

p -adically resolving trinomials

Robert Dougherty-Bliss, [Dartmouth College](#)

Computer Assisted Mathematics, St. Petersburg (online)

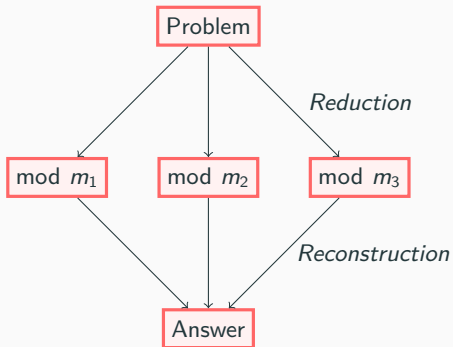
15 July 2025

Joint work with Mits Kobayashi, Natalya Ter-Saakov, and Eugene Zima

Computations are often sped up with the Chinese Remainder Theorem.

Criteria for “good” moduli:

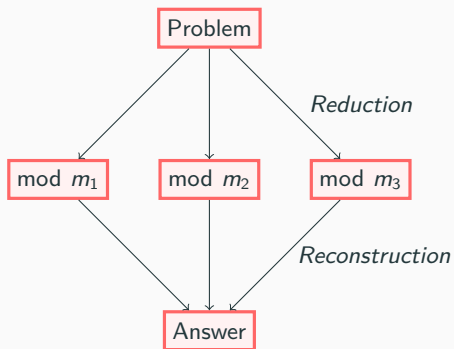
- Easy to find
- Fast to reduce and reconstruct
- Roughly the same size (balanced)



Computations are often sped up with the Chinese Remainder Theorem.

Criteria for “good” moduli:

- Easy to find
- Fast to reduce and reconstruct
- Roughly the same size (balanced)



Chen and Zima (2023) proposed “trinomial” moduli:

$$2^n - 2^k + 1 \quad (n \text{ is fixed, } 0 < k < n)$$

These are perfectly balanced and have fast reduction / reconstruction.

These moduli do something nice (sometimes).

$$m_1 = 2^5 - 2^1 + 1$$

$$m_2 = 2^5 - 2^3 + 1$$

$$m_1^{-1} \bmod m_2 = -2^2.$$

These moduli do something nice (sometimes).

$$m_1 = 2^5 - 2^1 + 1$$

$$m_2 = 2^5 - 2^3 + 1$$

$$m_1^{-1} \bmod m_2 = -2^2.$$

$$m_1 = 2^5 - 2^1 + 1$$

$$m_2 = 2^5 - 2^3 + 1$$

$$m_1^{-1} = -2^2 \bmod m_2$$

scale exponents by c

\implies

These moduli do something nice (sometimes).

$$\begin{aligned}m_1 &= 2^5 - 2^1 + 1 \\m_2 &= 2^5 - 2^3 + 1 \\m_1^{-1} \bmod m_2 &= -2^2.\end{aligned}$$

$$\begin{aligned}m_1 &= 2^5 - 2^1 + 1 \\m_2 &= 2^5 - 2^3 + 1 \\m_1^{-1} &= -2^2 \bmod m_2\end{aligned}$$

scale exponents by c
 \implies

$$\begin{aligned}m_1 &= 2^{5c} - 2^c + 1 \\m_2 &= 2^{5c} - 2^{3c} + 1\end{aligned}$$

$$m_1^{-1} = -2^{2c} \bmod m_2$$

The modular inverse $m_1^{-1} \bmod m_2$ is stable under scaling!

These moduli do something nice (sometimes).

$$\begin{aligned}m_1 &= 2^5 - 2^1 + 1 \\m_2 &= 2^5 - 2^3 + 1 \\m_1^{-1} \bmod m_2 &= -2^2.\end{aligned}$$

$$\begin{array}{ccc}m_1 = 2^5 - 2^1 + 1 & & m_1 = 2^{5c} - 2^c + 1 \\m_2 = 2^5 - 2^3 + 1 & \text{scale exponents by } c & m_2 = 2^{5c} - 2^{3c} + 1 \\m_1^{-1} = -2^2 \bmod m_2 & \implies & \\ & & m_1^{-1} = -2^{2c} \bmod m_2\end{array}$$

The modular inverse $m_1^{-1} \bmod m_2$ is stable under scaling!

