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 fifty-year-old conjecture of Erdős. Moreover, we show that, for some c > 0, there are infinitely many integers n such that $\phi(a) = n$ and $\sigma(b) = n$, each having more than n^c solutions. 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 fifty years ago, Paul Erdős conjectured that the ranges of ϕ and σ have an infinite intersection [7, p. 172; 27, p. 198]. This conjecture follows easily from some famous unsolved problems. For example, if there are infinitely many pairs of twin primes p and 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 [10] 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 95 145 common values of ϕ and σ between 1 and 10⁶. This is to be compared with a total of 180 184 ϕ -values and 189 511 σ -values in the same interval. In [8], 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 [17, Section B38]) that $\phi(a) = k!$ is solvable for every positive integer k, and 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 the 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 [13] (see Section 3 for a definition) and estimates for primes in arithmetic progressions. The possible existence of Siegel zeros (see Section 2 for a definition) creates a major obstacle for the success of our argument. Fortunately, Heath-Brown [19] 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 1.1. The equation $\phi(a) = \sigma(b)$ has infinitely many solutions. Moreover, for some positive α and all large x, there are at least $\exp((\log \log x)^{\alpha})$ integers $n \leq x$ that are common values of ϕ and σ .

Received 3 July 2009.

²⁰⁰⁰ Mathematics Subject Classification 11A25, 11N25, 11N64.

The research of the first author was supported in part by NSF grant DMS-0555367, that of the second author was supported in part by the projects PAPIIT 100508 and SEP-CONACyT 79685, and that of the third author was supported in part by NSF grants DMS-0555367 and DMS-0901339.

We also show that there are infinitely many integers n that 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 $\sigma(x) = n$. In 1929 Pillai [24] showed 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, 14, 25, 28]), 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 1.2. 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 $n \leq x$, for all 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 1.1. In Section 4, we present the additional arguments needed to deduce the conclusion of Theorem 1.2. Theorem 1.2 resolves another conjecture of Erdős (stated as Conjecture C_8 in [27, 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 $n = \sigma(\prod_{p \in S} p) = \prod_{p \in S} (p+1)$, where S is a set of primes $p \leq x$ for which all prime factors of p+1 are small, say at most z. In this way, n should be the product of some of the primes at most z, each to a possibly large power. We deduce that n is in the range of ϕ by exploiting the general implication

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

where $\operatorname{rad}(m)$ 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 $n = \sigma(\prod_{p \in S} p)$ that $v_q(\phi(\operatorname{rad}(n))) \leq v_q(n)$ for $q \leq z$; hence, the hypothesis in (1.1) should hold. Turning this into a proof requires lower bounds of the expected order for the number of $p \in S$ for which $q \mid p+1$.

We remark that, by our proofs below, the numbers n, which are constructed for Theorems 1.1 and 1.2, are also values taken by the Carmichael function $\lambda(m)$, the largest order of an element of $(\mathbb{Z}/m\mathbb{Z})^*$. Moreover, for the n in Theorem 1.2, there are at least n^c such values m. We thank Bill Banks for this observation.

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. The symbols p, q, and 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 $p \leq x$, with $p \equiv a \pmod{m}$, and let

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

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, Chapter 14]) that, for some constant $c_0 > 0$ and every $m \ge 3$, there is at most one zero of $\prod_{\chi \in C(m)} L(s, \chi)$ in the region

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

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

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

for some positive constant c_1 . Better upper bounds on β are known (Siegel's theorem [4, Chapter 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, Chapter 14].

LEMMA 2.1 (Landau). For some constant $c_2 > 0$, if $3 \leq m_1 < m_2$, $\chi_1 \in \mathcal{C}(m_1)$, 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 $\beta > 1 - c_2/\log(m_1m_2)$.

We immediately obtain the following.

LEMMA 2.2 (Page). For any $M \ge 3$, the function

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

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

McCurley [23] showed that $c_0 = 1/9.645908801$ holds in (2.1). Kadiri [21] showed that we may take $c_0 = 1/6.397$ and, in Lemmas 2.1 and 2.2, we may take $c_2 = 1/2.0452$.

