Modular arithmetic with trinomial moduli

Robert Dougherty-Bliss, Dartmouth College

April (25 - 1)th, 2025

Rutgers Experimental Mathematics Seminar

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

$$(2^{5} - 2^{1} + 1)^{-1} \equiv -2^{2} \pmod{2^{5} - 2^{3} + 1}$$

$$(2^{5} - 2^{1} + 1)^{-1} \equiv -2^{2} \pmod{2^{5} - 2^{3} + 1}$$
$$(2^{10} - 2^{2} + 1)^{-1} \equiv -2^{4} \pmod{2^{10} - 2^{6} + 1}$$

$$(2^{5} - 2^{1} + 1)^{-1} \equiv -2^{2} \pmod{2^{5} - 2^{3} + 1}$$
$$(2^{10} - 2^{2} + 1)^{-1} \equiv -2^{4} \pmod{2^{10} - 2^{6} + 1}$$
$$(2^{15} - 2^{3} + 1)^{-1} \equiv -2^{6} \pmod{2^{15} - 2^{9} + 1}$$

$$
\begin{aligned}
(2^{5} - 2^{1} + 1)^{-1} &\equiv -2^{2} \pmod{2^{5} - 2^{3} + 1} \\
(2^{10} - 2^{2} + 1)^{-1} &\equiv -2^{4} \pmod{2^{10} - 2^{6} + 1} \\
(2^{15} - 2^{3} + 1)^{-1} &\equiv -2^{6} \pmod{2^{15} - 2^{9} + 1} \\
(2^{20} - 2^{4} + 1)^{-1} &\equiv -2^{8} \pmod{2^{20} - 2^{12} + 1}
\end{aligned}
$$

$$(2^{5} - 2^{1} + 1)^{-1} \equiv -2^{2} \pmod{2^{5} - 2^{3} + 1}$$
$$(2^{10} - 2^{2} + 1)^{-1} \equiv -2^{4} \pmod{2^{10} - 2^{6} + 1}$$
$$(2^{15} - 2^{3} + 1)^{-1} \equiv -2^{6} \pmod{2^{15} - 2^{9} + 1}$$
$$(2^{20} - 2^{4} + 1)^{-1} \equiv -2^{8} \pmod{2^{20} - 2^{12} + 1}$$
$$(2^{5c} - 2^{c} + 1)^{-1} \equiv -2^{2c} \pmod{2^{5c} - 2^{3c} + 1}$$

$$
\begin{aligned}
(2^{5} - 2^{1} + 1)^{-1} &\equiv -2^{2} \pmod{2^{5} - 2^{3} + 1} \\
(2^{10} - 2^{2} + 1)^{-1} &\equiv -2^{4} \pmod{2^{10} - 2^{6} + 1} \\
(2^{15} - 2^{3} + 1)^{-1} &\equiv -2^{6} \pmod{2^{15} - 2^{9} + 1} \\
(2^{20} - 2^{4} + 1)^{-1} &\equiv -2^{8} \pmod{2^{20} - 2^{12} + 1} \\
(2^{5c} - 2^{c} + 1)^{-1} &\equiv -2^{2c} \pmod{2^{5c} - 2^{3c} + 1}
\end{aligned}
$$

Why? Plug in $x = 2^c$ into the identity

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

How do you find this identity? Extended GCD algorithm.

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

$$(2^{6} - 2^{2} + 1)^{-1} \equiv 2^{4} - 2^{2} + 1 \pmod{2^{6} - 2^{5} + 1}$$
$$(2^{12} - 2^{4} + 1)^{-1} \equiv N/A \pmod{2^{12} - 2^{10} + 1} \quad \text{(GCD is 7)}$$

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

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

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

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

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

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

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

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

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

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

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

What went wrong?

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

The 7 ruins us!

$$(x^5 - x + 1, x^5 - x^3 + 1) \rightarrow \text{good inverse pattern!}$$
$$(x^6 - x^2 + 1, x^6 - x^5 + 1) \rightarrow \text{bad inverse pattern!}$$

What's the difference?

$$\mathrm{res}(x^5 - x + 1, x^5 - x^3 + 1) = 1$$
$$\mathrm{res}(x^6 - x^2 + 1, x^6 - x^5 + 1) = 7,$$

where $\mathrm{res}(f, g)$ is the *resultant* of f and g.

