

CYCLOTOMIC COINCIDENCES

CARL POMERANCE AND SIMON RUBINSTEIN-SALZEDO

1. INTRODUCTION

For a positive integer n , let Φ_n denote the n th cyclotomic polynomial. In this paper we consider roots of $\Phi_m(x) - \Phi_n(x)$, where m, n are unequal positive integers. Our principal theorem is the following.

Theorem 1.1. *If $m \neq n$ are positive integers and x is a nonzero real number with $\Phi_m(x) = \Phi_n(x)$, then $\frac{1}{2} < |x| < 2$, except for $\Phi_2(2) = \Phi_6(2)$.*

We show that on the prime k -tuples conjecture the upper bound 2 in the theorem is optimal in that replacing it with $2 - \varepsilon$ for any fixed $\varepsilon > 0$, there are infinitely many counterexamples.

A corollary of Theorem 1.1 is the cyclotomic ordering conjecture of Glasby. He conjectured that if m, n are positive integers, then either $\Phi_m(q) \leq \Phi_n(q)$ for all integers $q \geq 2$ or the reverse inequality holds for all q . This would put a total ordering on the set of cyclotomic polynomials. This ordering is also the topic of the sequence A206225 in the On-Line Encyclopedia of Integer Sequences [Slo], where it seems to be tacitly assumed such a total ordering exists.

In addition, Glasby conjectured that in the total ordering of the cyclotomic polynomials, $\Phi_{2 \cdot 3^i}$ is adjacent to Φ_{3^i} for all $i \geq 2$. We prove a generalization of this, where 3 may be replaced with any odd prime; see Proposition 6.2.

2. BACKGROUND ON CYCLOTOMIC POLYNOMIALS

Definition 2.1. For a positive integer n , the n^{th} cyclotomic polynomial $\Phi_n(x)$ is defined as

$$\Phi_n(x) = \prod_{\substack{1 \leq a \leq n \\ \gcd(a, n) = 1}} (x - \zeta_n^a),$$

where ζ_n is a primitive n^{th} root of unity.

Let $\phi(n)$ denote Euler's function at the positive integer n , let $\mu(n)$ be the Möbius function at n , and let $\omega(n)$ denote the number of distinct primes that divide n . Also, let $\text{rad}(n)$ denote the largest squarefree divisor of n and $q(n) = \frac{n}{\text{rad}(n)}$. Some familiar facts about cyclotomic polynomials are as follows.

Proposition 2.2. *The degree of $\Phi_n(x)$ is $\phi(n)$. Further, $\Phi_n(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$.*

Proposition 2.3. *We have*

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \quad \text{and} \quad \Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}.$$

When $n > 1$, the latter equality can be rewritten as

$$\Phi_n(x) = \prod_{d|n} (1 - x^d)^{\mu(n/d)}.$$

Proposition 2.4. *When $n > 1$, $\Phi_n(x)$ is a reciprocal polynomial; i.e., $\Phi_n(x) = x^{\phi(n)}\Phi_n(1/x)$.*

Proposition 2.5. *If p is prime and $p \mid n$, then $\Phi_{np}(x) = \Phi_n(x^p)$. In general, $\Phi_n(x) = \Phi_{\text{rad}(n)}(x^{q(n)})$.*

Proposition 2.6. *If n is an odd positive integer, and $k \geq 2$ is an integer, then*

$$\Phi_n(-x) = \Phi_{2n}(x), \quad \Phi_{2n}(-x) = \Phi_n(x), \quad \text{and} \quad \Phi_{2^k n}(-x) = \Phi_{2^k n}(x).$$

Proposition 2.7. *If $\omega(n) \leq 2$, then all the coefficients of $\Phi_n(x)$ lie in $\{-1, 0, 1\}$.*

3. RATIONAL COINCIDENCES

Theorem 3.1. *Suppose m and n are distinct positive integers. Then $\Phi_m(r) \neq \Phi_n(r)$ for rational numbers $r \notin \{-1, 0, 1\}$ unless $r = 2$ and $\{m, n\} = \{2, 6\}$.*

Proof. For integers $a \geq 2$ with $r = a$, the result follows from Bang's Theorem [Ban86], which says that if $a, n > 1$ are integers and $(a, n) \neq (2, 6), (2^j - 1, 2)$ for some integer $j \geq 2$, then there is a prime p such that $p \mid (a^n - 1)$ but $p \nmid (a^k - 1)$ for any $k < n$. Now, suppose $n > m$ with $n \neq 6$, and let p be a prime dividing $a^n - 1$ but not $a^k - 1$ for any $k < n$. Then by Proposition 2.3, $p \mid \Phi_n(a)$ but $p \nmid \Phi_m(a)$. Thus $\Phi_m(a) \neq \Phi_n(a)$. When $a = 2$ and $n = 6$, we can just check the values of $\Phi_m(2)$: we have $\Phi_m(2) = 1, 3, 7, 5, 31$ for $m = 1, 2, 3, 4, 5$, respectively, while $\Phi_6(2) = 3$. Finally, in the case of $m = 1, n = 2$, we see that $\Phi_m(x) - \Phi_n(x)$ has no roots at all. For integers $a \leq -2$, the result follows from Proposition 2.6 by considering the separate cases where m is odd, $2 \pmod{4}$, or divisible by 4, and the same for n .

When $r = a/b \notin \mathbb{Z}$, where a, b are coprime integers, we use the generalization of Bang's theorem due to Zsigmondy [Zsi92]. This asserts that $a^n - b^n$ has a prime divisor that does not divide any $a^k - b^k$ for $1 \leq k \leq n - 1$ but for the Bang exceptions. Let

$$\Phi_n(x, y) = y^{\phi(n)}\Phi_n(x/y),$$

so that $\Phi_n(x, y)$ is a homogeneous polynomial with integer coefficients, and as in Proposition 2.3, we have

$$\Phi_n(x, y) = \prod_{d|n} (x^d - y^d)^{\mu(n/d)}.$$

If $\Phi_m(a/b) = \Phi_n(a/b)$ with $\phi(m) \leq \phi(n)$, then $\Phi_m(a, b) = b^{\phi(n) - \phi(m)}\Phi_n(a, b)$, yet the side of this equation corresponding to the larger of m, n has a prime factor that does not divide the other side. This completes the proof. \blacksquare

4. AN INEQUALITY

The following result will be useful.

