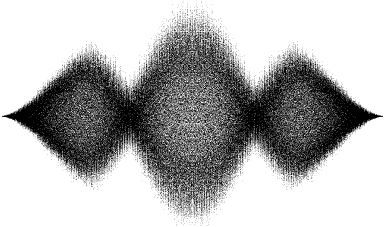
Cyclotomic Coefficients: Progress and Promise

Pieter Moree (MPIM, Bonn)



CIRM, Luminy
March 29, 2016

Some definitions

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

Some definitions

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

Write $\Phi_n(X) = \sum_{k=0}^{\infty} a_n(k) X^k$.

Some definitions

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

Write $\Phi_n(X) = \sum_{k=0}^{\infty} a_n(k) X^k$.
The height of $\Phi_n(X)$, $A(n)$, is defined as $\max\{|a_n(k)| : k \geq 0\}$.

Some definitions

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

Write $\Phi_n(X) = \sum_{k=0}^{\infty} a_n(k) X^k$.
The height of $\Phi_n(X)$, $A(n)$, is defined as $\max\{|a_n(k)| : k \geq 0\}$.

If $A(n) = 1$, then $\Phi_n(X)$ is said to be flat

Some definitions

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

Write $\Phi_n(X) = \sum_{k=0}^{\infty} a_n(k) X^k$.
The height of $\Phi_n(X)$, $A(n)$, is defined as $\max\{|a_n(k)| : k \geq 0\}$.

If $A(n) = 1$, then $\Phi_n(X)$ is said to be flat

Example:

$\Phi_{21}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1$.

Some definitions

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

Write $\Phi_n(X) = \sum_{k=0}^{\infty} a_n(k) X^k$.
The height of $\Phi_n(X)$, $A(n)$, is defined as $\max\{|a_n(k)| : k \geq 0\}$.

If $A(n) = 1$, then $\Phi_n(X)$ is said to be flat

Example:

$\Phi_{21}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1$.
It seems that the coefficients are small, e.g., $A(n) = 1$ for

$n < 105$.

Some definitions

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

Write $\Phi_n(X) = \sum_{k=0}^{\infty} a_n(k) X^k$.
The height of $\Phi_n(X)$, $A(n)$, is defined as $\max\{|a_n(k)| : k \geq 0\}$.

If $A(n) = 1$, then $\Phi_n(X)$ is said to be flat

Example:

$\Phi_{21}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1.$
It seems that the coefficients are small, e.g., $A(n) = 1$ for

$n < 105$.

Connections

-simplicial complexes (G. Musiker and V. Reiner, 2012)
-Kloosterman sums
-numerical semigroups
-cryptography

Elementary properties

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

Elementary properties

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

-$\deg(\Phi_n) = \varphi(n)$

Elementary properties

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

-$\deg(\Phi_n) = \varphi(n)$
-integer coefficients

Elementary properties

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

-$\deg(\Phi_n) = \varphi(n)$
-integer coefficients

-irreducible over $\mathbb{Q}$

Elementary properties

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

-$\deg(\Phi_n) = \varphi(n)$
-integer coefficients

-irreducible over $\mathbb{Q}$

-$X^{\varphi(n)}\Phi_n(1/X) = \Phi_n(X)$ if $n > 1$ (self-reciprocal)

Elementary properties

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

-$\deg(\Phi_n) = \varphi(n)$
-integer coefficients

-irreducible over $\mathbb{Q}$

-$X^{\varphi(n)}\Phi_n(1/X) = \Phi_n(X)$ if $n > 1$ (self-reciprocal)

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

Elementary properties

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

-$\deg(\Phi_n) = \varphi(n)$
-integer coefficients

-irreducible over $\mathbb{Q}$

-$X^{\varphi(n)}\Phi_n(1/X) = \Phi_n(X)$ if $n > 1$ (self-reciprocal)

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

-$\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$ (by Möbius inversion)

Elementary properties

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

-$\deg(\Phi_n) = \varphi(n)$
-integer coefficients

-irreducible over $\mathbb{Q}$

-$X^{\varphi(n)}\Phi_n(1/X) = \Phi_n(X)$ if $n > 1$ (self-reciprocal)

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

-$\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$ (by Möbius inversion)

-$\Phi_n(X) = \Phi_{\gamma(n)}(X^{n/\gamma(n)}),\ \gamma(n) = \prod_{p|n} p$

Elementary properties

$$\Phi_n(X) = \prod_{j=1,\ (j,n)=1}^{n} (X - \zeta_n^j)$$

-$\deg(\Phi_n) = \varphi(n)$
-integer coefficients

-irreducible over $\mathbb{Q}$

-$X^{\varphi(n)}\Phi_n(1/X) = \Phi_n(X)$ if $n > 1$ (self-reciprocal)

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

-$\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$ (by Möbius inversion)

-$\Phi_n(X) = \Phi_{\gamma(n)}(X^{n/\gamma(n)}),\ \gamma(n) = \prod_{p|n} p$

-$\Phi_{2n}(X) = \Phi_n(-X)$, $n > 1$ odd

Some plots...

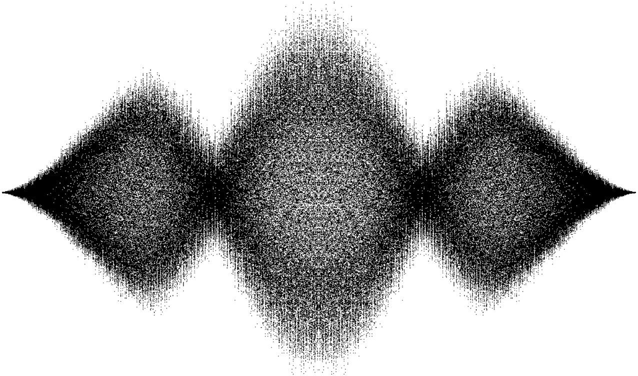
Courtesy of

Andrew
Arnold

Some plots...

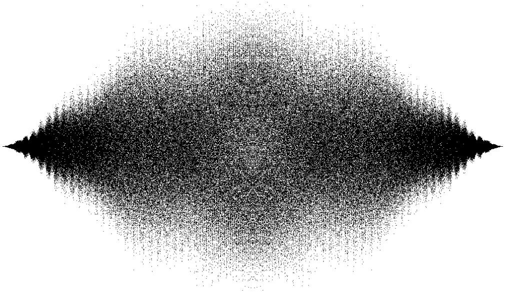
Courtesy of

Andrew
Arnold



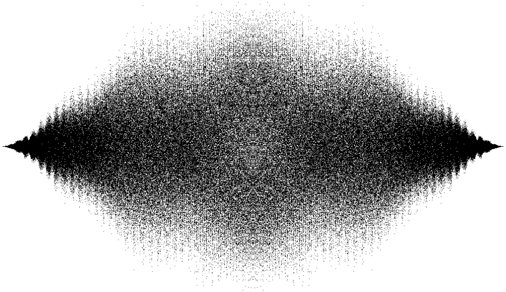
$4849845 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

$\Phi_{111546435}(X)$ and $\Phi_{3234846615}(X)$

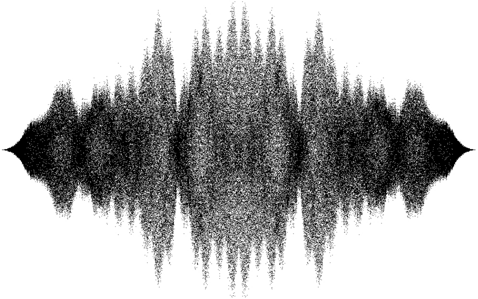


$111546435 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$

$\Phi_{111546435}(X)$ and $\Phi_{3234846615}(X)$



$111546435 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$



$3234846615 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$

height 2888582082 500892851

Very rough outline of talk

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\text{odd}}(n)$ small

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\text{odd}}(n)$ small
Mostly elementary methods.

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\text{odd}}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\text{odd}}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\text{odd}}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).
Young mathematicians playground:

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\text{odd}}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).
Young mathematicians playground:
Some stubbornly keep playing:

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\mathrm{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\mathrm{odd}}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).
Young mathematicians playground:
Some stubbornly keep playing:
Examples: Florian Luca, M., Igor Shparlinski

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\text{odd}}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).
Young mathematicians playground:
Some stubbornly keep playing:
Examples: Florian Luca, M., Igor Shparlinski

Numerical semigroups

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\rm odd}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\rm odd}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).
Young mathematicians playground:
Some stubbornly keep playing:
Examples: Florian Luca, M., Igor Shparlinski

Numerical semigroups
New approach. PROMISE?

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\rm odd}(n)=\sum_{p|n,\ p>2}1$.

Φ_n with $\omega_{\rm odd}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).
Young mathematicians playground:
Some stubbornly keep playing:
Examples: Florian Luca, M., Igor Shparlinski

Numerical semigroups
New approach. PROMISE?

