Prime Walk to Infinity in $\mathbb{Z}[\sqrt{2}]$

Daniel Sarnecki, Bencheng Li

Polymath REU

Adviced by Steven J. Miller (sjm1@williams.edu)
Popescu Tudor-Dimitrie, Wattanawanichkul Nawapan

September 20, 2020

Introduction

- Can one walk to Infinity with bounded steps on real line just using primes?

Introduction

- Can one walk to Infinity with bounded steps on real line just using primes?

  No. Pick a prime p such that $p > N$, then $p\# + 2, p\# + 3, ..., p\# + p$ are $N - 1$ consecutive composite numbers where $p\#$ is the primorial of p, meaning the product of all primes less than or equal to p.

Introduction

- Can one walk to Infinity with bounded steps on real line just using primes?

  No. Pick a prime p such that $p > N$, then $p\# + 2, p\# + 3, ..., p\# + p$ are $N - 1$ consecutive composite numbers where $p\#$ is the primorial of p, meaning the product of all primes less than or equal to p.

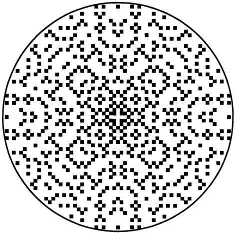
- What if we consider Gaussian primes or primes in $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$ instead of $\mathbb{Z}$?
  The figure below shows all Gaussian primes of norm less than 1000.

Introduction

- Can one walk to Infinity with bounded steps on real line just using primes?

  No. Pick a prime p such that $p > N$, then $p\# + 2, p\# + 3, ..., p\# + p$ are $N - 1$ consecutive composite numbers where $p\#$ is the primorial of p, meaning the product of all primes less than or equal to p.

- What if we consider Gaussian primes or primes in $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$ instead of $\mathbb{Z}$?
  The figure below shows all Gaussian primes of norm less than 1000.



Gaussian Moat Problem

- Gaussian primes are prime elements of $\mathbb{Z}[i]$. The number of Gaussian primes in a disk of radius n is about $O(\frac{n^2}{\log n})$.

Gaussian Moat Problem

- Gaussian primes are prime elements of $\mathbb{Z}[i]$. The number of Gaussian primes in a disk of radius n is about $O(\frac{n^2}{\log n})$.

Theorem (Nobuyuki Tsuchimura)

There exists a moat (or gaps between primes) of width 6 in $\mathbb{Z}[i]$.

Gaussian Moat Problem

- Gaussian primes are prime elements of $\mathbb{Z}[i]$. The number of Gaussian primes in a disk of radius n is about $O(\frac{n^2}{\log n})$.

Theorem (Nobuyuki Tsuchimura)

There exists a moat (or gaps between primes) of width 6 in $\mathbb{Z}[i]$.

Therefore, it's impossible to walk to infinity with step size 6. And it's widely believed that we cannot walk to infinity with any bounded step size.

Gaussian Moat Problem

- Gaussian primes are prime elements of $\mathbb{Z}[i]$. The number of Gaussian primes in a disk of radius n is about $O(\frac{n^2}{\log n})$.

Theorem (Nobuyuki Tsuchimura)

There exists a moat (or gaps between primes) of width 6 in $\mathbb{Z}[i]$.

Therefore, it's impossible to walk to infinity with step size 6. And it's widely believed that we cannot walk to infinity with any bounded step size.

- What if we consider $\mathbb{Z}[\sqrt{m}]$ for any integer m instead of just $\mathbb{Z}[i]$?

Gaussian Moat Problem

- Gaussian primes are prime elements of $\mathbb{Z}[i]$. The number of Gaussian primes in a disk of radius n is about $O(\frac{n^2}{\log n})$.

Theorem (Nobuyuki Tsuchimura)

There exists a moat (or gaps between primes) of width 6 in $\mathbb{Z}[i]$.

Therefore, it's impossible to walk to infinity with step size 6. And it's widely believed that we cannot walk to infinity with any bounded step size.