We can make c very large but the inverse has a “constant” pattern.

Nice inverses do not always happen.

Definition

$x^n - x^k + 1$ and $x^n - x^j + 1$ *dyadically resolve* if their resultant is a signed power of 2.

The inverse sequence

$$(2^{cn} - 2^{ck} + 1)^{-1} \bmod (2^{cn} - 2^{cj} + 1)$$

will be “nice” if and only if $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve.

Basic questions

Nice inverses do not always happen.

Definition

$x^n - x^k + 1$ and $x^n - x^j + 1$ *dyadically resolve* if their resultant is a signed power of 2.

The inverse sequence

$$(2^{cn} - 2^{ck} + 1)^{-1} \bmod (2^{cn} - 2^{cj} + 1)$$

will be “nice” if and only if $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve.

Basic questions

1. When do $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve?

Nice inverses do not always happen.

Definition

$x^n - x^k + 1$ and $x^n - x^j + 1$ *dyadically resolve* if their resultant is a signed power of 2.

The inverse sequence

$$(2^{cn} - 2^{ck} + 1)^{-1} \bmod (2^{cn} - 2^{cj} + 1)$$

will be “nice” if and only if $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve.

Basic questions

1. When do $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve?
2. Are there arbitrarily large sets of dyadically resolving trinomials?

Nice inverses do not always happen.

Definition

$x^n - x^k + 1$ and $x^n - x^j + 1$ *dyadically resolve* if their resultant is a signed power of 2.

The inverse sequence

$$(2^{cn} - 2^{ck} + 1)^{-1} \bmod (2^{cn} - 2^{cj} + 1)$$

will be “nice” if and only if $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve.

Basic questions

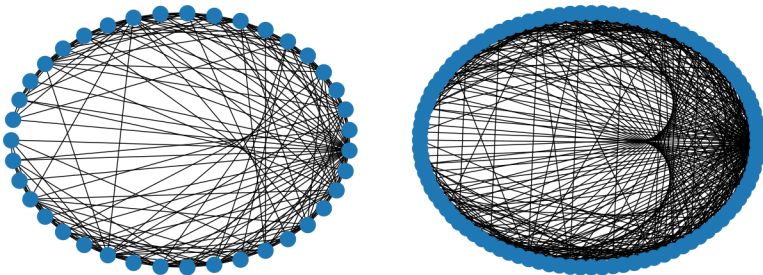
1. When do $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve?
2. Are there arbitrarily large sets of dyadically resolving trinomials?
3. How can we efficiently find these sets?

Definition

Let $T(n)$ be the graph with vertices $\{1, 2, 3, \dots, n-1\}$ that contains the edge $\{k, j\}$ if and only if $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve.

Definition

Let $T(n)$ be the graph with vertices $\{1, 2, 3, \dots, n-1\}$ that contains the edge $\{k, j\}$ if and only if $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve.

