Cyclotomic Numerical Semigroups II –Polynomials playing pingpong–

Pieter Moree,
Max Planck Institute for Mathematics, Bonn

Levico Terme, July 7, 2016

Overview

1. The pingpong players: $P_S(x)$ and $\Phi_n(x)$
2. First match
   - Semigroup polynomial $P_{\langle p,q\rangle}(x)$
   - Binary cyclotomic polynomials
   - Exponent gaps
   - Gapblocks
3. Second match
   - General cyclotomic polynomials
   - Cyclotomic numerical semigroups
   - Symmetric non-cyclotomic numerical semigroups
   - Counting cyclotomic semigroups of given Frobenius number
4. Polynomially related numerical semigroups
   - An Application

Papers to be discussed

- E.-A. Ciolan, P.A. García-Sánchez and P. Moree, Cyclotomic numerical semigroups, *SIAM J. Discrete Math.* **30** (2016), 650–668
- Cyclotomic numerical semigroups. II, in preparation.
- Pedestrian: P. Moree, Numerical semigroups, cyclotomic polynomials and Bernoulli numbers, *Amer. Math. Monthly* **121** (2014), 890–902.
- O.-M. Camburu, E.-A. Ciolan, F. Luca, P. Moree and I.E. Shparlinski, Cyclotomic coefficients: gaps and jumps, *J. Number Theory*, **163** (2016), 211–237
- H. Hong, E. Lee, H.-S. Lee and C. Park, Maximum gap in (inverse) cyclotomic polynomial, *J. Number Theory* **132** (2012), 2297–2315
- P. Moree, Inverse cyclotomic polynomials, *J. Number Theory* **129** (2009), 667–680
- Some other results from older papers by the speaker (and Y. Gallot)

Semigroup polynomials

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

Semigroup polynomials

We have $H_S(x) = \sum_{s\in S} x^s = (1-x)^{-1} - \sum_{s\not\in S} x^s$. Hence

$$P_S(x) := (1-x)H_S(x) = 1 + (x-1)\sum_{s\not\in S} x^s.$$

Semigroup polynomials

We have $H_S(x) = \sum_{s \in S} x^s = (1-x)^{-1} - \sum_{s \notin S} x^s$. Hence

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

Observe that $P_S(x)$ is a monic polynomial of degree $F(S)+1$.

Semigroup polynomials

We have $H_S(x) = \sum_{s\in S} x^s = (1-x)^{-1} - \sum_{s\not\in S} x^s$. Hence

$$P_S(x) := (1-x)H_S(x) = 1 + (x-1)\sum_{s\not\in S} x^s.$$

Observe that $P_S(x)$ is a monic polynomial of degree $F(S)+1$.

Lemma

Write $P_S(x) = a_0 + a_1 x + \cdots + a_k x^k$.

Semigroup polynomials

We have $H_S(x) = \sum_{s\in S} x^s = (1-x)^{-1} - \sum_{s\not\in S} x^s$. Hence

$$P_S(x) := (1-x)H_S(x) = 1 + (x-1)\sum_{s\not\in S} x^s.$$

Observe that $P_S(x)$ is a monic polynomial of degree $F(S)+1$.

Lemma

Write $P_S(x) = a_0 + a_1 x + \cdots + a_k x^k$. Then, for $j \in \{0,\ldots,k\}$,

$$a_j = \begin{cases} 1 & \text{if } j \in S \text{ and } j-1 \not\in S; \\ -1 & \text{if } j \not\in S \text{ and } j-1 \in S; \\ 0 & \text{otherwise.} \end{cases}$$

Semigroup polynomials

We have $H_S(x) = \sum_{s\in S} x^s = (1-x)^{-1} - \sum_{s\notin S} x^s$. Hence

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

Observe that $P_S(x)$ is a monic polynomial of degree $F(S)+1$.

Lemma

Write $P_S(x) = a_0 + a_1 x + \cdots + a_k x^k$. Then, for $j \in \{0,\ldots,k\}$,

$$a_j = \begin{cases} 1 & \text{if } j \in S \text{ and } j-1 \notin S; \\ -1 & \text{if } j \notin S \text{ and } j-1 \in S; \\ 0 & \text{otherwise.} \end{cases}$$

Corollary

The nonzero coefficients of $P_S(x)$ alternate between 1 and -1.

Example

Example

0	1	2	3	4	5	6	7	8	9	10	...	...
1	0	0	1	0	1	1	0	1	1	1	...	1
1	-1	0	1	-1	1	0	-1	1	0	0	...	0

Example

0	1	2	3	4	5	6	7	8	9	10	...	...
1	0	0	1	0	1	1	0	1	1	1	...	1
1	-1	0	1	-1	1	0	-1	1	0	0	...	0

It follows that $P_{\langle 3,5\rangle}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$

Example

0	1	2	3	4	5	6	7	8	9	10	...	...
1	0	0	1	0	1	1	0	1	1	1	...	1
1	-1	0	1	-1	1	0	-1	1	0	0	...	0

It follows that $P_{\langle 3,5\rangle}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$
We have $\Phi_{15}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$

Example

0	1	2	3	4	5	6	7	8	9	10	...	...
1	0	0	1	0	1	1	0	1	1	1	...	1
1	-1	0	1	-1	1	0	-1	1	0	0	...	0

It follows that $P_{\langle 3,5\rangle}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$
We have $\Phi_{15}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$
The equality is no coincidence!

Example

0	1	2	3	4	5	6	7	8	9	10	...	...
1	0	0	1	0	1	1	0	1	1	1	...	1
1	-1	0	1	-1	1	0	-1	1	0	0	...	0

It follows that $P_{\langle 3,5\rangle}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$
We have $\Phi_{15}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$
The equality is no coincidence!

Lemma (Folklore)

$P_{\langle p,q\rangle}(x) = \Phi_{pq}(x)$.

Example

0	1	2	3	4	5	6	7	8	9	10	...	...
1	0	0	1	0	1	1	0	1	1	1	...	1
1	-1	0	1	-1	1	0	-1	1	0	0	...	0

It follows that $P_{\langle 3,5\rangle}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$
We have $\Phi_{15}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$
The equality is no coincidence!

Lemma (Folklore)

$P_{\langle p,q\rangle}(x) = \Phi_{pq}(x)$.

Corollary (Sylvester, 1884)

$F(\langle p, q\rangle) = \deg(\Phi_{pq}(X)) - 1 = (p-1)(q-1) - 1 = pq - p - q.$

Example

0	1	2	3	4	5	6	7	8	9	10	...	...
1	0	0	1	0	1	1	0	1	1	1	...	1
1	-1	0	1	-1	1	0	-1	1	0	0	...	0

It follows that $P_{\langle 3,5\rangle}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$
We have $\Phi_{15}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$
The equality is no coincidence!

Lemma (Folklore)

$P_{\langle p,q\rangle}(x) = \Phi_{pq}(x)$.

Corollary (Sylvester, 1884)

$F(\langle p, q\rangle) = \deg(\Phi_{pq}(X)) - 1 = (p-1)(q-1) - 1 = pq - p - q.$

Corollary (Migotti, 1887)

Coefficients of $\Phi_{pq}(x)$ *are in* $\{-1, 0, 1\}$.

Binary cyclotomic polynomials

Write $1+pq=\rho p+\sigma q,\ 0\le\rho\le q-1,\ 0\le\sigma\le p-1.$

Binary cyclotomic polynomials

Write $1+pq=\rho p+\sigma q,\ 0\le\rho\le q-1,\ 0\le\sigma\le p-1$.
Note that $\rho p\equiv 1 \pmod q$ and $\sigma q\equiv 1 \pmod p$.

Binary cyclotomic polynomials

Write $1 + pq = \rho p + \sigma q,\ 0 \leq \rho \leq q - 1,\ 0 \leq \sigma \leq p - 1.$
Note that $\rho p \equiv 1 \pmod{q}$ and $\sigma q \equiv 1 \pmod{p}$.
Thus ρ is the inverse of p modulo q, σ the inverse of q modulo p.

Binary cyclotomic polynomials

Write $1 + pq = \rho p + \sigma q,\ 0 \leq \rho \leq q - 1,\ 0 \leq \sigma \leq p - 1$.
Note that $\rho p \equiv 1 \pmod q$ and $\sigma q \equiv 1 \pmod p$.
Thus ρ is the inverse of p modulo q, σ the inverse of q modulo p.

$$\Phi_{pq}(X) = \sum_{m=0}^{\varphi(pq)} a_{pq}(m)x^m = \sum_{i=0}^{\rho-1} X^{ip} \sum_{j=0}^{\sigma-1} X^{jq} - X^{-pq} \sum_{i=\rho}^{q-1} X^{ip} \sum_{j=\sigma}^{p-1} X^{jq}$$

Binary cyclotomic polynomials

Write $1 + pq = \rho p + \sigma q,\ 0 \le \rho \le q - 1,\ 0 \le \sigma \le p - 1.$
Note that $\rho p \equiv 1 \pmod q$ and $\sigma q \equiv 1 \pmod p$.
Thus ρ is the inverse of p modulo q, σ the inverse of q modulo p.

$$\Phi_{pq}(X) = \sum_{m=0}^{\varphi(pq)} a_{pq}(m)x^m = \sum_{i=0}^{\rho-1} X^{ip} \sum_{j=0}^{\sigma-1} X^{jq} - X^{-pq} \sum_{i=\rho}^{q-1} X^{ip} \sum_{j=\sigma}^{p-1} X^{jq}$$

Lemma

$$a_{pq}(m) = \begin{cases} 1 & \textit{if } m = ip + jq \textit{ with } 0 \le i \le \rho - 1,\ 0 \le j \le \sigma - 1; \\ -1 & \textit{if } m = ip + jq - pq \textit{ with } \rho \le i \le q - 1,\ \sigma \le j \le p - 1; \\ 0 & \textit{otherwise.} \end{cases}$$

Gapblocks

Let $\theta(n)$ denote the number of non-zero cyclotomic coefficients in $\Phi_n(x)$.

