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, e.g., $p = 11$. 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 $p = 136{,}279{,}841$, see [11]. 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 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: May 2, 2025.

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 [19], 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 $p\,\|\,\phi_m$. 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, see [3]. The numbers ψ_m

are pairwise coprime and except for $m = 1$ or 6, they are all > 1 (cf. [22]).

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

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

By dividing out an intrinsic prime factor if it exists, we have

$$\psi_{8k+4} =: \psi^+_{8k+4}\psi^-_{8k+4}.$$

Further, this factorization is nontrivial for $k \geq 3$, a result due to Schinzel [23]. The factorization (1) is known under the name Aurifeuille, see [5].

Note that

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

see [12, Theorem 3.6], [22, Theorem 4.3]. Also, using [5, eqs. (13), (14)] it is not hard to show that

$$(3)\qquad \phi^+_{8k+4}, \phi^-_{8k+4} \asymp 2^{\varphi(8k+4)/2},$$

where the notation indicates the 2 items on the left side are of the same magnitude as the item on the right side.

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. *For sufficiently large values of x, the set C_1 contains more than $x^{3/5}$ composite numbers ψ_m with $m \leq x$, and the set C_2 contains more than $x^{3/5}$ numbers ψ_m with $m \leq x$ that are not the product of two primes.*

The exponent 3/5 in the theorem is not optimal, this is discussed below. 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 and that x is sufficiently large. The set C_1 contains $\ge x^{3/5}$ numbers ψ_m divisible by at least 2 distinct primes with $m \le x$, and the set C_2 contains $\ge x^{3/5}$numbers numbers ψ_m divisible by at least 3 distinct primes with $m \le x$.*

We remark that the abc conjecture has been used for similar purposes in [24] and [4, Theorem 3]. We also remark that this theorem gives an abc-conjecture-conditional solution of a problem of Schinzel [23, p. 561].

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. An elementary approach

Here we prove a somewhat weaker version of Theorem 1 where the exponent $3/5$ is replaced with $1/2$. Let x be large and consider primes $p \le x$. It follows from Erdős–Murty [8, Theorem 1] that the number of such primes p with $\ell(p) > 5x^{1/2}(\log x)^2$ is $\sim x/\log x$. For any positive integer d let $L_d(x)$ denote the set of primes $p \in (x/2, x]$ with

$$\begin{aligned} p &\equiv 3 \pmod 4, \\ \ell(p) &= (p-1)/d, \\ \ell(p) &> 5x^{1/2}(\log x)^2. \end{aligned}$$

It follows that

$$\sum_{d \le \frac{1}{5}x^{1/2}/(\log x)^2} \#L_d(x) \sim \frac{x}{4\log x}. \tag{4}$$

Thus, for large x there is some number $d_0 \le \frac{1}{5}x^{1/2}/(\log x)^2$ with

$$\#L_{d_0}(x) > x^{1/2}.$$

Consider now the values of $m = \ell(p) = (p-1)/d_0$ for $p \in L_{d_0}(x)$. They are all distinct, bounded by x, and $\not\equiv 4 \pmod 8$. For large x, ψ_m is easily seen to be $> x$ (using $m > x^{1/2}$ and (2)) and $p \,|\, \psi_m$. It follows that ψ_m is composite. Thus, C_1 contains more than $x^{1/2}$ composite numbers ψ_m with $m \le x$.

By changing 3 (mod 4) above to 5 (mod 8) and using (3), the analogous argument shows that at least one of $\psi_m^+,\ \psi_m^-$ is composite, so C_2 contains more than $x^{1/2}$ numbers ψ_m with $m \le x$ which are not the product of two primes.

4. Proof of Theorem 1

Denote by $\pi(x;d,a)$ the number of primes $p \le x$ 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 [2], 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 [15]); 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 [17]) 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,

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

Thus, with the prior display, we have

$$\sum_{q>x^\theta} \pi(x;4q,2q+1)\log q \ge 0.02x \tag{5}$$

for all large x, which shows the first assertion in Proposition 1. The second assertion follows in a similar manner.

To achieve a cosmetically more appealing version of our results, note that since

$$\sum_{x^\theta<q\le x^\theta(\log x)^2} \frac{1}{q} \ll \frac{\log\log x}{\log x} = o(1),$$

the Brun–Titchmarsh theorem implies that in both parts of Proposition 1 we may replace $q > x^\theta$ with $q > x^\theta(\log x)^2$.

Since no prime $p \le x$ has $p-1$ divisible by 2 different primes $q > x^\theta$, we have the following result.

