Recurrence Sequences and Diophantine Problems

Elisa Bellah

University of Toronto

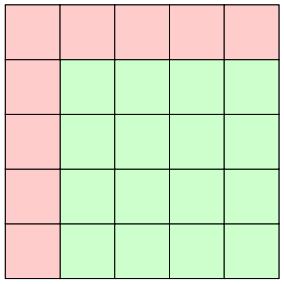
MAA Ohio Section Fall 2025 Meeting

"It looked so simple, and yet all the great mathematicians in history couldn't solve it. Here was a problem, that I, a ten year old, could understand and I knew from that moment that I would never let it go. I had to solve it."

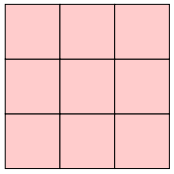
-Andrew Wiles

Plan

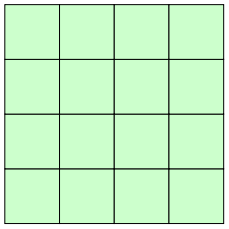
Arranging Blocks into Squares



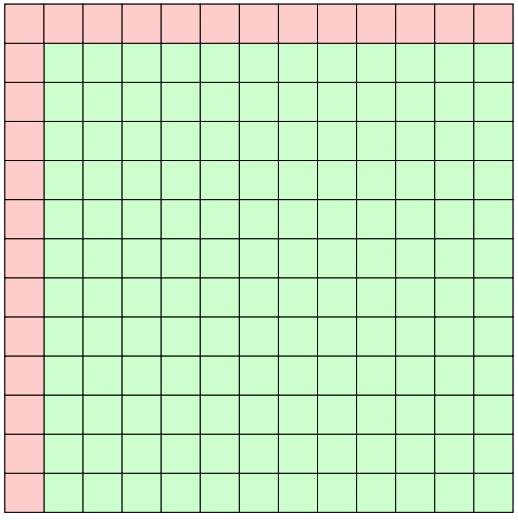
5×5



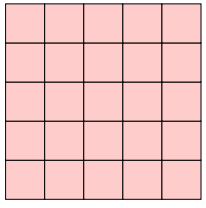
3×3



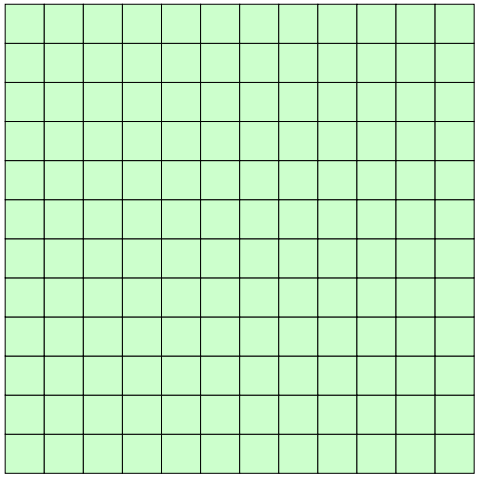
4×4



13×13

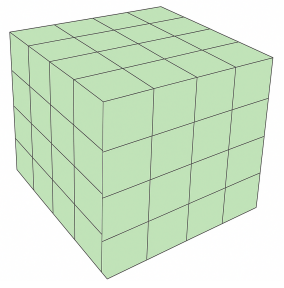


5×5



12×12

Arranging Blocks into Cubes



. . . cannot be broken into two smaller cubes!

Arranging Blocks

In 2D case, we're looking for integer solutions to

$$X^2 + Y^2 = Z^2.$$

Solutions to this equation are called *Pythagorean triples*.

- There are infinitely many Pythagorean triples.
- Can be generated explicitly.
- All of this can be done using elementary methods.

In higher dimensions, we're looking for integer solutions to

$$X^n + Y^n = Z^n,$$

where $n \geq 3$.

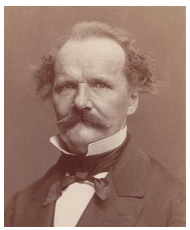
Fermat's Last Theorem

Fermat's Last Theorem

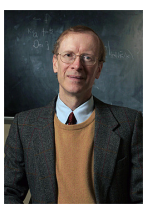
If $n \geq 3$, the only solution to $X^n + Y^n = Z^n$ is $(0, 0, 0)$.

" I have discovered a truly marvelous proof of this, which this margin is too narrow to contain." -Fermat (mid 1600s)

Over the next 300 years ...

- Special cases proven by Sophie Germain and Ernst Kummer (regular primes)
- Algebraic number theory developed
- Proven by Wiles in 1990s (later corrected in collaboration with Richard Taylor), using elliptic curves and modular forms.




