Cyclotomic Numerical Semigroups

Alexandru Ciolan

Max-Planck-Institut für Mathematik Bonn

Luxembourg Number Theory Seminar

University of Luxembourg, November 24, 2021

Joint work with:

Pedro García-Sánchez

Andrés Herrera-Poyatos

Pieter Moree

Overview

Preliminaries

- Cyclotomic numerical semigroups ... did not exist (!) until August 2013
- Term coined during a research internship at MPIM Bonn

  $\Rightarrow$ P. Moree, 2014: Numerical semigroups, cyclotomic polynomials, and Bernoulli numbers, *Amer. Math. Monthly*

  $\Rightarrow$ 2014: arXiv preprint $\Rightarrow$ ... (very!) long referee review ...

  $\Rightarrow$ 2016: published in *SIAM J. Discrete Math.*
- Conjecture (still unsolved!) $\Rightarrow$ lots of interest in the community

Preliminaries

Related references:

[1] P. Moree, Numerical semigroups, cyclotomic polynomials, and Bernoulli numbers, *Amer. Math. Monthly* **121** (2014).

[2] A. Ciolan, P. A. García-Sánchez, P. Moree, Cyclotomic numerical semigroups, *SIAM J. Discrete Math.* **30** (2016).

[3] O. M. Camburu, A. Ciolan, F. Luca, P. Moree, I. Shparlinski, Cyclotomic coefficients: Gaps and jumps, *J. Number Theory* **163** (2016).

[4] M. Sawhney, D. Stoner, On symmetric but not cyclotomic numerical semigroups, *SIAM J. Discrete Math.* **32** (2018).

[5] A. Borzì, A. Herrera-Poyatos, P. Moree, Cyclotomic numerical semigroup polynomials with at most two irreducible factors, *Semigroup Forum* **103** (2021).

[6] A. Herrera-Poyatos, P. Moree, Coefficients and higher order derivatives of cyclotomic polynomials: old and new, *Expo. Math.* **39** (2021).

[7] A. Ciolan, A. Herrera-Poyatos, P. A. García-Sánchez, P. Moree, Cyclotomic exponent sequences of numerical semigroups, `arxiv.org/abs/2101.08823`.

Preliminaries

So what are cyclotomic numerical semigroups?

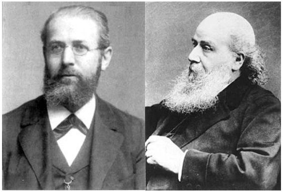
- A numerical semigroup S is a submonoid of $\mathbb{N}$ with finite complement
- Less abstract (but equivalent): given $a_1, \ldots, a_e \in \mathbb{N}^*$, the set

$$S = \langle a_1, \ldots, a_e \rangle = \{n_1 a_1 + \cdots + n_e a_e : n_i \in \mathbb{N}\}$$

  is a semigroup
- S numerical $\Leftrightarrow (a_1, \ldots, a_e) = 1$
- S contains all positive integers $> F(S) =$ the Frobenius number
- $S = \langle 3, 5 \rangle = \{0, 3, 5, 6, 8, 9, 10, \ldots\}, \quad F(S) = 7$
- $S = \langle 3, 6 \rangle = \{0, 3, 6, 9, 12, \ldots\}$ is not a numerical semigroup

Historical background

- 19th century: Frobenius and Sylvester



- Coin problem: largest amount that cannot be paid with given coins

  Example: $7 =$ largest amount that cannot be paid in coins of 3 and 5

  In other words: $S = \langle 3, 5 \rangle = \{0, 3, 5, 6, 8, 9, 10, \ldots\}, \quad F(S) = 7$

  Sylvester (1884): If $S = \langle a, b \rangle$, then $F(S) = (a-1)(b-1) - 1$

- Postage stamp problem

- Chicken McNuggets: largest non-McNugget number is 11
  (nugget boxes come in sizes of 4, 6, 9 and 20)

Numerical semigroups

$S = \langle 4, 7 \rangle = \langle 4, 7, 8 \rangle$
$= \{0, 1, 2, 3, \underline{4}, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, \underline{17}, 18, 19, 20, 21 \rightarrow\}$

- gaps of S : $1, 2, 3, 5, 6, 9, 10, 13, 17$
- number of gaps = genus of $S = 9$
- largest gap = Frobenius number $F(S) = 17$
- gapblocks: {1,2,3}, {5,6}, {9,10}, {13}, {17}
- elementblocks: {0}, {4}, {7,8}, {11,12}, {14,15,16}
- S admits a unique minimal generating system $\langle 4, 7 \rangle$
- embedding dimension = number of minimal generators, $e(S) = 2$
- multiplicity = smallest nonzero $s \in S$, $m(S) = 4$