Lemma 4.1. *Let x be a real number with $x \geq 2$ and let k be a positive integer. Then*

$$|\log(1 - x^{-k})| > \sum_{j>k} |\log(1 - x^{-j})|.$$

Proof. The left side of the inequality is

$$\sum_{i \geq 1} \frac{1}{i} x^{-ik},$$

while the right side is

$$\sum_{i \geq 1} \frac{1}{i} \sum_{j > k} x^{-ij} = \sum_{i \geq 1} \frac{1}{i} \cdot \frac{x^{-ik}}{x^i - 1} < \sum_{i \geq 1} \frac{1}{i} x^{-ik},$$

using $x \geq 2$. This completes the proof. \blacksquare

Note that the following result when x is integral is due to Hering [Her74, Theorem 3.6].

Theorem 4.2. *Let x be a real number with $x \geq 2$ and let n be a positive integer. Then if $\mu(\text{rad}(n)) = 1$, we have*

$$\frac{x^{q(n)} - 1}{x^{q(n)}} x^{\phi(n)} \leq \Phi_n(x) < x^{\phi(n)}$$

with equality only in the case $n = 1$, while if $\mu(\text{rad}(n)) = -1$, we have

$$x^{\phi(n)} < \Phi_n(x) < \frac{x^{q(n)}}{x^{q(n)} - 1} x^{\phi(n)}.$$

Proof. Let $f_n(x) = \Phi_n(x)/x^{\phi(n)}$. When $n > 1$, Propositions 2.3 and 2.4 imply that

$$(4.1) \quad f_n(x) = \Phi_n(x^{-1}) = \prod_{d|n} (1 - x^{-d})^{\mu(\frac{n}{d})}.$$

This formula continues to hold when $n = 1$.

First assume that n is squarefree. Taking the logarithm of (4.1) we have

$$\log f_n(x) = \mu(n) \log(1 - x^{-1}) + \sum_{\substack{d|n \\ d > 1}} \mu(n/d) \log(1 - x^{-d}),$$

so that

$$(4.2) \quad \mu(n) \log(1 - x^{-1}) + \sum_{j > 1} \log(1 - x^{-j}) < \log f_n(x) < \mu(n) \log(1 - x^{-1}) - \sum_{j > 1} \log(1 - x^{-j}).$$

Thus, by Lemma 4.1, we have

$$(1 + \mu(n)) \log(1 - x^{-1}) < \log f_n(x) < (-1 + \mu(n)) \log(1 - x^{-1}).$$

Since $\log(1 - x^{-1}) < 0$, we have $f_n(x) > 1$ when $\mu(n) = -1$ and $f_n(x) < 1$ when $\mu(n) = 1$. This proves two of the four inequalities of the theorem in the squarefree case.

Still assuming that n is squarefree, if p is a prime not dividing n , then we have

$$f_n(x) f_{np}(x) = \prod_{d|n} (1 - x^{-d})^{\mu(\frac{n}{d})} (1 - x^{-d})^{\mu(\frac{pn}{d})} (1 - x^{-pd})^{\mu(\frac{pn}{pd})} = \prod_{d|n} (1 - x^{-pd})^{\mu(\frac{n}{d})}.$$

We claim first that $f(n) f(np) < 1$ if $\mu(n) = 1$ and $f(n) f(np) > 1$ if $\mu(n) = -1$. To see this, take logarithms, and this is equivalent to saying that

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \log(1 - x^{-pd}) < 0$$

if $\mu(n) = 1$ and

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \log(1 - x^{-pd}) > 0$$

if $\mu(n) = -1$. Let us consider the case where $\mu(n) = 1$; the other case is similar. We have

$$\begin{aligned} \sum_{d|n} \mu\left(\frac{n}{d}\right) \log(1 - x^{-pd}) &\leq \log(1 - x^{-p}) - \sum_{\substack{d|n \\ d>1}} \log(1 - x^{-pd}) \\ &< \log(1 - x^{-p}) - \sum_{j>p} \log(1 - x^{-j}) < 0, \end{aligned}$$

by Lemma 4.1.

We now complete the proof of the theorem for squarefree numbers by induction on n . The base case is $n = 1$, where we have $f_1(x) = \Phi_1(x)/x = (x - 1)/x$, so the theorem holds here. Now, suppose that the result is true for n . We prove it for np , where p is a prime not dividing n . If $\mu(n) = 1$, then $\mu(np) = -1$. To get the upper bound, we have $(x - 1)/x \leq f_n(x) < 1$ and $f_n(x)f_{np}(x) < 1$, so

$$f_{np}(x) < \frac{1}{f_n(x)} \leq \frac{x}{x - 1},$$

as desired. The case where $\mu(n) = -1$ is similar.

Finally, we must handle the case where n is not squarefree. Using Proposition 2.5 and noting that $\phi(n) = q(n)\phi(\text{rad}(n))$, we apply the squarefree case to $\Phi_{\text{rad}(n)}(x^{q(n)})$. \blacksquare

Corollary 4.3. *Under the same assumptions as in Theorem 4.2, we have*

$$\frac{1}{2}x^{\phi(n)} \leq \Phi_n(x) < x^{\phi(n)}$$

when $\mu(\text{rad}(n)) = 1$, with equality only in the case $n = 1$ and $x = 2$. Else, if $\mu(\text{rad}(n)) = -1$,

$$x^{\phi(n)} < \Phi_n(x) < 2x^{\phi(n)}.$$

We now give a proof of a similar result that holds as well for complex numbers.

Proposition 4.4. *For $z \in \mathbb{C}$ with $|z| \geq 2$,*

$$\frac{1}{2}|z|^{\phi(n)} \leq |\Phi_n(z)| < 2|z|^{\phi(n)},$$

with equality only in the cases $n = 1, z = 2$ and $n = 2, z = -2$.