Diophantine Questions

A Diophantine Equation is any polynomial equation

$$f(X_1, \ldots, X_n) = 0,$$

where $f \in \mathbb{Z}[X_1, \ldots, X_n]$. *Diophantine Analysis* is interested in learning about the **integer** solutions.

Questions

(1) Does the equation have an integer solution?

(2) If so, how many?

(3) If finitely many, can you list them all?

(4) If infinitely many, can you generate them explicitly?

(5) Can you say anything about their arithmetic properties?

Hilbert 10

In 1900, David Hilbert published a list of 23 problems. The 10th problem on this list asked:

"Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers."

. . . i.e. does there exist a finite algorithm to determine whether an arbitrary Diophantine equation has a solution?

Theorem (MRDP, 1970)

No.

Philosophy: no "unifying theory" for Diophantine problems.

Finding Square Roots

Let's find a good rational approximation for $\sqrt{2}$ ...

- We want $x, y \in \mathbb{Z}$ so that $\frac{x}{y} \approx \sqrt{2}$
- Rearranging gives

$$\frac{x^2}{y^2} \approx 2 \Leftrightarrow \underbrace{x^2 - 2y^2}_{\text{integer}} \approx 0$$

So we want $x^2 - 2y^2 = \pm 1$. Rearranging again gives

$$\frac{x}{y} = \sqrt{2 \pm \frac{1}{y^2}}.$$

- Best approximations are integer solutions (x, y) to

$$X^2 - 2Y^2 = \pm 1$$

with $|y|$ large

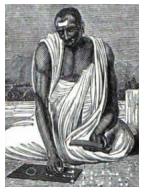
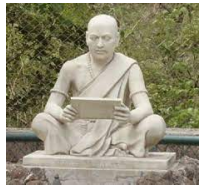
Pell's Equation

The Diophantine Equations

$$X^2 - nY^2 = \pm 1$$

are called PELL EQUATIONS. This name is a historical mistake ...

- Studied in India for about one thousand years before Pell (Brahmagupta, Bhaskara)

- Independently, in 17th century England, Wallis and Brouncker worked on these equations.


- Pell communicated these results to Euler, but never actually worked on them himself. Euler, who was a major authority at the time, referred to them as "Pell's equation"

Solving Pell's Equation

Observe, we can factor

$$\underbrace{X^2 - nY^2}_{(X+\sqrt{n}Y)(X-\sqrt{n}Y)} = \pm 1,$$

to rewrite Pell's equation as

$$N_K(X + \sqrt{n}Y) = \pm 1,$$

where $K = \mathbb{Q}(\sqrt{n})$ and N_K is the field norm.

That is, we want elements α in the $\mathbb{Z}$-module

$$M = \{x + \sqrt{n}y : x, y \in \mathbb{Z}\}$$

with $N_K(\alpha) = \pm 1$.

Generalization

Definition

Let K be a number field and $W = \{w_1, \ldots, w_n\}$ any $\mathbb{Q}$-linearly independent subset of K. The NORM FORM associated to W is the rational form F_W defined by

$$F_W(X_1, \ldots, X_n) := N_K(X_1 w_1 + \cdots + X_n w_n).$$

Example: The Pell equation $X^2 - nY^2 = 1$ is the norm form equation $F_W(X, Y) = 1$ where $W = \{1, \sqrt{n}\}$ in $K = \mathbb{Q}(\sqrt{n})$.

Key Observation: Solutions to a norm form equation

$$F_W(X_1, \ldots, X_n) = c$$

correspond to elements α in the $\mathbb{Z}$-module $M \subseteq \mathcal{O}_K$ generated by W (that is, $M = \{x_1 w_1 + \cdots + x_n w_n : x_i \in \mathbb{Z}\}$) with $N_K(\alpha) = c$.

Characterization of Solutions to Full Norm Form Equations

Given a *full* module $M \subseteq K$ (i.e. $\operatorname{rank} M = [K : \mathbb{Q}]$), let

- $\mathcal{O}_M := \{\alpha \in K : \alpha M \subseteq M\}$ be the coefficient ring of M
- $\mathcal{U}_M^+ := \{\varepsilon \in \mathcal{O}_M : N_K(\varepsilon) = 1\}$ be the positive unit group of $\mathcal{O}_M$

Fact. All $\alpha \in M$ with $N_K(\alpha) = c$ lie in finitely many disjoint families

$$\alpha_1 \mathcal{U}_M^+, \ldots, \alpha_\ell \mathcal{U}_M^+.$$

Fact. $\mathcal{O}_M$ is an order in $K \overset{\text{DUT}}{\Rightarrow} \mathcal{U}_M^+$ is a f.g. abelian group.