Numerical semigroups

- Hilbert series of S : $H_S(x) = \sum_{s \in S} x^s$
- Semigroup polynomial of S : $P_S(x) = (1-x)H_S(x)$
- $\deg P_S = F(S) + 1$
- The non-zero coefficients of $P_S(x)$ alternate between 1 and -1
- If $P_S(x) = a_0 + a_1 x + \cdots + a_k x^k$, then, for $s \in \{0, \ldots, k\}$,

$$a_s = \begin{cases} 1 & \text{if } s \in S \text{ and } s-1 \notin S, \\ -1 & \text{if } s \notin S \text{ and } s-1 \in S, \\ 0 & \text{otherwise.} \end{cases}$$

- $P_S(1) = 1, \quad P'_S(1) = g(s)$

Cyclotomic polynomials

If $\zeta = e^{2\pi i/n}$, the n-th cyclotomic polynomial is given by

$$\Phi_n(x) = \prod_{(j,n)=1} (x - \zeta^j).$$

$\Phi_n \in \mathbb{Z}[x]$ is monic, irreducible and self-reciprocal for $n > 1$, $\deg \Phi_n = \varphi(n)$.

Over $\mathbb{Q}[x]$ we have

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

By Möbius inversion,

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

The n-th inverse cyclotomic polynomial is defined by

$$\Psi_n(x) = \prod_{(j,n)>1} (x - \zeta^j) = (x^n - 1)/\Phi_n(x).$$

Cyclotomic polynomials

- If $p \mid n$, then
$$\Phi_{pn}(x) = \Phi_n(x^p).$$
- If $p \nmid n$, then
$$\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x).$$
- If $n > 1$ is odd, then
$$\Phi_{2n}(x) = \Phi_n(-x).$$
- It is well-known that
$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1, \\ p & \text{if } n = p^m, \\ 1 & \text{otherwise.} \end{cases}$$

Cyclotomic numerical semigroups

Setting $n = pq$, we obtain

$$\Phi_n(x) = \frac{(1-x)(1-x^{pq})}{(1-x^p)(1-x^q)}.$$

Carlitz (1966), Moree (2014): If $S = \langle a, b \rangle$, then

$$P_S(x) = \frac{(1-x)(1-x^{ab})}{(1-x^a)(1-x^b)}.$$

Thus, if $S = \langle p, q \rangle$, then

$$P_S(x) = \Phi_{pq}(x).$$

Cyclotomic numerical semigroups

Definition 1

A numerical semigroup S is cyclotomic if all the roots of P_S lie on the unit circle. Alternatively but equivalently, S is cyclotomic if

$$P_S(x) = \prod_{d \in \mathcal{D}} \Phi_d^{h_d},$$

with $\mathcal{D}$ a finite set and h_d positive integers.

Cyclotomic coefficients

$\Phi_1(x) = x - 1,\ \Phi_2(x) = x + 1,\ \Phi_3(x) = x^2 + x + 1,$

$\Phi_4(x) = x^2 + 1,\ \Phi_5(x) = x^4 + x^3 + x^2 + x + 1,\ \Phi_6(x) = x^2 - x + 1,$

$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$

$\vdots$

$\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$

$\vdots$

- 19th century mathematicians thought coefficients are always 0 or ± 1.

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - \cdots - x^5 + x^2 + x + 1$$

- Schur in a letter to Landau sketched an argument showing that the coefficients are unbounded. His proof shows that every integer is assumed as a cyclotomic coefficient.

Motivation

- Connections between numerical semigroups and cyclotomic polynomials: from $\Phi_{pq}(x) = P_{\langle p,q\rangle}(x)$, one can study Φ_{pq} using numerical semigroups.
- Bachman, Bzdęga, Carlitz, Kaplan, Moree etc. studied the coefficients of cyclotomic polynomials and divisors of $x^n - 1$.
- In general, given a (product of) cyclotomic polynomial(s), it is hard to conclude anything about the coefficients.
- However, if a polynomial were of the form $P_S(x)$, then its non-zero coefficients would alternate between 1 and -1.