Proof. Our starting point is (4.1), which holds as well for complex numbers. Also, as in the proof of Theorem 4.2, it suffices to handle the case when n is squarefree. The cases $n = 1, 2$ are true by inspection, so we take $n > 2$. Assume that $\mu(n) = 1$; the case when $\mu(n) = -1$ will follow by the same argument. Let p be the least prime factor of n . By (4.1) we have

$$(4.3) \quad \frac{|\Phi_n(z)|}{|z|^{\phi(n)}} = \frac{|1 - z^{-1}|}{|1 - z^{-p}|} \prod_{\substack{d|n \\ d>p}} |1 - z^{-d}|^{\mu(d)},$$

using $\mu(n/d) = \mu(d)$ when n is squarefree and $\mu(n) = 1$. By the triangle inequality, when $|z| \geq 2$,

$$(4.4) \quad \begin{aligned} \frac{|1 - z^{-1}|}{|1 - z^{-p}|} &= \frac{1}{|1 + z^{-1} + \dots + z^{-(p-1)}|} \geq \frac{1}{1 + |z|^{-1} + \dots + |z|^{-(p-1)}} \\ &\geq \frac{1}{2 - 2^{-(p-1)}} = \frac{1}{2}(1 - 2^{-p})^{-1}. \end{aligned}$$

We now find a lower bound for the remaining product in (4.3). For $|z| \geq 2$, we have

$$|(1 - z^{-d})^{\mu(d)}| \geq 1 - 2^{-d},$$

so that

$$\log \prod_{\substack{d|n \\ d>p}} |(1 - z^{-d})^{\mu(d)}| \geq \sum_{d>p} \log(1 - 2^{-d}) > \log(1 - 2^{-p}),$$

by Lemma 4.1. Hence with (4.3) and (4.4), the lower bound in the proposition holds.

For the upper bound, first assume that $p > 2$. Referring to (4.3), note that

$$(4.5) \quad \frac{|1 - z^{-1}|}{|1 - z^{-p}|} = \frac{|z^{p-1}(z - 1)|}{|z^p - 1|} \leq \frac{|z|^{p-1}(|z| + 1)}{|z|^p - 1} = 1 + \frac{|z|^{p-1} + 1}{|z|^p - 1} \leq \frac{12}{7},$$

when $|z| \geq 2$ and $p \geq 3$. Note that $|(1 - z^{-d})^{\mu(d)}| \leq (1 - |z|^{-d})^{-1}$ for $|z| > 1$. So, for $|z| \geq 2$ and referring to (4.3),

$$\prod_{\substack{d>p \\ d|n}} |(1 - z^{-d})^{\mu(d)}| \leq \prod_{d>p} (1 - 2^{-d})^{-1} \leq \prod_{d \geq 4} (1 - 2^{-d})^{-1} < 1.14.$$

With (4.5) this completes the upper bound proof when $p \geq 3$.

Suppose $p = 2$. Since $n > 2$ and n is squarefree, we may assume that n has an odd prime factor, let q be the least one. Again from (4.3) we have

$$(4.6) \quad \frac{|\Phi_n(z)|}{|z|^{\phi(n)}} = \frac{1}{|1 + z^{-1}||1 - z^{-q}|} \prod_{\substack{d|n \\ d>q}} |1 - z^{-d}|^{\mu(d)} = \frac{|z|^{q+1}}{|1 + z||1 - z^q|} \prod_{\substack{d|n \\ d>q}} |1 - z^{-d}|^{\mu(d)}$$

Writing $z = re^{i\theta}$, we have

$$\begin{aligned} (|1 + z||1 - z^q|)^2 &= (r^2 + 1 + 2\Re(z))(r^{2q} + 1 - 2\Re(z^q)) \\ &= (r^2 + 1)(r^{2q} + 1) + 2r(r^{2q} + 1) \cos \theta - 2r^q(r^2 + 1) \cos q\theta - 4r^{q+1} \cos \theta \cos q\theta. \end{aligned}$$

Taking the derivative with respect to θ and setting it equal to 0 gives us either $\sin \theta = 0$ or

$$2r(r^{2q} + 1) = 2r^q(r^2 + 1)q \frac{\sin q\theta}{\sin \theta} + 4r^{q+1} \cos q\theta + 4r^{q+1}q \cos \theta \frac{\sin q\theta}{\sin \theta}.$$

If $\sin \theta \neq 0$, using $|\sin q\theta / \sin \theta| < q$ and $r \geq 2$, we see that for $q \geq 11$ this last equation has no solutions. So, our expression reaches a minimum at $\theta = 0$ or $\theta = \pi$, that is, $z = r$ or $z = -r$. We see that $z = -r$ gives the minimum for $|1 + z||1 - z^q|$. For $q = 3, 5, 7$ we check directly that the minimum for $|1 + z||1 - z^q|$ also occurs at $z = -r$. Since the logarithmic derivative of $1/((1 - r^{-1})(1 + r^{-q}))$ as a function of r is negative, this implies that

$$(4.7) \quad \frac{|z|^{q+1}}{|1 + z||1 - z^q|} \leq \frac{r^{q+1}}{(r - 1)(r^q + 1)} \leq \frac{2^{q+1}}{2^q + 1} = 2 \left(1 - \frac{1}{2^q + 1} \right).$$

Referring to (4.6), we thus have for $|z| \geq 2$,

$$\begin{aligned} \log \prod_{\substack{d>q \\ d|n}} |(1 - z^{-d})^{\mu(d)}| &\leq \log \prod_{\substack{d>q \\ 4 \nmid d}} (1 - 2^{-d})^{-1} = \sum_{j \geq 1} \frac{1}{j} \left(\frac{1}{2^{qj}(2^j - 1)} - \frac{1}{2^{4j \lfloor q/4 \rfloor} (2^{4j} - 1)} \right) \\ &< \frac{13}{15 \cdot 2^q} + \sum_{j \geq 2} \frac{1}{j 2^{qj} (2^j - 1)}. \end{aligned}$$

Since

$$\log \left(1 - \frac{1}{2^q + 1} \right) = - \sum_{j \geq 1} \frac{1}{j} \frac{1}{(2^q + 1)^j},$$

with the prior calculation, we see that

$$\left(1 - \frac{1}{2^q + 1} \right) \prod_{\substack{d>q \\ d|n}} |(1 - z^{-d})^{\mu(d)}| < 1.$$

With (4.6) and (4.7), this completes the proof when $p = 2$. ■

5. REAL COINCIDENCES

In this section we discuss solutions to $\Phi_m(x) = \Phi_n(x)$, where $x \in \mathbb{R}$, beginning with the case $x \in (0, 1/2]$.

Theorem 5.1. *Let m and n be distinct positive integers, and let x be a real number with $0 < x \leq \frac{1}{2}$. Then $\Phi_m(x) \neq \Phi_n(x)$.*

Proof. First, we handle the case where one of m and n is equal to 1, say $m = 1$ and $n > 1$. Then we have

$$\Phi_n(x) = \prod_{d|n} (1 - x^d)^{\mu(\frac{n}{d})} > 0$$

whereas $\Phi_1(x) = x - 1 < 0$. Thus $\Phi_n(x) \neq \Phi_1(x)$.

