CYCLOTOMIC PRIMES

CARL POMERANCE

Abstract. Mersenne primes and Fermat primes may be thought of as primes of the form $\Phi_m(2)$, where $\Phi_m(x)$ is the mth cyclotomic polynomial. This paper discusses the more general problem of primes and composites of this form.

1. Introduction

Studied since antiquity, we have the Mersenne primes. These are prime numbers 1 less than a power of 2, so of the form $2^n - 1$. To be prime it is necessary that $n = p$ is prime, but this is not sufficient, eg. $p = 11$. The first 4 of these primes were known to Euclid and they played a key role in his work on perfect numbers. We now know more than 50 Mersenne primes, the largest at present being $2^p - 1$ with $p = 82{,}589{,}933$, see [8]. Evidently it takes some doing to check the primality of numbers this large!

It is widely believed that there are infinitely many Mersenne primes, and also that there are infinitely many primes p with $2^p - 1$ composite. Though both assertions are still unsolved, there is a conditional proof of the second one based on the prime k-tuples hypothesis: If $p \equiv 3 \pmod 4$ is prime with $p > 3$ and $q = 2p + 1$ is prime, then $2^p - 1$ is composite. Indeed, the conditions imply that $q \equiv 7 \pmod 8$ so that $(2/q) = 1$. This implies that $q \mid 2^{(q-1)/2} - 1 = 2^p - 1$, and the condition $p > 3$ implies that $q < 2^p - 1$. Thus q is a proper divisor of $2^p - 1$ implying the latter is composite. For example, $23 \mid 2^{11} - 1$. It remains to note that the prime k-tuples hypothesis implies there are infinitely many primes $p \equiv 3 \pmod 4$ with $2p + 1$ prime.

Also studied for centuries are the Fermat primes. These are primes that are 1 more than a power of 2, so of the form $2^n + 1$. To be prime (and > 2) it is necessary that n itself is a power of 2. Again, this is not sufficient. Fermat knew that $2^{2^k} + 1$ is prime for $k = 0, 1, 2, 3, 4$ and

Mathematics Department, Dartmouth College, Hanover, NH 03755, USA. email: carlp@math.dartmouth.edu

Date: October 11, 2024.

2010 *Mathematics Subject Classification.* 11N32, 11N25.

Key words and phrases. Mersenne prime, Fermat prime, cyclotomic polynomial, abc conjecture.

he conjectured that it is always prime. However, Euler showed that $641 \mid 2^{2^5}+1$. It is now known that $2^{2^k}+1$ is composite for all larger values of k up to 32, and also some sporadic larger values as well. It is conjectured that all but finitely many are composite and that perhaps $2^{2^4}+1$ is the largest Fermat prime. Nothing has been proved here, even conditionally.

What Mersenne primes and Fermat primes have in common is that they are *cyclotomic primes*. These are primes of the form $\Phi_m(2)$, where Φ_m is the mth cyclotomic polynomial. This is the minimal polynomial in $\mathbb{Q}[x]$ for $e^{2\pi i/m}$ and it has degree $\varphi(m)$, Euler's function. We have the twin identities:

$$x^m - 1 = \prod_{d \mid m} \Phi_d(x), \quad \Phi_m(x) = \prod_{d \mid m} (x^d - 1)^{\mu(m/d)}.$$

Note that if p is prime, then $\Phi_p(x) = (x^p - 1)/(x-1)$, so that $\Phi_p(2) = 2^p - 1$. Further $\Phi_{2^{k+1}}(x) = (x^{2^{k+1}} - 1)/(x^{2^k} - 1) = x^{2^k} + 1$, so that $\Phi_{2^{k+1}}(2) = 2^{2^k} + 1$. We also have the Wagstaff primes, see [15], which are primes of the form $\Phi_{2p}(2) = (2^p + 1)/3$, where p is an odd prime.

So, a cyclotomic prime is a prime of the form $\Phi_m(2)$. We can ask if there are infinitely many of them and also if there are infinitely many numbers of this form that are composite. It turns out that there are infinitely many composites for fairly trivial reasons. The substance of this paper is to show that there are infinitely many nontrivial composites. We make this precise in the next section.