Gapblocks

Let $\theta(n)$ denote the number of non-zero cyclotomic coefficients in $\Phi_n(x)$.

Lemma (Carlitz, 1966)

We have $\theta(pq) = 2\rho\sigma - 1$.

Gapblocks

Let $\theta(n)$ denote the number of non-zero cyclotomic coefficients in $\Phi_n(x)$.

Lemma (Carlitz, 1966)

We have $\theta(pq) = 2\rho\sigma - 1$.

Proof.

The number of non-zero coefficients is $\rho\sigma + (q-\rho)(p-\sigma) = 2\rho\sigma - 1$. □

Gapblocks

Let $\theta(n)$ denote the number of non-zero cyclotomic coefficients in $\Phi_n(x)$.

Lemma (Carlitz, 1966)

We have $\theta(pq) = 2\rho\sigma - 1$.

Proof.

The number of non-zero coefficients is $\rho\sigma + (q-\rho)(p-\sigma) = 2\rho\sigma - 1$. □

Corollary

The number of gapblocks in $\langle p, q\rangle$ *equals* $\rho\sigma - 1$.

Gapblocks

Let $\theta(n)$ denote the number of non-zero cyclotomic coefficients in $\Phi_n(x)$.

Lemma (Carlitz, 1966)

We have $\theta(pq) = 2\rho\sigma - 1$.

Proof.

The number of non-zero coefficients is $\rho\sigma + (q-\rho)(p-\sigma) = 2\rho\sigma - 1$. □

Corollary

The number of gapblocks in $\langle p, q\rangle$ *equals* $\rho\sigma - 1$.

0	1	2	3	4	5	6	7	8	9	10	...	...
1	1	1	1	2	1	1	3	1	1	1	...	1

$\rho = 3^{-1} \pmod 5 = 2$, $\sigma = 5^{-1} \pmod 3 = 2$,
$g(\langle p, q\rangle) = (p-1)(q-1)/2$

Sparse binary cyclotomic polynomials

Correspond to a NS having few (and hence large) gapblocks.

Sparse binary cyclotomic polynomials

Correspond to a NS having few (and hence large) gapblocks.
Put $H_\gamma(x) := \{m = pq \le x : \theta(m) \le m^{1/2+\gamma}\}$.

Sparse binary cyclotomic polynomials

Correspond to a NS having few (and hence large) gapblocks.
Put $H_\gamma(x) := \{m = pq \le x : \theta(m) \le m^{1/2+\gamma}\}$.
Bzdęga (2012) showed:

$$c(\epsilon,\gamma)x^{1/2+\gamma-\epsilon} \le H_\gamma(x) \le C(\gamma)x^{1/2+\gamma}.$$

Sparse binary cyclotomic polynomials

Correspond to a NS having few (and hence large) gapblocks.
Put $H_\gamma(x) := \{m = pq \le x : \theta(m) \le m^{1/2+\gamma}\}$.
Bzdęga (2012) showed:

$$c(\epsilon,\gamma)x^{1/2+\gamma-\epsilon} \le H_\gamma(x) \le C(\gamma)x^{1/2+\gamma}.$$

Fouvry (2013): For $\gamma \in (\frac{12}{25}, \frac{1}{2})$ we have

$$H_\gamma(x) \sim D(\gamma)\frac{x^{1/2+\gamma}}{\log x},$$

with $D(\gamma)$ an explicit constant.

Sparse binary cyclotomic polynomials

Correspond to a NS having few (and hence large) gapblocks.
Put $H_\gamma(x) := \{m = pq \le x : \theta(m) \le m^{1/2+\gamma}\}$.
Bzdęga (2012) showed:

$$c(\epsilon,\gamma)x^{1/2+\gamma-\epsilon} \le H_\gamma(x) \le C(\gamma)x^{1/2+\gamma}.$$

Fouvry (2013): For $\gamma \in (\frac{12}{25}, \frac{1}{2})$ we have

$$H_\gamma(x) \sim D(\gamma)\frac{x^{1/2+\gamma}}{\log x},$$

with $D(\gamma)$ an explicit constant.
-Bounds for Kloosterman-Ramanujan sums over primes

Sparse binary cyclotomic polynomials

Correspond to a NS having few (and hence large) gapblocks.
Put $H_\gamma(x) := \{m = pq \le x : \theta(m) \le m^{1/2+\gamma}\}$.
Bzdęga (2012) showed:

$$c(\epsilon,\gamma)x^{1/2+\gamma-\epsilon} \le H_\gamma(x) \le C(\gamma)x^{1/2+\gamma}.$$

Fouvry (2013): For $\gamma \in (\frac{12}{25}, \frac{1}{2})$ we have

$$H_\gamma(x) \sim D(\gamma)\frac{x^{1/2+\gamma}}{\log x},$$

with $D(\gamma)$ an explicit constant.
-Bounds for Kloosterman-Ramanujan sums over primes
-Bombieri-Vinogradov theorem

Sparse binary cyclotomic polynomials

Correspond to a NS having few (and hence large) gapblocks.
Put $H_\gamma(x) := \{m = pq \le x : \theta(m) \le m^{1/2+\gamma}\}$.
Bzdęga (2012) showed:

$$c(\epsilon,\gamma)x^{1/2+\gamma-\epsilon} \le H_\gamma(x) \le C(\gamma)x^{1/2+\gamma}.$$

Fouvry (2013): For $\gamma \in (\frac{12}{25}, \frac{1}{2})$ we have

$$H_\gamma(x) \sim D(\gamma)\frac{x^{1/2+\gamma}}{\log x},$$

with $D(\gamma)$ an explicit constant.
-Bounds for Kloosterman-Ramanujan sums over primes
-Bombieri-Vinogradov theorem
-Two-dimensional sieve

Sparse binary cyclotomic polynomials

Correspond to a NS having few (and hence large) gapblocks.
Put $H_\gamma(x) := \{m = pq \le x : \theta(m) \le m^{1/2+\gamma}\}$.
Bzdęga (2012) showed:

$$c(\epsilon,\gamma)x^{1/2+\gamma-\epsilon} \le H_\gamma(x) \le C(\gamma)x^{1/2+\gamma}.$$

Fouvry (2013): For $\gamma \in (\frac{12}{25}, \frac{1}{2})$ we have

$$H_\gamma(x) \sim D(\gamma)\frac{x^{1/2+\gamma}}{\log x},$$

with $D(\gamma)$ an explicit constant.
-Bounds for Kloosterman-Ramanujan sums over primes
-Bombieri-Vinogradov theorem
-Two-dimensional sieve
-Linnik's famous theorem concerning the least prime in AP

Exponent gaps after Hong et al.

We describe some work of Hong-Lee-Lee-Park (2012).

Exponent gaps after Hong et al.

We describe some work of Hong-Lee-Lee-Park (2012).

Definition (Maximum gap)

Given $f(x) = c_1x^{e_1} + \cdots + c_tx^{e_t} \in \mathbb{Z}[x]$, with $c_i \neq 0$ and $e_1 < \cdots < e_t$, we define the maximum gap of f as

$$g(f) = \max_{1 \le i < t}(e_{i+1} - e_i).$$

Exponent gaps after Hong et al.

We describe some work of Hong-Lee-Lee-Park (2012).

Definition (Maximum gap)

Given $f(x) = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{Z}[x]$, with $c_i \neq 0$ and $e_1 < \cdots < e_t$, we define the maximum gap of f as

$$g(f) = \max_{1 \leq i < t} (e_{i+1} - e_i).$$

- Initiated the study of $g(\Phi_n)$ and $g(\Psi_n)$ and reduced the study of these gaps to the case when n is square-free and odd.

Exponent gaps after Hong et al.

We describe some work of Hong-Lee-Lee-Park (2012).

Definition (Maximum gap)

Given $f(x) = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{Z}[x]$, with $c_i \neq 0$ and $e_1 < \cdots < e_t$, we define the maximum gap of f as

$$g(f) = \max_{1 \le i < t} (e_{i+1} - e_i).$$

- Initiated the study of $g(\Phi_n)$ and $g(\Psi_n)$ and reduced the study of these gaps to the case when n is square-free and odd.
- Simple and exact formula for the minimum Miller loop length in the Ate_i pairing arising in elliptic curve cryptography.

