WCNTC
Asilomar, December 16–20, 2019

Glasby's cyclotomic ordering conjecture

Carl Pomerance
Dartmouth College

with Simon Rubinstein-Salzedo

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:

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

We know that $\Phi_n(x)$ has degree $\varphi(n)$.

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 $\psi_{p-1}(x) := x^{p-1} - x^{p-2} - x^{p-3} \ldots - x - 1$, 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 $k \leq 246$. 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 $q(n) = n/\text{rad}(n)$, where 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, $q(n) \geq 4$.
Case 3: m squarefree, $q(n) = 3$.
Case 4: m squarefree, $q(n) = 2$.
Case 5: $2 \leq q(m) \leq q(n)$.

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