Takeaway. We can solve any norm form equation if we have:

1. Algorithm to compute $\alpha_1, \ldots, \alpha_\ell$
2. The roots of unity in $\mathcal{O}_M$
3. Algorithm to compute a basis $\{\varepsilon_1, \ldots, \varepsilon_r\}$ of $F(\mathcal{U}_M^+)$.

Generating Infinite Families of Solutions

Let $\beta \in M$ with $N_K(\beta) = c$. For an element $\varepsilon \in F(\mathcal{U}_M^+)$ let

$$\alpha(k) := \beta\varepsilon^k, \text{ for } k \in \mathbb{Z}_{\geq 0}.$$

Then $\alpha(k)$ is an infinite sequence of elements in M of norm c. If $W = \{w_1, \ldots, w_n\}$ is a $\mathbb{Q}$-basis for M and we write

$$\alpha(k) = x_1(k)w_1 + \cdots + x_n(k)w_n,$$

then we get infinitely many solutions $(x_1(k), \ldots, x_n(k))$ to the norm form equation $F_W(X_1, \ldots, X_n) = c$.

Definition.

We call the integer sequences $x_i(k)$ the COORDINATE SEQUENCES of $\alpha(k)$, with respect to the basis W.

Question. Without finding β or ε explicitly (which may be hard), what can be said about the coordinate sequences $x_i(k)$?

Generating Solutions

Let $\alpha(k) = \beta\varepsilon^k$ be our sequence of elements in the module $M \subseteq K$ of norm c and write

$$\alpha(k) = x_1(k)w_1 + \cdots + x_n(k)w_n.$$

Key Lemma.

Suppose that ε has minimal polynomial

$$f(X) = X^d - s_1X^{d-1} - \cdots - s_d.$$

Then, the coordinate sequences $x_i(k)$ of $\alpha(k)$ satisfy the **linear** recurrence

$$x_i(k+d) = s_1x_i(k+d-1) + \cdots + s_dx_i(k).$$

Obs: All coordinates satisfy the same recurrence, which only depends on ε. The sequences only differ by their initial conditions.

Back to Finding Square Roots

We wanted to solve the norm form equations

$$(1)\ X^2 - 2Y^2 = 1$$
$$(2)\ X^2 - 2Y^2 = -1.$$

Let $W = \{1, \sqrt{2}\}$ and $M = \{x + y\sqrt{2} : x, y \in \mathbb{Z}\}$ be the $\mathbb{Z}$-module in $K = \mathbb{Q}(\sqrt{2})$ generated by W. Can calculate

$$\mathcal{U}_M^+ = \{\pm(3 + 2\sqrt{2})^k : k \in \mathbb{Z}\}$$

Positive solutions to (1) are $(x(k), y(k))$ so that

$$(3 + 2\sqrt{2})^k = x(k) + y(k)\sqrt{2}$$

Positive solutions to (2) are $(x(k), y(k))$ so that

$$(1 + \sqrt{2})(3 + 2\sqrt{2})^k = x(k) + y(k)\sqrt{2}$$

Back to Finding Square Roots

Punchline: All positive solutions $(x(k), y(k))$ to the norm form equations $X^2 - 2Y^2 = \pm 1$ are

$$(1+\sqrt{2})^k = x(k) + y(k)\sqrt{2}.$$

From Key Lemma, we have

$$x(k+2) = 2x(k+1) + x(k), \text{initializing at } x(0) = 1, x(1) = 1$$

$$y(k+2) = 2y(k+1) + y(k), \text{initializing at } y(0) = 0, y(1) = 1$$

So, we can find good rational approximations

$$\frac{x(k)}{y(k)}$$

to $\sqrt{2}$ by finding terms where $y(k)$ is large.

Finding Square Roots

Let's calculate approximations for $\sqrt{2} \approx 1.41421356\ldots$ using our coordinate sequences. Recall that

$$\frac{x(k)}{y(k)} = \sqrt{2 + \frac{1}{y(k)^2}}$$

k	x(k)	y(k)	x(k)/y(k)
0	1	0	n/a
1	1	1	1
2	3	2	1.5
3	7	5	1.4
4	17	12	$1.4\overline{16}$
5	41	29	$1.4137931\ldots$
6	99	70	$1.4142857\ldots$
7	239	169	$1.4142156\ldots$
8	577	408	$1.4142156\ldots$
9	1393	985	$1.4142131\ldots$
10	3363	2378	$1.4142136\ldots$

Using the recurrence from previous slide, we get:

- $y(k)$, which controls the error, grows exponentially
- $y(k)$ is a *Lucas sequence*, and has nice arithmetic structure.

