PaNTS XXXIII

Clemson U., December 14–15 2019

Cyclotomic Polynomials: Problems and Results

Carl Pomerance

Dartmouth College

Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial. It is defined as the minimum polynomial of $e^{2\pi i/n}$ over $\mathbb{Z}$. For example:

$$\begin{aligned}
\Phi_1(x) &= x - 1\\
\Phi_2(x) &= x + 1\\
\Phi_3(x) &= x^2 + x + 1\\
\Phi_4(x) &= x^2 + 1\\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1\\
\Phi_6(x) &= x^2 - x + 1\\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\\
\Phi_8(x) &= x^4 + 1
\end{aligned}$$

Lemma. Suppose $\Phi_n(\zeta) = 0$ and p is a prime that does not divide n. Then $\Phi_n(\zeta^p) = 0$.

Proof Let $f(x)$ be the minimum polynomial of ζ^p over $\mathbb{Z}$ and assume that $f \neq \Phi_n$. Then $f(x)\Phi_n(x) \mid x^n - 1$. Now ζ is a root of $f(x^p)$, so that $\Phi_n(x) \mid f(x^p)$. But $f(x^p) \equiv f(x)^p \pmod{p}$, so in $(\mathbb{Z}/p\mathbb{Z})[x]$, $\Phi_n(x)$ and $f(x)$ have a common irreducible factor of positive degree, say $g(x)$. Then $g(x)^2 \mid x^n - 1$ in $(\mathbb{Z}/p\mathbb{Z})[x]$, contradicting $x^n - 1$ squarefree (here is where $p \nmid n$ is used). □

By iterating, one can get $\Phi_n(e^{2\pi i m/n}) = 0$ for every m coprime to n. That is, every primitive n-th root of 1 is a root of Φ_n. And there are no other roots since an isomorphism of $\mathbb{Q}(e^{2\pi i/n})$ must take $e^{2\pi i/n}$ to another primitive n-th roof of unity.

We conclude that $\deg(\Phi_n(x)) = \varphi(n)$.

The following cute observation is not so well-known. Suppose there is no primitive root mod n. So, $n = 8, 12, 15, 16, 20, \ldots$.

Claim. If there is no primitive root mod n, then $\Phi_n(x)$ is reducible in $(\mathbb{Z}/p\mathbb{Z})[x]$ for every prime p.
Proof. Suppose $\Phi_n(x)$ is irreducible mod p. The Galois group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$, the group of reduced residues mod n. (Consider the $\varphi(n)$ automorphisms: the general one sends the roots ζ to ζ^m, where m is coprime to n.) But a Galois group over the field $\mathbb{Z}/p\mathbb{Z}$ must be cyclic, so n must have a primitive root. □

For example, $x^4 + 1$ is reducible mod p for every prime p.

Michael's first paper: *On an irreducibility theorem of A. Cohn*, with J. D. Brillhart and A. M. Odlyzko.
Among other results, they prove that if a prime is written in the base $b \geq 2$ as $\sum a_i b^i$ with each b-digit a_i satisfying $0 \leq a_i < b$, then the polynomial $\sum a_i x^i$ is irreducible in $\mathbb{Z}[x]$. (In a later paper, Michael relaxed the condition on the coefficients a_i to still allow for the necessary irreducibility of the polynomial, and he relaxed the condition on the value being prime.)

This theorem was invaluable in the number field sieve factorization algorithm. There one needs to procure an irreducible polynomial $f(x)$ of a given moderate degree d and an integer m with $f(m) = n$, the number to be factored. So, the algorithm sets $m = \lfloor n^{1/d} \rfloor$ and writes n in the base m. Michael's theorem does not guarantee that f is irreducible, but if it can be factored as $g(x)h(x)$, then the proof of his theorem guarantees that $g(m)h(m)$ is a nontrivial factorization of n.

It has been a dream to turn this around: instead of using primes to produce irreducible polynomials, use irreducible polynomials to produce primes.

For example, is $\Phi_n(2)$ prime?

$$\begin{aligned}
\Phi_1(2) &= 1\\
\Phi_2(2) &= 3\\
\Phi_3(2) &= 7\\
\Phi_4(2) &= 5\\
\Phi_5(2) &= 31\\
\Phi_6(2) &= 3\\
\Phi_7(2) &= 127\\
\Phi_8(2) &= 17
\end{aligned}$$

Conjecture?