Now assume that $m, n > 1$. Define $g(m, n) = g(m, n, x)$ by

$$g(m, n) = g(m, n, x) = \log \frac{\Phi_m(x)}{\Phi_n(x)}.$$

We have

$$(5.1) \quad g(m, n) = \sum_{d|m} \mu \left(\frac{m}{d} \right) \log(1 - x^d) - \sum_{e|n} \mu \left(\frac{n}{e} \right) \log(1 - x^e).$$

Recall that for a positive integer k , we let $q(k) = \frac{k}{\text{rad}(k)}$. We may assume that $q(n) \geq q(m)$. We split the remainder of the proof up into the following different cases, depending on m and n :

- m and n are squarefree,
- m is squarefree and $q(n) \geq 4$,
- m is squarefree and $q(n) = 3$,
- m is squarefree and $q(n) = 2$,
- neither m nor n is squarefree.

First, assume that m and n are squarefree. Suppose that $\mu(m) \neq \mu(n)$, i.e. $\mu(n) = -\mu(m)$. Then the coefficient of $\log(1-x)$ in (5.1) is $2\mu(m)$, and the coefficient of each other $\log(1-x^d)$ lies in $\{-2, -1, 0, 1, 2\}$. Hence the sign of $g(m, n)$ is the same as that of $\mu(m) \log(1-x)$ by Lemma 4.1, and in particular $g(m, n) \neq 0$. On the other hand, suppose that $\mu(m) = \mu(n)$. Let d_0 be the least divisor of either m or n that does not divide $\gcd(m, n)$, and assume without loss of generality that $d_0 \mid m$. If $d \mid \gcd(m, n)$ then $\mu(m/d) = \mu(n/d)$. Thus, from (5.1)

$$g(m, n) = \mu(m/d_0) \log(1-x^{d_0}) + \sum_{\substack{d \mid m \\ d \nmid n \\ d > d_0}} \mu(m/d) \log(1-x^d) - \sum_{\substack{e \mid n \\ e \nmid m}} \mu(n/e) \log(1-x^e).$$

Since the d 's and e 's in these two sums are all different, it follows from Lemma 4.1 that the sign of $g(m, n)$ is the same as the sign of $\mu(m/d_0) \log(1-x^{d_0})$. In particular, it is not 0. Thus, the case when m, n are squarefree is complete.

Next, we tackle the case where n is not squarefree. In general, (5.1) reduces to

$$(5.2) \quad g(m, n) = \sum_{d \mid \text{rad}(m)} \mu\left(\frac{\text{rad}(m)}{d}\right) \log(1-x^{dq(m)}) - \sum_{e \mid \text{rad}(n)} \mu\left(\frac{\text{rad}(n)}{e}\right) \log(1-x^{eq(n)}).$$

Assume that m is squarefree (that is, $q(m) = 1$) and n is not squarefree (that is, $q(n) > 1$). As in the proof of Theorem 4.2, the sum of all of the e -terms is of the same sign as the $e = 1$ term and is majorized by that term. Hence, if $q(n) \geq 4$, we may majorize all of the e -terms by a single term with exponent 4 (which doesn't appear in the d -sum). Thus, by Proposition 4.1, $g(m, n)$ has the same sign as the $d = 1$ term, and so is not 0.

Now say m is squarefree and $q(n) = 3$. If $3 \nmid m$, then we can majorize the e -terms with a term with exponent 3. So, assume that $3 \mid m$. We similarly may assume that $2 \mid m$. Note that the $d = 6$ term appears with the same sign as the $d = 1$ term, and the $d = 6$ term majorizes the sum of all higher d -terms via Lemma 4.1. Assume without essential loss of generality that $\mu(m) = 1$. Then, majorizing the e -terms with an exponent 3 term and allowing for the possibility of an exponent 5 term, we have

$$g(m, n) < \log(1-x) - \log(1-x^2) - 2\log(1-x^3) - \log(1-x^5).$$

Thus,

$$e^{g(m, n)} < \frac{1-x}{(1-x^2)(1-x^3)^2(1-x^5)} = \frac{1}{(1+x)(1-x^3)^2(1-x^5)}.$$

By inspection, this expression is less than 1 for $0 < x \leq \frac{1}{2}$. Thus, $g(m, n) \neq 0$, completing the proof in this case.

Now assume that m is squarefree and $q(n) = 2$. Assume that $\mu(m) = 1$; the case $\mu(m) = -1$ is essentially the same. There is an $e = 2$ term and it appears with the same sign as the $d = 1$ term. We may assume that $2 \mid m$, since otherwise we may replace a putative $d = 2$ term with the $e = 1$ term and the sum of all e -terms with $e > 2$ with a putative $d = 4$ term. If $3 \nmid m$, we replace the terms with $e > 2$ with a putative $d = 3$ term and observe that

$$g(m, n) < \log(1-x) - 2\log(1-x^2) - \log(1-x^3) + \log(1-x^4) - \log(1-x^5) - \log(1-x^6),$$

so that

$$\begin{aligned} e^{g(m,n)} &= \frac{1+x^2}{(1+x)(1-x^3)(1-x^5)(1-x^6)} \\ &= \frac{1+x^2}{1+x-x^3-x^4-x^5-2x^6-x^7+x^8+2x^9+x^{10}+x^{11}+x^{12}-x^{14}-x^{15}}. \end{aligned}$$

Again, by inspection this shows that $e^{g(m,n)} < 1$ for $0 < x \leq \frac{1}{2}$.

Next, assume that $3 \mid m$. Then $d = 6$ occurs and with the same sign as $d = 1$. If $e = 3$ occurs, then this too gives a term with exponent 6 and the same sign as $d = 1$, and so the sum of all e terms with $e \geq 3$ gives a contribution with the same sign as $d = 1$. Otherwise, if $3 \nmid n$, then the e -terms with $e > 2$ all have exponent 10 or greater, and so their sum is majorized by a term with exponent 9, which is not a d -term. Thus, we have

$$\begin{aligned} g(m,n) &< \log(1-x) - 2\log(1-x^2) - \log(1-x^3) + \log(1-x^4) \\ &\quad - \log(1-x^5) + \log(1-x^6) - \log(1-x^9), \end{aligned}$$

which is smaller than the expression for $g(m,n)$ in the case $3 \nmid m$. Thus, we have handled the case $q(n) = 2$, and so all of the cases with m squarefree.

