so that from (3.4) we have $N \geqslant (\gamma/4)x/\log x$ for x large. Also, $N \leqslant 2x/\log x$. Let $\mathcal{Q}$ be the set of primes $q \leqslant x^{1/2-\delta}$ with $q \notin \mathcal{T}$. For $q \in \mathcal{Q}$, by (3.6) and the Brun–Titchmarsh inequality, we have

$$(4.4) \qquad N_q := \#\{p \in \widetilde{\mathcal{S}} : q \mid p+1\} \asymp \frac{N}{q}.$$

Suppose k is an integer with $N^{1/2} \leqslant k \leqslant N^{3/4}$. For $q \in \mathcal{Q}$, if we choose a k-element subset $\mathcal{M}$ of $\widetilde{\mathcal{S}}$ at random, we expect that the number of $p \in \mathcal{M}$ with $q \mid p+1$ to be kN_q/N. That is, we are viewing a prime p as corresponding to the random variable which is 1 if $q \mid p+1$ and 0 otherwise. By a standard result in the theory of large deviations (see [17, Sec. 5.11, (5)]) we have that the number of choices of $\mathcal{M}$ with

$$(4.5) \qquad \#\{p \in \mathcal{M} : q \mid p+1\} \geqslant \frac{kN_q}{2N} \qquad \text{for all } q \in \mathcal{Q}$$

is at least, for some absolute positive constant ν,

$$\left(1 - \sum_{q \in \mathcal{Q}} e^{-\nu k N_q/N}\right)\binom{N}{k} \geqslant \frac{1}{2}\binom{N}{k} \geqslant \frac{1}{2}\left(\frac{N}{k}\right)^k$$

for large x. (That the probabilistic model has us choosing "with replacement" is easily seen to be negligible). As in the proof of the previous lemma, $n(\mathcal{M}) = \sigma(\prod_{p \in \mathcal{M}} p) < x^k$ and $P(n(\mathcal{M})) \leqslant x^{1/2-\delta} < \log(x^k)$. By (4.1), there are $\leqslant x^{k/30} \leqslant N^{k/29}$ distinct values $n(\mathcal{M})$. Hence, for large x there is some integer $n < x^k$ with many representations as $n(\mathcal{M})$ where $\mathcal{M}$ satisfies (4.5); in particular

$$B(n) \geqslant \frac{1}{2}\left(\frac{N}{k}\right)^k N^{-k/29} \geqslant x^{k/5} > n^{1/5}.$$

We next show that for each such n we have $A(n)$ large. Note that generalizing (1.1), we have that if w is a positive integer with $\phi(w \cdot \text{rad}(n)) \mid n$, then

$$n = \phi\left(w \cdot \text{rad}(n) \frac{n}{\phi(w \cdot \text{rad}(n))}\right).$$

Thus, we can show that $A(n)$ is large if we can show that there are many such integers w with $(w, n) = 1$ (to ensure that the integers $w \cdot \text{rad}(n) \cdot n / \phi(w \cdot \text{rad}(n))$ are distinct for different w's). Towards this end, let

$$\mathcal{S}' = \{p \leqslant x : p > \sqrt{x},\ q \mid p - 1 \text{ implies } q \in \mathcal{Q}\}, \quad N' = \#\mathcal{S}'.$$

By Lemma 2.6 and (3.3) we have $N' \gg x / \log x$, so that $N' \asymp N$. For each q^j with $q \in \mathcal{Q}$, let

$$N'_{q^j} := \#\{p \in \mathcal{S}' : q^j \| p - 1\}$$

so that the Brun–Titchmarsh inequality implies that $N'_{q^j} \ll x/(q^j \log(ex/q^j))$ for $q^j \leqslant x$. Put $k' = \lceil \xi k \rceil$, where ξ is a small, fixed positive number. For each k'-element subset $\mathcal{M}'$ of $\mathcal{S}'$, let $w(\mathcal{M}') = \prod_{p \in \mathcal{M}'} p$. If $\mathcal{M}'$ is chosen at random, the expected value of $\sum_{p \in \mathcal{M}'} v_q(p - 1) = v_q(\phi(w(\mathcal{M}')))$ is $k' \sum_{j \geqslant 1} j N'_{q^j}/N'$ (we are now viewing our random variable as $v_q(p - 1)$). By the same result in [17], there are at least $\frac{1}{2}\binom{N'}{k'}$ choices for $\mathcal{M}'$ with

$$v_q(\phi(w(\mathcal{M}'))) \leqslant \frac{3}{2} k' \sum_{j \geqslant 1} \frac{j N'_{q^j}}{N'} \qquad \text{for all } q \in \mathcal{Q}.$$