Motivation

Applications to:

- Algebraic Geometry: study of planar irreducible curves, Gorenstein rings; Diophantine modular inequalities $\Rightarrow$ proportionally modular semigroups
- Coding Theory: Feng-Rao distance, elliptic curve cryptography
- Topology: simplicial complexes, Euler characteristic, etc.
- Linear Integer Programming used to find factorizations

Goals:

- Bring Number Theory to an area treated from an algebraic point of view
- Find an intrinsic characterization of cyclotomic numerical semigroups (e.g., one that does not involve the roots of P_S)

Symmetric numerical semigroups

Definition 2

A numerical semigroup S is symmetric if $S \cup (F(S) - S) = \mathbb{Z}$.

- This does not involve the roots of P_S in any way.
- S symmetric $\Leftrightarrow F(S)$ is odd $\Leftrightarrow P_S$ is self-reciprocal.

Example 1

$S = \langle 3, 7 \rangle = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\}$ is symmetric: $F(S) = 11$

$S \cup (F(S) - S) = \{\ldots, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \ldots\}$

Example 2

$S = \langle 3, 4, 5 \rangle = \{0, 3, 4, 5, 6, 7, 8, \ldots\}$ is not symmetric: $F(S) = 2$

$S \cup (F(S) - S) = \{\ldots, -1, 0, 2, 3, 4, 5, 6, 7, \ldots\}$

Symmetric numerical semigroups

Theorem 1 (C.–García-Sánchez–Moree, 2016)

If S is cyclotomic, then S is symmetric.

Proof. Φ_n is self-reciprocal for $n > 1$.

We have $P_S(x) = 1 + (x-1)\sum_{s \notin S} x^s$.

Thus, $P_S(1) = 1$ and so $\Phi_1(x) = x - 1$ is not a factor of P_S. □

Non-cyclotomic symmetric numerical semigroups

The converse is false!

Example 3 ([4, 6])

If $k \geq 3$ then $S_k = \langle k, k+1, \ldots, 2k-2 \rangle = \{0, k, k+1, \ldots\} \setminus \{2k-1\}$ is symmetric, but not cyclotomic.

$$F(S_k) = 2k-1, \quad e(S_k) = k-1, \quad P_{S_k}(x) = 1 - x + x^k - x^{2k-1} + x^{2k}$$

Theorem 2 ([6])

a) For every $e \geq 4$ there is a symmetric numerical semigroup with embedding dimension e that is not cyclotomic.

b) For every $F \geq 9$ there is a symmetric numerical semigroup with Frobenius number F that is not cyclotomic.

A simple criterion

Criterion

If a numerical semigroup S satisfies

$$\sum_{s \notin S,\ 2 \nmid S} 1 < \sum_{s \notin S,\ 2 | S} 1, \qquad (\star)$$

then S is not cyclotomic.

Proof. Claim $(\star)$ is equivalent to $P_S(-1) < 0$, since we have

$$P_S(-1) = 1 + 2g(S) - 4 \sum_{s \notin S,\ 2 | s} 1.$$

We know that $\Phi_1(-1) = -2$, $\Phi_2(-1) = 0$ and, for $n > 2$,

$$\Phi_n(-1) = \begin{cases} p & \text{if } n = 2p^m, \\ 1 & \text{otherwise.} \end{cases}$$

If S were cyclotomic, then $P_S(-1) \geq 0$, a contradiction. □

An application to cryptography: Maximal gaps

The maximal gap of a polynomial

$$f(x) = a_1 x^{n_1} + \cdots + a_k x^{n_k} \in \mathbb{Z}[x]$$

with $a_i \neq 0$ and $n_1 < \ldots < n_k$ is defined by

$$g(f) = \max_{1 \leq i < k} (n_{i+1} - n_i).$$

Hong, Lee, Lee & Park (2012) initiated the study of $g(\Phi_n)$ and $g(\Psi_n)$ in an attempt to provide a simple and exact formula for the minimum Miller loop length arising in the Ate_i pairing from elliptic curve cryptography.

They reduced the problem to the case where n is square-free and odd.

Easy: $g(\Phi_p) = 1, \quad g(\Psi_p) = 1, \quad g(\Psi_{pq}) = q - p + 1.$

Simplest non-trivial case: $g(\Phi_{pq}) = p - 1, \quad$ with $2 < p < q$.

Gaps in Φ_{pq}

Theorem 3 (C., 2016)

If $p < q$, then

a) $g(\Phi_{pq}) = p - 1$ and the number of maximal gaps equals $2\lfloor q/p \rfloor$.

b) Φ_{pq} contains the sequence of consecutive coefficients $\pm 1, \underbrace{0, \dots, 0}_{m}, \mp 1$ for all $m = 0, 1, \dots, p-2 \Leftrightarrow q \equiv \pm 1 \pmod{p}$.