Corollary 1. *We have*

$$\sum_{\substack{p\equiv 3 \pmod 4\\ P^+(p-1)>x^\theta(\log x)^2\\ p\le x}} 1 \gg x/\log x \quad \textit{and} \quad \sum_{\substack{p\equiv 5 \pmod 8\\ P^+(p-1)>x^\theta(\log x)^2\\ p\le x}} 1 \gg x/\log x.$$

An elementary argument shows that the number of primes p with $\ell(p) = k$ is $\ll k/\log k$, so it follows that the number of primes $p \le x$ with $\ell(p) \le x^{1-\theta}/(\log x)^2$ is $\ll x^{2(1-\theta)} = o(\pi(x))$. (Note that there is a similar argument in [10]. Also here one could appeal to [8, Theorem 1].) However, a prime p counted in either part of Corollary 1 either has $\ell(p) \le x^{1-\theta}/(\log x)^2$ or $\ell(p) > x^\theta(\log x)^2$. Hence we have

$$\sum_{\substack{p\equiv 3 \pmod 4\\ \ell(p)>x^\theta(\log x)^2\\ p\le x}} 1 \gg x/\log x \ \text{ and } \sum_{\substack{p\equiv 5 \pmod 8\\ \ell(p)>x^\theta(\log x)^2\\ p\le x}} 1 \gg x/\log x. \tag{6}$$

Thus, using the notation of the previous section we have the improvement on (4):

$$\sum_{d\le x^{1-\theta}/(\log x)^2} \#L_d(x) \gg \frac{x}{\log x},$$

and an analogous result holds for primes $p \equiv 5 \pmod 8$. Thus, by the same argument as in the previous section, we have Theorem 1.

5. Conditional results

For a positive integer n let $\mathrm{rad}(n)$ 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 $\mathrm{rad}(abc) < c^{1-\epsilon}$. 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. We follow the proof of Theorem 1 showing that most of the composites generated are not prime powers. First note that using that $\varphi(p-1)/(p-1)$ has a continuous, strictly increasing distribution function on $[0, 1/2]$ (see for example Kátai [14], Elliott [7], and Hildebrand [13]) there is a positive number ϵ such that if we add the condition $\varphi(p-1)/(p-1) \geq \epsilon$ under each of the sums in (6), we obtain the same inequalities, albeit with possibly smaller constants.

First suppose that $m \not\equiv 4 \pmod 8$. As in the proof of Theorem 1 there is a value of $d \leq x^{1-\theta}/(\log x)^2$ with $\gg x/d \log x$ primes $p \leq x$ with $p \equiv 3 \pmod 4$, $\ell(p) > x^{\theta}(\log x)^2$ and $\varphi(p-1)/(p-1) \geq \epsilon$. Further, for each such $m = (p-1)/d$ we have that ψ_m is composite. We now show assuming the abc conjecture that for all sufficiently large x, ψ_m cannot be a prime power. Suppose it is a prime power, namely $\psi_m = p^i$ with $i \geq 2$. Consider the abc equation $1 + (2^m - 1) = 2^m$. Since $\psi_m \geq \phi_m/p$, we have

$$\mathrm{rad}(abc) = 2p\,\mathrm{rad}((2^m-1)/\psi_m) \leq 2pq(2^m-1)/\phi_m,$$

where $q = P^+(m)$. Assuming the abc conjecture this would be impossible for large m if there is some fixed $\delta > 0$ such that $\phi_m > 2^{\delta m}$ (since $2pq = O(x^2) = 2^{o(m)}$). Using (2) this follows since $\varphi(m)/m \geq \varphi(p-1)/(p-1) \geq \epsilon$. Thus, we have our claim.

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

We remark that a variant of our proof can show that for asymptotically all m, 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 8 and 9 form the only pair of consecutive numbers which are nontrivial powers (a result of Mihăilescu [16]), 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 $\gg x/(\log x)^2$.

We can prove there are more cyclotomic composites assuming Artin's primitive root conjecture. If 2 is a primitive root for p, we have p a prime factor of ψ_{p-1} and so ψ_{p-1} is composite for p large. By 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 usually 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 $p \ll x \log x$.