For the non-experts: Resultants are like determinants.

If f and g are monic, then

$$\mathrm{res}(f,g) = \pm \prod_{\substack{f(z)=0 \\ g(w)=0}} (z-w)$$

Important facts:

For the non-experts: Resultants are like determinants.

If f and g are monic, then

$$\begin{aligned}\operatorname{res}(f,g) &= \pm \prod_{\substack{f(z)=0\\ g(w)=0}} (z-w)\\ &= \pm \prod_{f(z)=0} g(z)\\ &= \pm \prod_{g(z)=0} f(z).\end{aligned}$$

Important facts:

For the non-experts: Resultants are like determinants.

If f and g are monic, then

$$\begin{aligned}\mathrm{res}(f,g) &= \pm \prod_{\substack{f(z)=0\\ g(w)=0}} (z-w)\\ &= \pm \prod_{f(z)=0} g(z)\\ &= \pm \prod_{g(z)=0} f(z).\end{aligned}$$

Important facts:

- Resultants can be computed without knowing any roots.

For the non-experts: Resultants are like determinants.

If f and g are monic, then

$$\begin{aligned} \mathrm{res}(f,g) &= \pm \prod_{\substack{f(z)=0 \\ g(w)=0}} (z-w) \\ &= \pm \prod_{f(z)=0} g(z) \\ &= \pm \prod_{g(z)=0} f(z). \end{aligned}$$

Important facts:

- Resultants can be computed without knowing any roots.
- If f and g have integer coefficients, then $\mathrm{res}(f,g)$ is an integer.

For the non-experts: Resultants are like determinants.

If f and g are monic, then

$$\begin{aligned}\operatorname{res}(f, g) &= \pm \prod_{\substack{f(z)=0 \\ g(w)=0}} (z - w) \\ &= \pm \prod_{f(z)=0} g(z) \\ &= \pm \prod_{g(z)=0} f(z).\end{aligned}$$

Important facts:

- Resultants can be computed without knowing any roots.
- If f and g have integer coefficients, then $\operatorname{res}(f, g)$ is an integer.
- $\operatorname{res}(f, g) = 0$ iff f and g have a common factor.

$$\mathrm{res}(x^5 - x + 1, x^5 - x^3 + 1) = 1$$
$$\mathrm{res}(x^6 - x^2 + 1, x^6 - x^5 + 1) = 7$$

The inverse sequence

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

will be "nice" if and only if $\mathrm{res}(x^n - x^k + 1, x^n - x^j + 1)$ is $\pm$ a power of 2.

Definition

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

Original motivation: Faster Chinese remaindering for integer computations.

The "trinomial moduli"

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

have nice binary properties, but we need nice inverse sequences!

Basic questions

Original motivation: Faster Chinese remaindering for integer computations.

The "trinomial moduli"

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

have nice binary properties, but we need nice inverse sequences!

Basic questions

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

Original motivation: Faster Chinese remaindering for integer computations.

The "trinomial moduli"

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

have nice binary properties, but we need nice inverse sequences!

Basic questions

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

Original motivation: Faster Chinese remaindering for integer computations.

The "trinomial moduli"

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

have nice binary properties, but we need nice inverse sequences!

Basic questions

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?

Original motivation: Faster Chinese remaindering for integer computations.

The "trinomial moduli"

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

have nice binary properties, but we need nice inverse sequences!

Basic questions

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?

Basic questions (new)

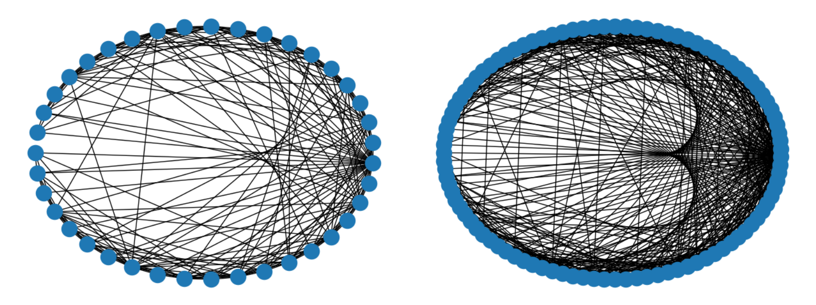
1. When do $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve?
2. Are there arbitrarily large sets of dyadically resolving trinomials?
3. How can we efficiently find these sets?