Some cases where $\Phi_n(2)$ is composite:

- $n = 2 \cdot 3^j$ with $j \geq 2$. Then $3 \mid \Phi_n(2)$ and $\Phi_n(2) > 3$.

- More generally, if $p \mid \Phi_m(2)$ with $2 < m < p$, then $p \mid \Phi_{p^j m}(2)$ for $j \geq 1$ and $\Phi_{p^j m}(2) > p$.

- If $n \equiv 4 \pmod 8$ and $n > 12$, then $\Phi_n(2)$ is composite.

This last condition arises from the identity

$$2^{4m+2} + 1 = (2^{2m+1} + 2^{m+1} + 1)(2^{2m+1} - 2^{m+1} + 1).$$

Other than these cases, it may be that all but finitely often $\Phi_n(2)$ is prime, or all but finitely often, $\Phi_n(2)$ is composite!

What can be said about $P(\Phi_n(2))$, the greatest prime factor of $\Phi_n(2)$?

For $n \geq 2$, we have $P(\Phi_n(2)) \geq n+1$. In fact, $\Phi_n(2)$ is divisible by a prime $p \equiv 1 \pmod{n}$. In fact, for $n > 6$, $\Phi_n(2)$ is divisible by a prime p not dividing any $\Phi_m(2)$ with $m < n$ and such a prime is $\equiv 1 \pmod{n}$.

This last, for $\Phi_n(a)$ with $a \geq 2$, is A. S. Bang's theorem from 1886. It was generalized to expressions $a^n - b^n$ by K. Zsigmondy in 1892.

Bang and/or Zsigmondy has been rediscovered many times:
J. J. Sylvester, 1888
G. D. Birkhoff and H. S. Vandiver, 1904
L. E. Dickson, 1905
H.-J. Kanold, 1950
E. Artin, 1955
H. W. Leopoldt, 1966
B. Richter, 1972

And they have been further generalized:
R. D. Carmichael, 1913
M. Ward, 1955
A. Schinzel, 1962/63
Y. Bilu, G. Hanrot, & P. M. Voutier, 2001

But surely we should be able to prove that $P(\Phi_n(2)) > n + 1 \ldots .$

A. Schinzel, in 1962, showed that $P(\Phi_n(2)) \geq 2n + 1$ for $n > 12$.

P. Erdős, in 1965, conjectured that $P(\Phi_n(2))/n \to \infty$ as $n \to \infty$.

C. L. Stewart, in 2013, proved the Erdős conjecture and more: $P(\Phi_n(2)) > n^{1+1/(104 \log\log n)}$ for all large n.

Assuming the ABC conjecture, M. R. Murty and S. Wong, in 2002, showed that $P(2^n - 1) \geq n^{2+o(1)}$.

In 2003, L. Murata and Pomerance obtained some related results conditional on GRH.

Coefficients of cyclotomic polynomials

Are they always in $\{0, \pm 1\}$?

Yes, for n up to 104, but $\Phi_{105}(x)$ has a coefficient of –2.

Say $\Phi_n(x)$ is *flat* if all of its coefficients are in $\{0, \pm 1\}$.

It is not so difficult to see that $\Phi_n(x)$ is flat if n has at most 2 distinct odd prime factors. Note that 105 is the least number with at least 3 distinct odd prime factors.

The converse is not true. For example, Φ_{231} is flat.

P. Moree (2014) has a neat interpretation on why $\Phi_{pq}(x)$ is flat, where p, q are unequal primes. Let S be the semigroup $\{ap + bq\}$ where a, b run over non-negative integers. As is well-known, the largest number not in S is $pq - p - q = \varphi(pq) - 1$. Thus, if $z(x) = \sum_{s \in S} x^s$, we have $(1 - x)z(x)$ equal to a polynomial, and in fact this polynomial is $\Phi_{pq}(x)$. Since the difference of two power series each with coefficients in $\{0, 1\}$ has coefficients in $\{0, \pm 1\}$, we see that $\Phi_{pq}(x)$ is flat.

Let $A(n)$ denote the largest absolute value of a coefficient of $\Phi_n(x)$.

Also, let $M(p)$ be the maximum value of $A(pm)$ where m has exactly 2 odd prime factors, both larger than p. (It's known that, more generally, the maximum of $A(nm)$ exists, where m has exactly 2 odd prime factors both larger than $P(n)$.)

Sister M. Beiter, in 1968, conjectured that $M(p) \le (p+1)/2$ for $p > 2$ and proved, in 1971, that $M(p) \le \lceil 3p/4 \rceil$.

