Relative primality and other properties of trinomials

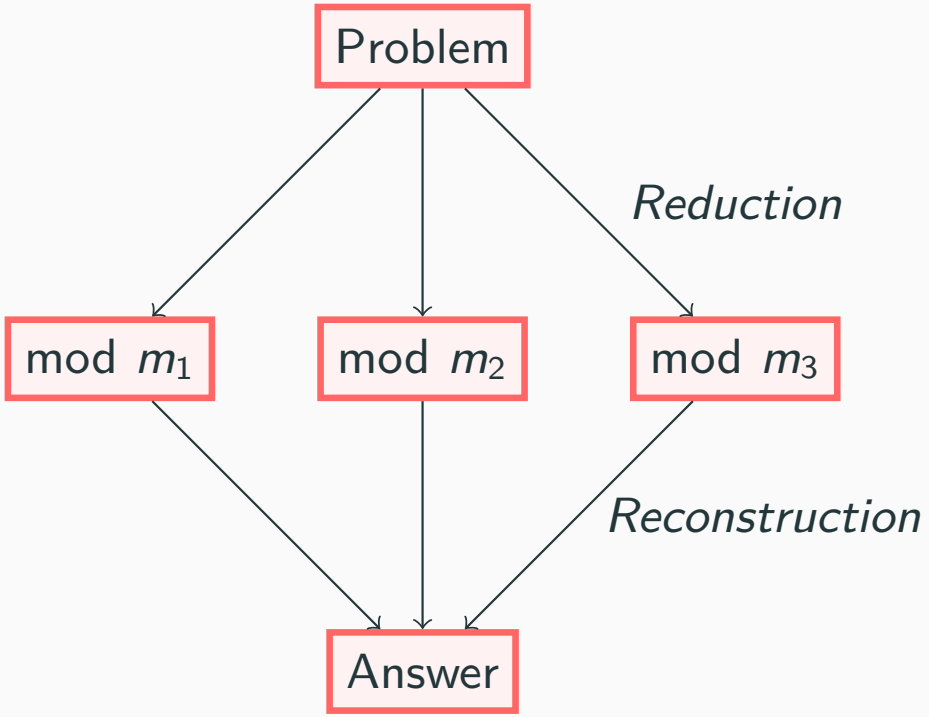
Robert Dougherty-Bliss, Dartmouth College

International Conference *Computer Algebra*, Moscow (online)
24 June 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:

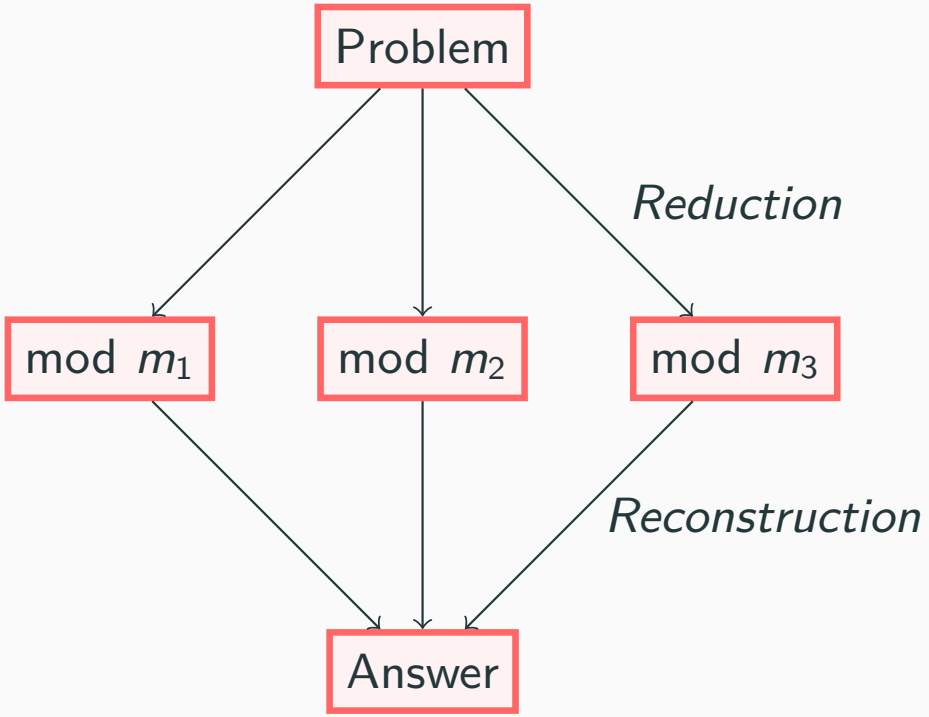
- Easy to find
- Fast to reduce and reconstruct
- Roughly the same size (balanced)



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.

