Connectivity of Markoff mod p Graphs and Maximal Divisors

Matthew Litman
Joint work J. Eddy, E. Fuchs, D. Martin, & N. Tripeny

Joint Mathematics Meetings
AMS Special Session on Recent Developments on Markoff Triples
January 4th, 2024

Outline of the Talk

1. Introduce $\mathcal{G}_p$ and a Conjecture on Markoff mod p Connectivity

Outline of the Talk

1. Introduce $\mathcal{G}_p$ and a Conjecture on Markoff mod p Connectivity
2. A Lower Bound for Connectivity of $\mathcal{G}_p$

Outline of the Talk

1. Introduce $\mathcal{G}_p$ and a Conjecture on Markoff mod p Connectivity
2. A Lower Bound for Connectivity of $\mathcal{G}_p$
3. Introduce Maximal Divisors $M_d(n)$

Outline of the Talk

1. Introduce $\mathcal{G}_p$ and a Conjecture on Markoff mod p Connectivity
2. A Lower Bound for Connectivity of $\mathcal{G}_p$
3. Introduce Maximal Divisors $M_d(n)$
4. A Better Lower Bound from $M_d(n)$

Markoff Triples – What Are They?

A *Markoff triple* (x, y, z) is a non-negative integer triple satisfying the *Markoff equation*

$$\mathcal{M} : x^2 + y^2 + z^2 = 3xyz$$

A coordinate of a triple is called a *Markoff number*.

Markoff Triples – What Are They?

A *Markoff triple* (x, y, z) is a non-negative integer triple satisfying the *Markoff equation*

$$\mathcal{M} : x^2 + y^2 + z^2 = 3xyz$$

A coordinate of a triple is called a *Markoff number*.

- First introduced by A. Markoff in 1879 in constructing rational approximations by continued fraction expansions

Markoff Triples – What Are They?

A *Markoff triple* (x, y, z) is a non-negative integer triple satisfying the *Markoff equation*

$$\mathcal{M} : x^2 + y^2 + z^2 = 3xyz$$

A coordinate of a triple is called a *Markoff number*.

- First introduced by A. Markoff in 1879 in constructing rational approximations by continued fraction expansions
- Zagier (1982) showed that the number of Markoff triples with $x \leq y \leq z \leq T$ as $T \to \infty$ grows like

$$C(\log(T))^2 + O(\log(T)\log(\log(T))^2)$$
$$\text{with } C \approx 0.180717047$$

Orbit Structure of Markoff Triples

There are three involutions acting on $\mathcal{M}(\mathbb{Z})$ (Vieta moves):

$$R_1(x,y,z) = (3yz - x, y, z), \quad R_2(x,y,z) = (x, 3xz - y, z),$$
$$R_3(x,y,z) = (x, y, 3xy - z)$$

Orbit Structure of Markoff Triples

There are three involutions acting on $\mathcal{M}(\mathbb{Z})$ (Vieta moves):

$$R_1(x, y, z) = (3yz - x, y, z), \quad R_2(x, y, z) = (x, 3xz - y, z),$$
$$R_3(x, y, z) = (x, y, 3xy - z)$$

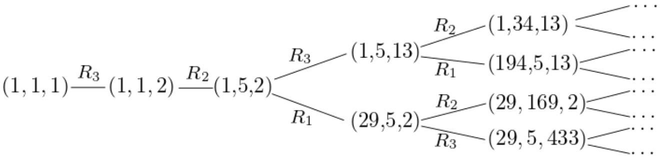
Markoff showed that under the action of the R_1, R_2, R_3, $\mathcal{M}(\mathbb{Z})$ consists of two orbits, one "small" (solely $(0, 0, 0)$) and one "large" (generated by $(1, 1, 1)$)

Orbit Structure of Markoff Triples

There are three involutions acting on $\mathcal{M}(\mathbb{Z})$ (Vieta moves):

$$R_1(x,y,z) = (3yz - x, y, z), \quad R_2(x,y,z) = (x, 3xz - y, z),$$
$$R_3(x,y,z) = (x, y, 3xy - z)$$

Markoff showed that under the action of the R_1, R_2, R_3, $\mathcal{M}(\mathbb{Z})$ consists of two orbits, one "small" (solely $(0,0,0)$) and one "large" (generated by $(1,1,1)$)



Markoff Graph mod p

Consider the graph $\mathcal{G}_p$ where vertices are given by non-$(0,0,0)$ solutions to $\mathcal{M}(\mathbb{F}_p)$ and an edge exists between two vertices if they are related by a Vieta involution.

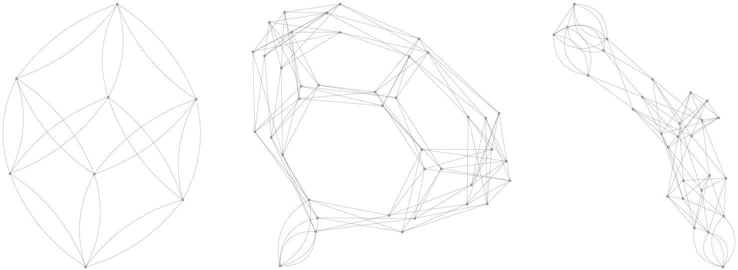


Figure: The Markoff mod-p graphs G_p for $p = 3$, 5, and 7.

Markoff Graph mod p

Consider the graph $\mathcal{G}_p$ where vertices are given by non-$(0,0,0)$ solutions to $\mathcal{M}(\mathbb{F}_p)$ and an edge exists between two vertices if they are related by a Vieta involution.