It is known from McCurley [23] that $c_0 = 1/9.645908801$ holds in (2.1); Kadiri [21] showed that we may take $c_0 = 1/6.397$; and, by Lemmas 2.1 and 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 $(1 - \beta) \log m \rightarrow 0$, then such zeros are known as Siegel zeros, and their existence would have profound implications on the distribution of primes in arithmetic progressions [4, Chapter 20, (9)]). As mentioned before, Heath-Brown showed that the existence of Siegel zeros implies that there are infinitely many prime twins.

LEMMA 2.3 [19, Corollary 2]. If $\chi \in C(m)$ and $L(\beta, \chi) = 0$ for $\beta = 1 - \lambda(\log m)^{-1}$, then, for $m^{300} < z \leq m^{500}$, the number of primes $p \leq z$ with p + 2 prime is

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

If Siegel zeros do not exist, then there still may be some Dirichlet L-function zeros with real part greater than 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 Theorem 7 in [15]). Let

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

3

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 $0 < \alpha \leq 1$ and x_0 so that, for $x \geq x_0$, we have

$$\sum_{\substack{\leqslant m \leqslant x^{\alpha} \\ m \neq m_{0}}} \Psi(x,m) \leqslant \varepsilon x.$$

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, then 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 $1 \leq M \leq x$, we have

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

Proof. This is [4, Chapter 28, (2)].

For positive reals δ, γ, y , and x, with $1 \leq y \leq x^{1/2-\delta}$, and a nonzero integer a, we 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 $\Psi(x; m) \leq \varepsilon x$ for $3 \leq m \leq x^{\alpha}$. Roughly speaking, this means that the exceptional modulus in Lemma 2.4 does not exist (for appropriate λ).

LEMMA 2.6. There are absolute constants $\delta > 0$ and $\gamma > 0$ such that the following holds. For every $\alpha > 0$, there are constants $\eta > 0$ and $x_1 > 0$ such that, if $x \ge x_1$ and x is $(\alpha, \frac{1}{10})$ -good, then, for all $y \le x^{1/2-\delta}$, we have

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

Proof. We may assume that $0 < \delta < 1/6$. Let k be a positive integer such that $Q = 2^{-k}x^{1/2-\delta} \ge 1$. Let $R_1 = \max\{Q^{-1}x^{1/2-5\delta/4}, x^{\delta/4}\}$ and let $R_2 = R_1x^{\delta/4}$. By standard estimates [4, Chapter 20, (3)], if $q \in (Q, 2Q]$ and $r \in (R_1, R_2]$, then, for $a = \pm 1$, we have

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

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 $Q \leq \frac{1}{2}x^{\alpha}$. Otherwise, by Lemma 2.5, we have

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

Let

$$\mathcal{E}_2(Q) = \{ q \in (Q, 2Q] : \Psi(x, qr) > x/10 \text{ for at least } R_1 x^{-\delta/8} \text{ primes } r \in (R_1, R_2] \}.$$

By Lemma 2.5 and the inequality $R_2 Q \leq x^{1/2-\delta/2}$, we have

$$\#\mathcal{E}_2(Q) \ll \frac{(x+x^{5/6}R_2Q+x^{1/2}(R_2Q)^2)\log^4 x}{R_1x^{1-\delta/8}} \ll Qx^{-\delta/8}\log^4 x.$$

Also, by Lemma 2.5, we have

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

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

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

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

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

Also, by the above estimates and Mertens' formula, we have

$$\sum_{r \in \mathcal{R}(q)} \frac{1}{r} \ge \sum_{R_1 < r \leqslant R_2} \frac{1}{r} - O(x^{-\delta/8} \log^4 x) \ge \frac{\delta}{2}.$$
(2.5)