Now assume that neither m nor n is squarefree and that $1 < q(m) \leq q(n)$. First suppose that $q(m) = q(n) = q$. Then (5.2) becomes

$$g(m,n) = \sum_{d \mid \text{rad}(m)} \mu\left(\frac{\text{rad}(m)}{d}\right) \log(1-x^{dq}) - \sum_{e \mid \text{rad}(n)} \mu\left(\frac{\text{rad}(n)}{e}\right) \log(1-x^{eq})$$

and the proof of the case when m, n are both squarefree can be carried over here.

So, assume that $1 < q(m) < q(n)$. As before, assume that $\mu(\text{rad}(m)) = 1$. We claim that the $d = 1$ term in (5.2) dominates all of the others. The sum of the e -terms is majorized by the $e = 1$ term, which has exponent $q(n) \geq 3$. The sum of the d terms with $d > 1$ is majorized by $|\log(1-x^{2q(m)-1})|$. If $q(m) = 2$, we thus have exponents 2 (from $d = 1$), at least 3 (from $d > 1$), and $q(n) \geq 3$, so that

$$g(m,n) < \log(1-x^2) - 2\log(1-x^3).$$

Hence,

$$e^{g(m,n)} < \frac{1-x^2}{(1-x^3)^2} = \frac{1+x}{1+x+x^2-x^3-x^4-x^5}$$

which is < 1 for $0 < x \leq \frac{1}{2}$. If $q(m) > 2$ the bound is better, so we are done. \blacksquare

Corollary 5.2. *Suppose that x is a real number with $x \geq 2$. If m, n are unequal positive integers, then $\Phi_m(x) \neq \Phi_n(x)$, except when $x = 2$ and $\{m, n\} = \{2, 6\}$.*

Proof. We first note that Corollary 4.3 immediately gives us the cases when $|\phi(m) - \phi(n)| \geq 2$, so we may assume that either $\phi(m) = \phi(n)$ or they are the numbers 1, 2. In the latter case we quickly verify the sole solution $\Phi_2(2) = \Phi_6(2)$, which leaves $\phi(m) = \phi(n) \geq 4$. If $x \geq 2$ and $\Phi_m(x) = \Phi_n(x)$, then Proposition 2.4 implies that $\Phi_m(1/x) = \Phi_n(1/x)$, in violation of Theorem 5.1. This completes the proof. \blacksquare

Corollary 5.3. *Suppose that x is a real number with either $x \leq -2$ or $x \in [-\frac{1}{2}, 0)$. Then for distinct positive integers m, n , we have $\Phi_m(x) \neq \Phi_n(x)$.*

Proof. Using Proposition 2.6, this result follows immediately from Theorem 5.1 in the case that $x \in [-\frac{1}{2}, 0)$ and from Corollary 5.2 when $x \leq -2$. ■

Note that Theorem 5.1, Corollary 5.2, and Corollary 5.3 immediately give us Theorem 1.1.

6. AN ORDERING BASED ON CYCLOTOMIC POLYNOMIALS

A consequence of Corollary 5.2 is that we can put an ordering on the positive integers based on the values of cyclotomic polynomials at any $x > 2$. More precisely, fix any $x > 2$. We write $m \prec n$ if $\Phi_m(x) < \Phi_n(x)$. By Corollary 5.2, \prec is a strict total ordering on the positive integers which does not depend on the choice of x . It is natural to ask about the properties of this ordering.

The first observation is that this ordering is the lexicographic ordering on cyclotomic polynomials. More precisely, suppose m and n are distinct positive integers, and write

$$\Phi_m(x) = \sum_{i=0}^{\infty} a_i x^i, \quad \Phi_n(x) = \sum_{i=0}^{\infty} b_i x^i,$$

so that $a_i = 0$ for $i > \phi(m)$ and $b_i = 0$ for $i > \phi(n)$, and each a_i and b_i is an integer. Let i be the smallest integer such that $a_i \neq b_i$. Then $\Phi_m < \Phi_n$ in the lexicographic ordering if $a_i < b_i$, and $\Phi_m > \Phi_n$ if $a_i > b_i$.

Proposition 6.1. *The ordering \prec on the positive integers coincides with the lexicographic ordering on the cyclotomic polynomials.*

Proof. Let $f_{m,n}(x) = \Phi_m(x) - \Phi_n(x)$. If $\Phi_m > \Phi_n$ in the lexicographic ordering, then the leading coefficient of $f_{m,n}$ is positive, so for sufficiently large x , we have $f_{m,n}(x) > 0$. ■

Note in particular that if $m \prec n$, then $\phi(m) \leq \phi(n)$. Thus in the ordering, we first sort the positive integers by their ϕ -value, and then sort the cyclotomic polynomials lexicographically within each ϕ -value. Since for any k there are only finitely many positive integers n with $\phi(n) = k$, it follows that the order type of the positive integers with respect to \prec is ω .

It is interesting to identify consecutive pairs in the ordering \prec . While this seems to be difficult in general, we can identify certain consecutive pairs.

Proposition 6.2. *Let p be an odd prime and $i \geq 2$ an integer. Then $2p^i$ and p^i are consecutive with respect to \prec , and $2p^i \prec p^i$.*

We defer the proof until later in this section.

Definition 6.3. The *gap* $\gamma(n)$ of n is equal to $\phi(n) - i$, where i is the largest integer less than $\phi(n)$ for which the coefficient of x^i in $\Phi_n(x)$ is nonzero.