2. Basics and statement of results

Let

$$\phi_m := \Phi_m(2).$$

We say a prime factor p of ϕ_m is *primitive* if it does not divide any ϕ_k for $k < m$. Otherwise we say p is *intrinsic*. For an odd prime p let $\ell(p)$ denote the mutlplicative order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$. We have that p is a primitive prime factor of ϕ_m if and only if $\ell(p) = m$. Further, ϕ_m has an intrinsic prime factor p if and only if $m = p^j \ell(p)$ for some positive integer j, in which case p is the largest prime factor of m and $p \parallel \phi_m$. If m is of this form, let $\delta_m = p$, and otherwise let $\delta_m = 1$. Thus, every prime factor of

$$\psi_m := \phi_m / \delta_m$$

is primitive.

We know that for each $m \notin \{1, 6\}$, there is at least one primitive prime factor of ϕ_m; this is Bang's theorem. The numbers ψ_m are pairwise coprime and except for $m = 1$ or 6, they are all > 1 (cf. [17]).

Due to the factorization

$$4x^4 + 1 = (2x^2 + 2x + 1)(2x^2 - 2x + 1),$$

there is a further generic factorization of ϕ_m beyond $\delta_m\psi_m$ when $m \equiv 4 \pmod 8$. Note that

$$2^{4k+2} + 1 = 4(2^k)^4 + 1 = (2^{2k+1} + 2^{k+1} + 1)(2^{2k+1} - 2^{k+1} + 1),$$

which leads to the factorization

$$\begin{aligned}(1)\quad \psi_{8k+4} &= \gcd(\psi_{8k+4}, 2^{2k+1} + 2^{k+1} + 1)\gcd(\psi_{8k+4}, 2^{2k+1} - 2^{k+1} + 1)\\ &=: \psi^+_{8k+4}\psi^-_{8k+4}.\end{aligned}$$

Further, this factorization is nontrivial for $k \geq 3$, a result due to Schinzel [18]. The factorization (1) is known under the name Aurifeuille, see [3].

Note that

$$\phi_m \in [2^{\varphi(m)-1}, 2^{\varphi(m)+1}), \tag{2}$$

see [9, Theorem 3.6], [17, Theorem 4.3].

To state our results, consider the sets

$$C_1 = \{\psi_m : m \not\equiv 4 \pmod 8\}, \quad C_2 = \{\psi_m : m \equiv 4 \pmod 8\}.$$

Theorem 1. *The set C_1 contains infinitely many composite numbers. The set C_2 contains infinitely many numbers that are not the product of two primes.*

The proof uses the deep result that for some θ with $1/2 < \theta < 1$, there are infinitely many primes p such that $p - 1$ has a large prime factor $q > p^\theta$. We can also prove a slightly stronger result conditional on the abc conjecture.

Theorem 2. *Assume the abc conjecture. The set C_1 contains infinitely many numbers divisible by at least 2 distinct primes. The set C_2 contains infinitely many numbers divisible by at least 3 distinct primes.*

We remark that the abc conjecture has been used for similar purposes in [19] and [2, Theorem 3].

Throughout the letters p, q will always denote prime numbers. We also let $P^+(n)$ denote the largest prime factor of $n > 1$, and we let $P^+(1) = 1$.

3. Proof of Theorem 1

Denote by $\pi(x; d, a)$ the number of primes $p \leq x$ with $p \equiv a \pmod d$. Our principal tool is the following theorem. Let $\theta = 3/5$.

Proposition 1. *We have*

$$\sum_{q>x^\theta} \pi(x;4q,2q+1)\log q \gg x \quad \textit{and} \quad \sum_{q>x^\theta} \pi(x;8q,4q+1)\log q \gg x.$$

The analogous result for $\pi(x;q,1)$ is well known with varying values of "θ" in the literature. The current champions are Baker and Harman [1], who essentially have $\theta = 0.677$, though they do not state their result in the same way. Probably the techniques of their paper would allow the same value of θ in Proposition 1, but we do not pursue the optimal value at this point. Other results in their paper have been recently strengthened (see [12]); conjecturally any value of $\theta < 1$ may be used.