- What if we consider $\mathbb{Z}[\sqrt{m}]$ for any integer m instead of just $\mathbb{Z}[i]$?

If $m < 0$, the ring has only finitely many units but if $m > 0$, the ring would have infinitely many units. So the number of prime elements would differ a lot.

Primes in $\mathbb{Z}[\sqrt{2}]$

Since the number of primes is much larger in $\mathbb{Z}[\sqrt{m}]$ for positive m, we conjecture it's more possible to have a prime walk in these rings. We start with the easiest one $\mathbb{Z}[\sqrt{2}]$.

Primes in $\mathbb{Z}[\sqrt{2}]$

Since the number of primes is much larger in $\mathbb{Z}[\sqrt{m}]$ for positive m, we conjecture it's more possible to have a prime walk in these rings. We start with the easiest one $\mathbb{Z}[\sqrt{2}]$.

Definition

The norm of an element $a + \sqrt{2}b \in \mathbb{Z}[\sqrt{2}]$ is $|a^2 - 2b^2|$. Two elements are associates if they have the same norm. We define **standard prime** in $\mathbb{Z}[\sqrt{2}]$ as the following forms with minimal Euclidean norm:

- $\sqrt{2}$
- $a + \sqrt{2}b$ such that $a^2 - 2b^2$ is a real prime $\equiv 1, 7 \mod 8$
- $a + \sqrt{2}b$ such that $b = 0$ and a is a real prime $\equiv 3, 5 \mod 8$

And **regular primes** or **primes** are these standard primes with associates.

Primes in $\mathbb{Z}[\sqrt{2}]$

Since the number of primes is much larger in $\mathbb{Z}[\sqrt{m}]$ for positive m, we conjecture it's more possible to have a prime walk in these rings. We start with the easiest one $\mathbb{Z}[\sqrt{2}]$.

Definition

The norm of an element $a + \sqrt{2}b \in \mathbb{Z}[\sqrt{2}]$ is $|a^2 - 2b^2|$. Two elements are associates if they have the same norm. We define **standard prime** in $\mathbb{Z}[\sqrt{2}]$ as the following forms with minimal Euclidean norm:

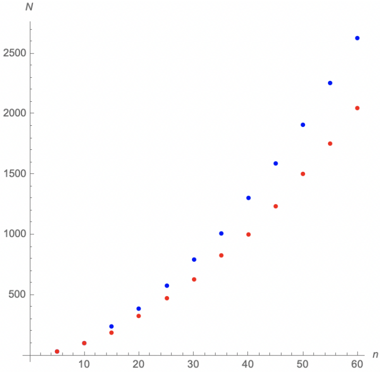
- $\sqrt{2}$
- $a + \sqrt{2}b$ such that $a^2 - 2b^2$ is a real prime $\equiv 1, 7 \mod 8$
- $a + \sqrt{2}b$ such that $b = 0$ and a is a real prime $\equiv 3, 5 \mod 8$

And **regular primes** or **primes** are these standard primes with associates.

Notice that primes in $\mathbb{Z}[\sqrt{2}]$ has a 4-fold symmetry.

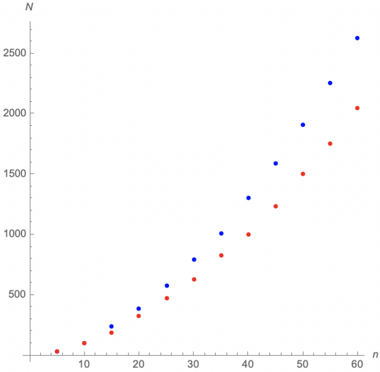
Comparison between $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$

The figure below shows the number of primes in a disk of radius n in $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$. Blue points are in $\mathbb{Z}[\sqrt{2}]$ and red points are in $\mathbb{Z}[i]$.