Exponent gaps after Hong et al.

We describe some work of Hong-Lee-Lee-Park (2012).

Definition (Maximum gap)

Given $f(x) = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{Z}[x]$, with $c_i \neq 0$ and $e_1 < \cdots < e_t$, we define the maximum gap of f as

$$g(f) = \max_{1 \le i < t} (e_{i+1} - e_i).$$

- Initiated the study of $g(\Phi_n)$ and $g(\Psi_n)$ and reduced the study of these gaps to the case when n is square-free and odd.
- Simple and exact formula for the minimum Miller loop length in the Ate_i pairing arising in elliptic curve cryptography.
- More manageable when turned into a problem involving the maximum gaps of inverse cyclotomic polynomials.

Inverse cyclotomic polynomials

Definition (Inverse cyclotomic polynomial)

$$\Psi_n(x) = \prod_{d|n,\ d<n} \Phi_d(x) = \frac{X^n - 1}{\Phi_n(X)} = \sum_{k=0}^{\infty} c_n(k) X^k.$$

Inverse cyclotomic polynomials

Definition (Inverse cyclotomic polynomial)

$$\Psi_n(x) = \prod_{d|n,\ d<n} \Phi_d(x) = \frac{X^n - 1}{\Phi_n(X)} = \sum_{k=0}^{\infty} c_n(k) X^k.$$

Put $B(n) = \max\{|c_n(k)|\ :\ k \geq 0\}$, $A(n) = \max\{|a_n(k)|\ :\ k \geq 0\}$

Inverse cyclotomic polynomials

Definition (Inverse cyclotomic polynomial)

$$\Psi_n(x) = \prod_{d|n,\ d<n} \Phi_d(x) = \frac{X^n - 1}{\Phi_n(X)} = \sum_{k=0}^{\infty} c_n(k) X^k.$$

Put $B(n) = \max\{|c_n(k)| \ : \ k \geq 0\}$, $A(n) = \max\{|a_n(k)| \ : \ k \geq 0\}$
We have $B(n) = 1$ for $n < 561$, in contrast $A(n) = 1$ for $n < 105$.

Inverse cyclotomic polynomials

Definition (Inverse cyclotomic polynomial)

$$\Psi_n(x) = \prod_{d|n,\ d<n} \Phi_d(x) = \frac{X^n - 1}{\Phi_n(X)} = \sum_{k=0}^{\infty} c_n(k) X^k.$$

Put $B(n) = \max\{|c_n(k)| \ : \ k \geq 0\}$, $A(n) = \max\{|a_n(k)| \ : \ k \geq 0\}$
We have $B(n) = 1$ for $n < 561$, in contrast $A(n) = 1$ for $n < 105$.

Theorem (Moree, JNTh, 2009)

We have $B(pqr) \leq p - 1$ and equality holds if and only if

$$q \equiv r \equiv \pm 1 \pmod p \text{ and } r < \frac{p-1}{p-2}(q-1)$$

Inverse cyclotomic polynomials

Definition (Inverse cyclotomic polynomial)

$$\Psi_n(x) = \prod_{d|n,\ d<n} \Phi_d(x) = \frac{X^n - 1}{\Phi_n(X)} = \sum_{k=0}^{\infty} c_n(k) X^k.$$

Put $B(n) = \max\{|c_n(k)| \ :\ k \geq 0\}$, $A(n) = \max\{|a_n(k)| \ :\ k \geq 0\}$
We have $B(n) = 1$ for $n < 561$, in contrast $A(n) = 1$ for $n < 105$.

Theorem (Moree, JNTh, 2009)

We have $B(pqr) \leq p - 1$ and equality holds if and only if

$$q \equiv r \equiv \pm 1 \pmod{p} \text{ and } r < \frac{p-1}{p-2}(q-1)$$

In contrast: $(2/3 - \epsilon)p \leq A(pqr) \leq 3p/4$.

Inverse cyclotomic polynomials

Definition (Inverse cyclotomic polynomial)

$$\Psi_n(x) = \prod_{d|n,\ d<n} \Phi_d(x) = \frac{X^n - 1}{\Phi_n(X)} = \sum_{k=0}^{\infty} c_n(k) X^k.$$

Put $B(n) = \max\{|c_n(k)| \ : \ k \geq 0\}$, $A(n) = \max\{|a_n(k)| \ : \ k \geq 0\}$
We have $B(n) = 1$ for $n < 561$, in contrast $A(n) = 1$ for $n < 105$.

Theorem (Moree, JNTh, 2009)

We have $B(pqr) \leq p - 1$ and equality holds if and only if

$$q \equiv r \equiv \pm 1 \pmod{p} \text{ and } r < \frac{p-1}{p-2}(q-1)$$

In contrast: $(2/3 - \epsilon)p \leq A(pqr) \leq 3p/4$.
Conjecturally $A(pqr) \leq 2p/3$.

Exponent gaps

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

Exponent gaps

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

Hong-Lee-Lee-Park

Exponent gaps

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

Hong-Lee-Lee-Park

Put $\mathcal{Q}_3 = \{n = pqr : \quad 2 < p < q < r \text{ primes}\}$ (ternary integers)

Exponent gaps

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

Hong-Lee-Lee-Park

Put $\mathcal{Q}_3 = \{n = pqr : \quad 2 < p < q < r \text{ primes}\}$ (ternary integers)

Put $\mathcal{R}_3 = \{n \in \mathcal{Q}_3 : \quad 4(p-1) > q, \quad p^2 > r\}$

Exponent gaps

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

Hong-Lee-Lee-Park

Put $\mathcal{Q}_3 = \{n = pqr : \quad 2 < p < q < r \text{ primes}\}$ (ternary integers)

Put $\mathcal{R}_3 = \{n \in \mathcal{Q}_3 : \quad 4(p-1) > q, \quad p^2 > r\}$

$$g(\Psi_n) = \frac{2n}{p} - \deg(\Psi_n) \text{ if } n \notin \mathcal{R}_3$$

Exponent gaps

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

Hong-Lee-Lee-Park

Put $\mathcal{Q}_3 = \{n = pqr : \quad 2 < p < q < r \text{ primes}\}$ (ternary integers)

Put $\mathcal{R}_3 = \{n \in \mathcal{Q}_3 : \quad 4(p-1) > q, \quad p^2 > r\}$

$$g(\Psi_n) = \frac{2n}{p} - \deg(\Psi_n) \text{ if } n \notin \mathcal{R}_3$$

Claimed without proof that $\mathcal{R}_3(x) = o(\mathcal{Q}_3(x))$,
where $\mathcal{R}_3(x) = \#\{n \in \mathcal{R}_3 : n \leq x\}$ and $\mathcal{Q}_3(x)$ is defined similarly.

Exponent gaps

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

Hong-Lee-Lee-Park

Put $\mathcal{Q}_3=\{n=pqr:\quad 2<p<q<r \text{ primes}\}$ (ternary integers)

Put $\mathcal{R}_3=\{n\in\mathcal{Q}_3:\quad 4(p-1)>q,\quad p^2>r\}$

$$g(\Psi_n)=\frac{2n}{p}-\deg(\Psi_n)\ \text{ if } n\notin\mathcal{R}_3$$

Claimed without proof that $\mathcal{R}_3(x)=o(\mathcal{Q}_3(x))$,

where $\mathcal{R}_3(x)=\#\{n\in\mathcal{R}_3:n\le x\}$ and $\mathcal{Q}_3(x)$ is defined similarly.

Camburu, Ciolan, Luca, M., Shparlinski

$$\mathcal{R}_3(x)=\frac{cx}{(\log x)^2}+O\left(\frac{x\log\log x}{(\log x)^3}\right),\ c=(1+\log 4)\log 4.$$

Exponent gaps

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

Hong-Lee-Lee-Park

Put $\mathcal{Q}_3=\{n=pqr:\quad 2<p<q<r \text{ primes}\}$ (ternary integers)

Put $\mathcal{R}_3=\{n\in\mathcal{Q}_3:\quad 4(p-1)>q,\quad p^2>r\}$

$$g(\Psi_n)=\frac{2n}{p}-\deg(\Psi_n)\ \text{ if } n\notin\mathcal{R}_3$$

Claimed without proof that $\mathcal{R}_3(x)=o(\mathcal{Q}_3(x))$,
where $\mathcal{R}_3(x)=\#\{n\in\mathcal{R}_3: n\le x\}$ and $\mathcal{Q}_3(x)$ is defined similarly.

Camburu, Ciolan, Luca, M., Shparlinski

$$\mathcal{R}_3(x)=\frac{cx}{(\log x)^2}+O\left(\frac{x\log\log x}{(\log x)^3}\right),\ c=(1+\log 4)\log 4.$$

Compare witht the classical estimate (Gauss, Landau)

$$\mathcal{Q}_3(x)=(1+o(1))\frac{x(\log\log x)^2}{2\log x}.$$

Gapblocks

Lemma

Let $p < q$ be primes. Then $g(\Phi_{pq}) = p - 1$.