We now sketch a proof of Proposition 1. With Λ the von Mangoldt function, we have

$$\begin{aligned}\sum_{d\le x} \pi(x;4d,2d+1)\Lambda(d) &= \sum_{\substack{p\equiv 3 \pmod 4\\ p\le x}} \sum_{d\,|\,(p-1)/2} \Lambda(d) + O(x/\log x)\\ &= \sum_{\substack{p\equiv 3 \pmod 4\\ p\le x}} \log(p-1) + O(x/\log x)\\ &= \frac{1}{2}x + O(x/\log x).\end{aligned}$$

Further, by the Bombieri–Vinogradov theorem plus a small additional argument using the Brun–Titchmarsh inequality (see [14]) to clean up the boundary cases, we have

$$\sum_{d\le x^{1/2}} \pi(x;4d,2d+1)\Lambda(d) \sim \frac{1}{4}x, \quad x\to\infty.$$

Thus,

$$\sum_{d> x^{1/2}} \pi(x;4d,2d+1)\Lambda(d) \sim \frac{1}{4}x, \quad x\to\infty.$$

The contribution to this last sum when d is composite is $o(x)$, so we have

$$\sum_{q> x^{1/2}} \pi(x;4q,2q+1)\log q \sim \frac{1}{4}x, \quad x\to\infty.$$

By the Brun–Titchmarsh inequality,

$$\begin{aligned}\sum_{x^{1/2}<q\le x^\theta} \pi(x;4q,2q+1)\log q &\le \sum_{x^{1/2}<q\le x^\theta} \frac{2x\log q}{\varphi(4q)\log(x/4q)}\\ &\sim x\log(5/4) < 0.23x.\end{aligned}$$

Thus, with the prior display, we have

$$\sum_{q>x^\theta} \pi(x;4q,2q+1)\log q \gg x,$$

which shows the first assertion in Proposition 1. The second assertion follows in a similar manner.

Since no prime $p \le x$ is divisible by 2 different primes $q > x^\theta$, we have the following result.

Corollary 1. *We have*

$$\sum_{\substack{p\equiv 3 \pmod 4\\ P^+(p-1)>x^\theta\\ p\le x}} 1 \gg x/\log x \quad \textit{and} \quad \sum_{\substack{p\equiv 5 \pmod 8\\ P^+(p-1)>x^\theta\\ p\le x}} 1 \gg x/\log x.$$

An elementary argument shows that the number of primes p with $\ell(p) = k$ is $\ll k/\log k$, it follows that the number of primes $p \le x$ with $\ell(p) \le p^{0.49}$ is $\ll x^{0.98}$. We thus have the following result.

Corollary 2. *The number of primes $p \le x$ with $p \equiv 3 \pmod 4$, $P^+(p-1) > p^\theta$ and $P^+(p-1) \mid \ell(p)$ is $\gg \pi(x)$. Similarly, the number of primes $p \le x$ with $p \equiv 5 \pmod 8$, $P^+(p-1) > p^\theta$ and $P^+(p-1) \mid \ell(p)$ is $\gg \pi(x)$.*

Indeed, if $P^+(p-1) \nmid p-1$, then $\ell(p) \mid (p-1)/P^+(p-1) < p^{1-\theta} < p^{0.49}$, so there are few choices of such p. (Note that there is a similar argument in Goldfeld [7].)

Let $\pi_*(x;d,a)$ denote the number of primes $p \le x$ with $p \equiv a \pmod d$ and also with $\ell(p) > p^{0.49}$.

Corollary 3. *For all sufficiently large x the number of primes $q > x^\theta$ such that $\pi_*(x;4q,2q+1) > 0$ is $> x^\theta$. Similarly, the number of primes $q > x^\theta$ such that $\pi_*(x;8q,4q+1) > 0$ is $> x^\theta$.*

Proof. From the above we have

$$\sum_{q>x^\theta} \pi_*(x;4q,2q+1) \gg x/\log x.$$

The Brun–Titchmarsh theorem shows that

$$\sum_{x^\theta<q\le x^\theta(\log x)^2} \pi_*(x;4q,2q+1) \ll \sum_{x^\theta<q\le x^\theta(\log x)^2} \frac{x}{q\log x} \ll \frac{x\log\log x}{(\log x)^2}.$$

Subtracting this estimate from the prior one, we have

$$\sum_{q>x^\theta(\log x)^2} \pi_*(x;4q,2q+1) \gg x/\log x.$$

Since $\pi_*(x;4q,2q+1) \le x/q < x^{1-\theta}/(\log x)^2$ for $q > x^\theta(\log x)^2$ we have

$$\sum_{\substack{q > x^\theta(\log x)^2 \\ \pi_*(x;4q,2q+1)>0}} 1 \gg x^\theta \log x$$

and the first claim follows. The second one is proved by the analogous argument. □