Since $R_1 \ge x^{\delta/4}$, it follows that a shifted prime p + a is divisible by at most $\lfloor 4/\delta \rfloor$ primes in $\mathcal{R}(q)$. Hence, we have

$$S_q(x; \delta, a) \ge \frac{\delta}{4} \sum_{r \in \mathcal{R}(q)} \left(\pi(x; qr, -a) - \#\mathcal{U}(q, r) \right),$$

where

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

Since $r \leq R_2 \leq x^{1/2-\delta}$, if $p \in \mathcal{U}(q,r)$, then p + a = qrsb, where $s > x^{1/2-\delta}$ is prime and

$$b \leqslant \frac{x+1}{qrs} \leqslant \frac{x+1}{x^{1-9\delta/4}} \leqslant x^{3\delta}$$

For fixed b, q, r, and a, we estimate the number of possible choices for s using the sieve [18, Theorem 3.12]. We obtain

$$\#\mathcal{U}(q,r) \ll \sum_{b \leqslant x^{3\delta}} \frac{x}{bqr \log^2(x/bqr)} \frac{b}{\phi(b)} \ll \frac{x}{qr \log^2 x} \sum_{b \leqslant x^{3\delta}} \frac{1}{\phi(b)} \ll \frac{\delta x}{qr \log x}.$$

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

$$S_q(x; \delta, a) \ge \frac{\delta x}{16q \log x} \sum_{r \in \mathcal{R}(q)} \frac{1}{r} \ge \frac{\delta^2 x}{32q \log x}.$$

Finally, $\#\mathcal{E}_1(Q) + \#\mathcal{E}_2(Q) \leq \frac{1}{4}Qx^{-\eta}$ for $\eta = \min\{\alpha/2, \delta/9\}$ and large x. Summing over choices of the dyadic interval (Q, 2Q], with $Q \leq y$ and $a \in \{-1, 1\}$, completes the proof.

3. Prime chains and the proof of Theorem 1.1

Suppose that n is a positive integer with $\phi(\operatorname{rad}(n)) \mid n$ 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 $q \mid \phi(\operatorname{rad}(n))$, 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 $\phi(\operatorname{rad}(n)) \mid n$, 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 $t \leq y$ that are in a prime chain for q. Crucial to our proof is the following estimate.

LEMMA 3.1 [13]. For every $\varepsilon > 0$, there is a constant $C(\varepsilon)$ so that, if q is prime and y > q, then $\#\mathcal{T}(y,q) \leq C(\varepsilon)(y/q)^{1+\varepsilon}$.

More estimates for counts of prime chains with various properties may be found in [3, 9, 13, 22].

We now proceed to prove Theorem 1.1. There is an absolute constant $\lambda_0 > 0$ so that, if $\lambda \leq \lambda_0$, 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 that $x \ge \max(x_0, x_1)$. We show that there are many common values of ϕ and σ that are at most e^{2x} by considering two cases. First, suppose that x is not (α, ε) -good. Then, for some $m \le x^{\alpha}$ and $\chi \in \mathcal{C}(m)$, we have $L(\beta, \chi) = 0$ for some $\beta \ge 1 - \lambda_0/\log(x^{\alpha})$. By (2.2), we have

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

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

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

Let $S = \{p \in \mathcal{T} : P(p+1) > z^{\theta}\}$. Choose θ so small that $\#S \ge z/\log^2 z$. For $p \in S$, 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 $n(\mathcal{M}) = \prod_{p \in \mathcal{M}} (p+1)$, so that $n(\mathcal{M}) = \sigma(\prod_{p \in \mathcal{M}} p) = \phi(\prod_{p \in \mathcal{M}} (p+2))$. Furthermore, since each factor p+1 in the product $n(\mathcal{M})$ has the unique 'marker prime' P(p+1) that divides no other p'+1 in the product, the numbers $n(\mathcal{M})$ are distinct as \mathcal{M} varies. Since $n(\mathcal{M}) \leq z^{\#\mathcal{P}} \leq x^{500\alpha x^{500\theta\alpha}} \leq e^x$ for x large, there are at least $2^{\#\mathcal{P}} > \exp\{z^{\theta/2}\}$ common values of ϕ and σ that are at most 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

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

Consider

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Popular common values of ϕ and σ

In this section, we combine the proof of Theorem 1.1 with a method of Erdős [5]. A key estimate is [5, Lemma 2] as follows:

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

$$(4.1)$$

More results about the distribution of integers n with P(n) small may be found in [20].

