Cyclotomic ordering conjecture

Stephen Glasby[a]

[a] *Center for the Mathematics of Symmetry and Computation, University of Western Australia, 35 Stirling Highway, Perth 6009, Australia*

Abstract

This note describes a conjecture I made (in Aachen, Sept. 2018) and some initial thoughts towards a solution. Given positive integers m, n, the conjecture is that either $\Phi_m(q) \leqslant \Phi_n(q)$ or $\Phi_m(q) \geqslant \Phi_n(q)$ holds for all integers $q \geqslant 2$. Pomerance and Rubinstein-Salzedo proved the conjecture in [2].

We define a partial ordering $\preceq$ on the set $\mathcal{P}$ of positive integers. Recall that $t^n - 1 = \prod_{d|n} \Phi_d(t)$ where the roots of the dth cyclotomic polynomial $\Phi_d(t)$ are primitive roots of order d. Hence $\deg(\Phi_d(t)) = \phi(d)$. For $m, n \in \mathcal{P}$ write $m \preceq n$ if $\Phi_m(q) \leqslant \Phi_n(q)$ for all integers $q \geqslant 2$, and write $m \prec n$ if $m \preceq n$ and $m \neq n$. (Clearly $a \preceq a$; $a \preceq b$ and $b \preceq a$ implies $a = b$; and $a \preceq b$ and $b \preceq c$ implies $a \preceq c$.) Since

$$q - 1 < q + 1 < q^2 - q + 1 \leqslant q^2 + 1 < q^2 + q + 1 < q^4 - q^3 + q^2 - q + 1$$

holds for all $q \geqslant 2$, we have $1 \prec 2 \prec 6 \prec 4 \prec 3 \prec 10$. Similarly, one can show $10 \prec 12 \prec 8 \prec 5 \prec 14 \prec 18 \prec 9 \prec 7 \prec 15 \prec 20 \prec 24 \prec 16 \prec 30 \prec 22 \prec 11$.

Conjecture 1. *The set $\mathcal{P}$ of positive integers is totally ordered by $\prec$.*

Say that m *precedes* n (or n *succeeds* m) if $m \prec n$ and there is no x with $m \prec x \prec n$.

Conjecture 2. $2 \cdot 3^i$ *precedes* 3^i *for* $i \geqslant 2$*. For* $i = 1$*, we have* $6 \prec 4 \prec 3$.

Proving $\Phi_m(q) < \Phi_n(q)$ for all q is the same as proving $\Phi_n(q) - \Phi_m(q) > 0$. After canceling any equal terms, this inequality can be written $A(q) > B(q)$ where $A(t)$ and $B(t)$ are integer polynomials whose nonzero coefficients are all positive. If the largest nonzero coefficient is c, then $A(q) > B(q)$ holds for all $q > c$ provided the leading monomial of A is greater than the corresponding monomial of B. (The base-q expansion of $A(q)$ is greater than $B(q)$.) The conjecture asserts that the inequality also holds for $2 \leqslant q \leqslant c$.

This reasoning will determine a putative total ordering of $\mathcal{P}$ working for sufficiently large q but maybe not for small q. I wrote a program in Magma that proved that the integers $\{1, 2, \ldots, 2 \cdot 10^4\}$ can be totally ordered. Since the coefficients of $\Phi_n(t)$ are unbounded as $n \to \infty$, and their maximum absolute value grows slowly, one might suspect that the conjecture is false and the smallest incomparable pair (m, n) is large. What is positive evidence?

Lemma 1. *If $m, n \in \mathcal{P}$ and $\phi(m) < \phi(n)$, then $m \prec n$.*

Proof. It follows from [1, Theorem 3.6] that $cq^{\phi(n)} < \Phi_n(q) < c^{-1}q^{\phi(n)}$ holds for all $q \geqslant 2$ where $c = 1 - q^{-1}$. Clearly $\frac{1}{2} \leqslant c$ and $c^{-1} \leqslant 2$. For $n \geqslant 3$ we know that $\phi(n)$ is even, so if $m, n \geqslant 3$, then $\phi(m) \leqslant \phi(n) - 2$. Therefore

$$\Phi_m(q) < c^{-1}q^{\phi(m)} \leqslant c^{-1}q^{\phi(n)-2} \leqslant cq^{\phi(n)} < \Phi_n(q).$$

The cases when $m < 3$ or $n < 3$ are easily handled. □

Thus it suffices to consider whether distinct $m, n \in \mathcal{P}$ with $\phi(m) = \phi(n)$ are comparable, i.e. $m \prec n$ or $n \prec m$. Clearly $\phi(m) = \phi(2m)$ if m is odd.

Lemma 2. *If $m \in \mathcal{P}$ is odd, then $m \prec 2m$ or $2m \prec m$.*

Proof. Let m_0 be the radical (square-free part) of m. If $\mu(m_0) = 1$, i.e. m_0 is a product of an even number of primes, then [1, Theorem 3.6] implies that

$$cq^{\phi(m)} < \Phi_m(q) < q^{\phi(m)} < \Phi_{2m}(q) < c^{-1}q^{\phi(m)}$$

where $c = 1 - q^{-1}$. Similar inequalities (with $m \leftrightarrow 2m$) hold if $\mu(m_0) = -1$, i.e. m_0 is a product of an odd number of primes. □

Remark 3. The sequence $1, 2, 6, 4, 3, 10, 12, 8, 5, 14, \ldots$ is A206225 in the OEIS. It tacitly assumes (without proof) that $\prec$ is a total ordering.

Remark 4. If $m \neq n$ and $\phi(m) = \phi(n)$, then $\Phi_m(t) - \Phi_n(t)$ is a power of t times a self-reciprocal polynomial. Hence $\Phi_m(t) - \Phi_n(t) > 0$ for $t \geqslant 2$ implies $\Phi_m(t) - \Phi_n(t) > 0$ for $0 < t \leqslant \frac{1}{2}$.

References

[1] Christoph Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order. II*, J. Algebra **93** (1985), no. 1, 151–164.

[2] Carl Pomerance and Simon Rubinstein-Salzedo, *Cyclotomic coincidences.* `https://www.math.dartmouth.edu/~carlp/`.