Gapblocks

Lemma

Let $p < q$ be primes. Then $g(\Phi_{pq}) = p - 1$.

Proof.

Since $S = \langle p, q \rangle$ is symmetric, there is a one to one correspondence between k-gapblocks and k-elementblocks. We have that $g(\Phi_{pq})$ equals the largest gap block in S. Presence of $\langle p \rangle$ in $S = \langle p, q \rangle$ ensures that $g(\Phi_{pq}) \leq p - 1$. Since $S = \{1, p, \ldots\}$, we have $g(\Phi_{pq}) = p - 1$. □

Gapblocks

Lemma

Let $p < q$ be primes. Then $g(\Phi_{pq}) = p - 1$.

Proof.

Since $S = \langle p, q\rangle$ is symmetric, there is a one to one correspondence between k-gapblocks and k-elementblocks. We have that $g(\Phi_{pq})$ equals the largest gap block in S. Presence of $\langle p\rangle$ in $S = \langle p, q\rangle$ ensures that $g(\Phi_{pq}) \leq p - 1$. Since $S = \{1, p, \ldots\}$, we have $g(\Phi_{pq}) = p - 1$. □

Theorem

(i) $g(\Phi_{pq}) = p - 1$ *and the number of maximum gaps equals* $2[q/p]$;

Gapblocks

Lemma

Let $p < q$ be primes. Then $g(\Phi_{pq}) = p - 1$.

Proof.

Since $S = \langle p, q\rangle$ is symmetric, there is a one to one correspondence between k-gapblocks and k-elementblocks. We have that $g(\Phi_{pq})$ equals the largest gap block in S. Presence of $\langle p\rangle$ in $S = \langle p, q\rangle$ ensures that $g(\Phi_{pq}) \le p - 1$. Since $S = \{1, p, \ldots\}$, we have $g(\Phi_{pq}) = p - 1$. □

Theorem

(i) *$g(\Phi_{pq}) = p - 1$ and the number of maximum gaps equals $2[q/p]$;*

(ii) *Φ_{pq} contains the sequence of consecutive coefficients $\pm 1, \{0\}_m, \mp 1$ for all $m = 0, 1, \ldots, p-2$ iff $q \equiv \pm 1 \pmod{p}$.*

The notation $\{0\}_m$ indicates a string $\underbrace{0, \ldots, 0}_{m}$ of m consecutive zeros.

Gapblocks

Suppose $S = \langle a, b \rangle$ with a and b coprime.

Gapblocks

Suppose $S = \langle a, b \rangle$ with a and b coprime. In this case

$$P_S(x) = \frac{(1-x)(1-x^{ab})}{(1-x^a)(1-x^b)} = \prod_{d|ab,\ d\nmid a, d\nmid b} \Phi_d(x)$$

is an inclusion-exclusion polynomial (Bachman, 2010).

Theorem

Let $2 \leq a < b$ be coprime positive integers. Then

(i) *the maximum gap in*

$$\prod_{d|ab,\ d\nmid a, d\nmid b} \Phi_d(x)$$

equals $a-1$ and it occurs precisely $2\,[b/a]$ times;

Gapblocks

Suppose $S = \langle a, b \rangle$ with a and b coprime. In this case

$$P_S(x) = \frac{(1-x)(1-x^{ab})}{(1-x^a)(1-x^b)} = \prod_{d|ab,\ d\nmid a, d\nmid b} \Phi_d(x)$$

is an inclusion-exclusion polynomial (Bachman, 2010).

Theorem

Let $2 \le a < b$ be coprime positive integers. Then

(i) *the maximum gap in*

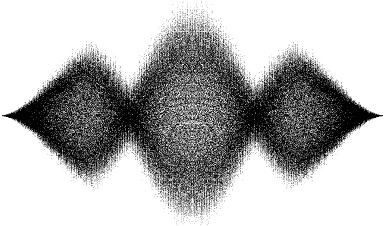
$$\prod_{d|ab,\ d\nmid a, d\nmid b} \Phi_d(x)$$

equals $a-1$ and it occurs precisely $2\,[b/a]$ times;

(ii) *the polynomial in* (i) *contains the sequence of consecutive coefficients $\pm 1, \{0\}_m, \mp 1$ for all $m = 0, 1, \ldots, a-2$ if and only if $b \equiv \pm 1 \pmod{a}$.*

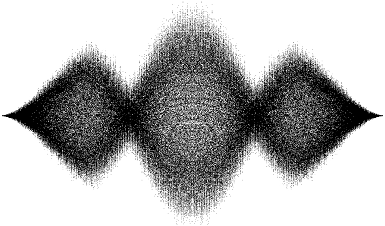
$\Phi_n(x)$ with more than two prime factors

$\Phi_n(x)$ with $n = 4849845 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

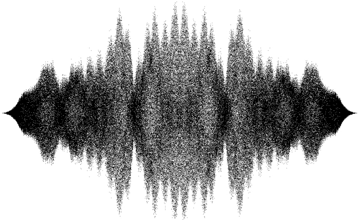


$\Phi_n(x)$ with more than two prime factors

$\Phi_n(x)$ with $n = 4849845 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$



$\Phi_n(x)$ with $n = 3234846615 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$



Calculation of $\Phi_n(1)$

Lemma (Value at 1)

$$\Phi_n(1) = \begin{cases} 0 & \textit{if } n = 1; \\ p & \textit{if } n = p^m; \\ 1 & \textit{otherwise.} \end{cases}$$

Calculation of $\Phi_n(1)$

Lemma (Value at 1)

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1; \\ p & \text{if } n = p^m; \\ 1 & \text{otherwise.} \end{cases}$$

We have

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

Calculation of $\Phi_n(1)$

Lemma (Value at 1)

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1; \\ p & \text{if } n = p^m; \\ 1 & \text{otherwise.} \end{cases}$$

We have

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

Thus $n = \prod_{d|n,\ d>1} \Phi_d(1)$.

Calculation of $\Phi_n(1)$

Lemma (Value at 1)

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1; \\ p & \text{if } n = p^m; \\ 1 & \text{otherwise.} \end{cases}$$

We have

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

Thus $n = \prod_{d|n,\ d>1} \Phi_d(1)$. We see that $p = \Phi_p(1)$.

Calculation of $\Phi_n(1)$

Lemma (Value at 1)

$$\Phi_n(1) = \begin{cases} 0 & \textit{if } n = 1; \\ p & \textit{if } n = p^m; \\ 1 & \textit{otherwise.} \end{cases}$$

We have

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

Thus $n = \prod_{d|n,\ d>1} \Phi_d(1)$. We see that $p = \Phi_p(1)$. Furthermore, $p^f = \Phi_p(1)\Phi_{p^2}(1)\cdots\Phi_{p^f}(1)$.

Calculation of $\Phi_n(1)$

Lemma (Value at 1)

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1; \\ p & \text{if } n = p^m; \\ 1 & \text{otherwise.} \end{cases}$$

We have

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

Thus $n = \prod_{d|n,\ d>1} \Phi_d(1)$. We see that $p = \Phi_p(1)$. Furthermore, $p^f = \Phi_p(1)\Phi_{p^2}(1)\cdots\Phi_{p^f}(1)$. Hence, by induction $\Phi_{p^f}(1) = p$.

Calculation of $\Phi_n(1)$

Lemma (Value at 1)

$$\Phi_n(1) = \begin{cases} 0 & \textit{if } n = 1; \\ p & \textit{if } n = p^m; \\ 1 & \textit{otherwise.} \end{cases}$$

We have

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

Thus $n = \prod_{d|n,\ d>1} \Phi_d(1)$. We see that $p = \Phi_p(1)$. Furthermore, $p^f = \Phi_p(1)\Phi_{p^2}(1) \cdots \Phi_{p^f}(1)$. Hence, by induction $\Phi_{p^f}(1) = p$. Next, note that

$$pq = \Phi_p(1)\Phi_q(1)\Phi_{pq}(1) = pq\Phi_{pq}(1).$$

Calculation of $\Phi_n(1)$

Lemma (Value at 1)

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1; \\ p & \text{if } n = p^m; \\ 1 & \text{otherwise.} \end{cases}$$

We have

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

Thus $n = \prod_{d|n,\ d>1} \Phi_d(1)$. We see that $p = \Phi_p(1)$. Furthermore, $p^f = \Phi_p(1)\Phi_{p^2}(1)\cdots\Phi_{p^f}(1)$. Hence, by induction $\Phi_{p^f}(1) = p$. Next, note that

$$pq = \Phi_p(1)\Phi_q(1)\Phi_{pq}(1) = pq\Phi_{pq}(1).$$

Hence, $\Phi_{pq}(1) = 1 = P_{\langle p,q\rangle}(1)$.