Φ_n with $\omega_{\rm odd}(n)$ large

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\text{odd}}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).
Young mathematicians playground:
Some stubbornly keep playing:
Examples: Florian Luca, M., Igor Shparlinski

Numerical semigroups
New approach. PROMISE?

Φ_n with $\omega_{\text{odd}}(n)$ large
The exclusive realm of analytic number theory.

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\text{odd}}(n) = \sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\text{odd}}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).
Young mathematicians playground:
Some stubbornly keep playing:
Examples: Florian Luca, M., Igor Shparlinski

Numerical semigroups
New approach. PROMISE?

Φ_n with $\omega_{\text{odd}}(n)$ large
The exclusive realm of analytic number theory.
Bateman, Maier, Pomerance, Vaughan...

Very rough outline of talk

Behaviour of Φ_n depends on $\omega_{\rm odd}(n)=\sum_{p|n,\ p>2} 1$.

Φ_n with $\omega_{\rm odd}(n)$ small
Mostly elementary methods.
Recently methods from analytic number theory. PROMISE?
Computer experiments (Yves Gallot).
Young mathematicians playground:
Some stubbornly keep playing:
Examples: Florian Luca, M., Igor Shparlinski

Numerical semigroups
New approach. PROMISE?

Φ_n with $\omega_{\rm odd}(n)$ large
The exclusive realm of analytic number theory.
Bateman, Maier, Pomerance, Vaughan...
Will not be discussed here...

Which $a_n(k)$ do occur?

I. Schur in letter to E. Landau: set of all $a_n(k)$ is infinite.

Which $a_n(k)$ do occur?

I. Schur in letter to E. Landau: set of all $a_n(k)$ is infinite.

$$\{a_n(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z} \text{ (Jiro Suzuki, 1987)}$$

Which $a_n(k)$ do occur?

I. Schur in letter to E. Landau: set of all $a_n(k)$ is infinite.

$$\{a_n(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z} \text{ (Jiro Suzuki, 1987)}$$

Problem: Given $m \geq 1$, determine $\{a_{mn}(k) : n \geq 1,\ k \geq 0\}$

Which $a_n(k)$ do occur?

I. Schur in letter to E. Landau: set of all $a_n(k)$ is infinite.

$$\{a_n(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z} \text{ (Jiro Suzuki, 1987)}$$

Problem: Given $m \geq 1$, determine $\{a_{mn}(k) : n \geq 1,\ k \geq 0\}$

Christine Jost
PhD in AG
2013
Stockholm
University

Janina Müttel
PhD in OR
2013
Ulm
University

Which $a_n(k)$ do occur?

I. Schur in letter to E. Landau: set of all $a_n(k)$ is infinite.

$$\{a_n(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z} \text{ (Jiro Suzuki, 1987)}$$

Problem: Given $m \geq 1$, determine $\{a_{mn}(k) : n \geq 1,\ k \geq 0\}$

Christine Jost
PhD in AG
2013
Stockholm
University

Janina Müttel
PhD in OR
2013
Ulm
University

This problem remained unsolved...

Ji and Li and . . .

Chun-Gang Ji and Wei-Ping Li (2008):

$$\{a_{p^e n}(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$$

Ji and Li and ...

Chun-Gang Ji and Wei-Ping Li (2008):

$$\{a_{p^e n}(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$$

Ji, Li and M. then solved the Problem (2009):

Ji and Li and . . .

Chun-Gang Ji and Wei-Ping Li (2008):

$$\{a_{p^e n}(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$$

Ji, Li and M. then solved the Problem (2009):

`Theorem`. *Let* $m \geq 1$ *be fixed. Then*

$$\{a_{mn}(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$$

Ji and Li and . . .

Chun-Gang Ji and Wei-Ping Li (2008):

$$\{a_{p^e n}(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$$

Ji, Li and M. then solved the Problem (2009):

`Theorem`. *Let $m \geq 1$ be fixed. Then*

$$\{a_{mn}(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$$

Jessica Fintzen (2011) determined

$$\{a_n(k) :\ n \equiv a(\text{mod } d),\ k \equiv b(\text{mod } f)\}$$

Ji and Li and . . .

Chun-Gang Ji and Wei-Ping Li (2008):

$$\{a_{p^e n}(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$$

Ji, Li and M. then solved the Problem (2009):

`Theorem`. *Let $m \geq 1$ be fixed. Then*

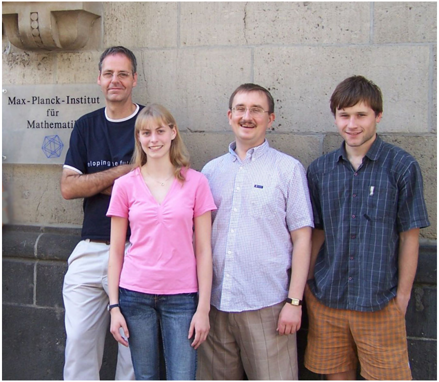
$$\{a_{mn}(k) : n \geq 1,\ k \geq 0\} = \mathbb{Z}$$

Jessica Fintzen (2011) determined

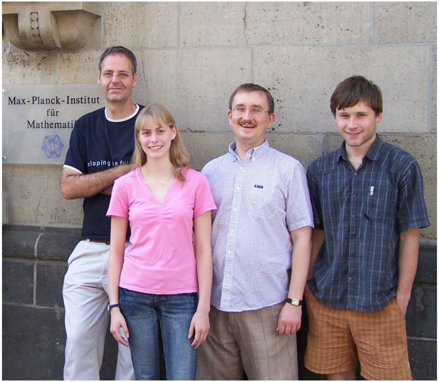
$$\{a_n(k) :\ n \equiv a (\text{mod } d),\ k \equiv b (\text{mod } f)\}$$

This is still the state of the art in this direction.

Jessica Fintzen



Jessica Fintzen



Defended her PhD in 2015 in Harvard...

Binary cyclotomic polynomials

Note that $\Phi_p(X) = (1 - X^p)/(1 - X) = 1 + X + X^2 + \cdots + X^{p-1}$.

Binary cyclotomic polynomials

Note that $\Phi_p(X) = (1 - X^p)/(1 - X) = 1 + X + X^2 + \cdots + X^{p-1}$.
We have

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

where

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

Binary cyclotomic polynomials

Note that $\Phi_p(X) = (1 - X^p)/(1 - X) = 1 + X + X^2 + \cdots + X^{p-1}$.
We have

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

where

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

Thus the cyclotomic coefficient $a_{pq}(m)$ equals

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

Flatness

Φ_p, Φ_{pq} are flat

Flatness

Φ_p, Φ_{pq} are flat
$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)

Flatness

Φ_p, Φ_{pq} are flat

$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)

Φ_{pqr} is flat if:

Flatness

Φ_p, Φ_{pq} are flat

$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)

Φ_{pqr} is flat if:

-$q \equiv -1 (\text{mod } p),\ r \equiv 1 (\text{mod } pq)$

Flatness

Φ_p, Φ_{pq} are flat
$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)
Φ_{pqr} is flat if:
-$q \equiv -1 (\text{mod } p),\ r \equiv 1 (\text{mod } pq)$
-$r \equiv \pm 1 (\text{mod } pq)$

Flatness

Φ_p, Φ_{pq} are flat

$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)

Φ_{pqr} is flat if:

-$q \equiv -1 (\text{mod } p),\; r \equiv 1 (\text{mod } pq)$

-$r \equiv \pm 1 (\text{mod } pq)$

-$r \equiv w (\text{mod } pq), p \equiv 1 (\text{mod } w), q \equiv 1 (\text{mod } pw)$

Flatness

Φ_p, Φ_{pq} are flat

$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)

Φ_{pqr} is flat if:

-$q \equiv -1 (\mathrm{mod}\ p),\ r \equiv 1 (\mathrm{mod}\ pq)$ Bachman, 2006

-$r \equiv \pm 1 (\mathrm{mod}\ pq)$ Kaplan, 2007

-$r \equiv w (\mathrm{mod}\ pq), p \equiv 1 (\mathrm{mod}\ w), q \equiv 1 (\mathrm{mod}\ pw)$ Elder, 2013

Flatness

Φ_p, Φ_{pq} are flat

$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)

Φ_{pqr} is flat if:

-$q \equiv -1 (\mathrm{mod}\ p),\ r \equiv 1 (\mathrm{mod}\ pq)$ Bachman, 2006

-$r \equiv \pm 1 (\mathrm{mod}\ pq)$ Kaplan, 2007

-$r \equiv w (\mathrm{mod}\ pq), p \equiv 1 (\mathrm{mod}\ w), q \equiv 1 (\mathrm{mod}\ pw)$ Elder, 2013

Φ_{pqrs} is flat if:

Flatness

Φ_p, Φ_{pq} are flat

$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)

Φ_{pqr} is flat if:

-$q \equiv -1 \pmod{p},\ r \equiv 1 \pmod{pq}$	Bachman, 2006
-$r \equiv \pm 1 \pmod{pq}$	Kaplan, 2007
-$r \equiv w \pmod{pq}, p \equiv 1 \pmod{w}, q \equiv 1 \pmod{pw}$	Elder, 2013