Proof of Theorem 1. Consider primes $p \le x$ with $P^+(p-1) = q > x^\theta$, $p \equiv 3 \pmod 4$, and with $q \mid \ell(p)$. There are at least x^θ distinct values of q that arise this way. For each such q there is a prime $p \le x$ such that $q \mid \ell(p)$, let p_q be the least one, and let $\ell(p_q) = k_q q$. Then $p_q \mid \psi_{k_q q}$ and the numbers $k_q q$ are distinct as q varies. Note that since $p \equiv 3 \pmod 4$, we have $k_q q \not\equiv 4 \pmod 8$. By (2), $\psi_{k_q q} \gg 2^{\varphi(k_q q)}/q$, so that for large x, p_q is a proper divisor. This proves that C_1 contains infinitely many composite numbers ψ_m, and in fact, the number of such ψ_m with $m \le x$ is $> x^\theta$ for all sufficiently large x.

We can repeat this argument for $p \equiv 5 \pmod 8$. Note that in this case we have $(2/p) = -1$ so that $k_q q \equiv 4 \pmod 8$. It follows from (2) that $\psi^+_{k_q q} \gg 2^{\varphi(k_q q)/2}/q$ and the same for $\psi^-_{k_q q}$, so we again have for sufficiently large x that p_q is a proper divisor. This concludes the proof of the theorem. □

4. Conditional results

For a positive integer n let $\operatorname{rad}(n)$ denote the largest squarefree divisor of n. The abc conjecture asserts that for each fixed $\epsilon > 0$, there are at most finitely many coprime positive integer triples a, b, c with $a + b = c$ and $\operatorname{rad}(abc) < c^{1-\epsilon}$. In this section we will prove Theorem 2, which is conditional on the abc conjecture, and also discuss some other conditional results.

Proof of Theorem 2. First suppose that $m \not\equiv 4 \pmod 8$. We know from Theorem 1 that there are infinitely many such m with ψ_m composite, and in fact, there are more than x^θ such $m \le x$ when x is large. Further, each such m is of the form $k_q q$ where $q > x^\theta$ and $\psi_{k_q q}$ is divisible by a prime $p = p_q \le x$ and $\ell(p) = k_q q$. The only way for a composite number not to be divisible by at least 2 distinct primes is if it is a prime power, namely p^j where $j \ge 2$, so suppose that $\psi_{k_q q} = p^j$. Consider the abc equation $1 + (2^{k_q q} - 1) = 2^{k_q q}$. Since $\psi_{k_q q} \ge \phi_{k_q q}/q$, we have

$$\operatorname{rad}(abc) \le 2pq2^{k_q q}/\phi_{k_q q}.$$

Assuming the abc conjecture this would be impossible for large q if there is some fixed $\epsilon > 0$ such that $\phi_{k_q q} > 2^{\epsilon k_q q}$ (since $2pq = O(x^2) =$

$2^{o(k_q q)}$). Using (2) this would follow if $\varphi(k_q) > 2\epsilon k_q$. We now show that we may assume this is indeed the case.

Recalling that $\ell(p) = k_q q$, write $j = (p-1)/q$, so that $k_q \mid j$. And so if $\varphi(k_q)/k_q \le 2\epsilon$, then $\varphi(j)/j \le 2\epsilon$. For a given value of $j \le x^{1-\theta}$ we consider primes $q \le x/j$ such that $jq+1$ is prime. By Brun's or Selberg's sieve, the number of such q is $\ll x/(\varphi(j)(\log x)^2)$. In the proof of Theorem 1 we showed there are $\ge (.02 + o(1))x/\log x$ pairs q, p. Let

$$J = \{j \le x^{1-\theta} : \varphi(j)/j \le 2\epsilon\}.$$

We will show that $\sum_{j \in J} 1/\varphi(j) \ll \epsilon \log x$, so with ϵ small enough, this will be negligible in comparison with $(.02 + o(1)) \log x$. This would follow from Erdős [5, Theorem 1] (also see [11, Theorem B]), but we prefer to use the simpler approach in [10, Section 3].