Calculation of $\Phi_n(1)$

Lemma (Value at 1)

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1; \\ p & \text{if } n = p^m; \\ 1 & \text{otherwise.} \end{cases}$$

We have

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

Thus $n = \prod_{d|n,\ d>1} \Phi_d(1)$. We see that $p = \Phi_p(1)$. Furthermore, $p^f = \Phi_p(1)\Phi_{p^2}(1)\cdots\Phi_{p^f}(1)$. Hence, by induction $\Phi_{p^f}(1) = p$. Next, note that

$$pq = \Phi_p(1)\Phi_q(1)\Phi_{pq}(1) = pq\Phi_{pq}(1).$$

Hence, $\Phi_{pq}(1) = 1 = P_{\langle p,q\rangle}(1)$. Now proceed with induction on the total number of prime factors.

Calculation of $\Phi_n(\pm 1)$

For $n > 1$, we have $\log(\Phi_n(1)) = \Lambda(n)$, with Λ the von Mangoldt function.

Calculation of $\Phi_n(\pm 1)$

For $n > 1$, we have $\log(\Phi_n(1)) = \Lambda(n)$, with Λ the von Mangoldt function. The Prime Number Theorem asserts that

$$\pi(x) := \sum_{p \le x} 1 \sim \frac{x}{\log x}, \text{ or equivalently } \sum_{n \le x} \Lambda(n) \sim x.$$

Calculation of $\Phi_n(\pm 1)$

For $n > 1$, we have $\log(\Phi_n(1)) = \Lambda(n)$, with Λ the von Mangoldt function. The Prime Number Theorem asserts that

$$\pi(x) := \sum_{p \le x} 1 \sim \frac{x}{\log x}, \text{ or equivalently } \sum_{n \le x} \Lambda(n) \sim x.$$

One also has $\prod_{1<n\le m} \Phi_n(1) = \mathrm{lcm}(1,\ldots,m)$.

Calculation of $\Phi_n(\pm 1)$

For $n > 1$, we have $\log(\Phi_n(1)) = \Lambda(n)$, with Λ the von Mangoldt function. The Prime Number Theorem asserts that

$$\pi(x) := \sum_{p \le x} 1 \sim \frac{x}{\log x}, \text{ or equivalently } \sum_{n \le x} \Lambda(n) \sim x.$$

One also has $\prod_{1<n\le m} \Phi_n(1) = \text{lcm}(1, \ldots, m)$.

Lemma (Value at -1)

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

Calculation of $\Phi_n(\pm 1)$

For $n > 1$, we have $\log(\Phi_n(1)) = \Lambda(n)$, with Λ the von Mangoldt function. The Prime Number Theorem asserts that

$$\pi(x) := \sum_{p \le x} 1 \sim \frac{x}{\log x}, \text{ or equivalently } \sum_{n \le x} \Lambda(n) \sim x.$$

One also has $\prod_{1<n\le m} \Phi_n(1) = \mathrm{lcm}(1, \ldots, m)$.

Lemma (Value at -1)

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

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{if } 2 \nmid n.$$

Calculation of $\Phi_n(\pm 1)$

For $n > 1$, we have $\log(\Phi_n(1)) = \Lambda(n)$, with Λ the von Mangoldt function. The Prime Number Theorem asserts that

$$\pi(x) := \sum_{p \le x} 1 \sim \frac{x}{\log x}, \text{ or equivalently } \sum_{n \le x} \Lambda(n) \sim x.$$

One also has $\prod_{1 < n \le m} \Phi_n(1) = \mathrm{lcm}(1, \ldots, m)$.

Lemma (Value at -1)

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

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{if } 2 \nmid n.$$

Calculation of $\Phi_n(\zeta)$ with ζ a general root of unity.

Calculation of $\Phi_n(\pm 1)$

For $n > 1$, we have $\log(\Phi_n(1)) = \Lambda(n)$, with Λ the von Mangoldt function. The Prime Number Theorem asserts that

$$\pi(x) := \sum_{p \le x} 1 \sim \frac{x}{\log x}, \text{ or equivalently } \sum_{n \le x} \Lambda(n) \sim x.$$

One also has $\prod_{1<n\le m} \Phi_n(1) = \mathrm{lcm}(1, \ldots, m)$.

Lemma (Value at -1)

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

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{if } 2 \nmid n.$$

Calculation of $\Phi_n(\zeta)$ with ζ a general root of unity.
Not much known. Work in progress.

Consequences for cyclotomic ns

As we have seen, if a NS is cyclotomic, then

$$P_S(x) = \prod_{d \in \mathcal{D}} \Phi_d(x)^{e_d}, \text{ with } e_d > 0 \text{ uniquely determined.}$$

Consequences for cyclotomic ns

As we have seen, if a NS is cyclotomic, then

$$P_S(x) = \prod_{d \in \mathcal{D}} \Phi_d(x)^{e_d}, \text{ with } e_d > 0 \text{ uniquely determined.}$$

Restrictions on the set $\mathcal{D}$?

Consequences for cyclotomic ns

As we have seen, if a NS is cyclotomic, then

$$P_S(x) = \prod_{d \in \mathcal{D}} \Phi_d(x)^{e_d}, \text{ with } e_d > 0 \text{ uniquely determined.}$$

Restrictions on the set $\mathcal{D}$?

Lemma (Cyclotomic restriction)

The set $\mathcal{D}$ does not contain 1 or prime powers.

Consequences for cyclotomic ns

As we have seen, if a NS is cyclotomic, then

$$P_S(x) = \prod_{d \in \mathcal{D}} \Phi_d(x)^{e_d}, \text{ with } e_d > 0 \text{ uniquely determined.}$$

Restrictions on the set $\mathcal{D}$?

Lemma (Cyclotomic restriction)

The set $\mathcal{D}$ does not contain 1 or prime powers.

Proof.

Since $P_S(1) = 1$ and $\Phi_1(x) = x - 1$ we infer that $e_1 = 0$.

Consequences for cyclotomic ns

As we have seen, if a NS is cyclotomic, then

$$P_S(x) = \prod_{d \in \mathcal{D}} \Phi_d(x)^{e_d}, \text{ with } e_d > 0 \text{ uniquely determined.}$$

Restrictions on the set $\mathcal{D}$?

Lemma (Cyclotomic restriction)

The set $\mathcal{D}$ does not contain 1 or prime powers.

Proof.

Since $P_S(1) = 1$ and $\Phi_1(x) = x - 1$ we infer that $e_1 = 0$. Let p^m be a prime power in $\mathcal{D}$. Then by the value at 1 lemma we have $p | \Phi_{p^m}(1) | P_S(1)$. Contradiction. □

Semigroup Polynomials

Lemma (Connection with genus)

Let $S \neq \mathbb{N}$ *be a numerical semigroup. Then* $P_S'(1) = g(S)$.

Semigroup Polynomials

Lemma (Connection with genus)

Let $S \neq \mathbb{N}$ be a numerical semigroup. Then $P'_S(1) = g(S)$.

Proof.

There exist $2 \leq k_1 < \cdots < k_{2n+1}$ such that

$$P_S(x) = 1 - x + x^{k_1} - x^{k_2} + \cdots - x^{k_{2n}} + x^{k_{2n+1}}.$$

Semigroup Polynomials

Lemma (Connection with genus)

Let $S \neq \mathbb{N}$ *be a numerical semigroup. Then* $P'_S(1) = g(S)$.

Proof.

There exist $2 \leq k_1 < \cdots < k_{2n+1}$ such that

$$P_S(x) = 1 - x + x^{k_1} - x^{k_2} + \cdots - x^{k_{2n}} + x^{k_{2n+1}}.$$

In fact, $k_1 = m(S) > 1$ and $k_{2n+1} = F(S) + 1$.

Semigroup Polynomials

Lemma (Connection with genus)

Let $S \neq \mathbb{N}$ be a numerical semigroup. Then $P'_S(1) = g(S)$.

Proof.

There exist $2 \leq k_1 < \cdots < k_{2n+1}$ such that

$$P_S(x) = 1 - x + x^{k_1} - x^{k_2} + \cdots - x^{k_{2n}} + x^{k_{2n+1}}.$$

In fact, $k_1 = m(S) > 1$ and $k_{2n+1} = F(S) + 1$. Gapblock correspondence:

$$\mathbb{N} \backslash S = [1, k_1 - 1] \cup [k_2, k_3 - 1] \cup \ldots \cup [k_{2n}, k_{2n+1} - 1] \quad (1)$$

$$P'_S(x) = (-1 + k_1 x^{k_1 - 1}) + \cdots + (-k_{2n} x^{k_{2n} - 1} + k_{2n+1} x^{k_{2n+1} - 1})$$

$$P'_S(1) = (k_1 - 1) + (k_3 - k_2) + \cdots + (k_{2n+1} - k_{2n}). \quad (2)$$

Semigroup Polynomials

Lemma (Connection with genus)

Let $S \neq \mathbb{N}$ be a numerical semigroup. Then $P'_S(1) = g(S)$.

Proof.