Φ_{pqrs} is flat if:

$q \equiv -1 \pmod{p}$, $r \equiv \pm 1 \pmod{pq},\ s \equiv 1 \pmod{pqr}$

Flatness

Φ_p, Φ_{pq} are flat
$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)
Φ_{pqr} is flat if:

-$q \equiv -1 \pmod{p},\ r \equiv 1 \pmod{pq}$	Bachman, 2006
-$r \equiv \pm 1 \pmod{pq}$	Kaplan, 2007
-$r \equiv w \pmod{pq}, p \equiv 1 \pmod{w}, q \equiv 1 \pmod{pw}$	Elder, 2013

Φ_{pqrs} is flat if:
$q \equiv -1 \pmod{p}$, $r \equiv \pm 1 \pmod{pq},\ s \equiv 1 \pmod{pqr}$
Φ_{pqrst}:

Flatness

Φ_p, Φ_{pq} are flat
$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)
Φ_{pqr} is flat if:

-$q \equiv -1 (\text{mod } p),\ r \equiv 1 (\text{mod } pq)$ Bachman, 2006
-$r \equiv \pm 1 (\text{mod } pq)$ Kaplan, 2007
-$r \equiv w (\text{mod } pq), p \equiv 1 (\text{mod } w), q \equiv 1 (\text{mod } pw)$ Elder, 2013

Φ_{pqrs} is flat if:
$q \equiv -1 (\text{mod } p)$, $r \equiv \pm 1 (\text{mod } pq),\ s \equiv 1 (\text{mod } pqr)$
Φ_{pqrst}:
`Conjecture`: Is never flat...

Flatness

Φ_p, Φ_{pq} are flat

$(X-1)\Phi_{pqr}(X)$ is flat (Gallot and M., 2009)

Φ_{pqr} is flat if:

- $q \equiv -1 (\text{mod } p),\ r \equiv 1 (\text{mod } pq)$ Bachman, 2006
- $r \equiv \pm 1 (\text{mod } pq)$ Kaplan, 2007
- $r \equiv w (\text{mod } pq), p \equiv 1 (\text{mod } w), q \equiv 1 (\text{mod } pw)$ Elder, 2013

Φ_{pqrs} is flat if:

$q \equiv -1 (\text{mod } p),\ r \equiv \pm 1 (\text{mod } pq),\ s \equiv 1 (\text{mod } pqr)$

Φ_{pqrst}:

`Conjecture`: Is never flat...

Sam  Elder

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.
-$C(n)$ is coefficient convex if it consists of consecutive integers.

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.
-$C(n)$ is coefficient convex if it consists of consecutive integers.

Gallot and M. (2009):

$$A((X-1)\Phi_{pqr}(X)) = 1, \text{ that is } |a_{pqr}(k) - a_{pqr}(k-1)| \leq 1$$

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.
-$C(n)$ is coefficient convex if it consists of consecutive integers.

Gallot and M. (2009):

$$A((X-1)\Phi_{pqr}(X)) = 1, \text{ that is } |a_{pqr}(k) - a_{pqr}(k-1)| \leq 1$$

A ternary Φ_n has the jump one property

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.
-$C(n)$ is coefficient convex if it consists of consecutive integers.

Gallot and M. (2009):

$$A((X-1)\Phi_{pqr}(X)) = 1, \text{ that is } |a_{pqr}(k) - a_{pqr}(k-1)| \leq 1$$

A ternary Φ_n has the jump one property

$C(p) = [0,1],\ C(pq) = [-1,1],\ C(pqr) = [-a,b],\ \max(a,b) = A(pqr)$

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.
-$C(n)$ is coefficient convex if it consists of consecutive integers.

Gallot and M. (2009):

$$A((X-1)\Phi_{pqr}(X)) = 1, \text{ that is } |a_{pqr}(k) - a_{pqr}(k-1)| \leq 1$$

A ternary Φ_n has the jump one property

$C(p) = [0,1],\ C(pq) = [-1,1],\ C(pqr) = [-a,b],\ \max(a,b) = A(pqr)$

$C(5 \cdot 7 \cdot 13 \cdot 17) = \{-9\} \cup [-7,5]$

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.
-$C(n)$ is coefficient convex if it consists of consecutive integers.

Gallot and M. (2009):

$$A((X-1)\Phi_{pqr}(X)) = 1, \text{ that is } |a_{pqr}(k) - a_{pqr}(k-1)| \leq 1$$

A ternary Φ_n has the jump one property

$C(p) = [0,1],\ C(pq) = [-1,1],\ C(pqr) = [-a,b],\ \max(a,b) = A(pqr)$

$C(5 \cdot 7 \cdot 13 \cdot 17) = \{-9\} \cup [-7,5]$
We have $\#C(pqr) = b + a \leq p$.

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.
-$C(n)$ is coefficient convex if it consists of consecutive integers.

Gallot and M. (2009):

$$A((X-1)\Phi_{pqr}(X)) = 1, \text{ that is } |a_{pqr}(k) - a_{pqr}(k-1)| \leq 1$$

A ternary Φ_n has the jump one property

$C(p) = [0, 1],\ C(pq) = [-1, 1],\ C(pqr) = [-a, b],\ \max(a, b) = A(pqr)$

$C(5 \cdot 7 \cdot 13 \cdot 17) = \{-9\} \cup [-7, 5]$
We have $\#C(pqr) = b + a \leq p$. If equality holds, then $\Phi_{pqr}(X)$ is said to have an optimally large set of coefficients.

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.
-$C(n)$ is coefficient convex if it consists of consecutive integers.

Gallot and M. (2009):

$$A((X-1)\Phi_{pqr}(X)) = 1, \text{ that is } |a_{pqr}(k) - a_{pqr}(k-1)| \leq 1$$

A ternary Φ_n has the jump one property

$C(p) = [0,1],\ C(pq) = [-1,1],\ C(pqr) = [-a,b],\ \max(a,b) = A(pqr)$

$C(5 \cdot 7 \cdot 13 \cdot 17) = \{-9\} \cup [-7,5]$
We have $\#C(pqr) = b + a \leq p$. If equality holds, then $\Phi_{pqr}(X)$ is said to have an optimally large set of coefficients.

Coefficient convexity

-Put $C(n) = \{a_n(k) : k \geq 0\}$.
-$C(n)$ is coefficient convex if it consists of consecutive integers.

Gallot and M. (2009):

$$A((X-1)\Phi_{pqr}(X)) = 1, \text{ that is } |a_{pqr}(k) - a_{pqr}(k-1)| \leq 1$$

A ternary Φ_n has the jump one property

$C(p) = [0,1],\ C(pq) = [-1,1],\ C(pqr) = [-a,b],\ \max(a,b) = A(pqr)$

$C(5 \cdot 7 \cdot 13 \cdot 17) = \{-9\} \cup [-7,5]$
We have $\#C(pqr) = b + a \leq p$. If equality holds, then $\Phi_{pqr}(X)$ is said to have an optimally large set of coefficients.
Example: Lehmer/Möller infinite family satisfies

$C(pqr) = [-\frac{p-1}{2}, \frac{p+1}{2}],$ (Bachman, 2004)

Jumps

-Gallot-M.: consecutive coefficients of ternary cyclotomic polynomials differ by at most one.

Jumps

-Gallot-M.: consecutive coefficients of ternary cyclotomic polynomials differ by at most one.

-Bzdęga: different reproof of this result.
Initiated the study of the number of “jumps”.

Jumps

-Gallot-M.: consecutive coefficients of ternary cyclotomic polynomials differ by at most one.

-Bzdęga: different reproof of this result.
Initiated the study of the number of “jumps”.

Number of jumps up with $a_n(k) = a_n(k-1) + 1$ is the same as the number of jumps down with $a_n(k) = a_n(k-1) - 1$.

Jumps

-Gallot-M.: consecutive coefficients of ternary cyclotomic polynomials differ by at most one.

-Bzdęga: different reproof of this result.
Initiated the study of the number of “jumps”.

Number of jumps up with $a_n(k) = a_n(k-1) + 1$ is the same as the number of jumps down with $a_n(k) = a_n(k-1) - 1$.

We denote this common number by J_n.

Jumps

-Gallot-M.: consecutive coefficients of ternary cyclotomic polynomials differ by at most one.

-Bzdęga: different reproof of this result.
Initiated the study of the number of “jumps”.

Number of jumps up with $a_n(k) = a_n(k-1) + 1$ is the same as the number of jumps down with $a_n(k) = a_n(k-1) - 1$.

We denote this common number by J_n.

-Bzdęga: $J_n > n^{1/3}$.

Jumps

-Gallot-M.: consecutive coefficients of ternary cyclotomic polynomials differ by at most one.

-Bzdęga: different reproof of this result.
Initiated the study of the number of “jumps”.