Lucas Sequences

Let $P, Q \in \mathbb{Z}_{\neq 0}$. The Lucas sequence $L(k)$ with parameters (P, Q) is the linear recurrence sequence

$$L(k+2) = PL(k+1) - QL(k), \text{ initializing at } L(0) = 0, L(1) = 1.$$

ex: the Fibonacci sequence is a Lucas sequence with parameters $(1, -1)$.

Lucas Sequence Properties

Let $L(k)$ be the Lucas sequence with parameters (P, Q).

- $L(k)$ is a *Linear Divisibility Sequence*; that is, $n \mid m \Rightarrow L(n) \mid L(m)$;
- If $p \nmid Q$ is prime, then $p^a \mid L(m)$ for some m and every $a \in \mathbb{Z}_{\geq 0}$.
- There are formulas for the first time p appears as a factor of $L(k)$.
- Conjectured that Lucas sequences contain infinitely many prime terms.

So, without performing any calculations, we can obtain arithmetic properties about solutions to Pell equations.

Archimedes's Cattle Problem

"The sun god had a herd of cattle consisting of bulls and cows, one part of which was white, a second black, a third spotted, and a fourth brown. Among the bulls, the number of white ones was one half plus one third the number of the black greater than the brown; the number of the black, one quarter plus one fifth the number of the spotted greater than the brown; the number of the spotted, one sixth and one seventh the number of the white greater than the brown. Among the cows, the number of white ones was one third plus one quarter of the total black cattle; the number of the black, one quarter plus one fifth the total of the spotted cattle; the number of spotted, one fifth plus one sixth the total of the brown cattle; the number of the brown, one sixth plus one seventh the total of the white cattle. What was the composition of the herd? "

Solutions correspond to a Pell equation

$$X^2 - 4729494\,Y^2 = 1.$$

Smallest solution has more than one hundred thousand digits (hard!). Without calculating this, we can say things like ...

- If $p \nmid 4729494$ is prime, then there are infinitely many solutions (x, y) to this Pell equation with $p \mid y$.
- We expect that this equation has infinitely many solutions (x, y) with y prime.

Quartic Equations with Lucas Sequence Solutions

Let K be a quartic field with real quadratic subfield L so that K contains a quartic unit of the form $\sqrt{\varepsilon}$ where ε is a unit in L of positive norm (arise from Kuroda's 1943 characterization of biquadratic fields)

Theorem (B. 2020).

Fix an element $\beta \in K$ and write $\alpha(k) = \beta\sqrt{\varepsilon}^k$. Then, there is a choice of basis $W = \{w_1, w_2, w_3, w_4\}$, which we construct explicitly, for the module $M' = \beta\mathbb{Z}[\sqrt{\varepsilon}]$ so that if we write

$$\alpha(k) = x_1(k)w_1 + x_2(k)w_2 + x_3(k)w_3 + x_4(k)w_4$$

then $x_1(k)$ is a LDS, and

k	$x_1(k)$	$x_2(k)$	$x_3(k)$	$x_4(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2n$	$L(n)$	0	$-L(n-1)$	0
$2n+1$	$L(n+1)+L(n)$	$L(n)$	0	$-L(n-1)$
$2n+2$	$L(n+1)$	0	$-L(n)$	0
$2n+3$	$L(n+2)+L(n+1)$	$L(n+1)$	0	$-L(n)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Rational Approximations and the Lagrange Spectrum

Recall again our rational approximations x/y for $\sqrt{2}$ satisfied

$$\frac{x}{y} = \sqrt{2 \pm \frac{1}{y^2}} \Rightarrow \left|\sqrt{2} - \frac{x}{y}\right| < \frac{1}{y^2}.$$

Dirichlet's Approximation Theorem.

For any $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, there are infinitely many integers x, y so that

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^2}.$$

- Ross (1900s): if α is algebraic, the exponent 2 cannot be improved.
- The LAGRANGE NUMBER of α is the largest L so that

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{Ly^2}$$

for infinitely many $x, y \in \mathbb{Z}$. In 1800s, Markoff related Lagrange numbers to a particular Diophantine equation.

Markoff Triples

The Markoff equation is the Diophantine equation

$$X^2 + Y^2 + Z^2 = 3XYZ$$

and the integer solutions (x, y, z) are called Markoff triples.