We have $(j/\varphi(j))^2 = \sum_{d \mid j} h(d)$, where h is multiplicative, supported on the squarefrees, and has $h(p) = (2p-1)/(p-1)^2$. Then

$$\sum_{n \le z} \left(\frac{n}{\varphi(n)}\right)^2 = \sum_{d \le z} h(d) \left\lfloor \frac{z}{d} \right\rfloor < z \prod_p \left(1 + \frac{h(p)}{p}\right) < 4.5z.$$

Thus, for any $\delta > 0$,

$$\sum_{\substack{n \le z \\ \varphi(n)/n \le \delta}} 1 < 4.5\delta^2 z.$$

A partial summation argument then shows that

$$\sum_{\substack{n \le z \\ \varphi(n)/n \le \delta}} \frac{1}{n} < 4.5\delta^2 \log(ez),$$

so that writing $1/\varphi(n) = 1/n \cdot n/\varphi(n)$,

$$\sum_{\substack{n \le z \\ \frac{1}{2}\delta < \varphi(n)/n \le \delta}} \frac{1}{\varphi(n)} < \frac{2}{\delta} 4.5\delta^2 \log(ez) = 9\delta \log(ez).$$

We apply this with $z = x^{1-\theta}$ and at $\delta = 2\epsilon, \epsilon, \frac{1}{2}\epsilon, \dots$ getting

$$\sum_{j \in J} \frac{1}{\varphi(j)} < 36\epsilon \log(ex).$$

Thus if $\epsilon = \epsilon_0$ is small enough, we would have the number of q, p pairs with $\varphi(j)/j \le \epsilon_0$ being $< .01x/\log x$. But we have seen in the previous section that the total number of q, p pairs generated is $\ge (.02 + o(1))x/\log x$. Thus, we can discard those with $\varphi(j)/j \le \epsilon_0$ and still be left with $\gg x/\log x$ pairs. So, we will have $\varphi(j)/j > \epsilon_0$, which implies that $\varphi(k_q)/k_q > \epsilon_0$. Thus, the abc conjecture is in play to show that the equation $1 + (2^{k_q q} - 1) = 2^{k_q q}$ with $\psi_{k_q q}$ a power of p cannot occur when x is large.

The situation for $kq \equiv 4 \pmod 8$ is completely analogous, we suppress the details. □

We remark that a variant of this argument can show that there are infinitely many m where ψ_m is not square-full, and the same goes for ψ^+_{8k+4} and ψ^-_{8k+4}.

We mentioned in the introduction that the prime k-tuples conjecture can be used to show that there are infinitely many primes p with $\psi_p = 2^p - 1$ composite. We add here a couple of thoughts. First, since we know that the only pair of consecutive numbers which are nontrivial powers is 8 and 9 (a result of Mihăilescu [13]), it follows that $2^p - 1$ cannot be a nontrivial power, so in this case, the abc conjecture is not necessary. Second, using the Hardy–Littlewood version of the k-tuples conjecture, we have the number of primes $p \le x$ with $2^p - 1$ divisible by at least 2 different primes is $\gg x/(\log x)^2$.

This last result can be improved assuming Artin's primitive root conjecture. If 2 is a primitive root for p, we have p a prime factor of ϕ_{p-1} and so ϕ_{p-1} is composite. Following Hooley's GRH conditional proof of Artin's conjecture, we have $\gg x/\log x$ primes $p \le x$ which have 2 as a primitive root. Further, the proof is amenable to insisting that $p \equiv 3 \pmod 4$ and also the same holds when $p \equiv 5 \pmod 8$. So the GRH implies there are quite a few cyclotomic composites. And as above, the abc conjecture can be used to show these composites are not prime powers. This result can be improved a little by considering primes $p \le kx$ with $\ell(p) = (p-1)/k$ for various small values of k and using sieve methods to show that $(p-1)/k = (p'-1)/k'$ has few solutions when $k \ne k'$ are small. Thus, with a little work it may be possible to show, assuming the GRH, that there are $\gg x \log\log x/\log x$ integers $l \le x$ of the form $\ell(p)$ for some prime $p \ll x \log x$.

5. Statistics and surmises

Concerning Table 1, Gallot [6] previously enumerated the cases where ϕ_m is prime for $m \le 6500$. Our calculations agree with his. In our work we used Mathematica and in particular their PrimeQ function, which we understand is a probabilistic test. So, it is possible that some of the prime declarations made are false, but this seems unlikely, given that there are not very many of them. One of the larger primes unearthed here is $\phi_{60,287}$ which has 17,090 decimal digits. Note that when PrimeQ declares a number is not prime, this conclusion is not in doubt. Since PrimeQ is notably slower than checking if the Fermat