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 $T(100)$

What's going on here?

Symmetry? Heart? Circle?

Queston 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 $T(n)$?

$$\begin{pmatrix} 0 & 1 & 3 & 1 & 3 & 31 & 9 & 8 & 3 \\ 1 & 0 & 1 & 1 & 4 & 1 & 31 & 16 & 8 \\ 3 & 1 & 0 & 1 & 3 & 1 & 3 & 31 & 9 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 31 \\ 3 & 4 & 3 & 1 & 0 & 1 & 3 & 4 & 3 \\ 31 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 9 & 31 & 3 & 1 & 3 & 1 & 0 & 1 & 3 \\ 8 & 16 & 31 & 1 & 4 & 1 & 1 & 0 & 1 \\ 3 & 8 & 9 & 31 & 3 & 1 & 3 & 1 & 0 \end{pmatrix}$$

$$M(k, j) = \mathrm{res}(x^{10} - x^k + 1, x^{10} - x^j + 1)$$

There are not usually “formulas” for resultants, so this could be hard.

Looks like mostly powers of 2?

Queston 1

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

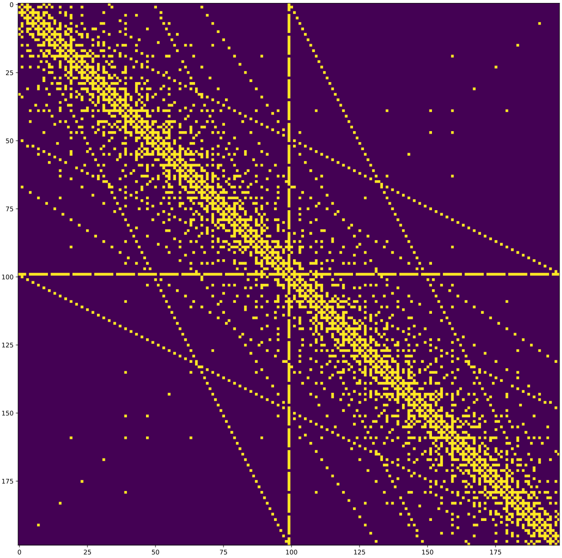
What are the edges of $T(n)$?

$$\begin{pmatrix} 0 & 1 & 3 & 1 & 3 & 31 & 9 & 8 & 3 \\ 1 & 0 & 1 & 1 & 4 & 1 & 31 & 16 & 8 \\ 3 & 1 & 0 & 1 & 3 & 1 & 3 & 31 & 9 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 31 \\ 3 & 4 & 3 & 1 & 0 & 1 & 3 & 4 & 3 \\ 31 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 9 & 31 & 3 & 1 & 3 & 1 & 0 & 1 & 3 \\ 8 & 16 & 31 & 1 & 4 & 1 & 1 & 0 & 1 \\ 3 & 8 & 9 & 31 & 3 & 1 & 3 & 1 & 0 \end{pmatrix}$$

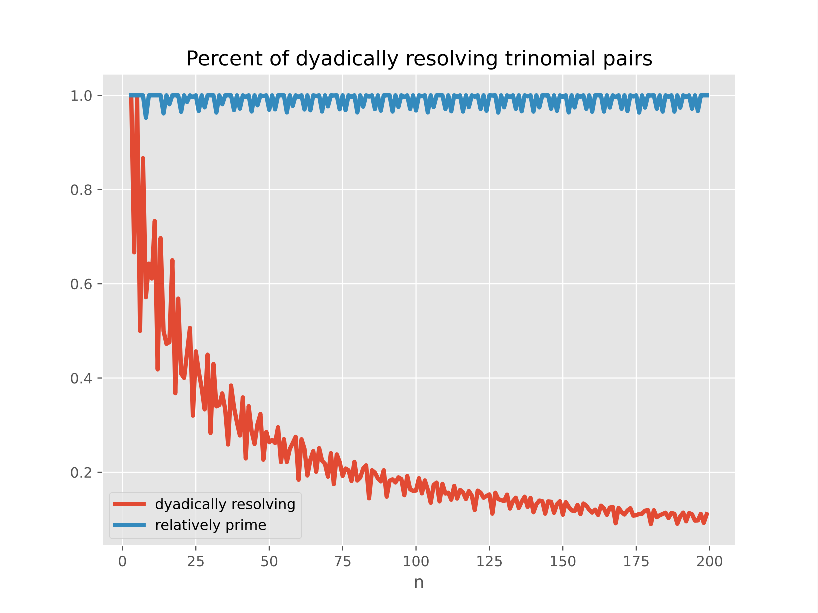
$$M(k, j) = \mathrm{res}(x^{10} - x^k + 1, x^{10} - x^j + 1)$$

There are not usually “formulas” for resultants, so this could be hard.