H. Möller, in 1971, proved that $M(p) \ge (p+1)/2$ for $p > 2$.

Beiter's conjecture is false for every $p > 7$, as proved in 2009 by Y. Gallot and P. Moree. They conjecture the bound $2p/3$ for all large p, and showed $> (2-\epsilon)p/3$ for all large p.

D. Duda has found a finite procedure to compute $M(p)$, but we don't yet know a practical method.

Are there any flat cyclotomic polynomials $\Phi_n(x)$ with n having more than 3 distinct odd prime factors? Yes, N. Kaplan, in 2010, showed the smallest such n is $3 \cdot 5 \cdot 31 \cdot 929$, and he showed there are infinitely many.

Does $A(n) \to \infty$ as $\omega(n) \to \infty$ (where $\omega(n)$ is the number of distinct prime divisors of n)? S. Elder, in 2012, conjectured that $A(n) > 1$ when n has at least 5 distinct odd prime divisors.

In 1935, I. Schur showed that $A(n)$ is unbounded over all n. And E. Lehmer, in 1936, proved this where n is restricted to numbers with $\omega(n) = 3$. (Cf. the Möller result mentioned earlier.)

So, how large can the maximal coefficient get (in absolute value)? It is convenient to measure this in terms of $k = \omega(n)$.

P. T. Bateman, in 1949, showed that $A(n) \le n^{2^{k-1}}$.

This was improved in 1984 by Bateman, Pomerance, and R. C. Vaughan to $A(n) \le n^{2^{k-1}/k-1}$. They conjectured this was best possible, for infinitely many n, up to a constant factor depending only on k, and proved this under the prime k-tuples conjecture. They also proved an unconditional result that is almost as sharp, up to a logarithmic factor in n.

In 2011, B. Bzdęga showed that $A(n) \le \varphi(n)^{2^{k-1}/k-1}$, proving a conjecture of Bateman, et al.

This is extreme behavior, one might ask what happens normally?

Here we have some neat results of H. Maier. He showed, in 1990, that for any function $\psi(n) \to \infty$, $A(n) \le n^{\psi(n)}$ for almost all n (i.e., except for a set of numbers n of asymptotic density 0).

He also showed, in 1993, that for any function $\epsilon(n) \to 0$, $A(n) > n^{\epsilon(n)}$ for almost all n.

In 1995, he showed that these results are best possible.

Glasby's cyclotomic ordering conjecture

Note that if $f(x), g(x) \in \mathbb{R}[x]$, then there is some x_0 such that $f(x) \geq g(x)$ for all $x \geq x_0$, or $g(x) \geq f(x)$ for all $x \geq x_0$. In this way, we can put a total ordering on the cyclotomic polynomials.

Recently (in 2018) Stephen Glasby conjectured that one could determine the ordering for cyclotomic polynomials by looking at integer arguments ≥ 2. Specifically, he conjectured that for any positive integers m, n we have $\Phi_m(j) \geq \Phi_n(j)$ for all integers $j \geq 2$ or $\Phi_m(j) \leq \Phi_n(j)$ for all integers $j \geq 2$.

Theorem (Pomerance and S. Rubinstein-Salzedo, 2019)
If m, n are unequal positive integers and x is a real root of $\Phi_m(x) - \Phi_n(x)$, then $1/2 < |x| < 2$, except for $\Phi_2(2) = \Phi_6(2)$.

Theorem (Pomerance and S. Rubinstein-Salzedo, 2019)
If m, n are unequal positive integers and x is a real root of $\Phi_m(x) - \Phi_n(x)$, then $1/2 < |x| < 2$, except for $\Phi_2(2) = \Phi_6(2)$.

In particular we can determine the cyclotomic ordering merely by looking at the values at 2, with the proviso that Φ_6 comes after Φ_2.

We conjecture the theorem holds as well for complex x.

We also conjecture that the upper bound 2 in the theorem is best possible in that for any fixed $\epsilon > 0$, there are infinitely many pairs of unequal positive integers m, n with $\Phi_m(x) = \Phi_n(x)$ for some $x \in (2 - \epsilon, 2)$.

We also conjecture that the upper bound 2 in the theorem is best possible in that for any fixed $\epsilon > 0$, there are infinitely many pairs of unequal positive integers m, n with $\Phi_m(x) = \Phi_n(x)$ for some $x \in (2 - \epsilon, 2)$.