Remark: The number of Φ_n with $n = pq \le x$, $q \equiv \pm 1 \pmod{p}$, equals

$$C \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

with $C = \frac{1}{2} + \sum_{p \ge 3} \frac{2}{p(p-1)} = 1.043133380995902\dots$

Ingredients: Siegel-Walfisz, Brun-Titchmarsh etc.

Gaps in Φ_{pq}

Proof. b) Recall that if $P_S(x) = a_0 + a_1 x + \cdots + a_k x^k$, then

$$a_s = \begin{cases} 1 & \text{if } s \in S \text{ and } s-1 \notin S, \\ -1 & \text{if } s \notin S \text{ and } s-1 \in S, \\ 0 & \text{otherwise.} \end{cases}$$

If $S = \langle p, q \rangle$, then S is symmetric and $P_S = \Phi_{pq}$ is self-reciprocal.

$\pm 1, \underbrace{0, \ldots, 0}_{m}, \mp 1$ in $P_S \iff (m+1)$-gapblock/elementblock in S.

Equivalent claim: S has gapblocks of sizes $1, 2, \ldots, p-1 \Leftrightarrow q \equiv \pm 1 \pmod{p}$.

Gaps in Φ_{pq}

"$\Rightarrow$" Assume $q \equiv 1 \pmod{p}$ and write $q = pk + 1,\ k \geq 1$.

The intervals $I_m = [mpk, \ldots, mpk + p)$ are disjoint for $1 \leq m \leq p - 1$.

If $a, b \in \mathbb{N}$ are so that $mpk \leq ap + bq < mpk + p$, then $b \leq m$. Conversely, for any $0 \leq b \leq m$, there is a unique $a \in \mathbb{N}$ with $mpk \leq ap + bq < mpk + p$, since exactly one number from $\{ap + bq : a \in \mathbb{N}\}$ lands in I_m.

We can write any number $mpk + h = (m - h)kp + hq$, for $h = 0, 1, \ldots, m$, in the form $ap + bq$, with $0 \leq b \leq m$, but no other element of I_m.

Thus $I_m \cap S = [mpk, \ldots, mpk + m]$ and $\{mpk + m + 1, \ldots, mpk + p - 1\}$ is a $(p - m)$-gapblock of S, for $m = 1, 2, \ldots, p - 1$.

"$\Leftarrow$" If $q \not\equiv \pm 1 \pmod{p}$, then S has no $(p - 2)$-gapblock, contradiction! $\square$

Complete intersections

Another example of an intrinsic characterization: complete intersection.

If $S = \langle n_1, \ldots, n_e \rangle$, then $\varphi\colon \mathbb{N}^e \to S$, defined by $\varphi(a_1, \ldots, a_e) = \sum_{i=1}^{e} a_i n_i$, is an epimorphism, and $\ker\varphi = \{(a, b) \in \mathbb{N}^e \times \mathbb{N}^e \colon \varphi(a) = \varphi(b)\}$ is a congruence (an equivalence compatible with $+$).

As monoids, $S \cong \mathbb{N}^e / \ker\varphi$.

A presentation of S is a system of generators of $\ker\varphi$ as a congruence.

A presentation is minimal if none of its proper subsets generates $\ker\varphi$.

All minimal presentations have the same cardinality $\geq e(S) - 1$.

If equality holds, S is called a complete intersection.

A conjecture

Conjecture 1 (C.–García-Sánchez–Moree, 2016)

A numerical semigroup S is a complete intersection $\Leftrightarrow$ S is cyclotomic.

Remark: The statement was checked in `GAP` for all numerical semigroups S up to $F(S) = 69$ using the package `numericalsgps`.

Apéry sets

- If $m \in \mathbb{Z}$, then $\mathrm{Ap}(S;m) = \{s \in S : s - m \notin S\}$ is the Apéry set of m.
- If $m \in S$, then $|\mathrm{Ap}(S;m)| = m$ and $S = \mathrm{Ap}(S;m) + m\mathbb{N}$.
- Useful in computing $H_S(x)$:

$$H_S(x) = \sum_{w \in \mathrm{Ap}(S;m)} x^w \sum_{i=0}^{\infty} x^{mi} = \frac{1}{1-x^m} \sum_{w \in \mathrm{Ap}(S;m)} x^w.$$

Betti elements

For $s \in S$ let $\varphi^{-1}(s)$ be the set of factorizations of s in S.