- 1800s: introduced by Markoff in context of rational approximations and quadratic forms.
- 1972: Cohn used Markoff triples to study free groups on two generators.
- 1974: Hirzebruch and Zagier used these triples to signatures of certain 4-dimensional manifolds
- 2021: Fuchs, Lauter, et. al used these triples to propose cryptographic hash functions

Vieta Involutions

Suppose that (x, y, z) is a Markoff triple. Then, the quadratic

$$X^2 + y^2 + z^2 = 3yzX$$

has solution x. So, we can write

$$(X - x)(X - x') = X^2 - 3yzX - (y^2 + z^2)$$

and compare coefficients to solve $x' = 3yz - x$. Working similarly with y, z, we obtain maps $\{\text{Markoff Triples}\} \to \{\text{Markoff Triples}\}$

$$R_1 : (x, y, z) \mapsto (3yz - x, y, z)$$

$$R_2 : (x, y, z) \mapsto (x, 3xz - y, z)$$

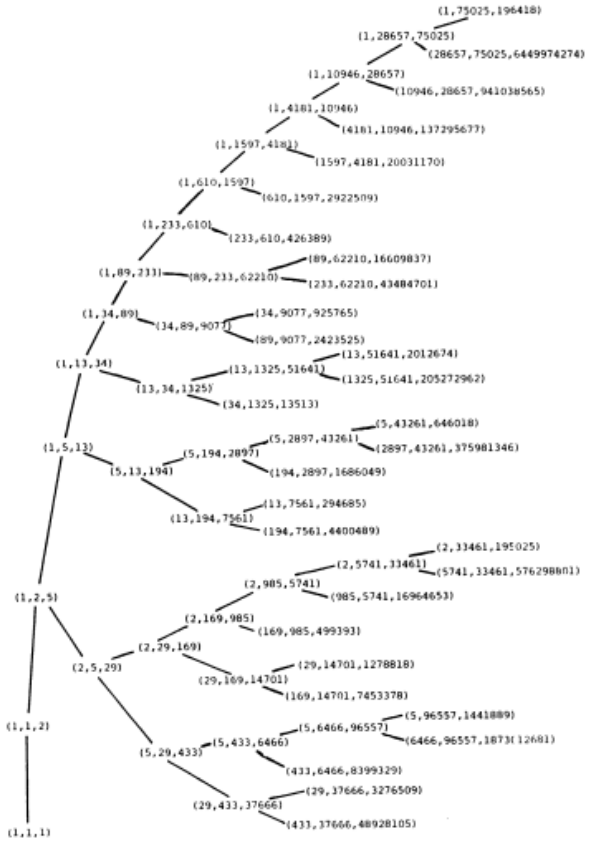
$$R_3 : (x, y, z) \mapsto (x, y, 3xy - z)$$

called the VIETA INVOLUTIONS.

Markoff Trees

If we iteratively apply the Vieta involutions to $(1, 1, 1)$, we obtain **all positive Markoff triples** (up to permutation of the coordinates).

Can organize these into a tree (see Aigner's book for more on this story!)



Mod p solutions

Diophantine Question.

Given a Diophantine equation $F(X_1, \ldots, X_n) = 0$ what is the relation between the integer solutions and the mod p solutions?

- **Example (linear Diophantine equations):** every mod p solution to

$$a_1X_1 + \cdots + a_nX_n = b$$

has an integer lift, for primes $p \nmid \gcd(a_1, \ldots, a_n)$
$\rightarrow$ Sun-tzu/Sunzi's Theorem (aka CRT).

- **Nonexample:** $X^2 + 1 = 0$ has no solutions in $\mathbb{Z}$, but solutions in $\mathbb{Z}/p\mathbb{Z}$ for all primes $p \equiv 1 (\mathrm{mod}\, 4)$.

- Seems to be very rare for integer solutions to surject onto mod p solutions (usually we obtain new mod p solutions for different primes p that do not come from integer solutions).

Strong Approximation

Conjecture (Strong Approximation).

Every mod p solution to the Markoff equation has an integer lift, for all primes p. That is, if (x, y, z) is a mod p solution to

$$X^2 + Y^2 + Z^2 = 3XYZ,$$

then there exists an integer solution $(\tilde{x}, \tilde{y}, \tilde{z})$ so that

$$(\tilde{x}, \tilde{y}, \tilde{z}) \equiv (x, y, z) \bmod p.$$

- Proven for "most" primes (Bourgain, Gamburd, Sarnak, 2016)
- Proven for all but finitely many primes (Chen, 2020)

In our last section, we'll see how linear recurrence sequences can play a role in studying explicit questions related to this conjecture.