For example,

- $\Phi_{209} - \Phi_{179}$ has a root at $1.99975454398254\cdots$,
- $\Phi_{221} - \Phi_{191}$ has a root at $1.99993512065828\cdots$,
- $\Phi_{527} - \Phi_{479}$ has a root at $1.99999618493891\cdots$,
- $\Phi_{713} - \Phi_{659}$ has a root at $1.99999994016248\cdots$.

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

By the prime k-tuples conjecture there are infinitely many prime triplets p, q, r with p, q large and $pq = p + q + r$. Indeed, for each fixed prime p, there should be infinitely many primes q with $q(p-1) - p$ prime.

Can the existence of infinitely many of these prime triplets be proved unconditionally?

Can we prove that there is some $c > 1$ such that for infinitely many unequal pairs m, n we have a real root of $\Phi_m - \Phi_n$ greater than c?

Yes, here is how. Suppose p, q are primes with q large and $p = q + k$, with $k > 0$ small. Then $\Phi_{2p} - \Phi_q$ has a real root near to the largest root ρ_k of $x^{k+1} - x^k - x - 1$. It's clear that $\rho_k > 1$. So, all we need to do is find infinitely many pairs of primes with gap k.

By Zhang, Maynard, Tao, and Polymath, this can be done for some $k \le 246$. So there are infinitely many real cyclotomic coincidences in $(1.01912, 2)$.

Theorem (Pomerance and S. Rubinstein-Salzedo, 2019)
If m, n are unequal positive integers and x is a real root of $\Phi_m(x) - \Phi_n(x)$, then $1/2 < |x| < 2$, except for $\Phi_2(2) = \Phi_6(2)$.

A few words on the proof: We reduce to showing that if $0 < x \le 1/2$, then $\Phi_m(x) \ne \Phi_n(x)$. Assume so, and now assume that $x \ge 2$, $\Phi_m(x) = \Phi_n(x)$, and $\max\{\varphi(m), \varphi(n)\} \ge 4$ (with the smaller cases easily handled). We show that $\Phi_n(x) \approx x^{\varphi(n)}$, when $x \ge 2$. Using this, we can show that $\varphi(m) = \varphi(n)$. Note that $x^{\varphi(n)}\Phi_n(1/x) = \Phi_n(x)$. Thus, $\Phi_m(1/x) = \Phi_n(1/x)$, a case we've handled.

So, how to handle the case $0 < x \le 1/2$?

Here, we consider various cases. Let $q(n) = n/\mathrm{rad}(n)$, where $\mathrm{rad}(n)$ is the largest squarefree divisor of n. So, if $n = \prod p_i^{a_i}$, then $q(n) = \prod p_i^{a_i - 1}$. It's a measure of how far n is from being squarefree.

Case 1: m, n squarefree.
Case 2: m squarefree, $q(n) \ge 4$.
Case 3: m squarefree, $q(n) = 3$.
Case 4: m squarefree, $q(n) = 2$.
Case 5: $2 \le q(m) \le q(n)$.

We found Case 4 the most tedious.

As mentioned, we believe our theorem holds for complex coincidences of Φ_m, Φ_n, in fact, we believe that if $z \notin \mathbb{R}$ and $\Phi_m(z) = \Phi_n(z)$, then $1/\sqrt{2} < |z| < \sqrt{2}$. This would be best possible on the prime k-tuples conjecture, since if m, n are odd with $\Phi_m - \Phi_n$ having a root near 2, them

$$\Phi_{4m}(x) - \Phi_{4n}(x) = \Phi_m(-x^2) - \Phi_n(-x^2)$$

has roots near $\pm i\sqrt{2}$.

We conjecture that if m, n are coprime then the non-real roots of $\Phi_m - \Phi_n$ cluster near the unit circle in that there are at most finitely many cases with a root z with $|z| > 1 + \epsilon$ or $|z| < 1 - \epsilon$.

Rubinstein-Salzedo and I considered $\Phi_m - \Phi_n$. As pointed out to me by Moree, C. Nicol, in 2000, considered $\Phi_m + \Phi_n$. He showed that if m, n are primes, the sum is irreducible. Further if m, n are coprime and $\Phi_m + \Phi_n$ is reducible, then it seems to contain a cyclotomic factor (and after dividing out by cyclotomic factors, the resulting polynomial is irreducible). This has been checked for $m, n \leq 150$. An example:

$$\Phi_{22}(x) + \Phi_7(x) = (x^2 + 1)(x^8 - x^7 + 2x^4 + 2).$$

Thank You

Thank You

and Happy Birthday Michael!