Proposition 6.4. *For any positive integer n , we have $\gamma(n) = q(n)$. More precisely, for $x \geq 2$, we have*

$$\Phi_n(x) = x^{\phi(n)} - \mu(\text{rad}(n))x^{\phi(n)-\gamma(n)} + O(x^{\phi(n)-\gamma(n)-1}).$$

Proof. We first prove that when n is squarefree, then $\gamma(n) = 1$ and that

$$\Phi_n(x) = x^{\phi(n)} - \mu(\text{rad}(n))x^{\phi(n)-1} + O(x^{\phi(n)-2}).$$

We prove this by induction on the number $\omega(n)$ of prime factors of n . When $\omega(n) = 0$, i.e. $n = 1$, we have $\Phi_1(x) = x - 1$, so the result follows. Next, suppose that the result holds for n , where $\omega(n) = k \geq 0$, and p is a prime such that $p \nmid n$. Then we have

$$\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}.$$

By the inductive hypothesis, we thus have

$$\begin{aligned} \Phi_{np}(x) &= \frac{x^{p\phi(n)} - \mu(n)x^{p\phi(n)-p} + O(x^{p\phi(n)-2p})}{x^{\phi(n)} - \mu(n)x^{\phi(n)-1} + O(x^{\phi(n)-2})} \\ &= \frac{x^{(p-1)\phi(n)} + O(x^{(p-1)\phi(n)-p})}{1 - \mu(n)x^{-1} + O(x^{-2})} \\ &= x^{(p-1)\phi(n)} + \mu(n)x^{(p-1)\phi(n)-1} + O(x^{(p-1)\phi(n)-2}). \end{aligned}$$

Since $(p-1)\phi(n) = \phi(pn)$, the proof is complete in the squarefree case.

We reduce the non-squarefree case to the squarefree case using Proposition 2.5, completing the proof. \blacksquare

We now prove Proposition 6.2.

Proof of Proposition 6.2. It suffices to show that, among all the numbers n with $\phi(n) = \phi(p^i)$, we have $\gamma(p^i) > \gamma(n)$ unless $n \in \{p^i, 2p^i\}$. We have $\phi(p^i) = (p-1)p^i$, so if n is not equal to p^i or $2p^i$ but $\phi(n) = \phi(p^i)$, then n must have a prime factor q such that $p \mid (q-1)$. In particular, $q > p$. Now, note that if $n = q_1^{e_1} \cdots q_r^{e_r}$, then we have

$$\frac{\gamma(n)}{\phi(n)} = \frac{\prod_{i=1}^r q_i^{e_i-1}}{\prod_{i=1}^r (q_i-1)q_i^{e_i-1}} = \prod_{i=1}^r \frac{1}{q_i-1} < \frac{1}{p-1} = \frac{\gamma(p^i)}{\phi(p^i)}.$$

Since $\phi(n) = \phi(p^i)$, we therefore have $\gamma(n) < \gamma(p^i)$, as desired. \blacksquare

If $i = 1$, then it is not always true that $2p$ and p are consecutive with respect to \prec . However, they are \prec -consecutive when $2p$ and p are the only integers whose ϕ -values are equal to $p-1$. When $p \equiv 3 \pmod{4}$, there is a simple criterion.

Proposition 6.5. *Let $p \equiv 3 \pmod{4}$ be prime. Then $2p$ and p are \prec -consecutive unless there is a prime q and an integer $j \geq 2$ such that $\phi(q^j) = p-1$.*

Proof. Note that $p-1 \equiv 2 \pmod{4}$, and that $\phi(q)$ is even for every odd prime q . Since ϕ is multiplicative, if n is odd, then $\phi(n) \equiv 0 \pmod{2^{\omega(n)}}$. Thus an odd n with $\phi(n) = p-1$ can only have one prime factor. Next, suppose that $n = 2^e m$, where m is odd and $e \geq 2$. Then $\phi(n) = 2^{e-1}\phi(m)$ is divisible by 4 unless $e = 2$ and $m = 1$, in which case n is a prime power. If $e = 1$, then $\phi(n) = \phi(m)$, so we have already analyzed this case. \blacksquare

We remark that very few primes $p \equiv 3 \pmod{4}$ have the property that $p-1 = \phi(q^j)$ for some prime q and exponent $j > 1$. An easy argument shows that the number of such primes $p \leq x$ is $O(\sqrt{x})$.

When $p \equiv 1 \pmod{4}$, there are more ways for there to exist an integer n other than p and $2p$ with $\phi(n) = p-1$. Still, this is relatively unusual behavior: Theorem 4.1 in [BFL⁺05] shows that the number of such primes up to x is $\leq \frac{x}{\log^{2+o(1)} x}$ as $x \rightarrow \infty$. On the other hand, it is not known unconditionally if there are infinitely many such primes, though this follows from Schinzel's Hypothesis H.

There is another total ordering we can put on the positive integers based on the values of cyclotomic polynomials at some $x \in (0, \frac{1}{2}]$, thanks to Theorem 5.1. Let us write $m \prec' n$ if $\Phi_m(x) < \Phi_n(x)$ for some (hence any) $x \in (0, \frac{1}{2}]$. Like \prec , \prec' is also a lexicographic ordering, but in reverse order of degrees. That is, suppose

$$\Phi_m(x) = \sum_{i=0}^{\infty} a_i x^i, \quad \Phi_n(x) = \sum_{i=0}^{\infty} b_i x^i.$$

If $m \neq n$, then let i be the smallest nonnegative integer for which $a_i \neq b_i$. Then $m \prec' n$ if $a_i < b_i$, and $n \prec' m$ if $b_i < a_i$.

Unlike \prec , \prec' is not a well-ordering. To see this, we produce an infinite decreasing sequence. Let p be any prime. Then for any positive integer i , we have $\Phi_{p^i}(x) = 1 + x^{p^{i-1}} + O(x^{p^{i-1}+1})$ as $x \rightarrow 0$. Thus we have $p^{i+1} \prec' p^i$, so the powers of p form an infinite decreasing sequence. In addition, the sequence of primes forms an infinite increasing sequence, which implies that the reverse of \prec' is not a well-ordering either. It would be interesting to describe the order type of \prec' .

7. NEAR MISSES

Other than $\Phi_2(2) = \Phi_6(2)$, we have shown that all real roots of $\Phi_m - \Phi_n$ are smaller than 2. It is natural to ask whether there are roots that get close. To this end, let

$$S = \{\alpha \in \mathbb{R} : \Phi_m(\alpha) = \Phi_n(\alpha) \text{ for some } m \neq n\}.$$

Thus we ask whether 2 is a limit point of S . We begin with some examples:

- $\Phi_{209} - \Phi_{179}$ has a root at $1.99975454398254 \dots$,
- $\Phi_{407} - \Phi_{359}$ has a root at $1.99975550093366 \dots$,
- $\Phi_{221} - \Phi_{191}$ has a root at $1.99993512065828 \dots$,
- $\Phi_{527} - \Phi_{479}$ has a root at $1.99999618493891 \dots$.