Markoff mod p graphs

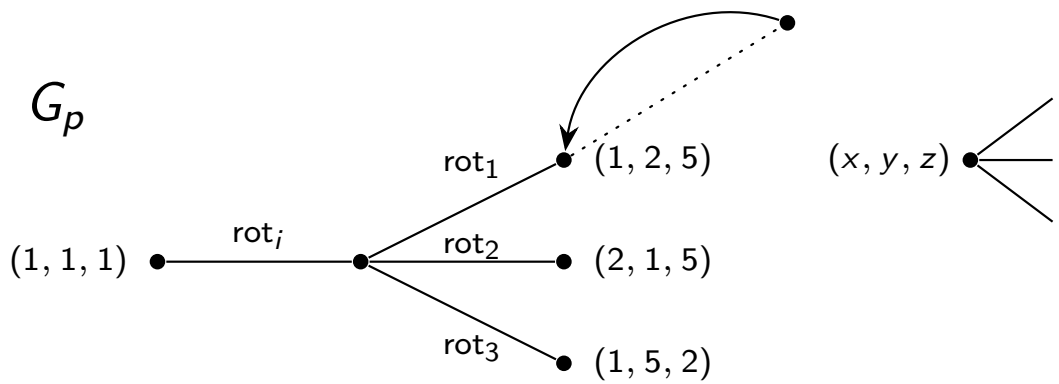
Define the ROTATIONS $\mathrm{rot}_i : \{\text{Markoff Triples}\} \to \{\text{Markoff Triples}\}$

$$\mathrm{rot}_1 = \sigma_{23} R_2 : (\mathbf{x}, y, z) \mapsto (\mathbf{x}, z, 3xz - y)$$

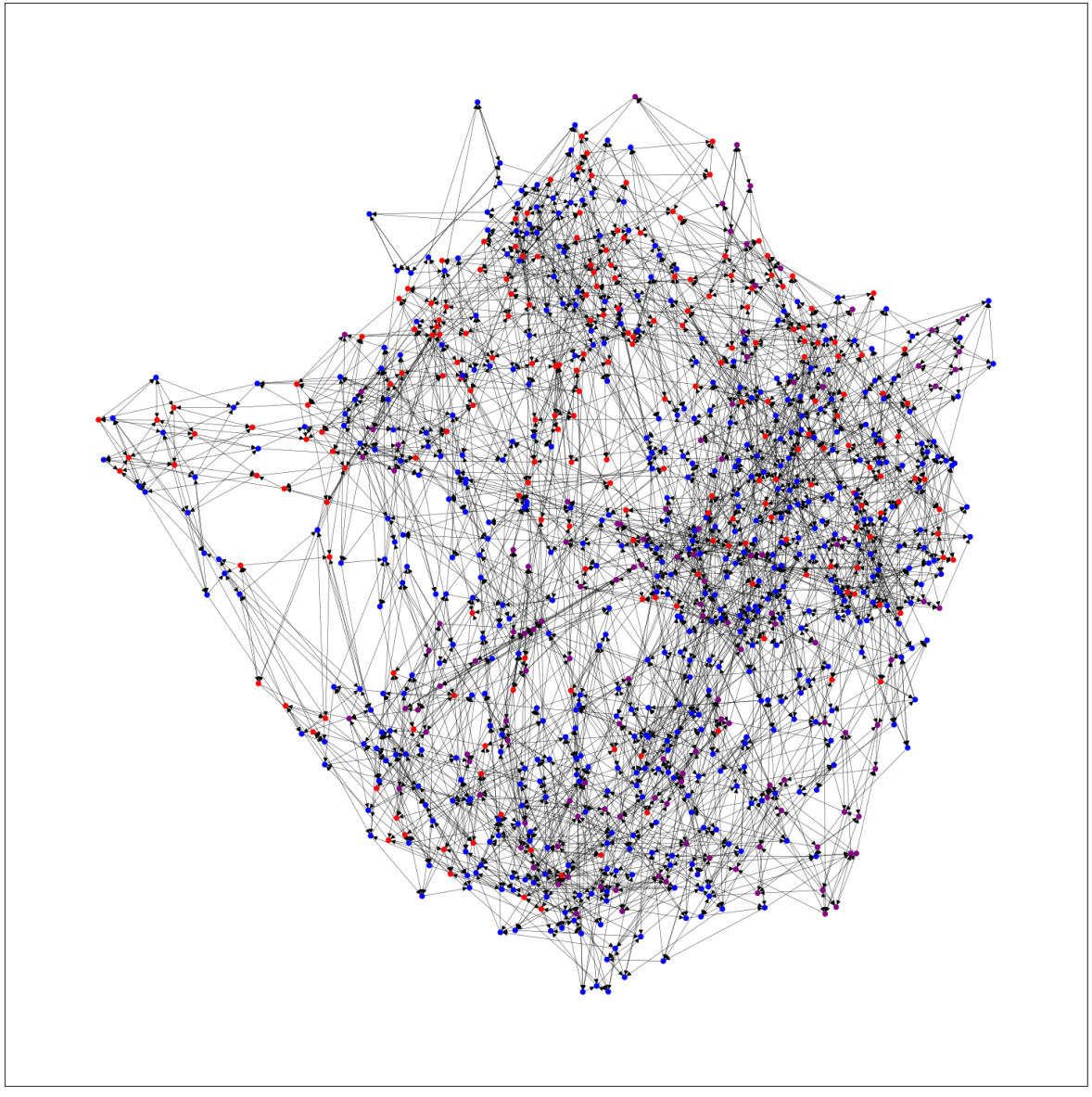
$$\mathrm{rot}_2 = \sigma_{13} R_1 : (x, \mathbf{y}, z) \mapsto (z, \mathbf{y}, 3yz - x)$$

$$\mathrm{rot}_3 = \sigma_{12} R_1 : (x, y, \mathbf{z}) \mapsto (y, 3yz - x, \mathbf{z}).$$