There exist $2 \leq k_1 < \cdots < k_{2n+1}$ such that

$$P_S(x) = 1 - x + x^{k_1} - x^{k_2} + \cdots - x^{k_{2n}} + x^{k_{2n+1}}.$$

In fact, $k_1 = m(S) > 1$ and $k_{2n+1} = F(S) + 1$. Gapblock correspondence:

$$\mathbb{N} \backslash S = [1, k_1 - 1] \cup [k_2, k_3 - 1] \cup \ldots \cup [k_{2n}, k_{2n+1} - 1] \qquad (1)$$

$$P'_S(x) = (-1 + k_1 x^{k_1 - 1}) + \cdots + (-k_{2n} x^{k_{2n} - 1} + k_{2n+1} x^{k_{2n+1} - 1})$$

$$P'_S(1) = (k_1 - 1) + (k_3 - k_2) + \cdots + (k_{2n+1} - k_{2n}). \qquad (2)$$

The conclusion now follows on comparing (1) and (2). □

Semigroup Polynomials

Lemma

Let S be a cyclotomic numerical semigroup and $p > 2$ a prime. Then

$$p \mid P_S(-1) \Leftrightarrow \Phi_{2p^k}(x) \mid P_S(x)$$

for some $k \geq 1$.

Semigroup Polynomials

Lemma

Let S be a cyclotomic numerical semigroup and $p > 2$ a prime. Then

$$p \mid P_S(-1) \Leftrightarrow \Phi_{2p^k}(x) \mid P_S(x)$$

for some $k \geq 1$.

Proof.

"$\Leftarrow$". The assumption $\Phi_{2p^k}(x) \mid P_S(x)$ implies that $\Phi_{2p^k}(-1) \mid P_S(-1)$. Now invoke the Lemma "Value at -1".

Semigroup Polynomials

Lemma

Let S be a cyclotomic numerical semigroup and $p > 2$ a prime. Then

$$p \mid P_S(-1) \Leftrightarrow \Phi_{2p^k}(x) \mid P_S(x)$$

for some $k \geq 1$.

Proof.

"$\Leftarrow$". The assumption $\Phi_{2p^k}(x) \mid P_S(x)$ implies that $\Phi_{2p^k}(-1) \mid P_S(-1)$.
Now invoke the Lemma "Value at -1".
"$\Rightarrow$". We must have $p \mid \Phi_n(-1)$ for some n and $\Phi_n(x) \mid P_S(x)$.

Semigroup Polynomials

Lemma

Let S be a cyclotomic numerical semigroup and $p > 2$ a prime. Then

$$p \mid P_S(-1) \Leftrightarrow \Phi_{2p^k}(x) \mid P_S(x)$$

for some $k \geq 1$.

Proof.

"$\Leftarrow$". The assumption $\Phi_{2p^k}(x) \mid P_S(x)$ implies that $\Phi_{2p^k}(-1) \mid P_S(-1)$. Now invoke the Lemma "Value at -1".

"$\Rightarrow$". We must have $p \mid \Phi_n(-1)$ for some n and $\Phi_n(x) \mid P_S(x)$. By the Lemma "Cyclotomic restriction" we must have $n > 2$ (in fact $n \geq 6$) and n is not a power of two.

Semigroup Polynomials

Lemma

Let S be a cyclotomic numerical semigroup and $p > 2$ a prime. Then

$$p \mid P_S(-1) \Leftrightarrow \Phi_{2p^k}(x) \mid P_S(x)$$

for some $k \geq 1$.

Proof.

"$\Leftarrow$". The assumption $\Phi_{2p^k}(x) \mid P_S(x)$ implies that $\Phi_{2p^k}(-1) \mid P_S(-1)$. Now invoke the Lemma "Value at -1".
"$\Rightarrow$". We must have $p \mid \Phi_n(-1)$ for some n and $\Phi_n(x) \mid P_S(x)$. By the Lemma "Cyclotomic restriction" we must have $n > 2$ (in fact $n \geq 6$) and n is not a power of two. By the Lemma "Value at -1" it now follows that $n = 2p^k$ for some $k \geq 1$. □

Semigroup Polynomials

Lemma

Let S be a cyclotomic numerical semigroup and $p > 2$ a prime. Then

$$p \mid P_S(-1) \Leftrightarrow \Phi_{2p^k}(x) \mid P_S(x)$$

for some $k \geq 1$.

Proof.

"$\Leftarrow$". The assumption $\Phi_{2p^k}(x) \mid P_S(x)$ implies that $\Phi_{2p^k}(-1) \mid P_S(-1)$. Now invoke the Lemma "Value at -1".
"$\Rightarrow$". We must have $p \mid \Phi_n(-1)$ for some n and $\Phi_n(x) \mid P_S(x)$. By the Lemma "Cyclotomic restriction" we must have $n > 2$ (in fact $n \geq 6$) and n is not a power of two. By the Lemma "Value at -1" it now follows that $n = 2p^k$ for some $k \geq 1$. □

Example. Take $S = \langle 6, 9, 11 \rangle$.

Semigroup Polynomials

Lemma

Let S be a cyclotomic numerical semigroup and $p > 2$ a prime. Then

$$p \mid P_S(-1) \Leftrightarrow \Phi_{2p^k}(x) \mid P_S(x)$$

for some $k \geq 1$.

Proof.

"$\Leftarrow$". The assumption $\Phi_{2p^k}(x) \mid P_S(x)$ implies that $\Phi_{2p^k}(-1) \mid P_S(-1)$. Now invoke the Lemma "Value at -1".

"$\Rightarrow$". We must have $p \mid \Phi_n(-1)$ for some n and $\Phi_n(x) \mid P_S(x)$. By the Lemma "Cyclotomic restriction" we must have $n > 2$ (in fact $n \geq 6$) and n is not a power of two. By the Lemma "Value at -1" it now follows that $n = 2p^k$ for some $k \geq 1$. □

Example. Take $S = \langle 6, 9, 11 \rangle$. Then $P_S(-1) = 3$ and $P_S = \Phi_{18}\Phi_{33}$.

Even beats odd

We let $\mathfrak{g}(a,d) := \#\{g \notin S : g \geq 0,\ g \equiv a \pmod{d}\}$.

Even beats odd

We let $\mathfrak{g}(a,d) := \#\{g \notin S : g \geq 0,\ g \equiv a \pmod d\}$. We have

$$\begin{aligned} P_S(-1) &= 1 - 2\sum_{s \notin S}(-1)^s = 1 - 2(\mathfrak{g}(0,2) - \mathfrak{g}(1,2)) \\ &= 1 - 2\mathfrak{g}(0,2) + 2\mathfrak{g}(1,2) = 1 + 2g(S) - 4\mathfrak{g}(0,2), \end{aligned}$$

Even beats odd

We let $\mathfrak{g}(a,d) := \#\{g \notin S : g \geq 0,\ g \equiv a \pmod{d}\}$. We have

$$\begin{aligned} P_S(-1) &= 1 - 2\sum_{s \notin S}(-1)^s = 1 - 2(\mathfrak{g}(0,2) - \mathfrak{g}(1,2)) \\ &= 1 - 2\mathfrak{g}(0,2) + 2\mathfrak{g}(1,2) = 1 + 2g(S) - 4\mathfrak{g}(0,2), \end{aligned}$$

where $g(S) = \mathfrak{g}(0,2) + \mathfrak{g}(1,2) =$ genus of S

Even beats odd

We let $\mathfrak{g}(a,d) := \#\{g \notin S : g \geq 0,\ g \equiv a \pmod{d}\}$. We have

$$\begin{aligned} P_S(-1) &= 1 - 2\sum_{s \notin S}(-1)^s = 1 - 2(\mathfrak{g}(0,2) - \mathfrak{g}(1,2)) \\ &= 1 - 2\mathfrak{g}(0,2) + 2\mathfrak{g}(1,2) = 1 + 2g(S) - 4\mathfrak{g}(0,2), \end{aligned}$$

where $g(S) = \mathfrak{g}(0,2) + \mathfrak{g}(1,2) =$ genus of S

Lemma (Even beats odd)

If $\mathfrak{g}(1,2) < \mathfrak{g}(0,2)$, then S is not cyclotomic.

Even beats odd

We let $\mathfrak{g}(a,d) := \#\{g \notin S : g \geq 0,\ g \equiv a \pmod{d}\}$. We have

$$\begin{aligned} P_S(-1) &= 1 - 2\sum_{s \notin S}(-1)^s = 1 - 2(\mathfrak{g}(0,2) - \mathfrak{g}(1,2)) \\ &= 1 - 2\mathfrak{g}(0,2) + 2\mathfrak{g}(1,2) = 1 + 2g(S) - 4\mathfrak{g}(0,2), \end{aligned}$$

where $g(S) = \mathfrak{g}(0,2) + \mathfrak{g}(1,2) =$ genus of S

Lemma (Even beats odd)

If $\mathfrak{g}(1,2) < \mathfrak{g}(0,2)$, then S is not cyclotomic.

Proof.

This inequality is equivalent with $P_S(-1) < 0$. If S were cyclotomic, then by the value at -1 lemma always $\Phi_n(-1) \geq 0$ and hence $P_S(-1) \geq 0$.