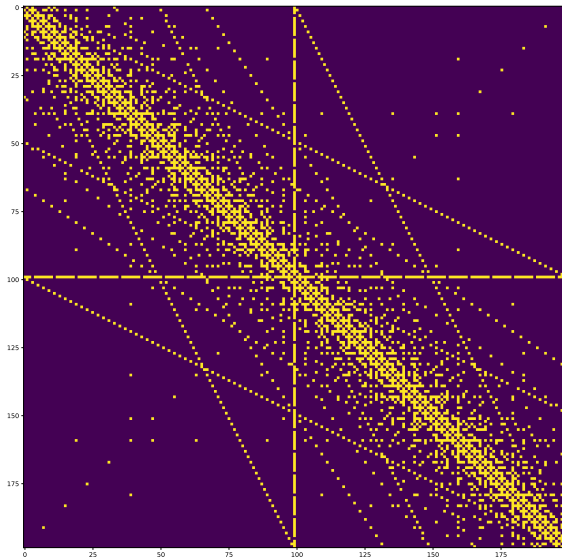


$T(40)$ and $T(100)$

Question 1

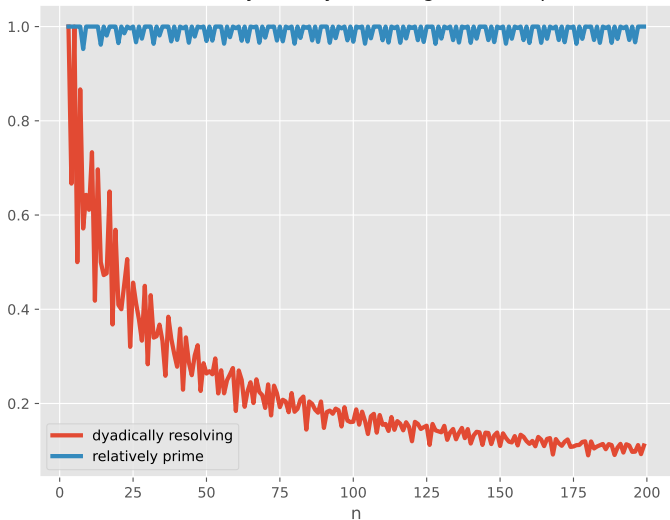
When is $\text{res}(x^n - x^k + 1, x^n - x^j + 1)$ a signed power of 2?

What are the edges of $T(n)$?



Adjacency matrix of $T(200)$.

Percent of dyadically resolving trinomial pairs



Very few powers of 2! But lots of relatively prime pairs?

Theorem (RDB, Kobayashi, Ter-Saakov, Zima)

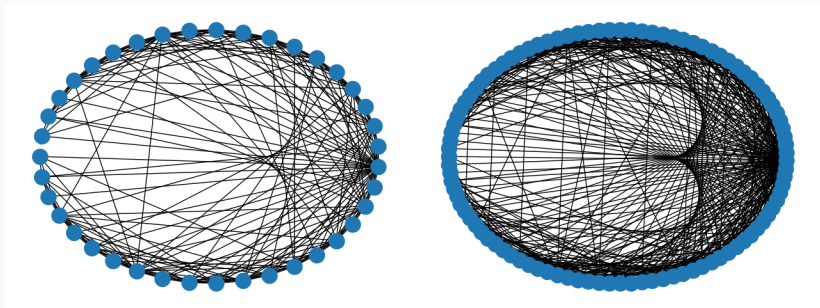
If $g(x) := \gcd(x^n - x^k + 1, x^n - x^j + 1) \neq 1$, then:

- n is even;
- $k - j$ is divisible by 6; and
- $g(x)$ is a product of cyclotomic polynomials whose orders are multiples of 6.

Approximately 97% of all pairs of trinomials for large n are relatively prime.

We have no corresponding statement for dyadically resolving pairs.

The proportion probably goes to 0.



$T(40)$ and $T(100)$

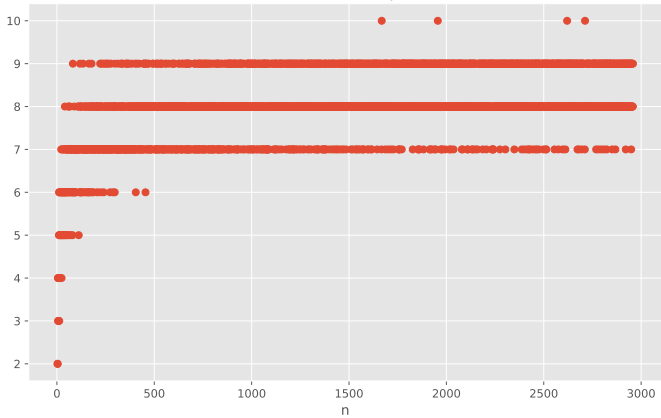
Questions 2 and 3

What is the largest set of *pairwise dyadically resolving* trinomials of degree n ?