For such choices of $\mathcal{M}'$, we have $v_q(\phi(w(\mathcal{M}'))) \ll k'/q$, so if we choose ξ small enough, we have

$$v_q(\phi(w(\mathcal{M}'))) \leqslant k \frac{N_q}{4N} \leqslant \frac{1}{2} v_q(n),$$

by (4.4) and (4.5). Since (cf. (3.5))

$$v_q(\phi(\text{rad}(n))) \leqslant \frac{x^{1/2-\delta}}{q - 1} \leqslant \frac{1}{2} v_q(n),$$

and since each prime factor of $w(\mathcal{M}')$ is $> x^{1/2} \geqslant P(n)$, we deduce that $\phi(w(\mathcal{M}') \cdot \text{rad}(n)) \mid n$ and that the numbers $w(\mathcal{M}') \cdot \text{rad}(n) \cdot n / \phi(w(\mathcal{M}') \cdot \text{rad}(n))$ are distinct for different choices of $\mathcal{M}'$. It follows that

$$A(n) \geqslant \frac{1}{2}\binom{N'}{k'} \geqslant \frac{1}{2}\left(\frac{N'}{k'}\right)^{k'} > x^{k'/5} \geqslant n^{\xi/5}.$$

Put $c = \min(1/5, \xi/5)$. Notice that our construction of n depends on k, and

$$x^{k/2} \leqslant n \leqslant x^k \leqslant e^x.$$

Letting k run over the powers of 2 in $[N^{1/2}, N^{3/4}]$ produces $\gg \log x$ distinct values of n, each $\leqslant e^x$, for which $A(n) > n^c$ and $B(n) > n^c$. $\qquad\square$

5. FURTHER PROBLEMS

(1) It is known that for any integer $k \geqslant 1$, there are integers n with $B(n) = k$ and for any integer $l \geqslant 2$, there are integers n with $A(n) = l$, see [12], [13]. The famous Carmichael conjecture states that $A(n)$ is never 1, but this is still open.

Conjecture 1. *For every $k \geqslant 1$ and $l \geqslant 2$, there are integers n with $A(n) = l$ and $B(n) = k$.*

Schinzel [27] asserts that this conjecture follows from his Hypothesis H.

(2) If, as conjectured by Hardy and Littlewood, the number of pairs of twin primes $\leqslant x$ is $\sim Cx/\log^2 x$, then the number of common values $n \leqslant x$ of ϕ and σ is $\gg x/\log^2 x$. What is the correct order of $\#\{n \leqslant x : A(n) \geqslant 1 \text{ and } B(n) \geqslant 1\}$?

(3) Does $\phi(a) = \sigma(b)$ have infinitely many solutions with squarefree integers a, b? Our construction, when using (α, ε)-good values of x, uses squarefree b while a is divisible by large powers of primes.

(4) As mentioned, Erdős showed that $A(k!) \geqslant 1$ for every positive integer k [18, sec. B38]. Is $B(k!) \geqslant 1$ for every $k \neq 2$? How about at least infinitely often? Note that our proof in Lemma 4.2 shows that there is some number $c > 0$ such that $A(k!) \geqslant (k!)^c$ for every k.

Remarks. There is an alternative approach to proving Theorems 1 and 2 (with a somewhat weaker conclusion about the number of common values below x), suggested to us by Sergei Konyagin. Namely, it is possible to prove, using Lemmas 2.1 and 2.2, that there is an $\alpha > 0$ such that for large u, there is a value of $x \in [\log u, u]$ which is $(\alpha, \frac{1}{10})$-good. Indeed, let $\lambda > 0$ be small, and let α be the constant from Lemma 2.2. Let γ be a constant satisfying $\gamma > 1/(10\alpha)$. Let $m_1, m_2, \ldots$ be the (possibly empty) list of moduli for which there is a character $\chi \in C(m_j)$ and zero $\beta_j \geqslant 1 - \lambda/\log m_j$ of $L(s, \chi)$. Let j be the largest index with $m_j \leqslant (\log x)^\alpha$. If there is no such j, then x is $(\alpha, \frac{1}{10})$-good. Otherwise, $u = \max(\log x, \exp\{\gamma(1 - \beta_j)^{-1}\})$ is $(\alpha, \frac{1}{10})$-good upon using the definition of j and applying Lemma 2.1.