Even beats odd

We let $\mathfrak{g}(a,d) := \#\{g \notin S : g \geq 0,\ g \equiv a \pmod{d}\}$. We have

$$\begin{aligned} P_S(-1) &= 1 - 2\sum_{s \notin S}(-1)^s = 1 - 2(\mathfrak{g}(0,2) - \mathfrak{g}(1,2)) \\ &= 1 - 2\mathfrak{g}(0,2) + 2\mathfrak{g}(1,2) = 1 + 2g(S) - 4\mathfrak{g}(0,2), \end{aligned}$$

where $g(S) = \mathfrak{g}(0,2) + \mathfrak{g}(1,2) =$ genus of S

Lemma (Even beats odd)

If $\mathfrak{g}(1,2) < \mathfrak{g}(0,2)$, then S is not cyclotomic.

Proof.

This inequality is equivalent with $P_S(-1) < 0$. If S were cyclotomic, then by the value at -1 lemma always $\Phi_n(-1) \geq 0$ and hence $P_S(-1) \geq 0$. This contradiction finishes the proof. □

Even beats odd in practice

Is the criterion actually of any practical use?

Even beats odd in practice

Is the criterion actually of any practical use?

YES. Suprisingly so!

Even beats odd in practice

Is the criterion actually of any practical use?

YES. Suprisingly so!

- For $S = \langle 3, 5 \rangle$ we have $G = \{1, 2, 4, 7\}$ and so $\mathfrak{g}(0, 2) = \mathfrak{g}(1, 2) = 2$

Even beats odd in practice

Is the criterion actually of any practical use?

YES. Suprisingly so!

- For $S = \langle 3, 5\rangle$ we have $G = \{1, 2, 4, 7\}$ and so $\mathfrak{g}(0, 2) = \mathfrak{g}(1, 2) = 2$
- $S = \langle 3, 5, 7\rangle$. We have $\mathfrak{g}(0, 2) = 2$ and $\mathfrak{g}(1, 2) = 1$ and so S is not cyclotomic.

Even beats odd in practice

Is the criterion actually of any practical use?

YES. Suprisingly so!

- For $S = \langle 3, 5 \rangle$ we have $G = \{1, 2, 4, 7\}$ and so $\mathfrak{g}(0, 2) = \mathfrak{g}(1, 2) = 2$
- $S = \langle 3, 5, 7 \rangle$. We have $\mathfrak{g}(0, 2) = 2$ and $\mathfrak{g}(1, 2) = 1$ and so S is not cyclotomic.
- $S = \langle 5, 6, 7, 8 \rangle$ is not cyclotomic. We have $\mathfrak{g}(0, 2) = 2$ and $\mathfrak{g}(1, 2) = 3$. Thus Lemma "Even beats odd" is not if and only if.

Even beats odd in practice

Is the criterion actually of any practical use?

YES. Suprisingly so!

- For $S = \langle 3, 5 \rangle$ we have $G = \{1, 2, 4, 7\}$ and so $\mathfrak{g}(0, 2) = \mathfrak{g}(1, 2) = 2$
- $S = \langle 3, 5, 7 \rangle$. We have $\mathfrak{g}(0, 2) = 2$ and $\mathfrak{g}(1, 2) = 1$ and so S is not cyclotomic.
- $S = \langle 5, 6, 7, 8 \rangle$ is not cyclotomic. We have $\mathfrak{g}(0, 2) = 2$ and $\mathfrak{g}(1, 2) = 3$. Thus Lemma "Even beats odd" is not if and only if.
- We took all numerical semigroups S that are symmetric and not complete intersection with $F(S) \le k$ and determined how often on average Lemma "Even beats odd" applies. Our computations (with $k \le 69$) indicate that likely an average exists and is in $[0.8, 0.85]$.

$P_S(\zeta)$

Let $\zeta = \zeta_m$ be a primitive m-th root of unity.

$P_S(\zeta)$

Let $\zeta = \zeta_m$ be a primitive m-th root of unity. We have

$$P_S(\zeta) = 1 + \sum_{0 \le a \le m-1} (\mathfrak{g}(a-1,m) - \mathfrak{g}(a,m))\zeta_m^a$$

$P_S(\zeta)$

Let $\zeta = \zeta_m$ be a primitive m-th root of unity. We have

$$P_S(\zeta) = 1 + \sum_{0 \le a \le m-1} (\mathfrak{g}(a-1,m) - \mathfrak{g}(a,m))\zeta_m^a$$

We have $P_S(\zeta) \in \mathbb{Z}[\zeta]$, the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta) \cong \mathbb{Q}[x]/(\Phi_m(x))$, which is of degree $\varphi(m)$.

$P_S(\zeta)$

Let $\zeta = \zeta_m$ be a primitive m-th root of unity. We have

$$P_S(\zeta) = 1 + \sum_{0 \le a \le m-1} (\mathfrak{g}(a-1, m) - \mathfrak{g}(a, m))\zeta_m^a$$

We have $P_S(\zeta) \in \mathbb{Z}[\zeta]$, the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta) \cong \mathbb{Q}[x]/(\Phi_m(x))$, which is of degree $\varphi(m)$.

Theorem

If $P_S(-1) \equiv 1 \pmod 4$ and $P_S(i)$ is not a real number, then S is not cyclotomic.

$P_S(\zeta)$

Let $\zeta = \zeta_m$ be a primitive m-th root of unity. We have

$$P_S(\zeta) = 1 + \sum_{0 \le a \le m-1} (\mathfrak{g}(a-1, m) - \mathfrak{g}(a, m))\zeta_m^a$$

We have $P_S(\zeta) \in \mathbb{Z}[\zeta]$, the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta) \cong \mathbb{Q}[x]/(\Phi_m(x))$, which is of degree $\varphi(m)$.

Theorem

If $P_S(-1) \equiv 1 \pmod 4$ and $P_S(i)$ is not a real number, then S is not cyclotomic.

Work in progress...

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Theorem

If $e(S) \leq 3$, then S is cyclotomic iff S is symmetric.

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Theorem

If $e(S) \leq 3$, then S is cyclotomic iff S is symmetric.

Question

What about $e(S) \geq 4$?

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Theorem

If $e(S) \leq 3$, then S is cyclotomic iff S is symmetric.

Question

What about $e(S) \geq 4$?

For $k \geq 5$ put $S_k = \{0, k, k+1, \ldots, 2k-2, 2k, \rightarrow\}$.

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Theorem

If $e(S) \leq 3$, then S is cyclotomic iff S is symmetric.

Question

What about $e(S) \geq 4$?

For $k \geq 5$ put $S_k = \{0, k, k+1, \ldots, 2k-2, 2k, \rightarrow\}$. Note that

$$P_{S_k}(x) = 1 - x + x^k - x^{2k-1} + x^{2k}.$$

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Theorem

If $e(S) \leq 3$, then S is cyclotomic iff S is symmetric.

Question

What about $e(S) \geq 4$?

For $k \geq 5$ put $S_k = \{0, k, k+1, \ldots, 2k-2, 2k, \rightarrow\}$. Note that

$$P_{S_k}(x) = 1 - x + x^k - x^{2k-1} + x^{2k}.$$

Thus S_k is a symmetric ns with $F(S) = 2k - 1$.

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Theorem

If $e(S) \leq 3$, then S is cyclotomic iff S is symmetric.

Question

What about $e(S) \geq 4$?

For $k \geq 5$ put $S_k = \{0, k, k+1, \ldots, 2k-2, 2k, \rightarrow\}$. Note that

$$P_{S_k}(x) = 1 - x + x^k - x^{2k-1} + x^{2k}.$$

Thus S_k is a symmetric ns with $F(S) = 2k-1$.
We have $S_k = \langle k, k+1, \ldots, 2k-2 \rangle$ and $e(S_k) = k-1$.

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Theorem

If $e(S) \leq 3$, then S is cyclotomic iff S is symmetric.

Question

What about $e(S) \geq 4$?

For $k \geq 5$ put $S_k = \{0, k, k+1, \ldots, 2k-2, 2k, \rightarrow\}$. Note that

$$P_{S_k}(x) = 1 - x + x^k - x^{2k-1} + x^{2k}.$$

Thus S_k is a symmetric ns with $F(S) = 2k - 1$.
We have $S_k = \langle k, k+1, \ldots, 2k-2 \rangle$ and $e(S_k) = k - 1$.

Example

$S = \langle 5, 6, 7, 8 \rangle$, with $F(S) = 9$ is the symmetric ns with the smallest Frobenius number that is not cyclotomic.

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Conjecture

Put $P_{S_k}(x) = 1 - x + x^k - x^{2k-1} + x^{2k}$. For every $k \geq 5$ this polynomial has a root not on the unit circle.

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Conjecture

Put $P_{S_k}(x) = 1 - x + x^k - x^{2k-1} + x^{2k}$. For every $k \geq 5$ this polynomial has a root not on the unit circle.

Corollary

For every $k \geq 5$ the symmetric ns S_k is non-cyclotomic and has embedding dimension $e(S_k) = k - 1 \geq 4$.