$|\varphi^{-1}(s)| =$ denumerant of $s \in S$.

$\nabla_s =$ the graph with vertices in $\varphi^{-1}(s)$ and edges that join factorizations having minimal generators in common.

$s \in S$ is a Betti element if ∇_s is not connected.

The cardinality of any minimal presentation equals $\sum_{s \in \mathrm{Betti}(S)} (\mathrm{nc}(\nabla_s) - 1)$.

Gluings and Complete intersections

If S_1, S_2 are numerical semigroups and $a_1 \in S_2, a_2 \in S_1$ are coprime integers that are not minimal generators, then $S = a_1 S_1 + a_2 S_2$ is a numerical semigroup, called the gluing of S_1 and S_2. We write $S = a_1 S_1 +_{a_1 a_2} a_2 S_2$.

Delorme (1976): A complete intersection equals either $\mathbb{N}$ or the gluing of two complete intersections.

Assi et al. (2015): If $S = a_1 S_1 +_{a_1 a_2} a_2 S_2$, then

$$\mathrm{Betti}(S) = \{a_1 a_2\} \cup \{a_1 b_1 \colon b_1 \in \mathrm{Betti}(S_1)\} \cup \{a_2 b_2 \colon b_2 \in \mathrm{Betti}(S_2)\},$$

$$H_S(x) = (1 - x^{a_1 a_2}) H_{S_1}(x^{a_1}) H_{S_2}(x^{a_2}),$$

and

$$P_S(x) = \frac{(1-x)(1-x^{a_1 a_2})}{(1-x^{a_1})(1-x^{a_2})} P_{S_1}(x^{a_1}) P_{S_2}(x^{a_2}).$$

Gluings and Complete intersections

If $S = \langle n_1, \ldots, n_e \rangle$ is a complete intersection and

$$S = n_1\mathbb{N} +_{b_1} n_2\mathbb{N} + \cdots +_{b_{e-1}} n_e\mathbb{N},$$

then

$$H_S(x) = \frac{\prod_{i=1}^{e-1}(1 - x^{b_i})}{\prod_{i=1}^{e}(1 - x^{n_i})}.$$

S is a complete intersection $\Leftrightarrow$ H_S satisfies

$$H_S(x) = \frac{\prod_{b \in \mathrm{Betti}(S)}(1 - x^{b})^{\mathrm{nc}(\nabla_b)-1}}{\prod_{i=1}^{e}(1 - x^{n_i})}.$$

Depths and heights

Definition 3

A cyclotomic numerical semigroup S has depth d and height h if

$$P_S(x) \mid (x^d - 1)^h,$$

where both d and h are minimal; that is,

$$P_S(x) \nmid (x^n - 1)^{h-1} \text{ for any } n, \quad P_S(x) \nmid (x^{d_1} - 1)^h \text{ for any } d_1 < d.$$

Depths and heights

Remark: If $P_S = \prod_{i=1}^{n} \Phi_{d_i}^{h_i}$, then $d = \mathrm{lcm}(d_1, \ldots, d_n)$ and $h = \max\{h_1, \ldots, h_n\}$.

Example 4 (Binomial semigroups)

$$B_n(p,q) = \langle p^n, p^{n-1}q, \ldots, pq^{n-1}, q^n \rangle, \quad P_{B_n} = \prod_{\ell=2}^{n+1} \prod_{\substack{i+j=\ell \\ 1\le i,j\le \ell}} \Phi_{p^i q^j}.$$

Depth $d = p^{n+1}q^{n+1}$, height $h = 1$.

Depths and heights

Problem 1

Classify all cyclotomic numerical semigroups of a given depth and height.

Theorem 4 (C.–García-Sánchez–Moree, 2016)

If S is cyclotomic of depth $d = pqr$ and height $h = 1$, then $S = \langle pq, r \rangle$.

Theorem 5 (C.–García-Sánchez–Moree, 2016)

If S is cyclotomic of depth $d = p^n q$ and height $h = 1$, then $S = \langle p^n, q \rangle$.

Cyclotomic exponent sequences

Moree (2004):

Let $f(x) = 1 + a_1 x + \cdots + a_d x^d \in \mathbb{Z}[x]$ have roots $\alpha_1, \ldots, \alpha_d$.