The MARKOFF MOD p GRAPHS are



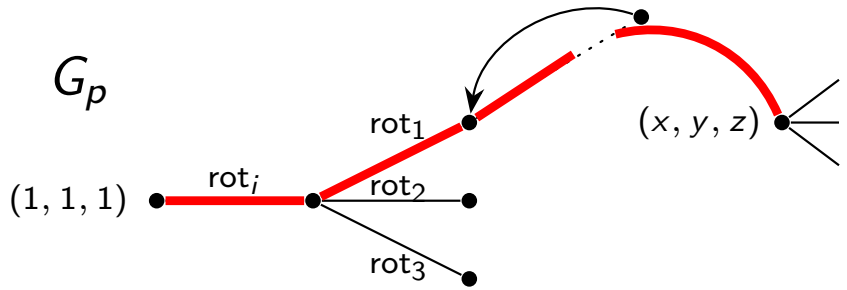
Markoff mod p graph G_{31}



Lifting via Paths

Key Observations.

- If $\mathcal{G}_p$ is connected, then Strong Approximation holds.
- Lifts of mod p points correspond to paths in $\mathcal{G}_p$ from $(1,1,1)$.



$$\mathrm{rot}_{i_s}^{n_s} \cdots \mathrm{rot}_{i_1}^{n_1}(1,1,1) = (x,y,z) \text{ in } \mathbb{Z}/p\mathbb{Z}$$

Applying the same operations to integer solutions gives

$$\mathrm{rot}_{i_s}^{n_s} \cdots \mathrm{rot}_{i_1}^{n_1}(1,1,1) = (\tilde{x},\tilde{y},\tilde{z}) \text{ in } \mathbb{Z}$$

and since the rot_i commutes with $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$ we get

$$(\tilde{x},\tilde{y},\tilde{z}) \equiv (x,y,z) \bmod p$$

Connection to Recurrence Sequences

Observation.

Recall $\text{rot}_1(\mathbf{x}, y, z) = (\mathbf{x}, z, \mathbf{3x}z - y)$. So,

$$\text{rot}_1^n(x, y, z) = (x, A(n), A(n+1)),$$

where $A(n)$ is the linear recurrence sequence

$$A(n+2) = \mathbf{3x}\, A(n+1) - A(n) \text{ initializing at } A(0) = y, A(1) = z.$$

ex: $\text{rot}_1^n(1, 1, 1) = (1, F(2n-1), F(2n+1))$ where $F(n)$ is the Fibonacci sequence.

Application #1: Linear Recurrence Sequences have Binet formulas (explicit).

Explicit Results: Bounding Lifts

Proposition (B., Chen*, Fuchs, Ye, 2025)

Let $n_i \in \mathbb{Z}_{\geq 1}$ and $i_j \in \{1, 2, 3\}$. Then we have

$$\text{size}(\text{rot}_{i_s}^{n_s} \cdots \text{rot}_{i_1}^{n_1}(1,1,1)) \leq (3\varepsilon)^{2^{s-1}(n_1+1)\cdots(n_s+1)},$$

where $\varepsilon = \frac{3+\sqrt{5}}{2}$.

- Switching between different rotations contributes doubly exponentially to growth, while staying along a single rotation contributes exponentially.
- Tells you how to look for "small lifts".

Explicit Results: Bounding Lifts

Theorem 1 (B., Chen*, Fuchs, Ye, 2025)

Let p be a prime so that $\mathrm{ord}_p(\mathrm{rot}_1^n(1,1,1)) \geq p-1$ for some n, and suppose that $\mathbf{x}$ is Markoff mod p point with $\mathrm{ord}_p(\mathbf{x}) > p^{\varepsilon}$ for $\varepsilon > 0$ fixed. Let $\tilde{\mathbf{x}}$ be a lift of $\mathbf{x}$ of minimal size. Then

$$\mathrm{size}(\tilde{\mathbf{x}}) < (3\varepsilon)^{2^{t+4}(2p+1)^{t+5}}$$

where $\varepsilon = (3+\sqrt{5})/2$ and $t = \tau(p^2-1)$.