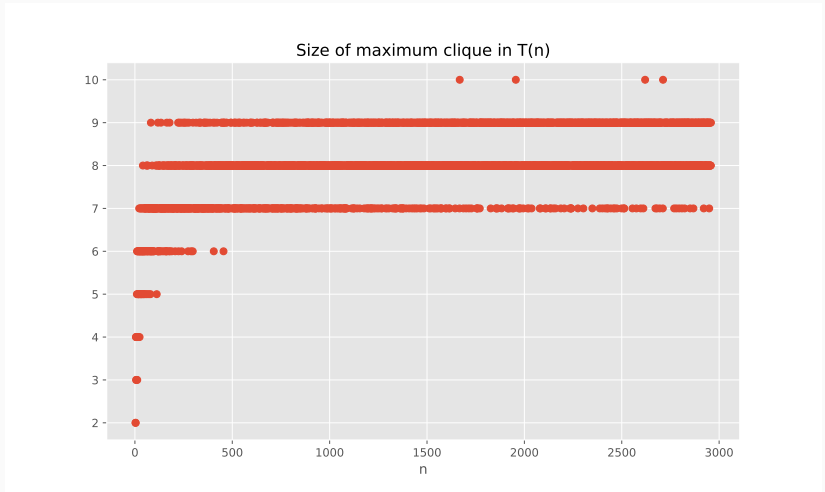
What is the largest clique in $T(n)$?

Computing maximum cliques is fast!

Size of maximum clique in $T(n)$



Clique growth looks slow, but...



Clique growth looks slow, but...

Theorem

The size of the largest clique in $T(n)$ goes to ∞ as $n \rightarrow \infty$.

We do not know the true growth rate of the largest cliques.

We have not found a *reasonable* clique of size 11.

clique size k	smallest n
2	3
3	5
4	5
5	10
6	11
7	22
8	41
9	82
10	1668
11	> 3000

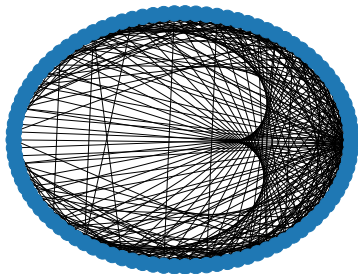
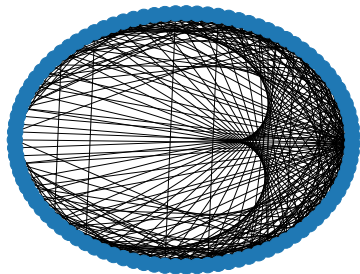
General primes

There is nothing special about 2 in most of this.

Definition

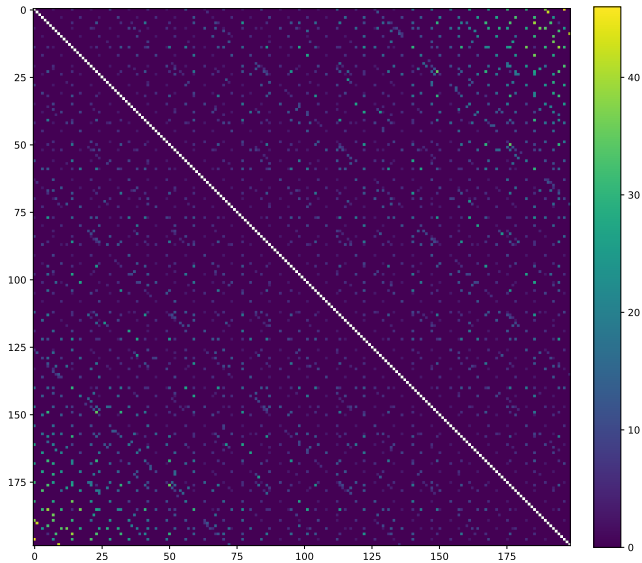
Two monic polynomials p -adically resolve if their resultant is $\pm p^k$.