These near-misses were constructed as follows: let p, q, r be primes such that $pq = p + q + r$, and $p < q$. Then we claim that $\Phi_{pq} - \Phi_r$ has a root very close to the largest real root of $\psi_{p-1}(x) = x^{p-1} - x^{p-2} - x^{p-3} \dots - x - 1$, with this root getting closer the larger that q is. Note that the latter polynomial has a root very close to 2, since $\psi_{p-1}(2) = 1$ and $\psi'_{p-1}(2) = 2^{p-1} - 1$, so the largest real root of ψ_{p-1} is approximately $2 - \frac{1}{2^{p-1}-1}$. Let us write α_{p-1} for the largest real root of ψ_{p-1} .

The reason why $\Phi_{pq} - \Phi_r$ has a root very close to α_{p-1} is that we have a near-factorization of $\Phi_{pq} - \Phi_r$, namely

$$\Phi_{pq}(x) - \Phi_r(x) = \psi_{p-1}(x)x^{\phi(pq)-\phi(p)} + \delta(x),$$

where $\deg(\delta) \leq \phi(pq) - p$. Furthermore, by Proposition 2.7, all the coefficients of δ lie in $\{-2, -1, 0, 1\}$. Note that the degree of δ is much smaller than the degree of the main term $\psi_{p-1}(x)x^{\phi(pq)-\phi(p)}$, so this is a small perturbation.

In general, suppose we have a polynomial $f(x)$ all of whose complex roots are distinct, and a perturbation polynomial $g(x)$ with $\deg(g) < \deg(f)$. Let us suppose that $f(x) + tg(x)$ factors as $\prod_{i=1}^d (x - \beta_i(t))$, where the β_i 's are continuous functions for small values of t . Then we have

$$\beta'_i(0) = -\frac{g(\beta_i(0))}{f'(\beta_i(0))}$$

p	q	r	β	α_{p-1}	$(\alpha_{p-1} - \beta)^{-1}$	$\frac{1}{2^q(\alpha_{p-1} - \beta)}$
3	5	7	1.90040519768798	1.92756197548293	36.8232198808926	1.15072562127789
3	7	11	1.92172452309274	1.92756197548293	171.307607010499	1.33834067976952
3	11	19	1.92717413781454	1.92756197548293	2578.39833911685	1.25898356402190
3	13	23	1.92745816209718	1.92756197548293	9632.66916662882	1.17586293537949
5	7	23	1.97926028654319	1.98358284342433	231.344555433128	1.80737933932131
5	13	47	1.98351307615232	1.98358284342433	14333.3682296163	1.74967873896684
5	19	71	1.9835169859533	1.98358284342433	873492.901563983	1.66605549156949
7	11	59	1.99577873757697	1.99603117973541	3961.30347707098	1.93423021341356
7	13	71	1.99596788607732	1.99603117973541	15799.3712194387	1.92863418206039
7	19	107	1.99603017934944	1.99603117973541	999614.177077968	1.90661273398964

Table 1

(see [Wil84]). In our case, with $g = \delta$, we expect to have a root of $\Phi_{pq} - \Phi_r$ near

$$\alpha_{p-1} - \frac{\delta(\alpha_{p-1})}{\Phi'_{pq}(\alpha_{p-1}) - \Phi'_r(\alpha_{p-1}) - \delta'(\alpha_{p-1})}.$$

Since $|\delta(\alpha_{p-1})| \leq 2^{pq-2p-q+3}$ and the denominator has size on the order of 2^{pq-p-q} , we have a root of $\Phi_{pq} - \Phi_r$ somewhere around

$$\alpha_{p-1} - \frac{1}{2^q}.$$

This matches experimental observation, as shown in Table 1. Here β is the root of $\Phi_{pq} - \Phi_r$ close to α_{p-1} .

Conjecture 7.1. *The largest limit point of S is 2.*

This would follow from the above work if we could show that, for infinitely many primes p , there exists a prime $q > p$ such that $pq - p - q$ is also prime. This would follow, for instance, from Dickson's prime k -tuples conjecture, which says that several linear polynomials in $\mathbb{Z}[x]$ will be simultaneously prime infinitely often unless there is a congruential obstruction. In this case, for any fixed p , we apply this to the two polynomials x and $(p-1)x - p$, and the conjecture implies there should be infinitely many x where both are prime. However, this is stronger than what we need. Indeed, it suffices to prove that for infinitely many primes p , there is at least one value of $x > p$ with both x and $(p-1)x - p$ simultaneously prime. It may be possible to prove this unconditionally. According to our calculations, this appears to be the only route to Conjecture 7.1: all points in S close to 2 appear to have this form.

On the other side, there are values of m and n such that $\Phi_m(x) - \Phi_n(x)$ has roots not far from $\pm\frac{1}{2}$. For instance, if p is a large prime, then $\Phi_{3p}(x) - \Phi_4(x)$ has a root near $\rho := -0.569840290998 \dots$, which is a root of $x^3 + x^2 + 2x + 1$. In fact, as $p \rightarrow \infty$, the polynomials $\Phi_{3p}(x) - \Phi_4(x)$ have roots that converge to ρ (and $\Phi_{6p}(x) - \Phi_4(x)$ have roots which converge to $-\rho$). To see this, note that $\Phi_{3p}(x) = 1 - x + x^3 - x^4 + x^6 - x^7 + \dots + x^{2p-5} - x^{2p-3} + x^{2p-2}$. As $p \rightarrow \infty$, these polynomials converge termwise to the power series $\sum_{n=0}^{\infty} (1-x)x^{3n} = \frac{1}{1+x+x^2}$. If $|x| < 1$, then $\Phi_{3p}(x) \approx \frac{1}{1+x+x^2}$, so $\Phi_{3p}(x) - \Phi_4(x)$ has a root near that of $\frac{1}{1+x+x^2} - \Phi_4(x)$, i.e., where $(1+x+x^2)(1+x^2) = 1$. This means that $x^4 + x^3 + 2x^2 + x = 0$. Curiously, roots of $\Phi_{4p}(x) - \Phi_3(x)$ also converge to the same number. We can do better however. The polynomial $\Phi_{30}(x) - \Phi_4(x)$ has a root at $\sigma := 0.5284555592772 \dots$, and as the prime

$p \rightarrow \infty$, $\Phi_{30p}(x) - \Phi_{4p}(x)$ has a root that converges to σ . Better still: Take m as the product of the first $k \geq 3$ primes and n as $\frac{2}{15}m$. Then $\Phi_m(x) - \Phi_n(x)$ seems to have a root converging to a number slightly below 0.52. For example, when $k = 5$, there is a root at $0.51976982658213 \dots$. Perhaps the number $\frac{1}{2}$ in Theorem 1.1 is best possible, but we do not have strong evidence either way.