Theorem 2 (B., Chen*, Fuchs, Ye, 2025)

Let p be a prime where Strong Approximation holds and let $h(p)$ be the expansion constant of the Markoff mod p graph $\mathcal{G}_p$. For a Markoff triple $\mathbf{x}$, let $\tilde{\mathbf{x}}$ be a lift of $\mathbf{x}$ of minimal size. Then

$$\mathrm{size}(\tilde{\mathbf{x}}) < (3\varepsilon)^{\left(\frac{p^3+3}{2}\right)^{20/\log\left(1+\frac{h(p)}{3}\right)}}.$$

Connection to Recurrence Sequences

Observation.

We have $\text{rot}_1^n(x, y, z) = (x, A(n), A(n+1))$, where $A(n)$ is an order 2 linear recurrence sequence.

Lemma (B., Chen*, Fuchs, Yi, 2025).

The *period* of $A(n)$ is equal to the period of the Lucas sequence $L(n)$ with parameters $(3x, 1)$.

Def: The PERIOD of $A(n)$ is smallest positive integer m so that $A(m) = A(0)$ and $A(m+1) = A(1)$ (so that recurrence repeats).

Application #2:

- Points with large orbits $\{\text{rot}_i^n(x, y, z) : n \in \mathbb{Z}\}$ are highly connected.
- BGS (2015) show that points with "large enough" orbits are guaranteed to be connected to each other.
- The size of this orbit is equal to the period of the corresponding Lucas sequence (widely studied).

Explicit Results: Connecting Special Points

Theorem (B., Dunn*, Naidu*, Wells*, 2025++).

If $p \equiv \pm 2 \pmod 5$ and $3x + 2$ is not a square mod p, then $2^{\nu_2(p+1)}$ divides the size of the orbit $\{\mathrm{rot}_i^n(x, y, z) : n \in \mathbb{Z}\}$.

Gives the following explicit consequence of BGS:

Consequence:

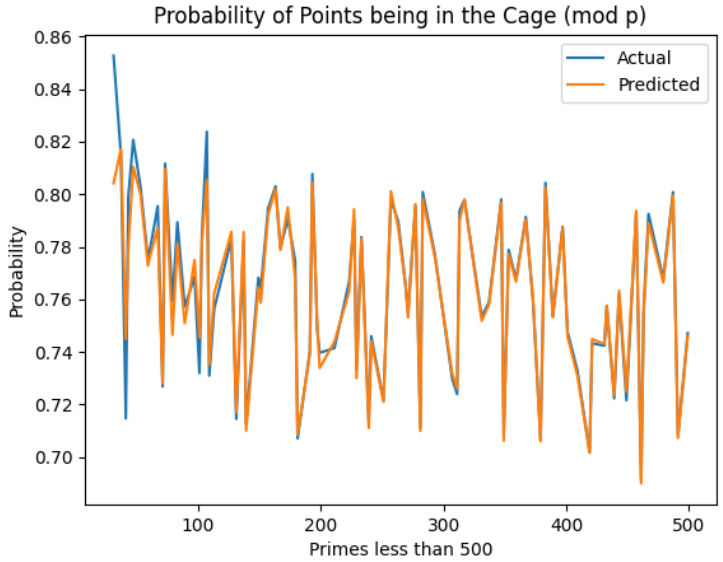
Let $p > 5$ be a Mersenne prime with $p \equiv \pm 2 \pmod 5$. If (x, y, z) is a mod p solution to the Markoff equation and the size of the orbit $\{\mathrm{rot}_i^n(x, y, z) : n \in \mathbb{Z}\}$ is at least $p + 1$ for some $i \in \{1, 2, 3\}$, then (x, y, z) has an integer lift.

Experimental Results: Points with Large Orbits

Theorem (B., Cho-Lee*, Okubo*, Sidhu*, 2025++).

Under some heuristic assumptions, the probability that a mod p solution (x, y, z) to the Markoff equation satisfies that the size of the orbit $\{\mathrm{rot}_i^n(x, y, z) : n \in \mathbb{Z}\}$ is at least $p + 1$ for $i \in \{1, 2, 3\}$ is approximately

$$1 - \left(1 - \left(\frac{1}{p} + \frac{\varphi(p-1)}{2p} + \frac{\varphi(p+1)}{2p}\right)\right)^3$$



Final Thoughts

Diophantine problems are ...

- Natural and intuitive
- Simple to state, but often very difficult to solve
- Generate new mathematics (no "unifying theory")
- Sometimes reveal "hidden structures" (sometimes via recurrence sequences)
- Can be studied explicitly and experimentally (good for undergraduate research!)

Thank you!