Comparison between $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$

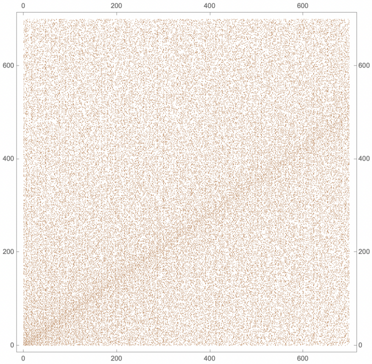
The figure below shows the number of primes in a disk of radius n in $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$. Blue points are in $\mathbb{Z}[\sqrt{2}]$ and red points are in $\mathbb{Z}[i]$.



Clearly, primes grows faster in $\mathbb{Z}[\sqrt{2}]$, which motivates us to study prime walks in this ring.

Visualization of Standard Primes

Each prime of the form $a + \sqrt{2}b$ is expressed as a dot $(a, b) \in \mathbb{R}^2$. The figure below shows all the standard primes for $x, y \leq 800$. Most primes seems to cluster along the asymptote $x - \sqrt{2}y = 0$.



Conjecture

Conjecture

There exists some finite step size k such that there exists an unbounded walk along the primes in $\mathbb{Z}[\sqrt{2}]$, where $\forall n\ d(p_{n+1}) > d(p_n)$, with d being the Euclidean distance.

Approaches

- Random Model
- Exhaustive Moat-finding

Random Model

Idea

1. Compute an estimate for the probability a given point is prime based on its norm
2. Use this estimate to build a greedy model that approximates an average walk

Random Model

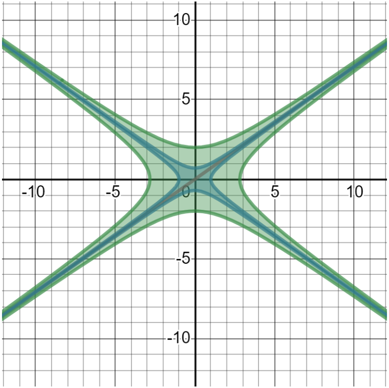
Idea

1. Compute an estimate for the probability a given point is prime based on its norm
2. Use this estimate to build a greedy model that approximates an average walk

This should allow us to then look at the long term behavior of walks when it becomes too computationally expensive to generate all walks.

Estimating the Number of Primes - Preliminaries

- We consider primes in the region $|a^2 - 2b^2| \leq r^2$, which straddles the asymptotes. This is a generalization of the disk region for Gaussian primes, using the norm of $\mathbb{Z}[\sqrt{2}]$.
- This region is unbounded as it approaches the asymptotes.



Estimating the Number of Primes - Extending PNT

Prime Number Theorem

If we consider the interval $[1, n]$, we have about $\frac{n}{\log n}$ primes.

Estimating the Number of Primes - Extending PNT

Prime Number Theorem

If we consider the interval $[1, n]$, we have about $\frac{n}{\log n}$ primes.

Utilizing the connection between ordinary primes and the primes in $\mathbb{Z}[\sqrt{2}]$, we were able to generalize PNT to the ring $\mathbb{Z}[\sqrt{2}]$.

Estimating the Number of Primes - Extending PNT

Prime Number Theorem

If we consider the interval $[1, n]$, we have about $\frac{n}{\log n}$ primes.

Utilizing the connection between ordinary primes and the primes in $\mathbb{Z}[\sqrt{2}]$, we were able to generalize PNT to the ring $\mathbb{Z}[\sqrt{2}]$.

Prime Number Theorem in $\mathbb{Z}[\sqrt{2}]$

The number of primes in $\mathbb{Z}[\sqrt{2}]$ within the region $|a^2 - 2b^2| \leq r^2$ is about $\frac{4r^2}{\log r} + \frac{r}{\log r} + 2$.

Estimating the Number of Primes - Extending PNT

Prime Number Theorem

If we consider the interval $[1, n]$, we have about $\frac{n}{\log n}$ primes.

Utilizing the connection between ordinary primes and the primes in $\mathbb{Z}[\sqrt{2}]$, we were able to generalize PNT to the ring $\mathbb{Z}[\sqrt{2}]$.