Fast reconstruction

Imagine Chinese Remaindering with these moduli:

$$m_1 = 2^5 - 2^1 + 1$$
$$m_2 = 2^5 - 2^3 + 1.$$

Reconstruction of x looks like this:

$$A = x \bmod m_1$$
$$B = x \bmod m_2$$

Fast reconstruction

Imagine Chinese Remaindering with these moduli:

$$m_1 = 2^5 - 2^1 + 1$$
$$m_2 = 2^5 - 2^3 + 1.$$

Reconstruction of x looks like this:

$$A = x \bmod m_1 \qquad x = x_0 + x_1 m_1$$
$$B = x \bmod m_2 \qquad \Longrightarrow$$

Fast reconstruction

Imagine Chinese Remaindering with these moduli:

$$m_1 = 2^5 - 2^1 + 1$$
$$m_2 = 2^5 - 2^3 + 1.$$

Reconstruction of x looks like this:

$$\begin{array}{lll} A = x \bmod m_1 & x = x_0 + x_1 m_1 & x_0 = A \\ B = x \bmod m_2 & \Longrightarrow & x_1 = (B - x_0) m_1^{-1} \pmod{m_2} \end{array}$$

By chance,

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

so the multiplication by $m_2^{-1} \bmod m_2$ is very fast.

There is more to these moduli.

$$m_1 = 2^5 - 2^1 + 1$$
$$m_2 = 2^5 - 2^3 + 1$$
$$m_1^{-1} = -2^2 \bmod m_2$$

scale exponents by c

$$\Longrightarrow$$

There is more to these moduli.

$$m_1 = 2^5 - 2^1 + 1$$
$$m_2 = 2^5 - 2^3 + 1$$
$$m_1^{-1} = -2^2 \bmod m_2$$

scale exponents by c

$\Longrightarrow$

$$m_1 = 2^{5c} - 2^c + 1$$
$$m_2 = 2^{5c} - 2^{3c} + 1$$

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

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

There is more to these moduli.

$$m_1 = 2^5 - 2^1 + 1$$
$$m_2 = 2^5 - 2^3 + 1$$
$$m_1^{-1} = -2^2 \bmod m_2$$

scale exponents by c

$\Longrightarrow$

$$m_1 = 2^{5c} - 2^c + 1$$
$$m_2 = 2^{5c} - 2^{3c} + 1$$

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

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

We can make c very large, but the reconstruction step

$$\begin{aligned} x_1 &= (B - x_0) m_1^{-1} \pmod{m_2} \\ &= -2^{2c}(B - x_0) \pmod{m_2} \end{aligned}$$

is always a bitshift.

Reconstruction is linear time (relative to the bitlength of moduli).

Nice inverses do not always happen.

$$(2^6 - 2^2 + 1)^{-1} \equiv 2^4 - 2^2 + 1 \pmod{2^6 - 2^5 + 1}$$

Nice inverses do not always happen.

$$(2^6 - 2^2 + 1)^{-1} \equiv 2^4 - 2^2 + 1 \pmod{2^6 - 2^5 + 1}$$

$$(2^{12} - 2^4 + 1)^{-1} \equiv N/A \pmod{2^{12} - 2^{10} + 1} \quad \text{(GCD is 7)}$$

Nice inverses do not always happen.

$$(2^6 - 2^2 + 1)^{-1} \equiv 2^4 - 2^2 + 1 \pmod{2^6 - 2^5 + 1}$$

$$(2^{12} - 2^4 + 1)^{-1} \equiv N/A \pmod{2^{12} - 2^{10} + 1} \quad \text{(GCD is 7)}$$

$$(2^{18} - 2^8 + 1)^{-1} \equiv 2^{18} - 2^{16} + 2^{14} + 2^{11} - 2^7 + 2^3 + 1 \pmod{2^{18} - 2^{15} + 1}$$

Nice inverses do not always happen.

$$(2^6 - 2^2 + 1)^{-1} \equiv 2^4 - 2^2 + 1 \pmod{2^6 - 2^5 + 1}$$

$$(2^{12} - 2^4 + 1)^{-1} \equiv N/A \pmod{2^{12} - 2^{10} + 1} \quad \text{(GCD is 7)}$$

$$(2^{18} - 2^8 + 1)^{-1} \equiv 2^{18} - 2^{16} + 2^{14} + 2^{11} - 2^7 + 2^3 + 1 \pmod{2^{18} - 2^{15} + 1}$$

$$(2^{6c} - 2^{2c} + 1)^{-1} \equiv ??? \pmod{2^{6c} - 2^{5c} + 1}$$

Basic questions

$$2^n - 2^k + 1$$

Nice inverses do not always happen.

$$(2^6 - 2^2 + 1)^{-1} \equiv 2^4 - 2^2 + 1 \pmod{2^6 - 2^5 + 1}$$

$$(2^{12} - 2^4 + 1)^{-1} \equiv N/A \pmod{2^{12} - 2^{10} + 1} \quad \text{(GCD is 7)}$$

$$(2^{18} - 2^8 + 1)^{-1} \equiv 2^{18} - 2^{16} + 2^{14} + 2^{11} - 2^7 + 2^3 + 1 \pmod{2^{18} - 2^{15} + 1}$$

$$(2^{6c} - 2^{2c} + 1)^{-1} \equiv ??? \pmod{2^{6c} - 2^{5c} + 1}$$

Basic questions

$$2^n - 2^k + 1$$

1. When do two trinomial moduli have "good" inverses?

Nice inverses do not always happen.