Number of jumps up with $a_n(k) = a_n(k-1) + 1$ is the same as the number of jumps down with $a_n(k) = a_n(k-1) - 1$.

We denote this common number by J_n.

-Bzdęga: $J_n > n^{1/3}$.

-Camburu-Ciolan-Luca-M.-Shparlinski (2016): For infinitely many $n = pqr$ with pairwise distinct odd primes p, q and r, we have

$$J_n \ll n^{7/8+o(1)}.$$

Is $\Phi_n(X)$ a special divisor of $X^n - 1$?

If $\Phi_n(X) | X^{p^2q} - 1$, then

$$\Phi_n = \Phi_1^{k_1}\Phi_p^{k_2}\Phi_q^{k_3}\Phi_{pq}^{k_4}\Phi_{p^2}^{k_4}\Phi_{p^2q}^{k_5},\ k_i \in \{0,1\}$$

Is $\Phi_n(X)$ a special divisor of $X^n - 1$?

If $\Phi_n(X) | X^{p^2 q} - 1$, then

$$\Phi_n = \Phi_1^{k_1} \Phi_p^{k_2} \Phi_q^{k_3} \Phi_{pq}^{k_4} \Phi_{p^2}^{k_4} \Phi_{p^2 q}^{k_5}, \; k_i \in \{0, 1\}$$

If q is odd, then all 64 divisors are coefficient convex
(Andreas Decker and M., Sarajevo Math. J., 2012)

Is $\Phi_n(X)$ a special divisor of $X^n - 1$?

If $\Phi_n(X) | X^{p^2 q} - 1$, then

$$\Phi_n = \Phi_1^{k_1} \Phi_p^{k_2} \Phi_q^{k_3} \Phi_{pq}^{k_4} \Phi_{p^2}^{k_4} \Phi_{p^2 q}^{k_5}, \ k_i \in \{0, 1\}$$

If q is odd, then all 64 divisors are coefficient convex
(Andreas Decker and M., Sarajevo Math. J., 2012)
Extends work of C. Pomerance, N.C. Ryan and N. Kaplan

Andreas Decker
PhD student
comp. analytic number th.
Bonn University

Φ_1	Φ_p	Φ_q	Φ_{pq}	Φ_{p^2}	Φ_{p^2q}	coefficients
1	0	0	0	1	0	$[-1, 1]$
0	1	0	0	1	0	$\{1\}$
1	1	0	0	1	0	$[-1, 1]$
0	0	1	0	1	0	$[\min([\frac{q}{p}], 1), \min([\frac{q-1}{p}] + 1, p)]$
1	0	1	0	1	0	$[-1, 1]$
0	1	1	0	1	0	$[1, \min(p^2, q)]$
1	1	1	0	1	0	$[-1, 1]$
0	0	0	1	1	0	$[-\min(p, q - p^*), \min(p, p^*)]$
1	0	0	1	1	0	$[-\gamma(p, q), \gamma(p, q)]$
0	1	0	1	1	0	$[0, 1]$
1	1	0	1	1	0	$[-1, 1]$
0	0	1	1	1	0	$[0, \min(p, q)]$
1	0	1	1	1	0	$[-\min(p, q), \min(p, q)]$
0	1	1	1	1	0	$[1, \min(p, q)]$

$\gamma(p.q) = \min(p, p^*) + \min(p, q - p^*)$.

Inverse cyclotomic polynomials

(Introduced by M. in 2009)
Consider

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

Inverse cyclotomic polynomials

(Introduced by M. in 2009)
Consider

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

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

Inverse cyclotomic polynomials

(Introduced by M. in 2009)
Consider

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

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

We have $B(n) = 1$ for $n < 561$

Inverse cyclotomic polynomials

(Introduced by M. in 2009)
Consider

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

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

We have $B(n) = 1$ for $n < 561$
We have $B(pqr) \leq p - 1$.

Inverse cyclotomic polynomials

(Introduced by M. in 2009)
Consider

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

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

We have $B(n) = 1$ for $n < 561$
We have $B(pqr) \leq p - 1$.

$$B(pqr) = p - 1 \iff q \equiv r \equiv \pm 1 (\mathrm{mod}\ p) \text{ and } r < \frac{p-1}{p-2}(q-1)$$

Maximum gaps, I

- 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

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

Maximum gaps, I

- 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

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

- Study of $g(\Phi_n)$ and $g(\Psi_n)$ has been initiated by Hong, Lee, Lee and Park (2012) who reduced the study of these gaps to the case where n is square-free and odd.

Maximum gaps, I

- 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

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

- Study of $g(\Phi_n)$ and $g(\Psi_n)$ has been initiated by Hong, Lee, Lee and Park (2012) who reduced the study of these gaps to the case where 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 (2015):

Maximum gaps, I

- 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

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

- Study of $g(\Phi_n)$ and $g(\Psi_n)$ has been initiated by Hong, Lee, Lee and Park (2012) who reduced the study of these gaps to the case where 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 (2015):

- More managable when turned into a problem involving the maximum gaps of inverse cyclotomic polynomials.

Maximum gaps, II

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

Maximum gaps, II

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

Hong-Lee-Lee-Park:
Put $\mathcal{Q}_3 = \{n = pqr : 2 < p < q < r \text{ primes}\}$.

Maximum gaps, II

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

Hong-Lee-Lee-Park:
Put $\mathcal{Q}_3 = \{n = pqr : 2 < p < q < r \text{ primes}\}$.

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

Maximum gaps, II

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

Hong-Lee-Lee-Park:
Put $\mathcal{Q}_3 = \{n = pqr : 2 < p < q < r \text{ primes}\}$.

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

Then

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

Maximum gaps, II

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

Hong-Lee-Lee-Park:
Put $\mathcal{Q}_3 = \{n = pqr : 2 < p < q < r \text{ primes}\}$.

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

Then

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

Claim: $\mathcal{R}_3(x) = o(\mathcal{Q}_3(x))$.

Maximum gaps, III

Camburu-Ciolan-Luca-M.-Shparlinksi (2016):
"Cyclotomic coefficients: gaps and jumps":

Maximum gaps, III

Camburu-Ciolan-Luca-M.-Shparlinksi (2016):
"Cyclotomic coefficients: gaps and jumps":
Working title: “Cyclotomic coefficients: an extramarginal affair.”

Maximum gaps, III

Camburu-Ciolan-Luca-M.-Shparlinksi (2016):
"Cyclotomic coefficients: gaps and jumps":
Working title: “Cyclotomic coefficients: an extramarginal affair.”

Showed that

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

with $c = (1 + \log 4)\log 4 = 3.30811\ldots$.

Maximum gaps, III

Camburu-Ciolan-Luca-M.-Shparlinksi (2016):
"Cyclotomic coefficients: gaps and jumps":
Working title: “Cyclotomic coefficients: an extramarginal affair.”

Showed that

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

with $c = (1 + \log 4)\log 4 = 3.30811\ldots.$

Classical estimate (Gauss, Landau):

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

Maximum gaps, III

Camburu-Ciolan-Luca-M.-Shparlinksi (2016):
"Cyclotomic coefficients: gaps and jumps":
Working title: “Cyclotomic coefficients: an extramarginal affair.”

Showed that

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

with $c = (1+\log 4)\log 4 = 3.30811\ldots.$

Classical estimate (Gauss, Landau):

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

Thus the claim is true and in particular

$$\#\mathcal{R}_3(x) \sim \frac{c\#\mathcal{Q}_3(x)}{2(\log x)(\log\log x)^2}.$$

$\omega(n) = 3$: THE TERNARY CASE

$\omega(n) = 3$: THE TERNARY CASE

...where Kloosterman and Sister Beiter meet...

$M(p)$: main problem

Recall that $A(n) = \max\{|a_n(k)| : k \geq 0\}$.

$M(p)$: main problem

Recall that $A(n) = \max\{|a_n(k)| : k \geq 0\}$.
Φ_n is *ternary*, if $n = pqr$ with $2 < p < q < r$.

$M(p)$: main problem

Recall that $A(n) = \max\{|a_n(k)| : k \geq 0\}$.
Φ_n is *ternary*, if $n = pqr$ with $2 < p < q < r$.

For ternary n we can have $A(n) > 1$, e.g. $a_{105}(7) = -2$ and

$A(105) = 2$.

$M(p)$: main problem

Recall that $A(n) = \max\{|a_n(k)| : k \geq 0\}$.
Φ_n is *ternary*, if $n = pqr$ with $2 < p < q < r$.

For ternary n we can have $A(n) > 1$, e.g. $a_{105}(7) = -2$ and

$A(105) = 2$.
If $2 < p_1 < \ldots < p_s$ then $A(p_1 p_2 \cdots p_s) \leq f(p_1, p_2, \ldots, p_{s-2})$.

(J. Justin, 1969)

$M(p)$: main problem

Recall that $A(n) = \max\{|a_n(k)| : k \geq 0\}$.
Φ_n is *ternary*, if $n = pqr$ with $2 < p < q < r$.