TABLE 1. Counts for $m \le 2^k$ with ϕ_m prime, ψ_m prime, ψ_m^+ prime, ψ_m^- prime

k	$\#m$ with ϕ_m prime	ψ_m prime	ψ_m^+ prime	ψ_m^- prime
1	1	1	0	0
2	3	3	1	0
3	7	6	1	0
4	14	13	2	0
5	23	25	4	1
6	33	36	7	5
7	49	52	13	8
8	64	68	20	16
9	81	86	24	25
10	99	106	30	33
11	122	129	34	43
12	140	147	44	54
13	167	174	50	59
14	195	202	61	64
15	221	228	72	74
16	255	262	85	83

congruence $3^n \equiv 3 \pmod{n}$ holds, we first used that and confirmed the few primality assertions with PrimeQ. (We used the base 3 since every ψ_m is either a prime or a base 2 pseudoprime. See [16] where these thoughts are developed.) Many of the large primes uncovered here have indeed been certified (including $\phi_{60,287}$) in the ongoing project factordb.com. (Thanks are due to Yves Gallot for informing me about this.)

Heuristically there are at most finitely many examples where $\psi_{p^i\ell(p)}$ is prime. Is $\psi_{127\cdot 7}$ the largest such example? It is a prime of 226 decimal digits. There are several examples where both ψ_m^+ and ψ_m^- are prime. The largest that we found in our calculations to 2^{16} is $m = 1132$, where the two primes each have 85 decimal digits. Probably there are at most finitely many of these "twin cyclotomic primes".

The counts in Table 1 look to be proportional to k^2, and this is supported heuristically as well. Indeed, one can model ψ_m as a random number near $2^{\varphi(m)}$ which has all prime factors larger than m. So the "probability" that it is prime (given that $m \not\equiv 4 \pmod 8$) is about $e^\gamma \log m/\varphi(m)\log 2$. The sum of these quantities up to 2^{15} is about 223.4, and up to 2^{16} is about 254.4, which are not bad matches with the table.

One can enlarge further the realm of cyclotomic primes to look at the primitive parts of $a^n - 1$, where $a > 2$. Also one can look at the Fibonacci sequence, as well as other Lucas sequences, for example see

Drobot [4]. We suspect our methods carry over, but we leave this topic for another day, and perhaps another person.

Acknowledgments

I thank Michael Filaseta, Yves Gallot, Florian Luca, Mits Kobayashi, Pieter Moree, Paul Pollack, and Sam Wagstaff for their valuable comments and interest.

References

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

[2] J. Browkin, M. Filaseta, G. Greaves, A. Schinzel, Squarefree values of polynomials and the abc-conjecture, (Cardiff, 1995), 65–85. London Math. Soc. Lecture Note Ser. **237**, Cambridge U. Press, Cambridge, 1997.

[3] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., Factorizations of $B^n \pm 1$, $B = 2, 3, 4, 5, 6, 7, 10, 11, 12$, up to high powers, *Contemporary Mathematics* **22**, Amer. Math. Soc. 1989.

[4] V. Drobot, On primes in the Fibonacci sequence, *Fibonacci Quart.* **38** (2000), 71–72.

[5] P. Erdős, Some remarks about additive and multiplicative functions, *Bull. Amer. Math. Soc.* **52** (1946), 527–537.

[6] Y. Gallot, Cyclotomic polynomials and prime numbers, citeseerx.ist.psu.edu/document?doi=36d4b33472e836538b728ecad04545da318c0094 .

[7] M. Goldfeld, On the number of primes p for which $p + a$ has a large prime factor, *Mathematika* **16** (1969), 23–27.

[8] Great Internet Mersenne Prime Search, mersenne.org.

[9] C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order, *Geom. Dedicata* **2** (1974), 425–460.

[10] P. Kinlaw, M. Kobayashi, and C. Pomerance, On the equation $\varphi(n) = \varphi(n+1)$, *Acta Arith.* 196 (2020), 69–92.

[11] M. Kobayashi, P. Pollack, and C. Pomerance, On the distribution of sociable numbers, *J. Number Theory* **129** (2009), 1990–2009.

[12] J. D. Lichtman, Primes in arithmetic progressions to large moduli, and shifted primes without large prime factors, arXiv:2211.09641 [math.NT].

[13] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, *J. Reine Angew. Math.* **572** (2004), 167–195,

[14] H. L. Montgormery and R. C. Vaughan, The large sieve, *Mathematika* **20** (1973), 119–134.

[15] OEIS, https://oeis.org/A000978.

[16] C. Pomerance, A new lower bound for the pseudoprime counting function, *Illinois J. Math.* **26** (1982), 4–9.