Let us define $\lambda = \lambda_0$, α , x_0 , x_1 , and η as in the proof of Theorem 1.1. Without loss of generality, suppose that $\alpha \leq \frac{1}{500}$. Theorem 1.2 is proved by considering the following two cases: x is not $(\alpha, \frac{1}{10})$ -good and x is $(\alpha, \frac{1}{10})$ -good. The following lemmas provide the necessary arguments.

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

Proof. As in the proof of Theorem 1.1, by (2.2), there is an exceptional modulus m satisfying

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

Page 8 of 11

and such that

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

$$(4.2)$$

Let δ be a positive absolute constant. Let \mathcal{P} be the set of primes $p \leq z$, with p+2 prime and $P(p+1) \leq z^{1-\delta}$. 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 $b \leq z^{\delta}$. By sieve methods [18, Theorem 2.4], for small enough δ , we have

$$\begin{aligned} \#\mathcal{P} \geqslant \frac{z}{\log^2 z} &- \sum_{b \leqslant z^{\delta}} \#\{q \leqslant z/b : q, \ qb-1, \ qb+1 \text{ prime}\} \\ \geqslant \frac{z}{\log^2 z} &- O\left(\sum_{b \leqslant z^{\delta}} \frac{z}{b \log^3 z} \left(\frac{b}{\phi(b)}\right)^2\right) \geqslant \frac{z}{\log^2 z} - O\left(\frac{\delta z}{\log^2 z}\right) \geqslant \frac{z}{2 \log^2 z}. \end{aligned}$$

Let $H = \lfloor z^{1-\delta/2} \rfloor$ and $J = \lfloor \# \mathcal{P}/H \rfloor$. Define the sets \mathcal{P}_j , with $1 \leq j \leq J$, as follows: \mathcal{P}_1 is the set of the smallest H primes in \mathcal{P} , and \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 $K \geq 2$, so that, if \mathcal{M} is a set of K primes from some \mathcal{P}_j , then

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

By (4.1), the function $n(\cdot)$ maps sets \mathcal{M} into a set of integers of cardinality $\leq z^{\delta K/6}$; 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 $j \leq J$, 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 $A(n_j), B(n_j) \geq z^{\delta K/3} \geq n_j^{\delta/3}$. Since $n_1 < n_2 < \ldots < n_J \leq z^K < e^x$ and $J \geq z^{\delta/2}/(2\log^2 z) - 1$, we conclude that the lemma holds with $c = \delta/3$ and $a = 499\delta$ once x is sufficiently large.

LEMMA 4.2. There is an absolute constant c > 0, so that, if $\alpha > 0$, and x is large (depending on α) and $(\alpha, \frac{1}{10})$ -good, then there are more than $(1/3) \log x$ integers $n \leq e^x$ 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) and \mathcal{S} as in (3.2), and consider $\widetilde{\mathcal{S}} = \{p \in \mathcal{S} : p \ge \sqrt{x}\}$. Let $N := \#\widetilde{\mathcal{S}}$, so that, from (3.4), we have $N \ge (\gamma/4)x/\log x$ for x large. Also, $N \le 2x/\log x$. Let \mathcal{Q} be the set of primes $q \le x^{1/2-\delta}$ with $q \notin \mathcal{T}$. For $q \in \mathcal{Q}$, by (3.6) and the Brun–Titchmarsh inequality, we have