For ternary n we can have $A(n) > 1$, e.g. $a_{105}(7) = -2$ and

$A(105) = 2$.
If $2 < p_1 < \ldots < p_s$ then $A(p_1 p_2 \cdots p_s) \leq f(p_1, p_2, \ldots, p_{s-2})$.

(J. Justin, 1969)
For fixed p, $M(p) = \max\{A(pqr) : p < q < r\}$ is well-defined.

$M(p)$: main problem

Recall that $A(n) = \max\{|a_n(k)| : k \geq 0\}$.
Φ_n is *ternary*, if $n = pqr$ with $2 < p < q < r$.

For ternary n we can have $A(n) > 1$, e.g. $a_{105}(7) = -2$ and $A(105) = 2$.
If $2 < p_1 < \ldots < p_s$ then $A(p_1 p_2 \cdots p_s) \leq f(p_1, p_2, \ldots, p_{s-2})$.

(J. Justin, 1969)
For fixed p, $M(p) = \max\{A(pqr) : p < q < r\}$ is well-defined.

Main Question: Determine $M(p)$.

$M(p)$: main problem

Recall that $A(n) = \max\{|a_n(k)| : k \geq 0\}$.
Φ_n is *ternary*, if $n = pqr$ with $2 < p < q < r$.

For ternary n we can have $A(n) > 1$, e.g. $a_{105}(7) = -2$ and

$A(105) = 2$.
If $2 < p_1 < \ldots < p_s$ then $A(p_1 p_2 \cdots p_s) \leq f(p_1, p_2, \ldots, p_{s-2})$.

(J. Justin, 1969)
For fixed p, $M(p) = \max\{A(pqr) : p < q < r\}$ is well-defined.

Main Question: Determine $M(p)$.
Question: Is there a finite procedure to compute $M(p)$?

$M(p)$: results and conjectures

Sister Beiter Conjecture (1968): $M(p) \leq (p+1)/2$.

$M(p)$: results and conjectures

Sister Beiter Conjecture (1968): $M(p) \leq (p+1)/2$.
Sister Beiter (1971): $M(2) = 1,\ M(3) = 2,\ M(5) = 3$

$M(p) \leq \lceil 3p/4 \rceil$.

$M(p)$: results and conjectures

Sister Beiter Conjecture (1968): $M(p) \leq (p+1)/2$.
Sister Beiter (1971): $M(2) = 1,\ M(3) = 2,\ M(5) = 3$

$M(p) \leq \lceil 3p/4 \rceil$.
Emma Lehmer (1936): $M(p) \geq (p-1)/2$ for $p \geq 5$.

$M(p)$: results and conjectures

Sister Beiter Conjecture (1968): $M(p) \le (p+1)/2$.
Sister Beiter (1971): $M(2) = 1,\ M(3) = 2,\ M(5) = 3$

$M(p) \le \lceil 3p/4 \rceil$.
Emma Lehmer (1936): $M(p) \ge (p-1)/2$ for $p \ge 5$.

Herbert Möller (1971): $M(p) \ge (p+1)/2$ for $p \ge 5$.

$M(p)$: results and conjectures

Sister Beiter Conjecture (1968): $M(p) \leq (p+1)/2$.
Sister Beiter (1971): $M(2) = 1,\ M(3) = 2,\ M(5) = 3$

$M(p) \leq \lceil 3p/4 \rceil$.
Emma Lehmer (1936): $M(p) \geq (p-1)/2$ for $p \geq 5$.

Herbert Möller (1971): $M(p) \geq (p+1)/2$ for $p \geq 5$.

Gallot and M. (2008):

-$M(p) > (p+1)/2$ for $p \geq 11$

$M(p)$: results and conjectures

Sister Beiter Conjecture (1968): $M(p) \leq (p+1)/2$.
Sister Beiter (1971): $M(2) = 1,\ M(3) = 2,\ M(5) = 3$

$M(p) \leq \lceil 3p/4 \rceil$.
Emma Lehmer (1936): $M(p) \geq (p-1)/2$ for $p \geq 5$.

Herbert Möller (1971): $M(p) \geq (p+1)/2$ for $p \geq 5$.

Gallot and M. (2008):

-$M(p) > (p+1)/2$ for $p \geq 11$
-$M(p) \geq (2/3 - \epsilon)p$, p sufficiently large.

$M(p)$: results and conjectures

Sister Beiter Conjecture (1968): $M(p) \leq (p+1)/2$.
Sister Beiter (1971): $M(2) = 1,\ M(3) = 2,\ M(5) = 3$

$M(p) \leq \lceil 3p/4 \rceil$.
Emma Lehmer (1936): $M(p) \geq (p-1)/2$ for $p \geq 5$.

Herbert Möller (1971): $M(p) \geq (p+1)/2$ for $p \geq 5$.

Gallot and M. (2008):

-$M(p) > (p+1)/2$ for $p \geq 11$
-$M(p) \geq (2/3 - \epsilon)p$, p sufficiently large.
Zhao and Zhang (2010): $M(7) = 4$.

$M(p)$: results and conjectures

Sister Beiter Conjecture (1968): $M(p) \le (p+1)/2$.
Sister Beiter (1971): $M(2) = 1,\ M(3) = 2,\ M(5) = 3$

$M(p) \le \lceil 3p/4 \rceil$.
Emma Lehmer (1936): $M(p) \ge (p-1)/2$ for $p \ge 5$.

Herbert Möller (1971): $M(p) \ge (p+1)/2$ for $p \ge 5$.

Gallot and M. (2008):

-$M(p) > (p+1)/2$ for $p \ge 11$
-$M(p) \ge (2/3 - \epsilon)p$, p sufficiently large.
Zhao and Zhang (2010): $M(7) = 4$.

Corrected Sister Beiter Conjecture (2008): $M(p) \le 2p/3$.

$M(p)$: results and conjectures

Sister Beiter Conjecture (1968): $M(p) \leq (p+1)/2$.
Sister Beiter (1971): $M(2) = 1,\ M(3) = 2,\ M(5) = 3$

$M(p) \leq \lceil 3p/4 \rceil$.
Emma Lehmer (1936): $M(p) \geq (p-1)/2$ for $p \geq 5$.

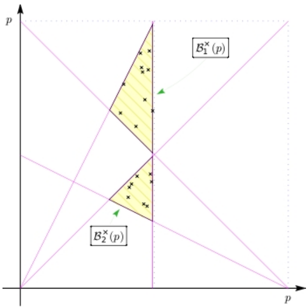
Herbert Möller (1971): $M(p) \geq (p+1)/2$ for $p \geq 5$.

Gallot and M. (2008):

-$M(p) > (p+1)/2$ for $p \geq 11$
-$M(p) \geq (2/3 - \epsilon)p$, p sufficiently large.
Zhao and Zhang (2010): $M(7) = 4$.

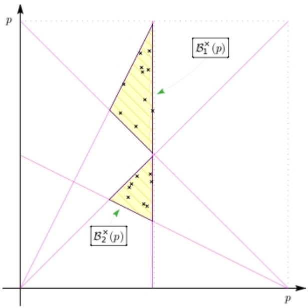
Corrected Sister Beiter Conjecture (2008): $M(p) \leq 2p/3$.

The Sister Beiter conjecture: $M(p) \geq (p+1)/2$



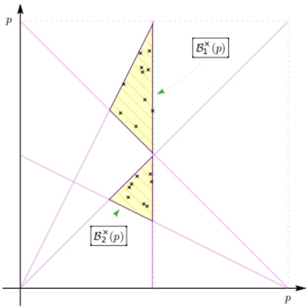
Crosses are at (x, y) with $xy \equiv 1 \pmod{p}$ ($p = 241$ in figure).

The Sister Beiter conjecture: $M(p) \geq (p+1)/2$



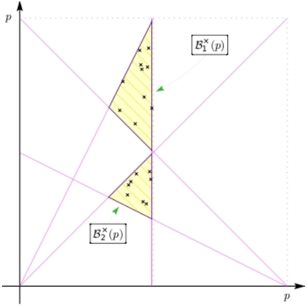
Crosses are at (x, y) with $xy \equiv 1 (\text{mod } p)$ ($p = 241$ in figure).
Each point (x, y) in a triangle leads to triples (p, q, r) with $q \equiv x (\text{mod } p)$ such that $A(pqr) \geq p - x$.

The Sister Beiter conjecture: $M(p) \geq (p+1)/2$



Crosses are at (x, y) with $xy \equiv 1 (\text{mod } p)$ ($p = 241$ in figure).
Each point (x, y) in a triangle leads to triples (p, q, r) with $q \equiv x (\text{mod } p)$ such that $A(pqr) \geq p - x$.
As $x \geq p/3,\ p - x \leq 2p/3$.