$$(2^6 - 2^2 + 1)^{-1} \equiv 2^4 - 2^2 + 1 \pmod{2^6 - 2^5 + 1}$$

$$(2^{12} - 2^4 + 1)^{-1} \equiv N/A \pmod{2^{12} - 2^{10} + 1} \quad \text{(GCD is 7)}$$

$$(2^{18} - 2^8 + 1)^{-1} \equiv 2^{18} - 2^{16} + 2^{14} + 2^{11} - 2^7 + 2^3 + 1 \pmod{2^{18} - 2^{15} + 1}$$

$$(2^{6c} - 2^{2c} + 1)^{-1} \equiv ??? \pmod{2^{6c} - 2^{5c} + 1}$$

Basic questions

$$2^n - 2^k + 1$$

1. When do two trinomial moduli have "good" inverses?
2. Are there arbitrarily large sets of moduli that have pairwise "good" inverses?

Nice inverses do not always happen.

$$(2^6 - 2^2 + 1)^{-1} \equiv 2^4 - 2^2 + 1 \pmod{2^6 - 2^5 + 1}$$

$$(2^{12} - 2^4 + 1)^{-1} \equiv N/A \pmod{2^{12} - 2^{10} + 1} \quad \text{(GCD is 7)}$$

$$(2^{18} - 2^8 + 1)^{-1} \equiv 2^{18} - 2^{16} + 2^{14} + 2^{11} - 2^7 + 2^3 + 1 \pmod{2^{18} - 2^{15} + 1}$$

$$(2^{6c} - 2^{2c} + 1)^{-1} \equiv ??? \pmod{2^{6c} - 2^{5c} + 1}$$

Basic questions

$$2^n - 2^k + 1$$

1. When do two trinomial moduli have "good" inverses?
2. Are there arbitrarily large sets of moduli that have pairwise "good" inverses?
3. How can we efficiently find these sets?

Good moduli

$$2^5 - 2^1 + 1$$

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

Inverses come from polynomial identity:

$$(x^5 - x + 1)(-x^2) + (x^5 - x^3 + 1)(x^2 + 1) = 1.$$

Good moduli

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

Inverses come from polynomial identity:

$$(x^5 - x + 1)(-x^2) + (x^5 - x^3 + 1)(x^2 + 1) = 1.$$

Bad moduli

$$2^6 - 2^2 + 1$$
$$2^6 - 2^5 + 1$$

GCD equation:

$$(x^6 - x^2 + 1)(-x^5 + 4x^4 - 5x^3 + x^2 - 3x + 2) + (x^6 - x^5 + 1)(x^5 - 3x^4 + 2x^3 + x^2 + 3x + 5) = 7.$$

The 7 ruins us!

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 (new)

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 (new)

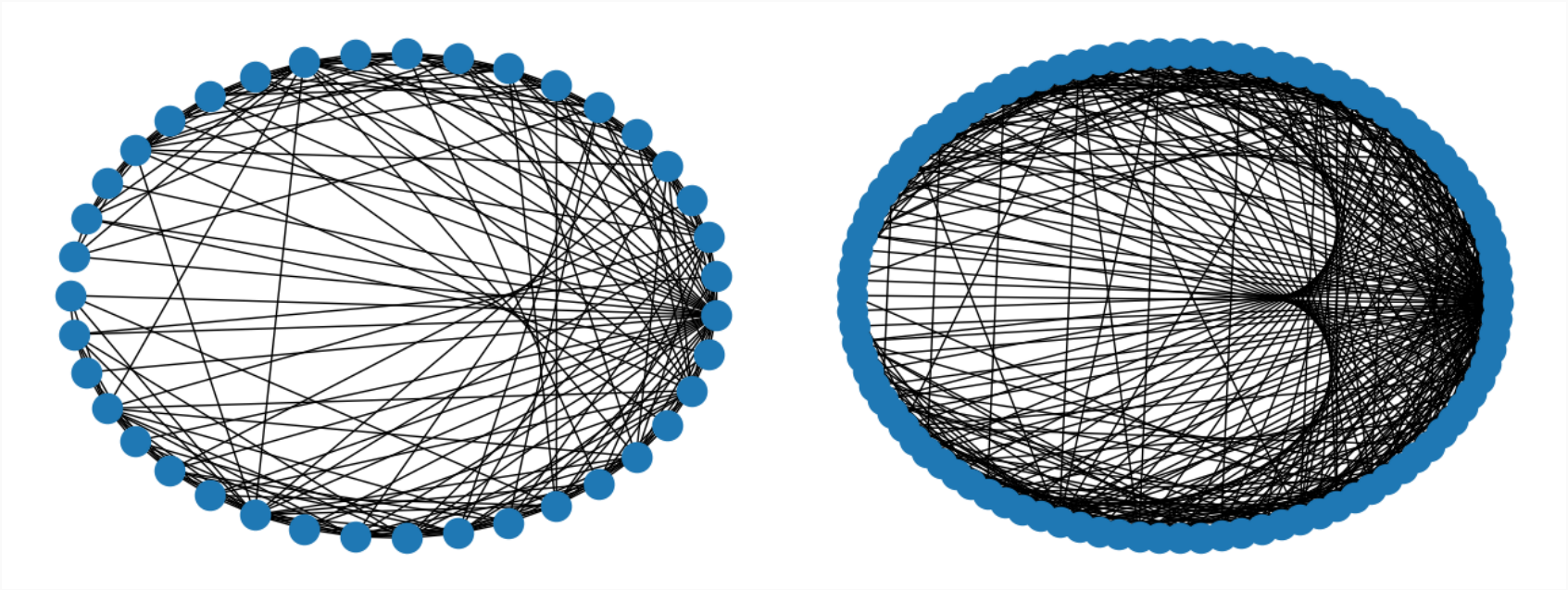
1. When do $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve?
2. Are there arbitrarily large sets of dyadically resolving trinomials?
3. How can we efficiently find these sets?