Prime Number Theorem in $\mathbb{Z}[\sqrt{2}]$

The number of primes in $\mathbb{Z}[\sqrt{2}]$ within the region $|a^2 - 2b^2| \leq r^2$ is about $\frac{4r^2}{\log r} + \frac{r}{\log r} + 2$.

Prime Number Theorem in $\mathbb{Z}[i]$

The number of Gaussian primes in the disk of radius r about the origin is $\frac{2r^2}{\log r} + \frac{2r}{\log r} + 4$.

Estimating the Number of Primes - Extending PNT

- How many primes are there in a circle C of radius r in the first quadrant?

Estimating the Number of Primes - Extending PNT

- How many primes are there in a circle C of radius r in the first quadrant?

Gauss Circle Problem

There are about πr^2 total lattice points inside a circle of radius r.

Estimating the Number of Primes - Extending PNT

- How many primes are there in a circle C of radius r in the first quadrant?

Gauss Circle Problem

There are about πr^2 total lattice points inside a circle of radius r.

- We can estimate the expected value by assuming each point in an annulus between circles of radius $d + r$ and $d - r$ has about the same probability of being prime.

Estimating the Number of Primes - Extending PNT

- How many primes are there in a circle C of radius r in the first quadrant?

Gauss Circle Problem

There are about πr^2 total lattice points inside a circle of radius r.

- We can estimate the expected value by assuming each point in an annulus between circles of radius $d + r$ and $d - r$ has about the same probability of being prime.
- If C is centered d from the origin, our estimate is $\left(\frac{(d+r)^2}{\log(d+r)} - \frac{(d-r)^2}{\log(d-r)}\right) \frac{r}{2d}$

Estimating the Total Number of Integers

- We have to find the total number of integers within the region $|a^2 - 2b^2| \leq r^2$.

Estimating the Total Number of Integers

- We have to find the total number of integers within the region $|a^2 - 2b^2| \leq r^2$.

- Would like to count families of infinite solutions that have the same magnitude as those we previously counted.

Estimating the Total Number of Integers

- We have to find the total number of integers within the region $|a^2 - 2b^2| \leq r^2$.

- Would like to count families of infinite solutions that have the same magnitude as those we previously counted.

- As before, any solution z belongs to a family of solutions $z(1+\sqrt{2})^{2n}$ which maintain the norm.

Estimating the Total Number of Integers

- We can find these families of solutions by considering $a^2 - 2b^2 = c$ for each integer c with $|c| \leq r^2$.

Estimating the Total Number of Integers

- We can find these families of solutions by considering $a^2 - 2b^2 = c$ for each integer c with $|c| \leq r^2$.

Theorem (Bernays)

Let $f(x, y) = rx^2 + sxy + ty^2$ be defined on the integers with integer coefficients such that $s^2 - rt$ is not square. Then the number of positive integers less than n that can be expressed as $f(x, y)$ is $O\left(\frac{n}{\sqrt{\log n}}\right)$

Estimating the Total Number of Integers

- We can find these families of solutions by considering $a^2 - 2b^2 = c$ for each integer c with $|c| \leq r^2$.

Theorem (Bernays)

Let $f(x, y) = rx^2 + sxy + ty^2$ be defined on the integers with integer coefficients such that $s^2 - rt$ is not square. Then the number of positive integers less than n that can be expressed as $f(x, y)$ is $O\left(\frac{n}{\sqrt{\log n}}\right)$

Theorem (Polymath 2020)

$\exists\ a_1, b_1 \in \mathbb{Z}$ such that $a_1^2 - 2b_1^2 = c \iff \exists\ a_2, b_2 \in \mathbb{Z}$ such that $a_2^2 - 2b_2^2 = -c$

Random Model - Summary

Combining our main two estimates, we obtain the following estimate:

Random Model - Summary

Combining our main two estimates, we obtain the following estimate:

Theorem (Polymath 2020)

The probability an integer in $\mathbb{Z}[\sqrt{2}]$ with norm n is prime is about $O\left(\frac{1}{\sqrt{\log n}}\right)$.