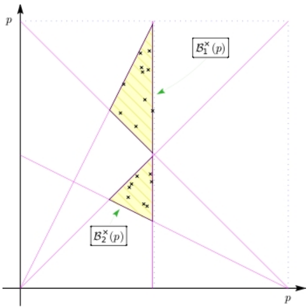
The Sister Beiter conjecture: $M(p) \geq (p+1)/2$



Crosses are at (x, y) with $xy \equiv 1 (\text{mod } p)$ ($p = 241$ in figure).
Each point (x, y) in a triangle leads to triples (p, q, r) with
$q \equiv x (\text{mod } p)$ such that $A(pqr) \geq p - x$.
As $x \geq p/3,\ p - x \leq 2p/3$.

It follows that $M(p) \geq p - \min\{x : (x, y) \in T_1(p) \cup T_2(p)\}$.

The Sister Beiter conjecture: $M(p) \geq (p+1)/2$

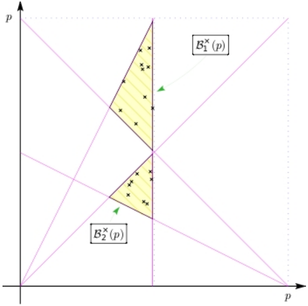


Crosses are at (x, y) with $xy \equiv 1 (\text{mod } p)$ ($p = 241$ in figure).
Each point (x, y) in a triangle leads to triples (p, q, r) with $q \equiv x (\text{mod } p)$ such that $A(pqr) \geq p - x$.
As $x \geq p/3,\ p - x \leq 2p/3$.

It follows that $M(p) \geq p - \min\{x : (x, y) \in T_1(p) \cup T_2(p)\}$.

For $p \geq 11$, at least one of the two triangles is non-empty.

The Sister Beiter conjecture: $M(p) \geq (p+1)/2$



Crosses are at (x, y) with $xy \equiv 1 \pmod{p}$ ($p = 241$ in figure).
Each point (x, y) in a triangle leads to triples (p, q, r) with $q \equiv x \pmod{p}$ such that $A(pqr) \geq p - x$.
As $x \geq p/3$, $p - x \leq 2p/3$.

It follows that $M(p) \geq p - \min\{x : (x, y) \in T_1(p) \cup T_2(p)\}$.

For $p \geq 11$, at least one of the two triangles is non-empty.
For p large enough, $M(p) \geq (2/3 - \epsilon)p$.

Sister Beiter and Kloosterman I

Sister Beiter and Kloosterman I

$$K(a,b;m) = \sum_{\substack{0\le x\le m-1\\ gcd(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^*)}$$

Sister Beiter and Kloosterman I

$$K(a,b;m) = \sum_{\substack{0 \le x \le m-1 \\ gcd(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^*)}$$

$|K(a,b;p)| \le 2\sqrt{p}$ (Weil, 1948)

Sister Beiter and Kloosterman I

$$K(a,b;m) = \sum_{\substack{0 \le x \le m-1 \\ gcd(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^*)}$$

$|K(a,b;p)| \le 2\sqrt{p}$ (Weil, 1948)

Modular hyperbola:
$\{(x,y) : 1 \le x \le p-1,\ 1 \le y \le p-1,\ xy \equiv 1 (\text{mod } p)\}$

Sister Beiter and Kloosterman I

$$K(a,b;m) = \sum_{\substack{0\le x\le m-1\\ gcd(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^*)}$$

$$|K(a,b;p)| \le 2\sqrt{p} \text{ (Weil, 1948)}$$

Modular hyperbola:

$\{(x,y) : 1 \le x \le p-1,\ 1 \le y \le p-1,\ xy \equiv 1 (\mathrm{mod}\ p)\}$

Let R be a rectangle with area A.

Sister Beiter and Kloosterman I

$$K(a,b;m) = \sum_{\substack{0\le x\le m-1\\ gcd(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^*)}$$

$$|K(a,b;p)| \le 2\sqrt{p} \text{ (Weil, 1948)}$$

Modular hyperbola:

$\{(x,y) : 1 \le x \le p-1,\ 1 \le y \le p-1,\ xy \equiv 1 (\bmod p)\}$

Let R be a rectangle with area A.

Put $N_R(p) := \#\{(x,y) \in R : xy \equiv 1 (\bmod p)\}$.

Sister Beiter and Kloosterman I

$$K(a,b;m) = \sum_{\substack{0\le x\le m-1\\ gcd(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^*)}$$

$$|K(a,b;p)| \le 2\sqrt{p} \text{ (Weil, 1948)}$$

Modular hyperbola:

$\{(x,y) : 1 \le x \le p-1,\ 1 \le y \le p-1,\ xy \equiv 1 (\text{mod } p)\}$

Let R be a rectangle with area A.

Put $N_R(p) := \#\{(x,y) \in R : xy \equiv 1(\text{mod } p)\}$.

We have $|N_R(p) - A/p| \le \sqrt{p}(2+\log p)^2$.

Sister Beiter and Kloosterman I

$$K(a,b;m) = \sum_{\substack{0\le x\le m-1\\ gcd(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^*)}$$

$|K(a,b;p)| \le 2\sqrt{p}$ (Weil, 1948)

Modular hyperbola:
$\{(x,y) : 1 \le x \le p-1,\ 1 \le y \le p-1,\ xy \equiv 1 (\mathrm{mod}\ p)\}$
Let R be a rectangle with area A.

Put $N_R(p) := \#\{(x,y) \in R : xy \equiv 1 (\mathrm{mod}\ p)\}$.

We have $|N_R(p) - A/p| \le \sqrt{p}(2 + \log p)^2$.

Problem: Estimate the number of modular hyperbolic points in the triangles $T_1(p)$ and $T_2(p)$.

Sister Beiter and Kloosterman I

$$K(a,b;m) = \sum_{\substack{0\le x\le m-1\\ gcd(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^*)}$$

$|K(a,b;p)| \le 2\sqrt{p}$ (Weil, 1948)

Modular hyperbola:
$\{(x,y) : 1 \le x \le p-1,\ 1 \le y \le p-1,\ xy \equiv 1 (\mathrm{mod}\ p)\}$
Let R be a rectangle with area A.

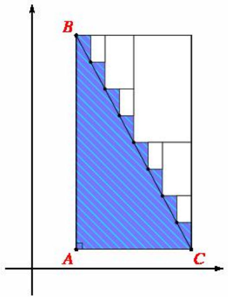
Put $N_R(p) := \#\{(x,y) \in R : xy \equiv 1(\mathrm{mod}\ p)\}$.

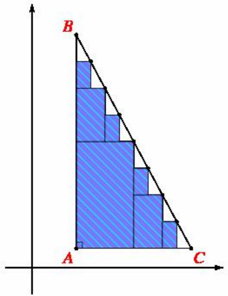
We have $|N_R(p) - A/p| \le \sqrt{p}(2+\log p)^2$.

Problem: Estimate the number of modular hyperbolic points in the triangles $T_1(p)$ and $T_2(p)$.
Cobeli, Gallot, M. and Zaharescu (Indag. Math., 2013):

$$\left|\#T_1(p) \cup T_2(p) - \frac{p}{16}\right| \le 24p^{3/4}\log p.$$

Sister Beiter and Kloosterman II





NUMERICAL SEMIGROUP APPROACH

Φ_{pq} and the Frobenius number

$S(p,q) = \{\alpha p + \beta q \ : \ \alpha \geq 0, \ \beta \geq 0\}$
Numerical semigroup generated by p and q

Φ_{pq} and the Frobenius number

$S(p,q) = \{\alpha p + \beta q \ : \ \alpha \geq 0, \ \beta \geq 0\}$
Numerical semigroup generated by p and q
Example: $S(3,5)$

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

Φ_{pq} and the Frobenius number

$S(p,q) = \{\alpha p + \beta q \ : \ \alpha \geq 0, \ \beta \geq 0\}$
Numerical semigroup generated by p and q
Example: $S(3,5)$

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

Largest number not in $S(p,q)$ is the Frobenius number

Φ_{pq} and the Frobenius number

$S(p,q) = \{\alpha p + \beta q \ : \ \alpha \geq 0, \ \beta \geq 0\}$
Numerical semigroup generated by p and q
Example: $S(3,5)$

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

Largest number not in $S(p,q)$ is the Frobenius number
$F(S(3,5)) = 7$

Φ_{pq} and the Frobenius number

$S(p,q) = \{\alpha p + \beta q \ : \ \alpha \geq 0, \ \beta \geq 0\}$
Numerical semigroup generated by p and q
Example: $S(3,5)$

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

Largest number not in $S(p,q)$ is the Frobenius number
$F(S(3,5)) = 7$
Claim: $\Phi_{pq}(X) = (1-X)\sum_{j \in S(p,q)} X^j$

Φ_{pq} and the Frobenius number

$S(p,q) = \{\alpha p + \beta q \ : \ \alpha \geq 0, \ \beta \geq 0\}$
Numerical semigroup generated by p and q
Example: $S(3,5)$

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

Largest number not in $S(p,q)$ is the Frobenius number
$F(S(3,5)) = 7$
Claim: $\Phi_{pq}(X) = (1 - X)\sum_{j \in S(p,q)} X^j$

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

(Sylvester, 1884)

Φ_{pq} and the Frobenius number

$S(p,q) = \{\alpha p + \beta q \;:\; \alpha \geq 0,\; \beta \geq 0\}$
Numerical semigroup generated by p and q
Example: $S(3,5)$

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

Largest number not in $S(p,q)$ is the Frobenius number
$F(S(3,5)) = 7$
Claim: $\Phi_{pq}(X) = (1-X)\sum_{j\in S(p,q)} X^j$

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

(Sylvester, 1884)
In example: $\Phi_{15}(X) = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$

Cyclotomic numerical semigroups, I

Cyclotomic numerical semigroups, I

with Pedro Garcia-Sanchez and Alexandru Ciolan

to appear in SIAM Journal on Discrete Mathematics (SIDMA)

Cyclotomic numerical semigroups, I

with Pedro Garcia-Sanchez and Alexandru Ciolan

to appear in SIAM Journal on Discrete Mathematics (SIDMA)

Note that $P_S(x) = (1 - X)\sum_{s \in S} X^s$ is a polynomial.