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Conjecture

Put $P_{S_k}(x) = 1 - x + x^k - x^{2k-1} + x^{2k}$. For every $k \geq 5$ this polynomial has a root not on the unit circle.

Corollary

For every $k \geq 5$ the symmetric ns S_k is non-cyclotomic and has embedding dimension $e(S_k) = k - 1 \geq 4$.

Expect that the conjecture can be proved using the methods B. Gross, E. Hironaka and C. McMullen used in 2009 to study the cyclotomic factors of the Coxeter polynomial

$$E_n(x) = \frac{x^{n-2}(x^3 - x - 1) + x^3 + x^2 - 1}{x - 1}$$

Symmetric non-cyclotomic ns with $e(S) \geq 4$

Conjecture

Put $P_{S_k}(x) = 1 - x + x^k - x^{2k-1} + x^{2k}$. For every $k \geq 5$ this polynomial has a root not on the unit circle.

Corollary

For every $k \geq 5$ the symmetric ns S_k is non-cyclotomic and has embedding dimension $e(S_k) = k - 1 \geq 4$.

Expect that the conjecture can be proved using the methods B. Gross, E. Hironaka and C. McMullen used in 2009 to study the cyclotomic factors of the Coxeter polynomial

$$E_n(x) = \frac{x^{n-2}(x^3 - x - 1) + x^3 + x^2 - 1}{x - 1}$$

They use results on linear relations between roots of unity.

Counting cyclotomic ns of given Frobenius number

Theorem (Upper bound)

Let $k \geq 1$ be odd and $N(k)$ denote the number of cyclotomic numerical semigroups having Frobenius number k.

Counting cyclotomic ns of given Frobenius number

Theorem (Upper bound)

Let $k \geq 1$ be odd and $N(k)$ denote the number of cyclotomic numerical semigroups having Frobenius number k. Then $N(k) < e^{3.577\sqrt{k}}$ for all k large enough.

Counting cyclotomic ns of given Frobenius number

Theorem (Upper bound)

Let $k \geq 1$ be odd and $N(k)$ denote the number of cyclotomic numerical semigroups having Frobenius number k. Then $N(k) < e^{3.577\sqrt{k}}$ for all k large enough.

On the other hand:

Theorem (Backelin)

For all odd k large enough there are $> e^{(\log 2)\lfloor k/8 \rfloor}$ symmetric numerical semigroups having Frobenius number k.

Counting cyclotomic ns of given Frobenius number

Theorem (Upper bound)

Let $k \geq 1$ be odd and $N(k)$ denote the number of cyclotomic numerical semigroups having Frobenius number k. Then $N(k) < e^{3.577\sqrt{k}}$ for all k large enough.

On the other hand:

Theorem (Backelin)

For all odd k large enough there are $> e^{(\log 2)\lfloor k/8 \rfloor}$ symmetric numerical semigroups having Frobenius number k.

It follows that there are abundantly many symmetric numerical semigroups that are not cyclotomic.

Counting cyclotomic ns of given Frobenius number

Sketch of proof of Theorem “Upper bound”.

Counting cyclotomic ns of given Frobenius number

Sketch of proof of Theorem "Upper bound". Let S be a cyclotomic ns with $F(S) = k$.

Counting cyclotomic ns of given Frobenius number

Sketch of proof of Theorem "Upper bound". Let S be a cyclotomic ns with $F(S) = k$. Write

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

with $e_d \geq 1$.

Counting cyclotomic ns of given Frobenius number

Sketch of proof of Theorem "Upper bound". Let S be a cyclotomic ns with $F(S) = k$. Write

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

with $e_d \geq 1$. From this identity we obtain that $F(s) + 1 = k + 1 = \sum_{d \in \mathcal{D}} e_d \varphi(d)$, which is a cyclotomic partition of $k + 1$.

Counting cyclotomic ns of given Frobenius number

Sketch of proof of Theorem “Upper bound”. Let S be a cyclotomic ns with $F(S) = k$. Write

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

with $e_d \geq 1$. From this identity we obtain that $F(s) + 1 = k + 1 = \sum_{d \in \mathcal{D}} e_d \varphi(d)$, which is a cyclotomic partition of $k + 1$. The number of cyclotomic partitions of n we denote by $c(n)$.

Counting cyclotomic ns of given Frobenius number

Sketch of proof of Theorem "Upper bound". Let S be a cyclotomic ns with $F(S) = k$. Write

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

with $e_d \geq 1$. From this identity we obtain that $F(s) + 1 = k + 1 = \sum_{d \in \mathcal{D}} e_d \varphi(d)$, which is a cyclotomic partition of $k + 1$. The number of cyclotomic partitions of n we denote by $c(n)$. We infer that $N(k) \leq c(k + 1)$.

Theorem (Boyd and Montgomery, 1988)

$$c(n) \sim A \frac{e^{B\sqrt{n}}}{n\sqrt{\log n}}, \;\; n \to \infty.$$

Polynomially Related Numerical Semigroups

Polynomially Related Numerical Semigroups

Definition

We say that the numerical semigroup S is polynomially related to the numerical semigroup T, and denote this by $S \leq_P T$, if there exist $f(x) \in \mathbb{Z}[x]$ and an integer $w \geq 1$ such that

$$H_S(x^w)f(x) = H_T(x),$$

or equivalently, $P_S(x^w)f(x) = P_T(x)(1 + x + \cdots + x^{w-1})$.

Polynomially Related Numerical Semigroups

Definition

We say that the numerical semigroup S is polynomially related to the numerical semigroup T, and denote this by $S \leq_P T$, if there exist $f(x) \in \mathbb{Z}[x]$ and an integer $w \geq 1$ such that

$$H_S(x^w)f(x) = H_T(x),$$

or equivalently, $P_S(x^w)f(x) = P_T(x)(1 + x + \cdots + x^{w-1})$.

Example

a) $\langle p^a, q^b \rangle \leq_P \langle p^m, q^n \rangle$ if $1 \leq a \leq m$ and $1 \leq b \leq n$.

b) $\langle p^a, q^b \rangle \leq_P B_n(p, q)$ if $a, b \geq 1$ and $2 \leq a + b \leq n + 1$.

Polynomially Related Numerical Semigroups

Definition

We say that the numerical semigroup S is polynomially related to the numerical semigroup T, and denote this by $S \leq_P T$, if there exist $f(x) \in \mathbb{Z}[x]$ and an integer $w \geq 1$ such that

$$H_S(x^w)f(x) = H_T(x),$$

or equivalently, $P_S(x^w)f(x) = P_T(x)(1 + x + \cdots + x^{w-1})$.

Example

a) $\langle p^a, q^b \rangle \leq_P \langle p^m, q^n \rangle$ if $1 \leq a \leq m$ and $1 \leq b \leq n$.

b) $\langle p^a, q^b \rangle \leq_P B_n(p, q)$ if $a, b \geq 1$ and $2 \leq a + b \leq n + 1$.

Problem

Find necessary and sufficient conditions such that $S \leq_P T$.

Polynomially Related Numerical Semigroups

Polynomially Related Numerical Semigroups

In proving the following, we make repeated use of the fact that $P_S(1) = 1$ and $P'_S(1) = g(S)$.

Polynomially Related Numerical Semigroups

In proving the following, we make repeated use of the fact that $P_S(1) = 1$ and $P'_S(1) = g(S)$.

Lemma

Suppose that $H_S(x^w)f(x) = H_T(x)$ holds with S, T numerical semigroups. Then

a) $f(0) = 1$.
b) $f(1) = w$.
c) $f'(1) = w(g(T) - wg(S) + (w-1)/2)$.
d) $F(T) = wF(S) + \deg f$.
e) *If w is even, then $f(-1) = 0$.*
f) *If w is odd, then $f(-1) = P_T(-1)/P_S(-1)$.*
g) *If T is cyclotomic, then so is S.*
h) *If S is cyclotomic, then T is cyclotomic iff f is Kronecker.*

An Application

An Application

Theorem

Let $p \neq q$ be primes and m, n positive integers. The quotient

$$Q(x) = P_{\langle p^m, q^n \rangle}(x)/\Phi_{p^m q^n}(x)$$

is in $\mathbb{Z}[x]$, is monic and has constant coefficient 1. Its non-zero coefficients alternate between 1 and -1.

An Application

Theorem

Let $p \neq q$ be primes and m, n positive integers. The quotient

$$Q(x) = P_{\langle p^m, q^n \rangle}(x) / \Phi_{p^m q^n}(x)$$

is in $\mathbb{Z}[x]$, is monic and has constant coefficient 1. Its non-zero coefficients alternate between 1 and -1.

In fact, a more general result holds.

Theorem

Suppose that S and T are numerical semigroups with $H_S(x^w)f(x) = H_T(x)$ for some $w \geq 1$ and $f \in \mathbb{N}[x]$. Put $Q(x) = P_T(x)/P_S(x^w)$. Then $Q(0) = 1$ and $Q(x)$ is a monic polynomial having non-zero coefficients that alternate between 1 and -1.

Thank you for attention!