Random Model - Summary

Combining our main two estimates, we obtain the following estimate:

Theorem (Polymath 2020)

The probability an integer in $\mathbb{Z}[\sqrt{2}]$ with norm n is prime is about $O\left(\frac{1}{\sqrt{\log n}}\right)$.

For comparison,

- In $\mathbb{Z}$: $O\left(\frac{1}{\log n}\right)$
- In $\mathbb{Z}[i]$: $O\left(\frac{1}{\log n}\right)$

Visualizing Prime Walks

Algorithm (Stan Wagon)

Visualizing Prime Walks

Algorithm (Stan Wagon)

- Identify all primes in a disk

Visualizing Prime Walks

Algorithm (Stan Wagon)

- Identify all primes in a disk
- For each prime, find its $d-$neighbors (d is step size)

Visualizing Prime Walks

Algorithm (Stan Wagon)

- Identify all primes in a disk
- For each prime, find its $d-$neighbors (d is step size)
- Form the road network connecting all the primes and their $d-$neighbors

Visualizing Prime Walks

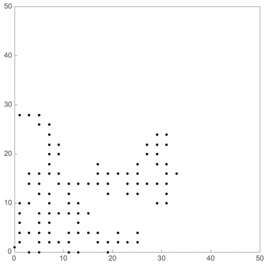
Algorithm (Stan Wagon)

- Identify all primes in a disk
- For each prime, find its $d-$neighbors (d is step size)
- Form the road network connecting all the primes and their $d-$neighbors
- Find the connected component of $\sqrt{2}$

Visualizing Prime Walks

Algorithm (Stan Wagon)

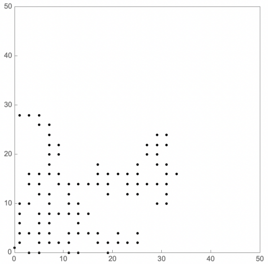
- Identify all primes in a disk
- For each prime, find its $d-$neighbors (d is step size)
- Form the road network connecting all the primes and their $d-$neighbors
- Find the connected component of $\sqrt{2}$

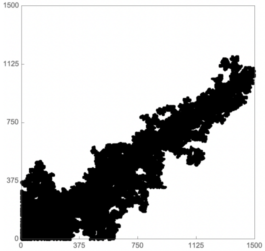


Visualizing Prime Walks

Algorithm (Stan Wagon)

- Identify all primes in a disk
- For each prime, find its $d-$neighbors (d is step size)
- Form the road network connecting all the primes and their $d-$neighbors
- Find the connected component of $\sqrt{2}$





Pell's Equation

Definition

Pell's equation is $x^2 - 2y^2 = 1$. A **generalized Pell's equation** is $x^2 - 2y^2 = c$ for constant c.

Pell's Equation

Definition

Pell's equation is $x^2 - 2y^2 = 1$. A **generalized Pell's equation** is $x^2 - 2y^2 = c$ for constant c.

- Solving the integer solutions to generalized Pell's equation is equivalent to finding all primes of norm c.

Pell's Equation

Definition

Pell's equation is $x^2 - 2y^2 = 1$. A **generalized Pell's equation** is $x^2 - 2y^2 = c$ for constant c.

- Solving the integer solutions to generalized Pell's equation is equivalent to finding all primes of norm c.

Lemma 1

There is only one nontrivial solution (up to associates) to any generalized Pell's equation with constant $c \equiv 1, 7 \mod 8$.

Pell's Equation

Definition

Pell's equation is $x^2 - 2y^2 = 1$. A **generalized Pell's equation** is $x^2 - 2y^2 = c$ for constant c.

- Solving the integer solutions to generalized Pell's equation is equivalent to finding all primes of norm c.