If $s_f(k) = \alpha_1^{-k} + \cdots + \alpha_d^{-k} \in \mathbb{Z}$, then

$$s_f(k) + a_1 s_f(k-1) + \cdots + a_{k-1} s_f(1) + k a_k = 0,$$

with $a_m = 0$ for $m > d$.

Defining

$$e_f(k) = \frac{1}{k} \sum_{j \mid k} s_f(j) \mu\left(\frac{k}{j}\right) \in \mathbb{Z},$$

we have

$$f(x) = \prod_{k=1}^{\infty} (1 - x^k)^{e_f(k)}.$$

Cyclotomic exponent sequences

There exist unique integers e_j such that

$$P_S(x) = \prod_{j=1}^{\infty} (1 - x^j)^{e_j}.$$

$\mathbf{e} = \{e_j\}_{j \geq 1}$ is the cyclotomic exponent sequence of S.

Definition 4

A numerical semigroup S is cyclotomic if $\mathbf{e} = \{e_j\}_{j \geq 1}$ has finite support.

Cyclotomic exponent sequences

Problem 2

Relate the properties of S to its cyclotomic exponent sequence.

Theorem 6 (C.–García-Sánchez–Herrera-Poyatos–Moree, 2021)

If $S \neq \mathbb{N}$ is a numerical semigroup, then

a) $e_1 = 1$;

b) $e_j = 0$ for every $j \geq 2$ not in S;

c) $e_j = -1$ for every minimal generator j of S;

d) $e_j = 0$ for every $j \in S$ that has only one factorization and is not a minimal generator.

The conjecture revisited

Recall that if $S = \langle n_1, \dots, n_e \rangle$ is a complete intersection, then

$$P_S(x) = (1-x)H_S(x) = \frac{(1-x)\prod_{b \in \mathrm{Betti}(S)}(1-x^b)^{\mathrm{nc}(\nabla_b)-1}}{\prod_{i=1}^{e}(1-x^{n_i})}.$$

Theorem 7 (C.–García-Sánchez–Moree, 2016)

Every complete intersection numerical semigroup is cyclotomic.

If $e \leq 3$, every symmetric numerical semigroup is a complete intersection.

Theorem 8 (C.–García-Sánchez–Moree, 2016)

If $e \leq 3$, we have: complete intersection $\Leftrightarrow$ cyclotomic $\Leftrightarrow$ symmetric.

In general: $\{\text{complete intersection}\} \subseteq \{\text{cyclotomic}\} \subsetneq \{\text{symmetric}\}$

Some progress

length $\ell(S) = \#$ irreducible factors of P_S (with multiplicity)

Theorem 9 ([5])

Conjecture 1 is true if $\ell(S) \leq 2$.

If $\ell(S) = 1$, then $S = \langle p, q \rangle$ and $P_S = \Phi_{pq}$.

If $\ell(S) = 2$, then

a) $S = \langle p, q^2 \rangle$ and $P_S = \Phi_{pq}\Phi_{pq^2}$.

b) $S = \langle p, q^2, qr \rangle$ with $p \in \langle q, r \rangle$ and $P_S = \Phi_{pq}\Phi_{q^2 r}$.

Some progress

Theorem 10 (C.–García-Sánchez–Herrera-Poyatos–Moree, 2021)

For $a, b \in S$, write $a \leq_S b$ if $b - a \in S$. If the Hasse diagram of the set

$$\mathcal{E}(S) = \{d \geq 2 : e_d \neq 0,\ d \text{ is not a minimal generator of } S\}$$

with respect to $\leq_S$ is a forest, then S is cyclotomic. If, in addition, the Hasse diagram of $\mathrm{Betti}(S)$ is also a forest, then Conjecture 1 is true for S.

Remark: Computations suggest that such forests arise very frequently; for instance, there are 197 complete intersection numerical semigroups S with $F(S) = 101$, and for 170 of them the Hasse diagram of $\mathrm{Betti}(S)$ is a forest.

Further questions

Conjecture 2

Let S be a cyclotomic numerical semigroup and let $\mathbf{e}$ be its cyclotomic exponent sequence. Then $n \in \mathbb{N}$ is a minimal generator of $S \Leftrightarrow e_n < 0$.

Conjecture 3

Let S be a cyclotomic numerical semigroup and let $\mathbf{e}$ be its cyclotomic exponent sequence. Then $e_b = \mathrm{nc}(\nabla_b) - 1$ for all $b \in \mathrm{Betti}(S)$.

Conjecture 1 is true $\Leftrightarrow$ Conjectures 2 and 3 are true.

Thank you for your attention!