Cyclotomic numerical semigroups, I

with Pedro Garcia-Sanchez and Alexandru Ciolan

to appear in SIAM Journal on Discrete Mathematics (SIDMA)

Note that $P_S(x) = (1 - X)\sum_{s \in S} X^s$ is a polynomial.

It is called semigroup polynomial and can be rewritten as:

Cyclotomic numerical semigroups, I

with
Pedro Garcia-Sanchez and Alexandru Ciolan

to appear in SIAM Journal on Discrete Mathematics (SIDMA)

Note that $P_S(x) = (1 - X)\sum_{s\in S} X^s$ is a polynomial.

It is called semigroup polynomial and can be rewritten as:

$$P_S(X) = 1 + (X - 1)\sum_{s\notin S} X^s, \ \deg(P_S) = F(S) + 1.$$

Cyclotomic numerical semigroups, I

with Pedro Garcia-Sanchez and Alexandru Ciolan

to appear in SIAM Journal on Discrete Mathematics (SIDMA)

Note that $P_S(x) = (1 - X)\sum_{s \in S} X^s$ is a polynomial.

It is called semigroup polynomial and can be rewritten as:

$$P_S(X) = 1 + (X - 1)\sum_{s \notin S} X^s, \ \deg(P_S) = F(S) + 1.$$

Question: To what extent are the properties of S reflected in P_S and vice versa?

Cyclotomic numerical semigroups, I

with Pedro Garcia-Sanchez and Alexandru Ciolan

to appear in SIAM Journal on Discrete Mathematics (SIDMA)

Note that $P_S(x) = (1 - X)\sum_{s\in S} X^s$ is a polynomial.

It is called semigroup polynomial and can be rewritten as:

$$P_S(X) = 1 + (X - 1)\sum_{s\notin S} X^s, \ \deg(P_S) = F(S) + 1.$$

Question: To what extent are the properties of S reflected in P_S and vice versa?

Example: S is symmetric iff P_S is self-reciprocal

Cyclotomic numerical semigroups, I

with Pedro Garcia-Sanchez and Alexandru Ciolan

to appear in SIAM Journal on Discrete Mathematics (SIDMA)

Note that $P_S(x) = (1 - X)\sum_{s \in S} X^s$ is a polynomial.

It is called semigroup polynomial and can be rewritten as:

$$P_S(X) = 1 + (X - 1)\sum_{s \notin S} X^s, \ \deg(P_S) = F(S) + 1.$$

Question: To what extent are the properties of S reflected in P_S and vice versa?

Example: S is symmetric iff P_S is self-reciprocal

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

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$
$F(S) - S : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$
$F(S) - S : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$
Either $s \in S$ or $s \in F(S) - S$

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$
$F(S) - S : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$
Either $s \in S$ or $s \in F(S) - S$
$S = \langle 3, 7 \rangle$ is symmetric since $\Phi_{21}(X)$ is self-reciprocal
Definition: We say S is cyclotomic if the roots of P_S are on the unit circle.

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$
$F(S) - S : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$
Either $s \in S$ or $s \in F(S) - S$
$S = \langle 3, 7 \rangle$ is symmetric since $\Phi_{21}(X)$ is self-reciprocal
Definition: We say S is cyclotomic if the roots of P_S are on the unit circle.

$$\Rightarrow P_S(X) = \prod_{d \in D} \Phi_d(X)^{e_d}.$$

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$
$F(S) - S : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$
Either $s \in S$ or $s \in F(S) - S$
$S = \langle 3, 7 \rangle$ is symmetric since $\Phi_{21}(X)$ is self-reciprocal
Definition: We say S is cyclotomic if the roots of P_S are on the unit circle.

$$\Rightarrow P_S(X) = \prod_{d \in D} \Phi_d(X)^{e_d}.$$

Q: Is S cyclotomic iff S is symmetric?

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$
$F(S) - S : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$
Either $s \in S$ or $s \in F(S) - S$
$S = \langle 3, 7 \rangle$ is symmetric since $\Phi_{21}(X)$ is self-reciprocal
Definition: We say S is cyclotomic if the roots of P_S are on the unit circle.

$$\Rightarrow P_S(X) = \prod_{d \in D} \Phi_d(X)^{e_d}.$$

Q: Is S cyclotomic iff S is symmetric?
A: NO. E.g., $S = \langle 5, 6, 7, 8 \rangle$ (cyclotomic but not symmetric).

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$
$F(S) - S : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$
Either $s \in S$ or $s \in F(S) - S$
$S = \langle 3, 7 \rangle$ is symmetric since $\Phi_{21}(X)$ is self-reciprocal
Definition: We say S is cyclotomic if the roots of P_S are on the unit circle.

$$\Rightarrow P_S(X) = \prod_{d \in D} \Phi_d(X)^{e_d}.$$

Q: Is S cyclotomic iff S is symmetric?
A: NO. E.g., $S = \langle 5, 6, 7, 8 \rangle$ (cyclotomic but not symmetric).
True: If $e(S) \leq 3$ the answer is YES, however.

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$
$F(S) - S : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$
Either $s \in S$ or $s \in F(S) - S$
$S = \langle 3, 7 \rangle$ is symmetric since $\Phi_{21}(X)$ is self-reciprocal
Definition: We say S is cyclotomic if the roots of P_S are on the unit circle.

$$\Rightarrow P_S(X) = \prod_{d \in D} \Phi_d(X)^{e_d}.$$

Q: Is S cyclotomic iff S is symmetric?
A: NO. E.g., $S = \langle 5, 6, 7, 8 \rangle$ (cyclotomic but not symmetric).
True: If $e(S) \leq 3$ the answer is YES, however.
Conjecture: S is cyclotomic iff S is a complete intersection numerical semigroup.

Cyclotomic numerical semigroups, II

$S = \langle 3, 7 \rangle : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots$
$F(S) - S : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$
Either $s \in S$ or $s \in F(S) - S$
$S = \langle 3, 7 \rangle$ is symmetric since $\Phi_{21}(X)$ is self-reciprocal
Definition: We say S is cyclotomic if the roots of P_S are on the unit circle.

$$\Rightarrow P_S(X) = \prod_{d \in D} \Phi_d(X)^{e_d}.$$

Q: Is S cyclotomic iff S is symmetric?
A: NO. E.g., $S = \langle 5, 6, 7, 8 \rangle$ (cyclotomic but not symmetric).
True: If $e(S) \leq 3$ the answer is YES, however.
Conjecture: S is cyclotomic iff S is a complete intersection numerical semigroup.
Easy: S complete intersection $\Rightarrow$ S is cyclotomic.

Numerical semigroup view of gaps

Let $P_S(X) = a_0 + a_1 X + \cdots + a_k X^k$. Then

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

Numerical semigroup view of gaps

Let $P_S(X) = a_0 + a_1 X + \cdots + a_k X^k$. Then

$$a_s = \begin{cases} 1 & \text{if } s \in S \text{ and } s-1 \not\in S, \\ -1 & \text{if } s \not\in S \text{ and } s-1 \in S, \\ 0 & \text{otherwise.} \end{cases}$$

Camburu-Ciolan-Luca-M.-Shparlinksi (2016): For $p < q$ primes

Numerical semigroup view of gaps

Let $P_S(X) = a_0 + a_1 X + \cdots + a_k X^k$. Then

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

Camburu-Ciolan-Luca-M.-Shparlinksi (2016): For $p < q$ primes -$g(\Phi_{pq}) = p - 1$ and # maximum gaps $= 2\lfloor q/p \rfloor$;

Numerical semigroup view of gaps

Let $P_S(X) = a_0 + a_1 X + \cdots + a_k X^k$. Then

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

Camburu-Ciolan-Luca-M.-Shparlinksi (2016): For $p < q$ primes
-$g(\Phi_{pq}) = p - 1$ and # maximum gaps $= 2\lfloor q/p \rfloor$;
-$\Phi_{pq}(X)$ contains the sequence of consecutive coefficients of the form $\pm 1, \{0\}_m, \mp 1$ for all $m = 0, 1, \ldots, p-2$ if and only if $q \equiv \pm 1 (\mathrm{mod}\ p)$.