Looks like mostly powers of 2?



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 *should* go to 0.

To understand how complicated this might be, look at this evaluation:

$$\mathrm{res}(x^{900} - x^{22} + 1, x^{900} - x^{72} + 1) = 1125899839733761.$$

Where does this number come from?

Special case

To understand how complicated this might be, look at this evaluation:

$$\mathrm{res}(x^{900} - x^{22} + 1, x^{900} - x^{72} + 1) = 1125899839733761.$$

Where does this number come from?

Special case

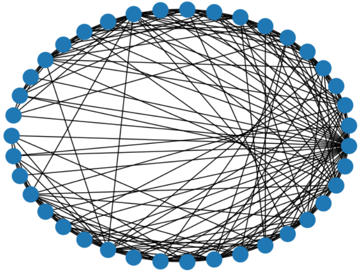
If $k - j$ divides n, then

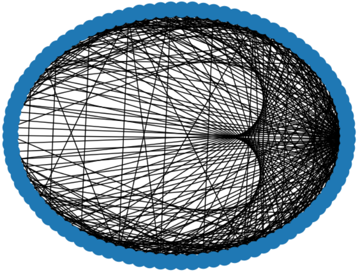
$$\mathrm{res}(x^n - x^k + 1, x^n - x^j + 1) = \pm \left(\prod_{m \mid \frac{k-j}{\gcd(k,j)}} \Phi_m(2) \right)^{\gcd(k,j)}$$

where Φ_m is the mth cyclotomic polynomial.

$$\begin{aligned}\mathrm{res}(x^{900} - x^{22} + 1, x^{900} - x^{72} + 1) &= 1125899839733761 \\ &= (\Phi_5(2)\Phi_{25}(2))^2.\end{aligned}$$

We know of essentially no other formulas!





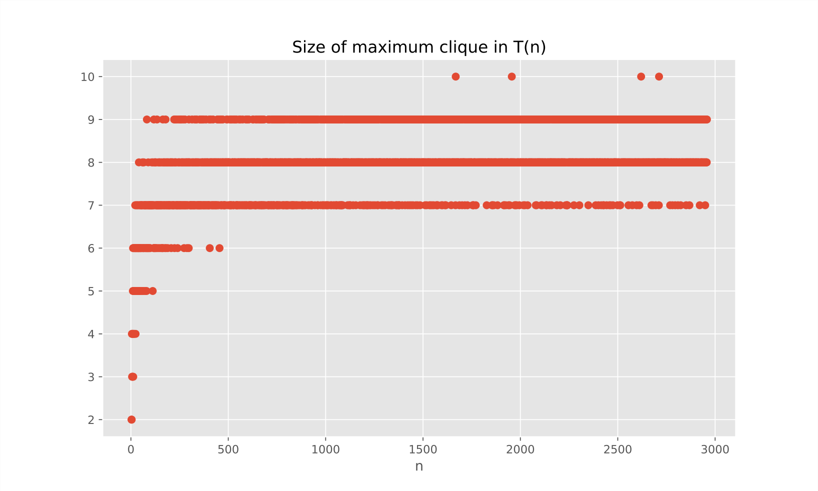
$T(40)$ and $T(100)$

Questions 2 and 3

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

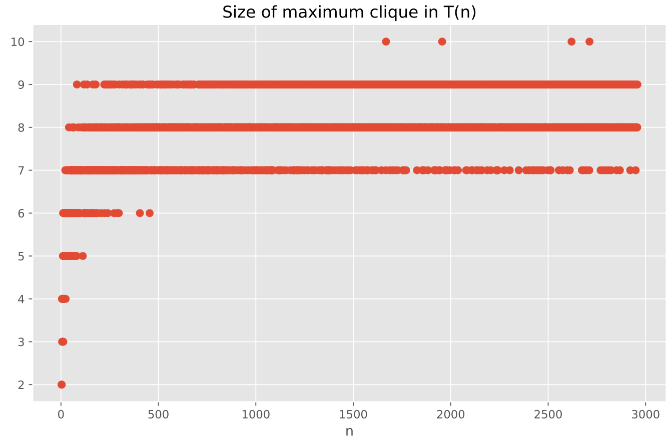
What is the largest clique in $T(n)$?