Definition

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

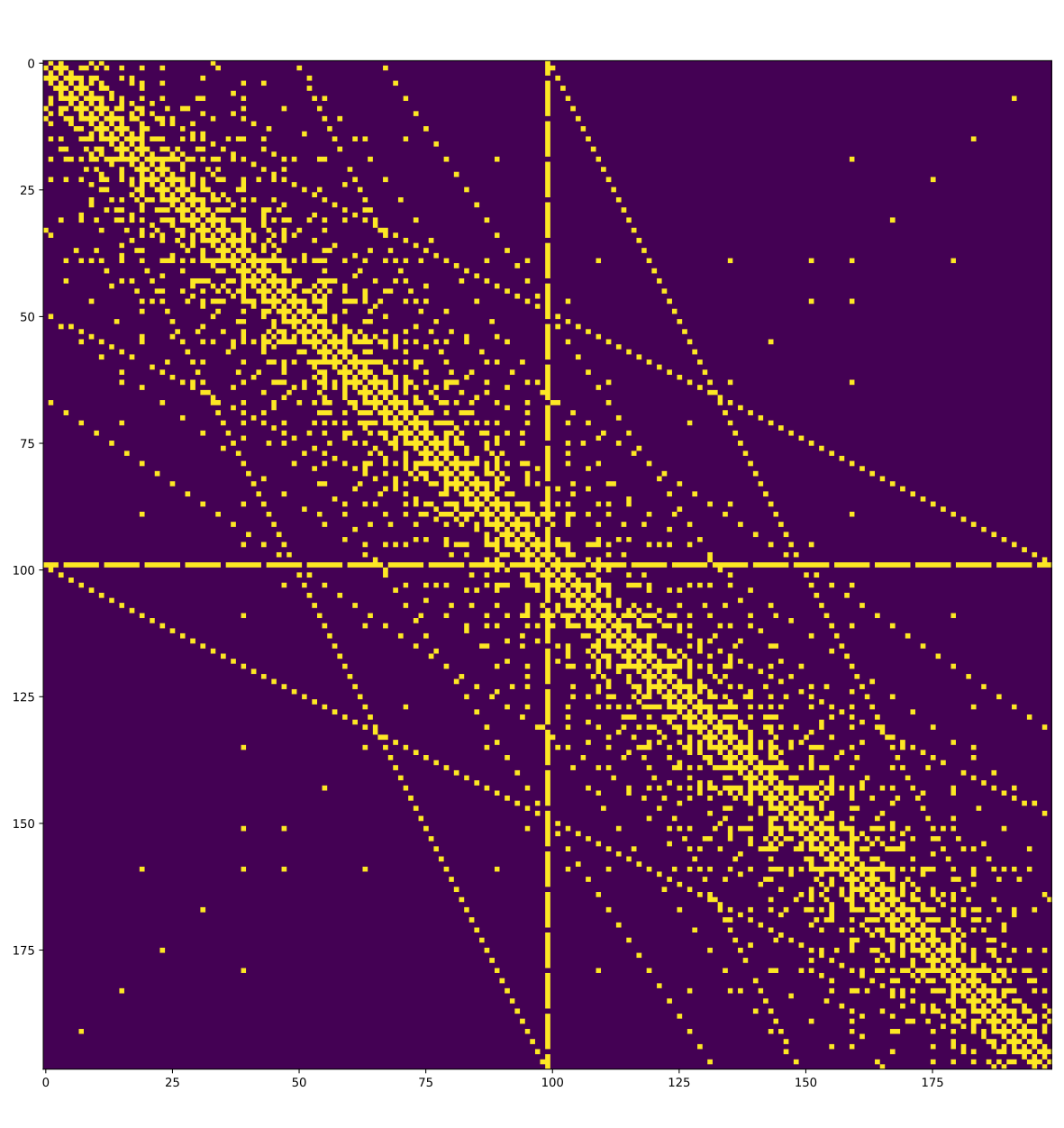


$T(40)$ and $T(100)$

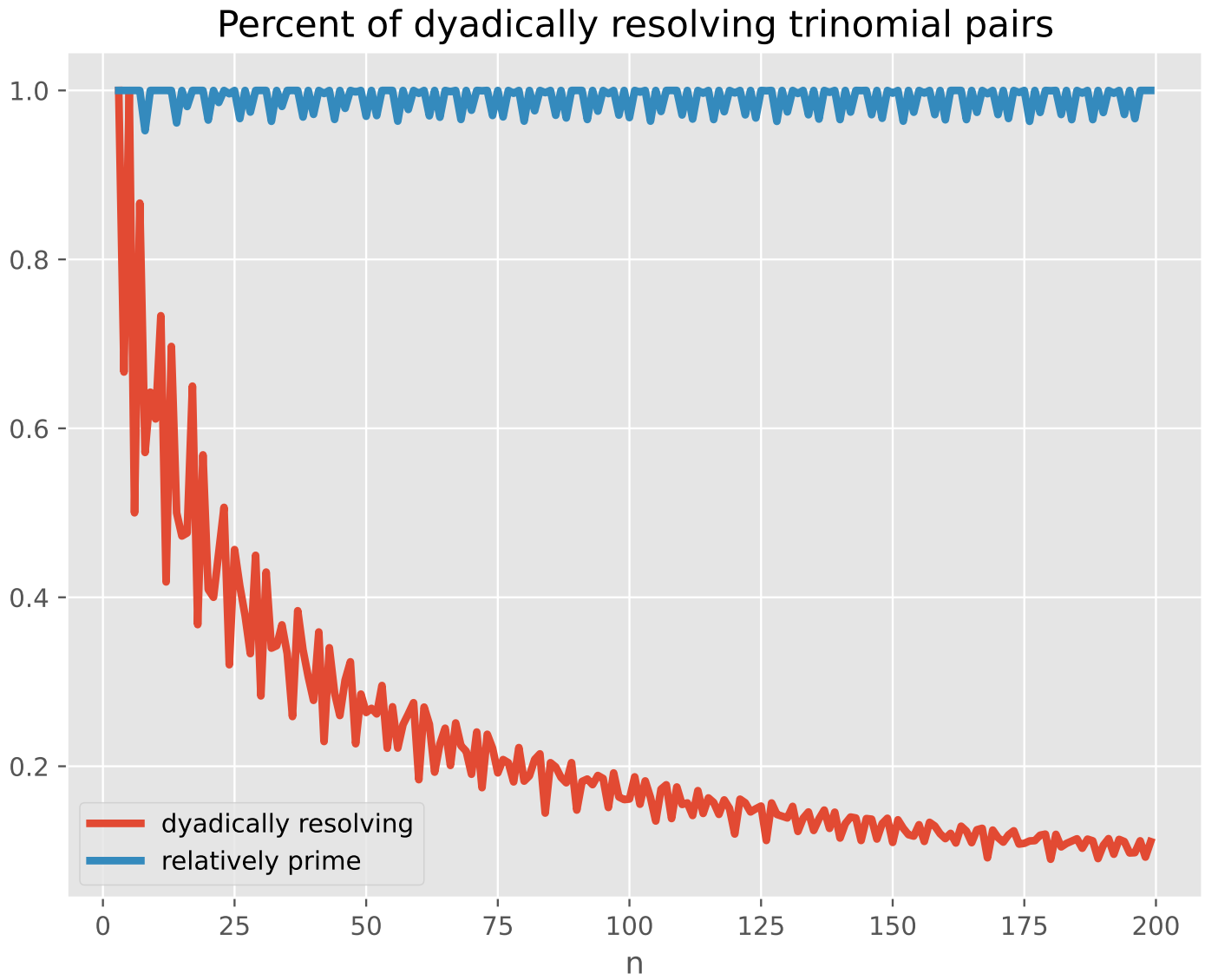
Question 1

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

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



Adjacency matrix of $T(200)$.