Lemma 1

There is only one nontrivial solution (up to associates) to any generalized Pell's equation with constant $c \equiv 1, 7 \mod 8$.

Using this lemma, we are able to prove the next theorem.

Number of Norms

Theorem (Polymath 2020)

It's impossible to walk to infinity using primes of only finitely many norms, or integer solutions to only finitely many generalized Pell's equations.

Number of Norms - Proof Sketch

We start with a weaker statement

Lemma 2

Number of Norms - Proof Sketch

We start with a weaker statement

Lemma 2

it's impossible to walk to infinity using integer solutions to only finitely many generalized Pell's equations including $x^2 - 2y^2 = \pm 1$.

Number of Norms - Proof Sketch

We start with a weaker statement

Lemma 2

it's impossible to walk to infinity using integer solutions to only finitely many generalized Pell's equations including $x^2 - 2y^2 = \pm 1$.

- All integer solutions in the first octant to $x^2 - 2y^2 = \pm 1$ stand for $(1+\sqrt{2})^m$ in $\mathbb{Z}[\sqrt{2}]$ for integer m.

Number of Norms - Proof Sketch

We start with a weaker statement

Lemma 2

it's impossible to walk to infinity using integer solutions to only finitely many generalized Pell's equations including $x^2 - 2y^2 = \pm 1$.

- All integer solutions in the first octant to $x^2 - 2y^2 = \pm 1$ stand for $(1+\sqrt{2})^m$ in $\mathbb{Z}[\sqrt{2}]$ for integer m.
- Assume $(1+\sqrt{2})^m = a + \sqrt{2}b$ for some a, b, then $(1+\sqrt{2})^{m+1} = (a+2b) + (a+b)\sqrt{2}$. So the vertical and horizontal gaps are both $O(b)$.

Number of Norms - Proof Sketch

We start with a weaker statement

Lemma 2

it's impossible to walk to infinity using integer solutions to only finitely many generalized Pell's equations including $x^2 - 2y^2 = \pm 1$.

- All integer solutions in the first octant to $x^2 - 2y^2 = \pm 1$ stand for $(1+\sqrt{2})^m$ in $\mathbb{Z}[\sqrt{2}]$ for integer m.
- Assume $(1+\sqrt{2})^m = a + \sqrt{2}b$ for some a, b, then $(1+\sqrt{2})^{m+1} = (a+2b) + (a+b)\sqrt{2}$. So the vertical and horizontal gaps are both $O(b)$.
- Then the number of primes between this gap should be at least $O(b)$.

Number of Norms - Proof Sketch

We start with a weaker statement

Lemma 2

it's impossible to walk to infinity using integer solutions to only finitely many generalized Pell's equations including $x^2 - 2y^2 = \pm 1$.

- All integer solutions in the first octant to $x^2 - 2y^2 = \pm 1$ stand for $(1+\sqrt{2})^m$ in $\mathbb{Z}[\sqrt{2}]$ for integer m.
- Assume $(1+\sqrt{2})^m = a + \sqrt{2}b$ for some a, b, then $(1+\sqrt{2})^{m+1} = (a+2b) + (a+b)\sqrt{2}$. So the vertical and horizontal gaps are both $O(b)$.
- Then the number of primes between this gap should be at least $O(b)$.
- By Lemma 1, we must have solutions to infinitely many Pell's equation to finish the gap as $b \to \infty$.

Boundedness from the Asymptote

Theorem (Polymath 2020)

It is impossible to perform a walk of bounded step size to infinity in $\mathbb{Z}[\sqrt{2}]$ if we remain within some bounded distance from the asymptote $y = \frac{1}{\sqrt{2}}x$.

Boundedness from the Asymptote - Proof Sketch

- Note that we take at most $\frac{x}{\sqrt{2}} = O(x)$ steps when we are x from the origin.

Boundedness from the Asymptote - Proof Sketch

- Note that we take at most $\frac{x}{\sqrt{2}} = O(x)$ steps when we are x from the origin.
- The gap between the asymptote and the curve $a^2 - 2b^2 = c$ grows at a rate of $O\left(\frac{1}{x}\right)$.