This seems more natural. We suspect that almost everything is the same.

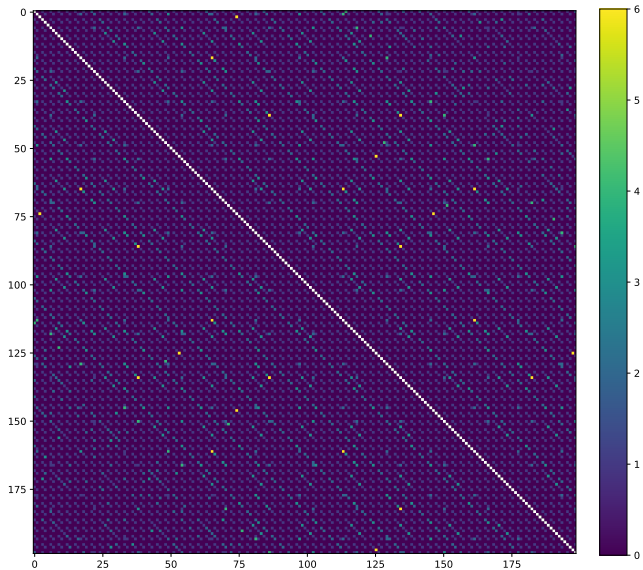


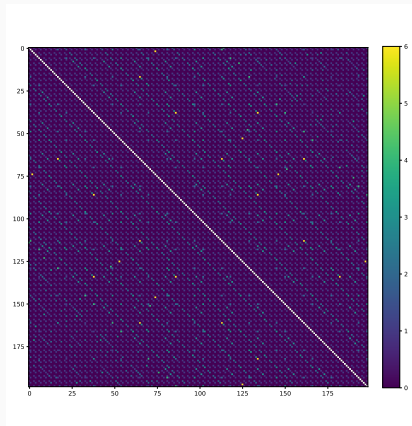
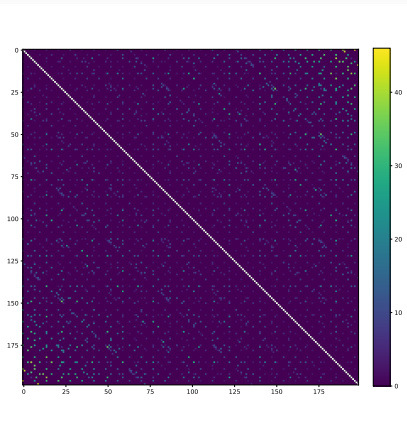
$T(100)$ for $p = 11$ and $p = 17$.

Heatmap of the 2-adic valuation of $\text{res}(x^{200} - x^j + 1, x^{200} - x^j + 1)$.



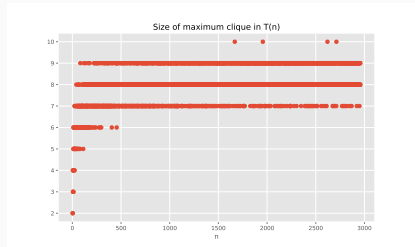
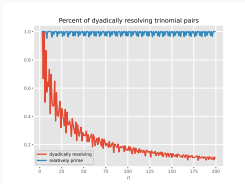
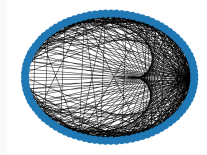
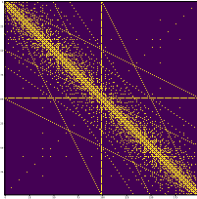
Heatmap of the 7-adic valuation of $\text{res}(x^{200} - x^j + 1, x^{200} - x^j + 1)$.





But maybe there are important differences!

Open questions



True growth of largest clique sizes?

Edge density of $T(n)$?

What happens with other primes?