Based on numerical computations, we present the following conjectures.

Conjecture 7.2. *For any distinct positive integers m and n , if $z \in \mathbb{C} \setminus \mathbb{R}$ and $\Phi_m(z) = \Phi_n(z)$, then $\frac{1}{\sqrt{2}} < |z| \leq \sqrt{2}$. The upper bound is attained only for $\{m, n\} = \{1, 3\}, \{1, 4\}, \{1, 5\}$.*

Conjecture 7.3. *Let $S_{\mathbb{C}}$ denote the set of all nonreal complex numbers z such that $\Phi_m(z) = \Phi_n(z)$ for some distinct coprime positive integers m and n . Then for any $\varepsilon > 0$, we have $1 - \varepsilon < |z| < 1 + \varepsilon$ for all but finitely many elements of $S_{\mathbb{C}}$.*

Without the coprime hypothesis Conjecture 7.3 is likely to be false. To see this, note that if m and n are both odd and α is a positive real root of $\Phi_m(x) - \Phi_n(x)$, then $i\alpha^{1/2}$ is a nonreal root of $\Phi_{4m}(x) - \Phi_{4n}(x)$. Since presumably polynomials of the form $\Phi_m(x) - \Phi_n(x)$ can have real roots arbitrarily close to 2, this implies that $\Phi_{4m}(x) - \Phi_{4n}(x)$ can have roots arbitrarily close to $\sqrt{-2}$.

However, there are infinitely many real roots bounded away from ± 1 . Thus we see that apparently there is a significant behavioral difference between the real and nonreal roots of differences of cyclotomic polynomials.

The observed behavior of roots of $\Phi_m(x) - \Phi_n(x)$ is consistent with typical behavior of random polynomials whose coefficients are each chosen uniformly in some large interval. Let d be a large positive integer and B a large positive real number, and let $f(x)$ be a degree- d polynomial in $\mathbb{R}[x]$ whose coefficients are chosen uniformly and independently from the interval $[-B, B]$. Then it is known (see [HN08]) that all but $o(d)$ of the roots of f are asymptotically almost surely very close to the unit circle.

On the other hand, the behavior of the real roots, of which there are $o(d)$, behave rather differently. Kac in [Kac49] showed that the expected number of real roots is $\frac{2}{\pi} \log d$. Similarly, Littlewood and Offord (see [LO38, LO43, LO45, LO48]) proved that for almost all f (with coefficients chosen independently from any of several different distributions), the number r_f of real roots satisfies

$$\frac{\log n}{\log \log \log n} \ll r_f \ll \log^2 n.$$

Kac also showed that for any $\alpha \in (0, 1)$, the expected number of real roots in the range $(0, \alpha)$ is $O(1)$, but not 0.

ACKNOWLEDGMENTS

We thank Gerry Myerson and Tim Trudgian for bringing Glasby's conjectures to our attention. We also thank Kevin Ford for reminding us of [BFL⁺05]. This project was started at the West Coast Number Theory Conference in Chico, California, in December 2018.

REFERENCES

- [Ban86] A. S. Bang. Taltheoretiske undersøgelser. *Tidsskrift for matematik*, 4:70–80, 1886. URL: <http://www.jstor.org/stable/24539988>.

- [BFL⁺05] W. D. Banks, K. Ford, F. Luca, F. Pappalardi, and I. E. Shparlinski. Values of the Euler function in various sequences. *Monatsh. Math.*, 146(1):1–19, 2005. URL: <https://doi.org/10.1007/s00605-005-0302-7>, doi:10.1007/s00605-005-0302-7.
- [Her74] C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geom. Dedicata*, 2:425–460, 1974.
- [HN08] C. P. Hughes and A. Nikeghbali. The zeros of random polynomials cluster uniformly near the unit circle. *Compos. Math.*, 144(3):734–746, 2008. URL: <https://doi.org/10.1112/S0010437X07003302>, doi:10.1112/S0010437X07003302.
- [Kac49] M. Kac. On the Average Number of Real Roots of a Random Algebraic Equation (II). *Proc. London Math. Soc. (2)*, 50(6):390–408, 1949. URL: <https://doi.org/10.1112/plms/s2-50.6.401>, doi:10.1112/plms/s2-50.6.401.
- [LO38] J. E. Littlewood and A. C. Offord. On the Number of Real Roots of a Random Algebraic Equation. *J. London Math. Soc.*, 13(4):288–295, 1938. URL: <https://doi.org/10.1112/jlms/s1-13.4.288>, doi:10.1112/jlms/s1-13.4.288.
- [LO43] J. E. Littlewood and A. C. Offord. On the number of real roots of a random algebraic equation. III. *Rec. Math. [Mat. Sbornik] N.S.*, 12(54):277–286, 1943.
- [LO45] J. E. Littlewood and A. C. Offord. On the distribution of the zeros and a -values of a random integral function. I. *J. London Math. Soc.*, 20:130–136, 1945. URL: <https://doi.org/10.1112/jlms/s1-20.3.130>, doi:10.1112/jlms/s1-20.3.130.
- [LO48] J. E. Littlewood and A. C. Offord. On the distribution of zeros and a -values of a random integral function. II. *Ann. of Math. (2)*, 49:885–952; errata 50, 990–991 (1949), 1948. URL: <https://doi.org/10.2307/1969404>, doi:10.2307/1969404.
- [Slo] N. J. A. Sloane. The On-Line Encyclopedia of Integer Sequences. Sequence A206225. URL: <http://oeis.org/>.
- [Wil84] James H. Wilkinson. The perfidious polynomial. In *Studies in numerical analysis*, volume 24 of *MAA Stud. Math.*, pages 1–28. Math. Assoc. America, Washington, DC, 1984.
- [Zsi92] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892. URL: <https://doi.org/10.1007/BF01692444>, doi:10.1007/BF01692444.

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

EULER CIRCLE, PALO ALTO, CA 94306
E-mail address: simon@eulercircle.com