Boundedness from the Asymptote - Proof Sketch

- Note that we take at most $\frac{x}{\sqrt{2}} = O(x)$ steps when we are x from the origin.
- The gap between the asymptote and the curve $a^2 - 2b^2 = c$ grows at a rate of $O\left(\frac{1}{x}\right)$.
- The number of norm-curves with norm $\pm 1 \pmod 8$ we could possibly access at x is $O\left(\frac{x}{\log x}\right)$.

Boundedness from the Asymptote - Proof Sketch

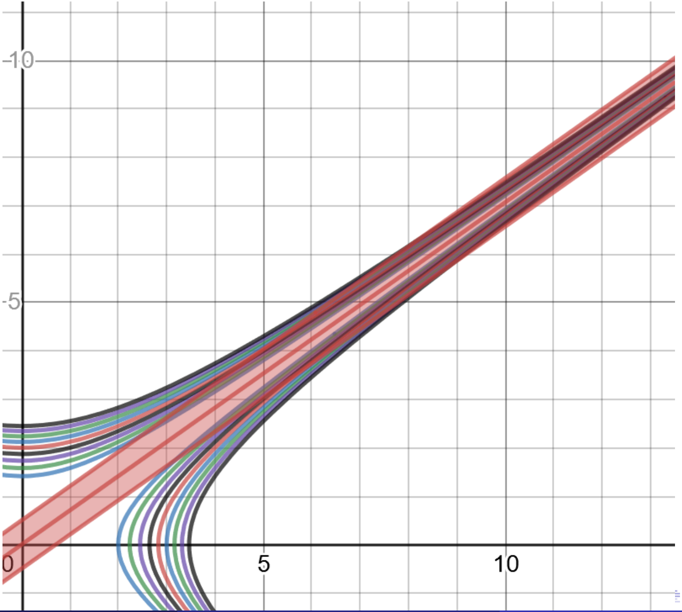
- Note that we take at most $\frac{x}{\sqrt{2}} = O\left(x\right)$ steps when we are x from the origin.

- The gap between the asymptote and the curve $a^2 - 2b^2 = c$ grows at a rate of $O\left(\frac{1}{x}\right)$.

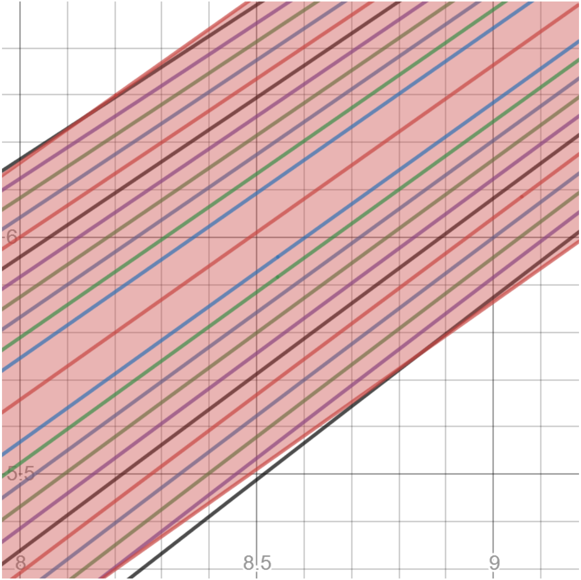
- The number of norm-curves with norm $\pm 1 \pmod 8$ we could possibly access at x is $O\left(\frac{x}{\log x}\right)$.

- We expect one prime for each such curve since associates grow exponentially, thus the number of steps grows faster than the number of options for steps!

Boundedness from the Asymptote - Proof Sketch



Boundedness from the Asymptote - Proof Sketch



Acknowledgement

We would like to thank our mentors Professor Steven J. Miller, Popescu Tudor-Dimitrie, Wattanawanichkul Nawapan and others from the Polymath REU for their help in this project.