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

Suppose that k is an integer with $N^{1/2} \leq k \leq N^{3/4}$. For $q \in Q$, if we choose a k-element subset \mathcal{M} of $\widetilde{\mathcal{S}}$ at random, then 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 that is 1 if $q \mid p+1$, and 0 otherwise. By a standard result in the theory of large deviations (see [16, Section 5.11, (5)]), we have that the number of choices of \mathcal{M} , with

$$\#\{p \in \mathcal{M} : q \mid p+1\} \ge \frac{kN_q}{2N} \quad \text{for all } q \in \mathcal{Q}$$

$$(4.5)$$

is at least

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

for some absolute positive constant ν , and for large x. (That the probabilistic model has us choosing 'with replacement' is easily seen to be negligible.) As in the proof of Lemma $4.1, n(\mathcal{M}) = \sigma(\prod_{p \in \mathcal{M}} p) < x^k$ and $P(n(\mathcal{M})) \leq x^{1/2-\delta} < \log(x^k)$. By (4.1), there are at most $x^{k/30} \leq N^{k/29}$ 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, we have

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

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 $\phi(w \cdot \operatorname{rad}(n)) \mid n$, then

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

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 $w \cdot \operatorname{rad}(n) \cdot n/\phi(w \cdot \operatorname{rad}(n))$ are distinct for the different w). Toward 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 $q^j \leqslant x$. Consider $k' = \lceil \xi k \rceil$, 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, then the expected value of $\sum_{p \in \mathcal{M}'} v_q(p-1) = v_q(\phi(w(\mathcal{M}')))$ is $k' \sum_{j \ge 1} j N'_{q^j}/N'$ (we are now viewing our random variable as $v_q(p-1)$). By the same result in [16], there are at least $\frac{1}{2} {N' \choose k'}$ choices for \mathcal{M}' with

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

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

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

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

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

Consider $c = \min(1/5, \xi/5)$. Note 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 more than $(1/3) \log x$ distinct values of n, each at most e^x , for which $A(n) > n^c$ and $B(n) > n^c$.

5. Further problems

The following are some additional problems concerning common values of ϕ and σ .

(1) It is known that, for any integer $k \ge 1$, there are integers n with B(n) = k and, for any integer $l \ge 2$, there are integers n with A(n) = l; see [11, 12]. The famous Carmichael conjecture states that A(n) is never 1, but this is still open.

CONJECTURE 5.1. For every $k \ge 1$ and $l \ge 2$, there are integers n with A(n) = l and B(n) = k.

Schinzel has shown (private communication; see also [26]) that this conjecture follows from his Hypothesis H.

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

(3) Does $\phi(a) = \sigma(b)$ have infinitely many solutions with squarefree integers a and 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 $A(k!) \ge 1$ for every positive integer k (see [17, Section B38]). Is $B(k!) \ge 1$ for every $k \ne 2$? How about at least infinitely often? Note that our proof of Lemma 4.2 shows that there is some number c > 0 such that $A(k!) \ge (k!)^c$ for every k.

REMARK 5.2. There is an alternative approach to proving Theorems 1.1 and 1.2 (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 $x \in [\log u, u]$ that 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 $\beta_j \ge 1 - \lambda/\log m_j$ of $L(s, \chi)$. Let j be the largest index with $m_j \le (\log x)^{\alpha}$. 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.

Acknowledgements. This paper was begun while the first two authors were visiting Dartmouth College; they thank the Mathematics Department for its hospitality. The authors thank Paul Pollack for some helpful conversations.

References

- 1. R. C. BAKER and G. HARMAN, 'Shifted primes without large prime factors', Acta Arith. 83 (1998) 331-361.
- A. BALOG, 'p + a without large prime factors', Seminar on number theory, 1983–1984 (Talence, 1983/1984), Exp. No. 31, 5 pp. (University of Bordeaux I, Talence, 1984).
- 3. J. BAYLESS, 'The Lucas–Pratt primality tree', Math. Comp. 77 (2008) 495–502.
- H. DAVENPORT, Multiplicative number theory, 3rd edn, Graduate Texts in Mathematics 74 (Springer, 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', Q. J. Math. 6 (1935) 205–213.