[17] C. Pomerance and S. Rubinstein-Salzedo, Cyclotomic coincidences, *Exp. Math.* **31** (2022), 596–605.

[18] A. Schinzel, On primitive prime factors of $a^n - b^n$, *Math. Proc. Cambridge Phil. Soc.* **58** (1962), 556–562.

[19] J. H. Silverman, Wieferich's condition and the *abc* conjecture, *J. Number Theory* **30** (1988), 226–237.

Appendix

Here we list the values of m corresponding to the counts in Table 1.

Values of m with ϕ_m prime:

2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 19, 22, 24, 26, 27, 30, 31, 32, 33, 34, 38, 40, 42, 46, 49, 56, 61, 62, 65, 69, 77, 78, 80, 85, 86, 89, 90, 93, 98, 107, 120, 122, 126, 127, 129, 133, 145, 150, 158, 165, 170, 174, 184, 192, 195, 202, 208, 234, 254, 261, 280, 296, 312, 322, 334, 345, 366, 374, 382, 398, 410, 414, 425, 447, 471, 507, 521, 550, 567, 579, 590, 600, 607, 626, 690, 694, 712, 745, 795, 816, 897, 909, 954, 990, 1106, 1192, 1224, 1230, 1279, 1384, 1386, 1402, 1464, 1512, 1554, 1562, 1600, 1670, 1683, 1727, 1781, 1834, 1904, 1990, 1992, 2008, 2037, 2203, 2281, 2298, 2353, 2406, 2456, 2499, 2536, 2838, 3006, 3074, 3217, 3415, 3418, 3481, 3766, 3817, 3927, 8370, 9583, 9689, 9822, 9941, 10192, 10967, 11080, 11213, 11226, 11581, 11614, 11682, 11742, 11766, 12231, 12365, 12450, 12561, 13045, 13489, 14166, 14263, 14952, 14971, 15400, 15782, 15998, 16941, 17088, 17917, 18046, 19600, 19937, 20214, 20678, 21002, 21382, 21701, 22245, 22327, 22558, 23209, 23318, 23605, 23770, 24222, 24782, 27797, 28958, 28973, 29256, 31656, 31923, 33816, 34585, 35565, 35737, 36960, 39710, 40411, 40520, 42679, 42991, 43830, 43848, 44497, 45882, 46203, 47435, 48387, 48617, 49312, 49962, 49986, 50414, 51603, 51945, 53977, 55495, 56166, 56898, 56955, 57177, 58315, 58534, 58882, 60287

Values of m with $\psi_m < \phi_m$ and ψ_m prime:

18, 20, 21, 54, 147, 342, 602, 889

Values of m with ψ_m^+ prime:

4, 12, 20, 28, 36, 44, 60, 68, 76, 84, 100, 108, 116, 132, 140, 180, 204, 220, 228, 252, 276, 340, 356, 484, 588, 628, 652, 700, 756, 924, 1132, 1292, 1452, 1516, 2300, 2484, 2604, 2964, 3116, 3276, 3420, 3540, 3940, 3988, 4892, 5100, 5268, 5908, 6620, 7812, 8964, 9084, 9324, 9468, 10308, 11980, 12188, 12204, 13724, 13860, 15252, 17052, 18476, 20676, 21916, 24252, 25004, 25508, 28692, 29460, 29492, 31692, 34236, 34380, 35700, 38428, 40564, 41316, 45028, 46076, 50332, 51148, 51204, 56588, 58796

Values of m with ψ_m^- prime:

28, 36, 44, 52, 60, 84, 108, 116, 132, 140, 172, 188, 196, 212, 220, 252, 260, 276, 292, 316, 348, 372, 420, 444, 452, 516, 604, 668, 812, 868, 924, 956, 964, 1044, 1132, 1204, 1276, 1412, 1468, 1500, 1540, 1564, 1828, 2124, 2172, 2228, 2252, 2452, 2532, 2716, 2764, 2868, 3484, 3852, 4844, 5316, 5468, 6164, 7828, 9516, 9684, 10924, 12164, 15860, 19516, 20588, 21292, 24180, 25100, 25212, 28612, 30988, 31460, 32340, 34404, 38132, 42660, 43084, 46292, 46980, 52740, 56668, 60676

Mathematics Department, Dartmouth College, Hanover, NH 03755, USA
E-mail address: carlp@math.dartmouth.edu