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

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

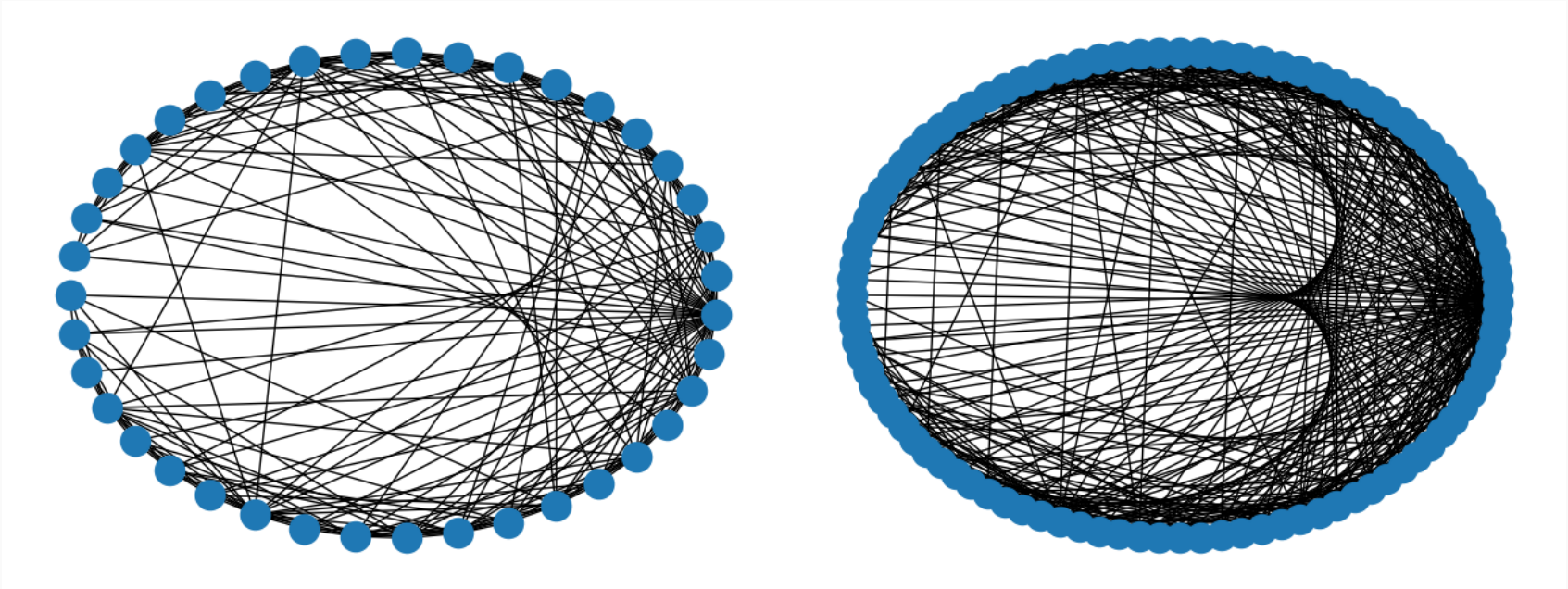
If $g(x) := \gcd(x^n - x^k + 1, x^n - x^j + 1) \neq 1$, *then:*

- 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.