6. Statistics and surmises

Concerning Table 1, Gallot [9] previously enumerated the cases where ϕ_m is prime for $m \le 6500$ and Noe [18] extended this to 10^5. Our calculations agree with theirs. In our work we used Mathematica and in particular their PrimeQ function. This function is discussed in [1], where it is said to be based on the Baillie–PSW primality test. This is not a rigorous primality test, though no counterexamples are known (and there is a reward for the first one to be identified). In fact, I have a heuristic argument that there are indeed infinitely many counterexamples, see [21]. 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 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 [20] 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 $\psi_{p^i\ell(p)}$, with $i \ge 1$, is prime. Is $\psi_{127\cdot 7}$ the largest such example? It is a prime

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
17	289	296	96	94

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^{17} 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, up to 2^{16} is about 254.4, and up to 2^{17} is about 287.4, which are not bad matches with the table. It would seem that the counts in the first column are asymptotically equal to k^2, but this is likely not true. One can sum $e^\gamma \log m/\varphi(m) \log 2$ for $m \le 2^k$ with $m \not\equiv 4 \pmod 8$, finding it to be $\sim ck^2$, where

$$c = \frac{5}{12} e^\gamma \zeta(2)\zeta(3)\zeta(6)^{-1} \log 2 = 0.999774\ldots.$$

So, close to 1, but not 1.

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

Acknowledgments

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

References

[1] R. Baillie, A. Fiori, and S. S. Wagstaff, Jr., Strengthening the Baillie–PSW primality test, *Math. Comp.* **90** (2021), 1931–1955.
[2] R. C. Baker and G. Harman, Shifted primes without large prime factors, *Acta Arith.* **83** (1998), 331–361.
[3] A. S. Bang, Talstheoritiske undersøgelser, *Tidsskrift Math.* 5, IV (1886), 70–80.
[4] 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.
[5] 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.
[6] V. Drobot, On primes in the Fibonacci sequence, *Fibonacci Quart.* **38** (2000), 71–72.
[7] P. D. T. A. Elliott, On the limiting distribution of $f(p+1)$ for non-negative additive functions, *Acta Arith.* **25** (1974), 259–264.
[8] P. Erdős and M. R. Murty, On the order of a (mod p), CRM Proc. Lecture Notes **19** (1999), 87–97.
[9] Y. Gallot, Cyclotomic polynomials and prime numbers, citeseerx.ist.psu.edu/document?doi=36d4b33472e836538b728ecad04545da318c0094 .
[10] M. Goldfeld, On the number of primes p for which $p + a$ has a large prime factor, *Mathematika* **16** (1969), 23–27.
[11] Great Internet Mersenne Prime Search, mersenne.org.
[12] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, *Geom. Dedicata* **2** (1974), 425–460.
[13] A. Hildebrand, Additive and multiplicative functions on shifted primes, *Proc. London Math. Soc.* **s3-59** (1989), 209–232.
[14] I. Kátai, On distribution of arithmetical functions on the set prime plus one, *Compos. Math.* **19** (1968), 278–289.
[15] J. D. Lichtman, Primes in arithmetic progressions to large moduli, and shifted primes without large prime factors, arXiv:2211.09641 [math.NT].
[16] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, *J. Reine Angew. Math.* **572** (2004), 167–195,
[17] H. L. Montgormery and R. C. Vaughan, The large sieve, *Mathematika* **20** (1973), 119–134.
[18] T. D. Noe, https://oeis.org/A072226/b072226.txt .
[19] OEIS, https://oeis.org/A000978.
[20] C. Pomerance, A new lower bound for the pseudoprime counting function, *Illinois J. Math.* **26** (1982), 4–9.

[21] C. Pomerance, Are there counterexamples to the Baillie–PSW primality test? In H. W. Lenstra, Jr., J. K. Lenstra, and P. Van Emde Boas, editors, Dopo le parole angeboden aan Dr. A. K. Lenstra. Amsterdam, 1984. https://www.math.dartmouth.edu/∼carlp/dopo.pdf

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

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

[24] 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, 4167, 4253, 4423, 4480, 5053, 5064, 5217, 5234, 5238, 5250, 5325, 5382, 5403, 5421, 6120, 6925, 7078, 7254, 7503, 7539, 7592, 7617, 7648, 7802, 7888, 7918, 8033, 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, 67235, 67854, 69933, 70129, 70617, 75302, 76912, 78077, 78426, 80160, 81165, 81432, 82569, 82730, 84897, 85474, 85881, 86243, 87005, 94914, 95349, 99992, 100917, 104550, 108535, 109965, 110503, 110845, 111065, 116629, 118080, 119210, 121806, 130002

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, 73668, 81900, 84020, 86508, 87420, 92324, 96204, 97524, 97620, 104620, 118748

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, 68748, 69828, 72948, 74220, 75484, 84900, 87940, 106412, 110116, 115292, 129836

Mathematics Department, Dartmouth College, Hanover, NH 03755, USA

E-mail address: carlp@math.dartmouth.edu