- P. ERDŐS, 'Some remarks on Euler's φ-function and some related problems', Bull. Amer. Math. Soc. 51 (1945) 540–544.
- 7. P. ERDŐS, 'Remarks on number theory, II. Some problems on the σ function', Acta Arith. 5 (1959) 171–177. 8. P. ERDŐS and R. L. GRAHAM, Old and new problems and results in combinatorial number theory,
- Monographies de L'Enseignement Mathématique 28 (L'Enseignment Mathématique, Geneva, 1980). 9. 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) (eds B.C. Berndt et al.), Progress in Mathematics 85 (Birkhäuser, Boston, MA, 1990) 165–204.
- 10. K. FORD, 'The distribution of totients', Ramanujan J. 2 (1998) 67–151.
- **11.** K. FORD, 'The number of solutions of $\phi(x) = n$ ', Ann. Math. 150 (1999) 283–311.
- 12. K. FORD and S. KONYAGIN, 'On two conjectures of Sierpiński concerning the arithmetic functions σ and ϕ ', Number theory in progress (eds K. Gröy and H. Iwaniec), vol. II (de Gruyter, Berlin, 1999) 795–803.
- K. FORD, S. V. KONYAGIN and F. LUCA, 'Prime chains and Pratt trees', Preprint, 2009, arXiv:math/0904.0473.
- J. FRIEDLANDER, 'Shifted primes without large prime factors', Number theory and applications (ed. R.A. Mollin) (Kluwer, Berlin, 1990) 393–401.
- **15.** P. X. GALLAGHER, 'A large sieve density estimate near $\sigma = 1$ ', Invent Math. 11 (1970) 329–339.
- G. R. GRIMMETT and D. R. STIRZAKER, Probability and random processes, 2nd edn (Oxford University Press, Oxford, 1992).
- 17. R. K. GUY, Unsolved problems in number theory, 3rd edn (Springer, New York, 2004).
- **18.** H. HALBERSTAM and H.-E. RICHERT, *Sieve methods*, London Mathematical Society Monographs 4 (Academic Press, London, 1974).
- 19. D. R. HEATH-BROWN, 'Prime twins and Siegel zeros', Proc. London Math. Soc. (3) 47 (1983) 193–224.
- 20. A. HILDEBRAND and G. TENENBAUM, 'Integers without large prime factors', J. Théor. Nombres Bordeaux
- 5 (1993) 411–484. 21. H. KADIRI, Une région explicite sans zéro pour les fonctions L de Dirichlet, PhD thesis, Université de Lille I, 2002.
- 22. F. LUCA and C. POMERANCE, 'Irreducible radical extensions and Euler-function chains', Combinatorial number theory (eds B. Landman et al.) (de Gruyter, Berlin, 2007) 351–361.
- K. MCCURLEY, 'Explicit estimates for the error term in the prime number theorem for arithmetic progressions', Math. Comp. 42 (1984) 265-285.
- **24.** S. PILLAI, 'On some functions connected with $\phi(n)$ ', Bull. Amer. Math. Soc. 35 (1929) 832–836.
- 25. C. POMERANCE, 'Popular values of Euler's function', Mathematika 27 (1980) 84-89.
- 26. A. SCHINZEL, 'Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers", Acta Arith. 7 (1961) 1–8.
- 27. A. SCHINZEL and W. SIERPIŃSKI, 'Sur certaines hypothèses concernant les nombres premiers', Acta Arith. 4 (1958) 185–208; Corrigendum, Acta Arith. 5 (1960) 259.
- K. WOOLDRIDGE, 'Values taken many times by Euler's phi-function', Proc. Amer. Math. Soc. 76 (1979) 229-234.

Kevin Ford Department of Mathematics University of Illinois at Urbana-Champaign 1409 W. Green St. Urbana, IL 61801 USA

ford@math.uiuc.edu

Florian Luca Instituto de Matemáticas Universidad Nacional Autonoma de México Ap. Postal 61-3 (Xangari) C.P. 58089, Morelia Michoacán México

fluca@matmor.unam.mx

Carl Pomerance Department of Mathematics Dartmouth College Hanover, NH 03755 USA

carl.pomerance@dartmouth.edu