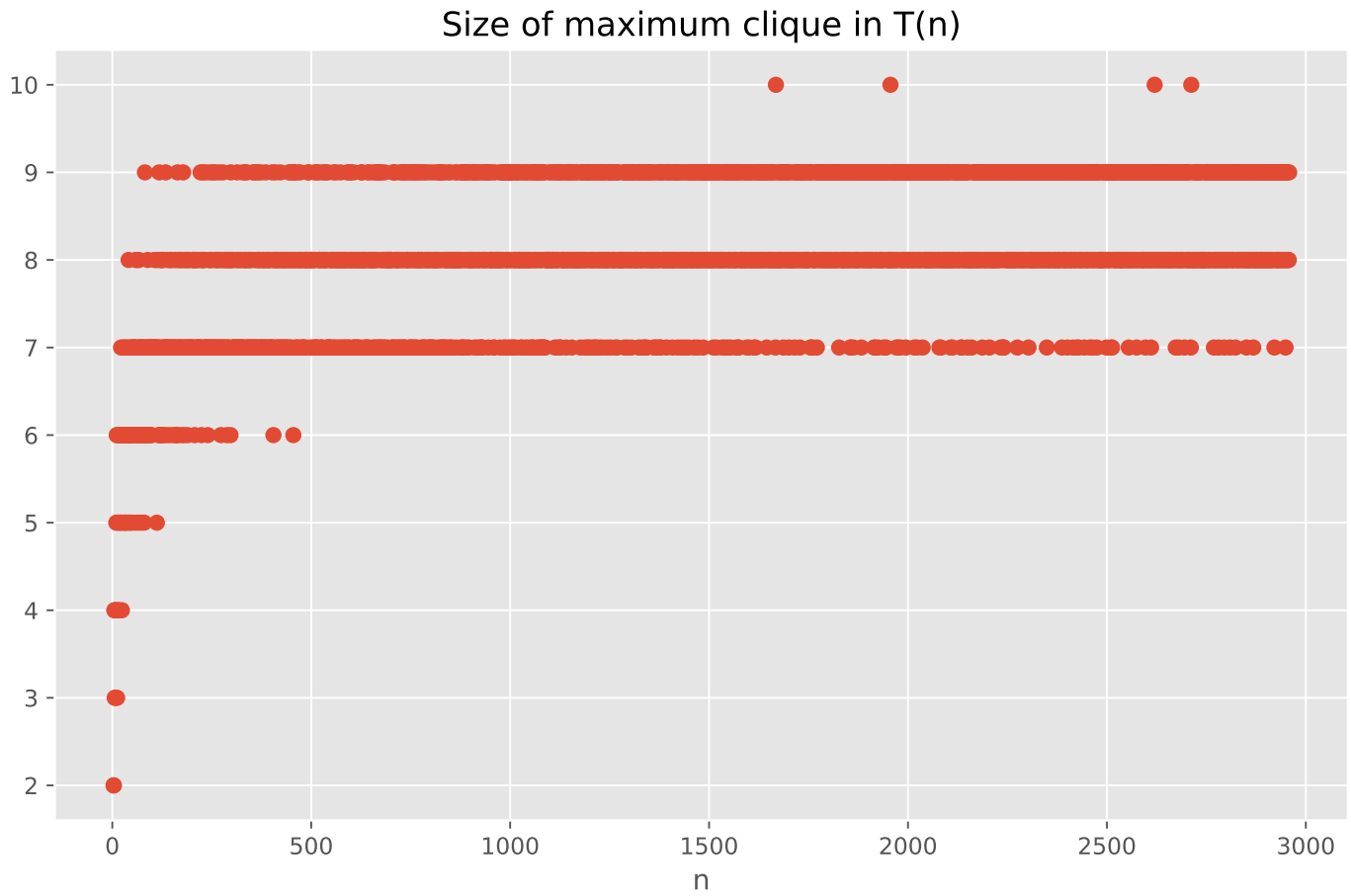
$T(40)$ and $T(100)$

Questions 2 and 3

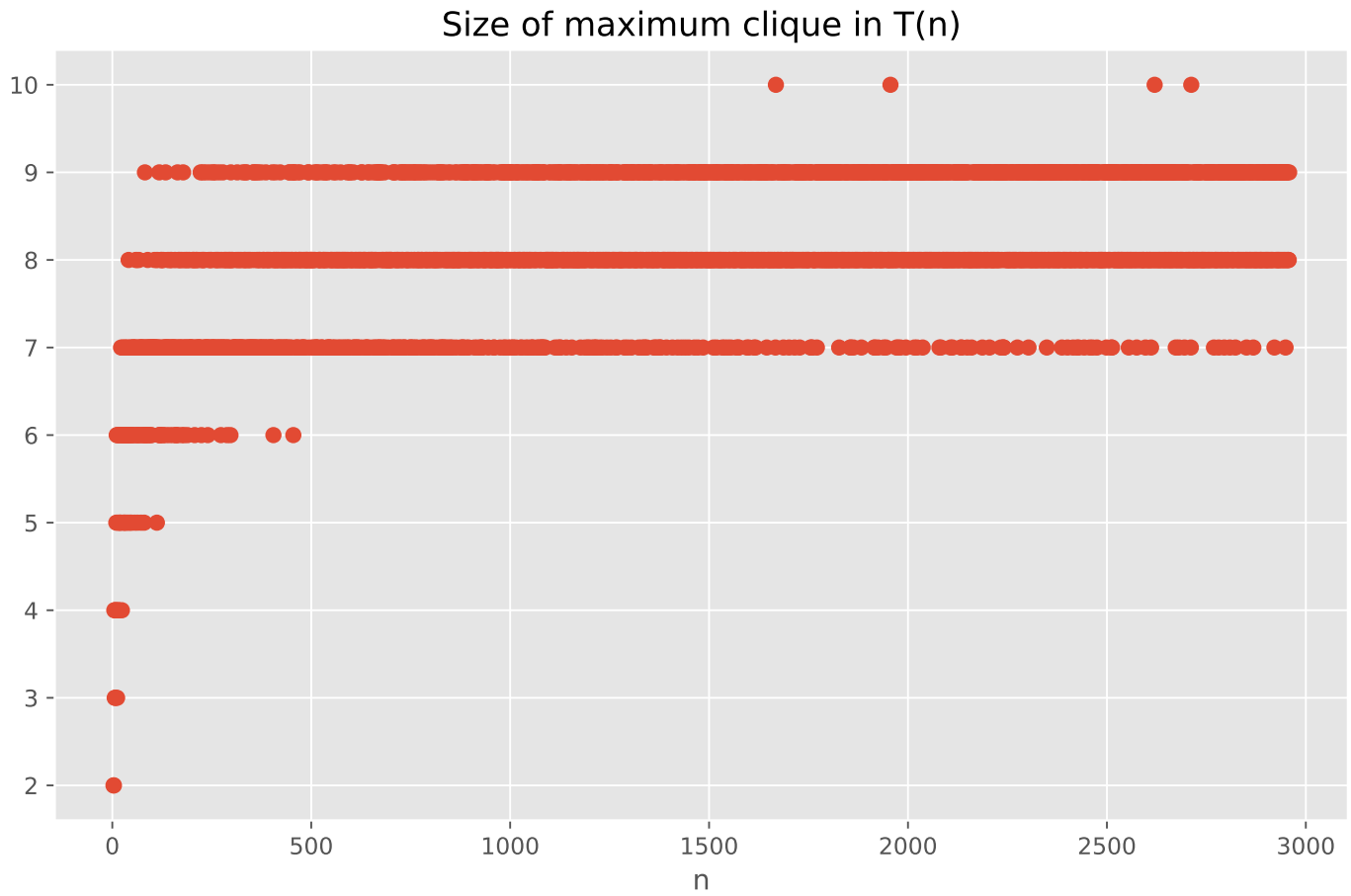
What is the largest set of *pairwise dyadically resolving* trinomials of degree n?