REFERENCES

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

[2] A. Balog, *p + a without large prime factors*, Sém. Théorie des Nombres Bordeaux (1983-84), exposé 31.

[3] J. Bayless, *The Lucas–Pratt primality tree*, Math. Comp. **77** (2008), 495–502.

[4] H. Davenport, *Multiplicative number theory, third edition*, Graduate Texts in Mathematics vol. 74, Springer-Verlag, New York, 2000.

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

[6] P. Erdős, *Some remarks on Euler's φ-function and some related problems*, Bull. Amer. Math. Soc. **51** (1945), 540–544

[7] P. Erdős, *Some remarks on Euler's ϕ-function*, Acta Arith. **4** (1958), 10–19.

[8] P. Erdős, *Remarks on number theory, II. Some problems on the σ function*, Acta Arith. **5** (1959), 171–177.

[9] P. Erdős and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématique **28**, Geneva, 1980.

[10] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, Analytic number theory (Allerton Park, IL, 1989), 165-204, Progr. Math., 85, Birkhäuser Boston, Boston, MA, 1990.

[11] K. Ford, *The distribution of totients*, Paul Erdős (1913–1996). Ramanujan J. **2** (1998), no. 1-2, 67–151.

[12] K. Ford, *The number of solutions of $\phi(x) = n$*, Ann. Math. **150** (1999), 283–311.

[13] K. Ford and S. Konyagin, *On two conjectures of Sierpiński concerning the arithmetic functions σ and ϕ*, Number Theory in Progress (Zakopane, Poland, 1997), vol. II, de Gruyter (1999), 795–803.

[14] K. Ford, S. V. Konyagin and F. Luca, *Prime chains and Pratt trees*, submitted (2009). ArXiv : `math/0904.0473`

[15] J. Friedlander, *Shifted primes without large prime factors*, in: Number Theory and Applications, 1989, Kluwer, Berlin, 1990, 393–401.

[16] P. X. Gallagher, *A large sieve density estimate near $\sigma = 1$*, Inv. Math. **11** (1970), 329–339.

[17] G. R. Grimmett and D. R. Stirzaker, *Probability and random processes, second edition*, Oxford U. Press, Oxford, 1992.

[18] R. K. Guy, *Unsolved problems in number theory, third edition*, Springer, New York, 2004.

[19] H. Halberstam and H.-E. Richert, *Sieve methods*, LMS Monographs No. 4, Academic Press, London, 1974.

[20] D. R. Heath-Brown, *Prime twins and Siegel zeros*, Proc. London Math. Soc. (3) **47** (1983), 193-224.

[21] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théorie Nombres Bordeaux **5** (1993), 411–484.

[22] H. Kadiri, *An explicit zero-free region for the Dirichlet L-functions*, ArXiv : `math.NT/0510570`.

[23] F. Luca and C. Pomerance, *Irreducible radical extensions and Euler-function chains*, Combinatorial number theory (Proc. Integers Conf. 2005), 351-361, de Gruyter, Berlin, 2007. Also: Integers **7**(2) (2007), A25.

[24] K. McCurley, *Explicit estimates for the error term in the prime number theorem for arithmetic progressions*, Math. Comp. **42** (1984), 265–285.

[25] S. Pillai , *On some functions connected with $\phi(n)$* , Bull. Amer. Math. Soc. **35** (1929), 832–836.

[26] C. Pomerance, *Popular values of Euler's function*, Mathematika **27** (1980), 84–89.

[27] A. Schinzel, *Remarks on the paper 'Sur certaines hypothèses concernant les nombres premiers'*, Acta Arith. **7** (1961), 1–8.

[28] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208. *Corrigendum*, ibid. **5** (1960), 259.

[29] K. Wooldridge, *Values taken many times by Euler's phi-function*, Proc. Amer. Math. Soc. **76** (1979), 229–234.

DEPARTMENT OF MATHEMATICS, 1409 W. GREEN ST., UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, URBANA, IL 61801, USA
E-mail address: `ford@math.uiuc.edu`

INSTITUTO DE MATEMÁTICAS, UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO, C.P. 58089, MORELIA, MICHOACÁN, MÉXICO
E-mail address: `fluca@matmor.unam.mx`

DEPARTMENT OF MATHEMATICS, DARTMOUTH COLLEGE, HANOVER, NH 03755, USA
E-mail address: `carl.pomerance@dartmouth.edu`