Computing maximum cliques is fast!



It took approximately 10 years of CPU time to produce this graph.

Clique growth looks slow, but…



It took approximately 10 years of CPU time to produce this graph.

Clique growth looks slow, but...

Theorem

The clique number of $T(n)$ goes to ∞ as $n \longrightarrow \infty$.

Theorem

The clique number of $T(n)$ goes to ∞ as $n \to \infty$.

Our proof is constructive, but the exponents are big:

$$\{1\}$$

$$\{1, 2\}$$

$$\{2, 3, 4\}$$

$$\{12, 15, 16, 18\}$$

$$\{720, 760, 765, 768, 780\}$$

$$\{48372480, 48434496, 48435465, 48435712, 48436128, 48439664\}$$

The last set implies that there is a clique of size 6 in $T(n)$ for $n > 48439664$.

But there's a clique of size 6 in $T(22)$!

We do not know the true growth rate of the clique numbers.

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	≥ 2985

The best estimate we have is the following.

We do not know the true growth rate of the clique numbers.

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	≥ 2985

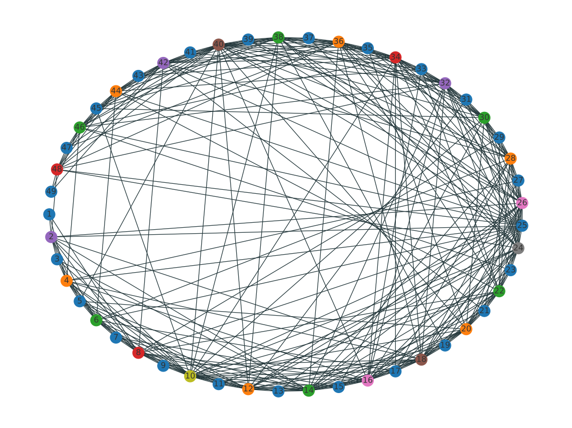
The best estimate we have is the following.

Theorem

The largest clique in $T(n)$ has size no larger than $2\lfloor \log_2 n \rfloor - v_2(n)$, where $v_2(n) = v$ is the largest v such that 2^v divides n.

Theorem

The largest clique in $T(n)$ has size no larger than $2\lfloor \log_2 n \rfloor - v_2(n)$.



A greedy coloring of $T(50)$ with nine colors.

If a graph can be colored with k colors, then it cannot have a clique of size bigger than k.

How we found the coloring

We found a coloring with the right number of colors purely by experimentation.

The `NetworkX` library does greedy coloring, so we asked nicely.

Colors for $n = 30$:

$$\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29\}$$

$$\{2, 8, 14, 20, 26\}$$

$$\{4, 10, 16, 22, 28\}$$

$$\{24\}$$

$$\{18\}$$

$$\{12\}$$

$$\{6\}$$

How we found the coloring

We found a coloring with the right number of colors purely by experimentation.

The `NetworkX` library does greedy coloring, so we asked nicely.

Colors for $n = 30$:

$$\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29\}$$

$$\{2, 8, 14, 20, 26\}$$

$$\{4, 10, 16, 22, 28\}$$

$$\{24\}$$

$$\{18\}$$

$$\{12\}$$

$$\{6\}$$

This is 1 mod 2, 2 mod 6, 4 mod 6, then some noise.

The library is slightly too eager, but you can get inspired.