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

Computing maximum cliques is fast!



Clique growth looks slow, but...



Clique growth looks slow, but...

Theorem

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

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

The best estimate we have is the following.

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

The best estimate we have is the following.

Theorem

The largest clique in $T(n)$ has size no larger than

$$2\lfloor \log_2 n \rfloor - v_2(n).$$

$v_2(n) = v$ is the largest v such that 2^v divides n.

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	smallest *possible* n
2	3	3
3	5	5
4	5	5
5	10	9
6	11	9
7	22	17
8	41	17
9	82	33
10	1668	33
11	> 3000	65

The best estimate we have is the following.

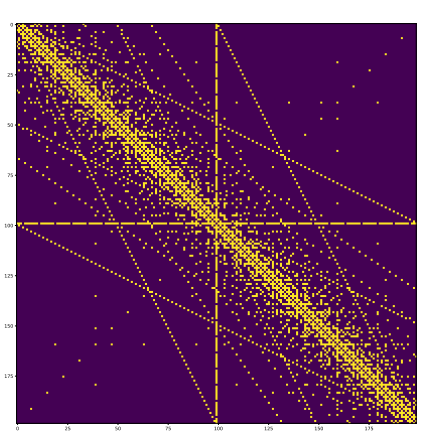
Theorem

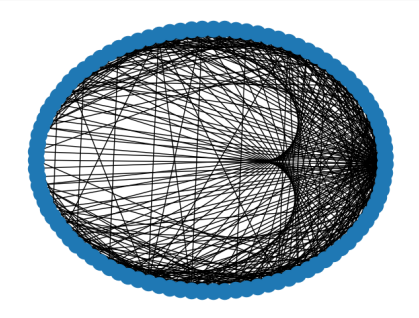
The largest clique in $T(n)$ has size no larger than

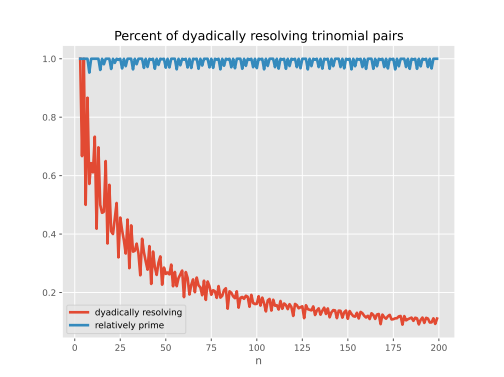
$$2\lfloor \log_2 n \rfloor - v_2(n).$$

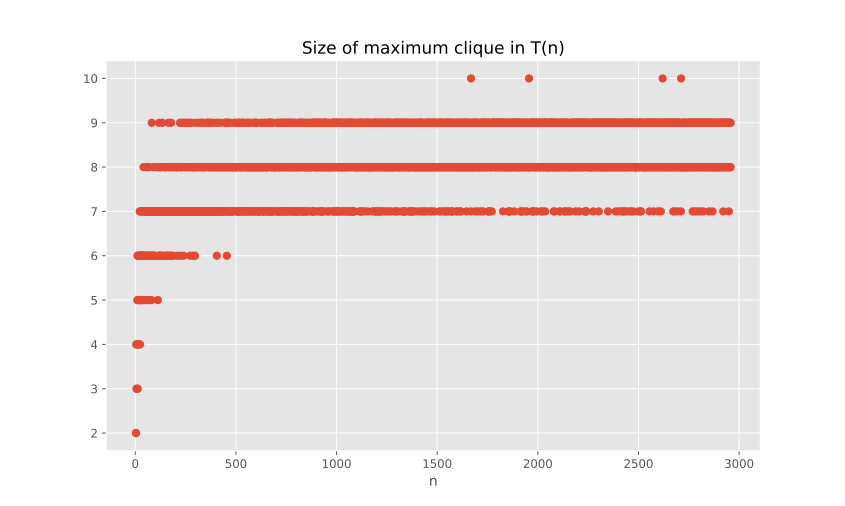
$v_2(n) = v$ is the largest v such that 2^v divides n.

Open questions









True growth of largest clique sizes?

Edge density of $T(n)$?

Other moduli shapes: $2^n \pm 2^k \pm 1$, ...