Numerical semigroup view of gaps

Let $P_S(X) = a_0 + a_1X + \cdots + a_kX^k$. Then

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

Camburu-Ciolan-Luca-M.-Shparlinksi (2016): For $p < q$ primes
-$g(\Phi_{pq}) = p - 1$ and # maximum gaps $= 2\lfloor q/p \rfloor$;
-$\Phi_{pq}(X)$ contains the sequence of consecutive coefficients of the form $\pm 1, \{0\}_m, \mp 1$ for all $m = 0, 1, \ldots, p-2$ if and only if $q \equiv \pm 1 (\mathrm{mod}\ p)$.
-Let $S = \langle p, q \rangle$. Coefficients gaps are related to gapblocks and elementblocks of S.

Thank you for listening!

Non-zero binary coefficients

Let $\theta(pq)$ denote number of non-zero coefficients of $\Phi_{pq}(x)$.

Non-zero binary coefficients

Let $\theta(pq)$ denote number of non-zero coefficients of $\Phi_{pq}(x)$.
We have $\theta(m) = \rho\sigma + (q - \rho)(p - \sigma) = 2\rho\sigma - 1$.
Recall that

$$\rho p + \sigma q = 1 + pq.$$

Non-zero binary coefficients

Let $\theta(pq)$ denote number of non-zero coefficients of $\Phi_{pq}(x)$.
We have $\theta(m) = \rho\sigma + (q-\rho)(p-\sigma) = 2\rho\sigma - 1$.
Recall that

$$\rho p + \sigma q = 1 + pq.$$

This result is due to Carlitz (1966).

Non-zero binary coefficients

Let $\theta(pq)$ denote number of non-zero coefficients of $\Phi_{pq}(x)$.
We have $\theta(m) = \rho\sigma + (q - \rho)(p - \sigma) = 2\rho\sigma - 1$.
Recall that

$$\rho p + \sigma q = 1 + pq.$$

This result is due to Carlitz (1966).
Example. Take $p = 5$, $q = 7$.

Non-zero binary coefficients

Let $\theta(pq)$ denote number of non-zero coefficients of $\Phi_{pq}(x)$.
We have $\theta(m) = \rho\sigma + (q-\rho)(p-\sigma) = 2\rho\sigma - 1$.
Recall that

$$\rho p + \sigma q = 1 + pq.$$

This result is due to Carlitz (1966).
Example. Take $p = 5$, $q = 7$.

$$\rho = 5^{-1} (\text{mod } 7) = 3,$$

Non-zero binary coefficients

Let $\theta(pq)$ denote number of non-zero coefficients of $\Phi_{pq}(x)$.
We have $\theta(m) = \rho\sigma + (q-\rho)(p-\sigma) = 2\rho\sigma - 1$.
Recall that

$$\rho p + \sigma q = 1 + pq.$$

This result is due to Carlitz (1966).
Example. Take $p = 5$, $q = 7$.

$$\rho = 5^{-1} (\mathrm{mod}\ 7) = 3,$$

$$\sigma = 7^{-1} (\mathrm{mod}\ 5) = 3.$$

Non-zero binary coefficients

Let $\theta(pq)$ denote number of non-zero coefficients of $\Phi_{pq}(x)$.
We have $\theta(m) = \rho\sigma + (q - \rho)(p - \sigma) = 2\rho\sigma - 1$.
Recall that

$$\rho p + \sigma q = 1 + pq.$$

This result is due to Carlitz (1966).
Example. Take $p = 5$, $q = 7$.

$$\rho = 5^{-1} (\text{mod } 7) = 3,$$

$$\sigma = 7^{-1} (\text{mod } 5) = 3.$$

Hence

$$\theta(35) = 2 \cdot 3 \cdot 3 - 1 = 17.$$

Sparse binary cyclotomic polynomials

Put $H_\gamma(x) := \{m = pq \le x : \theta(m) \le m^{1/2+\gamma}\}$.

Sparse binary cyclotomic polynomials

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

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

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

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

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

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

The Roşu construction I

Question: Can one construct non-Beiter ternary Φ_n with an optimally large set of coefficients. That is given $l \geq 1$ can one construct Φ_{pqr} with $C(pqr) = [-(p-1)/2 + l, (p+1)/2 + l]$?

The Roşu construction I

Question: Can one construct non-Beiter ternary Φ_n with an optimally large set of coefficients. That is given $l \geq 1$ can one construct Φ_{pqr} with $C(pqr) = [-(p-1)/2 + l, (p+1)/2 + l]$?

Eugenia
Roşu
PhD
student,
Berkeley

The Roşu construction II

-For every $l \geq 1$ Eugenia answered the Question in the positive.

The Roşu construction II

-For every $l \geq 1$ Eugenia answered the Question in the positive.

-Leads to a conjecture of Wilms (earlier intern) being resolved.

The Roşu construction II

-For every $l \geq 1$ Eugenia answered the Question in the positive.

-Leads to a conjecture of Wilms (earlier intern) being resolved.

-Leads to triangle $T_3(p)$ satisfying $T_2(p) \subset T_3(p)$

The Roşu construction II

-For every $l \geq 1$ Eugenia answered the Question in the positive.

-Leads to a conjecture of Wilms (earlier intern) being resolved.

-Leads to triangle $T_3(p)$ satisfying $T_2(p) \subset T_3(p)$

-Leads to $M_R(p) \leq M(p)$.

-Gallot/Moree construction gives $M_{GM}(p) \leq M(p)$.

The Roşu construction II

-For every $l \geq 1$ Eugenia answered the Question in the positive.

-Leads to a conjecture of Wilms (earlier intern) being resolved.

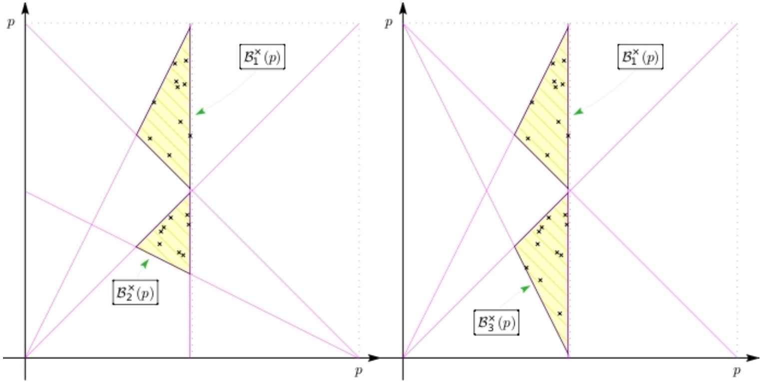
-Leads to triangle $T_3(p)$ satisfying $T_2(p) \subset T_3(p)$

-Leads to $M_R(p) \leq M(p)$.

-Gallot/Moree construction gives $M_{GM}(p) \leq M(p)$.

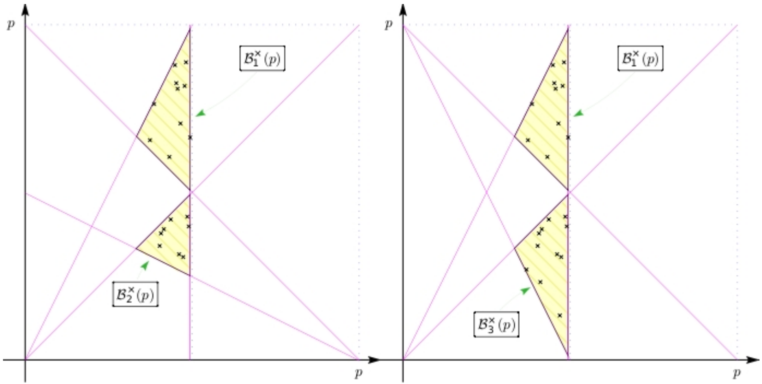
There are likely infinitely many primes p with $M_R(p) > M_{GM}(p)$:
$29, 37, 41, 83, 107, 109, 149, 179, 181, 223, 227, 233, 241, 269 \ldots$

Gallot/Moree versus Roşu $p = 241$



$xy \equiv 1 (\text{mod } p)$

Gallot/Moree versus Roşu $p = 241$



$xy \equiv 1 (\mathrm{mod}\ p)$

$B_1(p) = \{x : 1 \le x \le \frac{p-3}{2},\ x + y \ge p,\ y \le 2x\}$

$B_2(p) = \{x : 1 \le x \le \frac{p-3}{2},\ x + 2y + 1 \ge p,\ x > y\}$

$B_3(p) = \{x : 1 \le x \le \frac{p-3}{2},\ 2x + y \ge p,\ x \ge y\}$

Gallot/Moree versus Roşu $p = 29$