How you prove the coloring

Let's try to compute a resultant. Say that i and k are both odd.

$$\mathrm{res}(x^{10} - x^i + 1, x^n - x^k + 1) = \mathrm{res}(x^{10} - x^i + 1, x^k - x^i)$$

How you prove the coloring

Let's try to compute a resultant. Say that i and k are both odd.

$$\begin{aligned}\mathrm{res}(x^{10} - x^i + 1, x^n - x^k + 1) &= \mathrm{res}(x^{10} - x^i + 1, x^k - x^i) \\ &= \mathrm{res}(x^{10} - x^i + 1, x^i(x^{k-i} - 1))\end{aligned}$$

How you prove the coloring

Let's try to compute a resultant. Say that i and k are both odd.

$$\begin{aligned}\operatorname{res}(x^{10} - x^i + 1, x^n - x^k + 1) &= \operatorname{res}(x^{10} - x^i + 1, x^k - x^i) \\ &= \operatorname{res}(x^{10} - x^i + 1, x^i(x^{k-i} - 1)) \\ &= \operatorname{res}(x^{10} - x^i + 1, x^{k-i} - 1).\end{aligned}$$

How you prove the coloring

Let's try to compute a resultant. Say that i and k are both odd.

$$\begin{aligned}\operatorname{res}(x^{10} - x^i + 1, x^n - x^k + 1) &= \operatorname{res}(x^{10} - x^i + 1, x^k - x^i) \\ &= \operatorname{res}(x^{10} - x^i + 1, x^i(x^{k-i} - 1)) \\ &= \operatorname{res}(x^{10} - x^i + 1, x^{k-i} - 1).\end{aligned}$$

Because $k - i$ is even, $x + 1$ divides $x^{k-i} - 1$. So,

$$\operatorname{res}(x^{10} - x^i + 1, x + 1) = (-1)^{10} - (-1)^i + 1 = 3$$

divides our resultant.

These cannot dyadically resolve!

How you prove the coloring

Let's try to compute a resultant. Say that i and k are both odd.

$$\begin{aligned}\mathrm{res}(x^{10}-x^i+1, x^n-x^k+1) &= \mathrm{res}(x^{10}-x^i+1, x^k-x^i)\\ &= \mathrm{res}(x^{10}-x^i+1, x^i(x^{k-i}-1))\\ &= \mathrm{res}(x^{10}-x^i+1, x^{k-i}-1).\end{aligned}$$

Because $k-i$ is even, $x+1$ divides $x^{k-i}-1$. So,

$$\mathrm{res}(x^{10}-x^i+1, x+1) = (-1)^{10}-(-1)^i+1 = 3$$

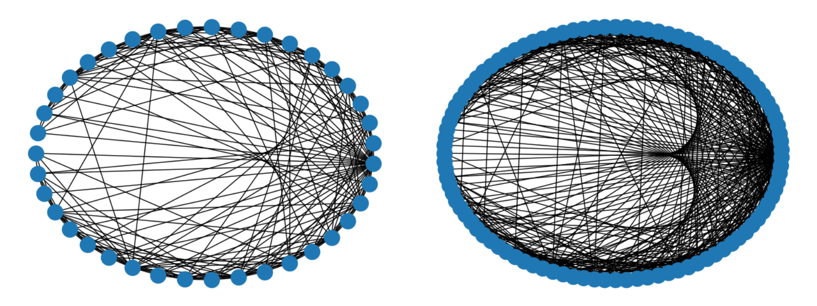
divides our resultant.

These cannot dyadically resolve!

Meaning: $\{1,3,5,7,\ldots\}$ is an independent set in $T(n)$.

Repeat this for different congruence classes.

Symmetries



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

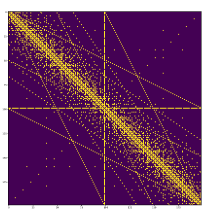
The heart is really there.

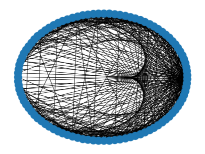
So is the circle.

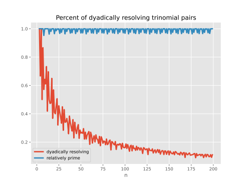
So is the reflectional symmetry.

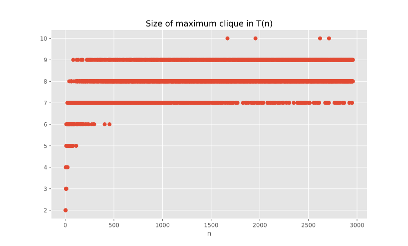
Conjecture: For n large enough, the automorphism group of $T(n)$ is $\mathbb{Z}_2$.

Open questions









True growth of the clique numbers?

Edge density of $T(n)$?

Faster way to compute $T(n)$?

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