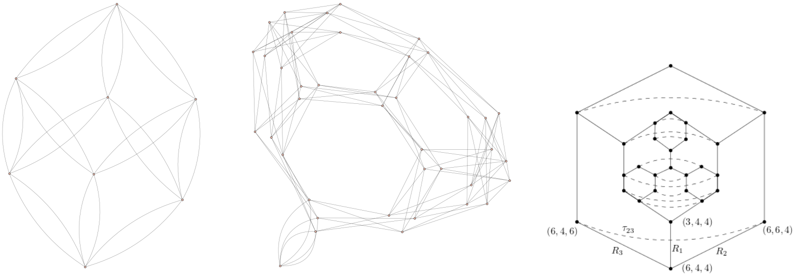


Figure: The Markoff mod-p graphs G_p for $p = 3$, 5, and 7.

Strong Approximation for $\mathcal{G}_p$

Conjecture (Strong Approximation Conjecture, Baragar (1991))

The projection map $\pi_p : \mathcal{M}(\mathbb{Z}) \to \mathcal{G}_p$ *is surjective, or equivalently, the Markoff mod* p *graphs are connected for all primes* p*.*

Strong Approximation for $\mathcal{G}_p$

Conjecture (Strong Approximation Conjecture, Baragar (1991))

The projection map $\pi_p : \mathcal{M}(\mathbb{Z}) \to \mathcal{G}_p$ is surjective, or equivalently, the Markoff mod p graphs are connected for all primes p.

Theorem (Bourgain-Gamburd-Sarnak (2016))

If $\mathcal{B}$ is the set of primes p for which strong approximation fails, then

$$|\mathcal{B} \cap [0, T]| \ll_\varepsilon T^\varepsilon \text{ for any } \varepsilon > 0.$$

Strong Approximation for $\mathcal{G}_p$

Conjecture (Strong Approximation Conjecture, Baragar (1991))

The projection map $\pi_p : \mathcal{M}(\mathbb{Z}) \to \mathcal{G}_p$ is surjective, or equivalently, the Markoff mod p graphs are connected for all primes p.

Theorem (Bourgain-Gamburd-Sarnak (2016))

If $\mathcal{B}$ is the set of primes p for which strong approximation fails, then

$$|\mathcal{B} \cap [0, T]| \ll_\varepsilon T^\varepsilon \text{ for any } \varepsilon > 0.$$

Theorem (Chen (2022))

There exists a prime p_0 such that for all $p \geq p_0$, $\mathcal{G}_p$ is connected.

What is Known About Connectivity of $\mathcal{G}_p$ and p_0?

- Strong Approximation Conjecture is equivalent to $p_0 = 2$

What is Known About Connectivity of $\mathcal{G}_p$ and p_0?

- Strong Approximation Conjecture is equivalent to $p_0 = 2$
- Chen (2022) showed that the size of any connected component of $\mathcal{G}_p$ is divisible by p (strengthened to $4p$)

What is Known About Connectivity of $\mathcal{G}_p$ and p_0?

- Strong Approximation Conjecture is equivalent to $p_0 = 2$
- Chen (2022) showed that the size of any connected component of $\mathcal{G}_p$ is divisible by p (strengthened to $4p$)
- de Courcy-Ireland and Lee (2020) showed that $\mathcal{G}_p$ is connected for $p \leq 3000$

What is Known About Connectivity of $\mathcal{G}_p$ and p_0?

- Strong Approximation Conjecture is equivalent to $p_0 = 2$
- Chen (2022) showed that the size of any connected component of $\mathcal{G}_p$ is divisible by p (strengthened to $4p$)
- de Courcy-Ireland and Lee (2020) showed that $\mathcal{G}_p$ is connected for $p \leq 3000$
- Brown (2023/24) verified connectivity for $p \leq 1,000,000$ (to be talked about later today)

What is Known About Connectivity of $\mathcal{G}_p$ and p_0?

- Strong Approximation Conjecture is equivalent to $p_0 = 2$
- Chen (2022) showed that the size of any connected component of $\mathcal{G}_p$ is divisible by p (strengthened to $4p$)
- de Courcy-Ireland and Lee (2020) showed that $\mathcal{G}_p$ is connected for $p \leq 3000$
- Brown (2023/24) verified connectivity for $p \leq 1,000,000$ (to be talked about later today)
- Eddy–Fuchs–L.–Martin–Tripeny (2023) showed that $p_0 \leq 3.448 \times 10^{392}$ (to be talked about now)

What is Known About Connectivity of $\mathcal{G}_p$ and p_0?

- Strong Approximation Conjecture is equivalent to $p_0 = 2$
- Chen (2022) showed that the size of any connected component of $\mathcal{G}_p$ is divisible by p (strengthened to $4p$)
- de Courcy-Ireland and Lee (2020) showed that $\mathcal{G}_p$ is connected for $p \leq 3000$
- Brown (2023/24) verified connectivity for $p \leq 1,000,000$ (to be talked about later today)
- Eddy–Fuchs–L.–Martin–Tripeny (2023) showed that $p_0 \leq 3.448 \times 10^{392}$ (to be talked about now)

The window from 10^6 to 10^{392} has yet to be filled in!

A Preliminary Bound

Proposition (Eddy–Fuchs–L.–Martin–Tripeny ('23))

$\mathcal{G}_p$ is connected for all primes $p > 10^{532}$.

A Preliminary Bound

Proposition (Eddy–Fuchs–L.–Martin–Tripeny ('23))

$\mathcal{G}_p$ is connected for all primes $p > 10^{532}$.

We will outline how this result is obtained to illuminate the general strategy for our stronger result

Parametrizing Markoff Triples

– A triple $(a, b, c) \in \mathbb{F}_p$ with $a \neq 0, \pm\frac{2}{3}$ solves $x^2 + y^2 + z^2 = 3xyz$ if and only if it is of the form

$$\left(r + r^{-1}, \frac{(r + r^{-1})(s + s^{-1})}{r - r^{-1}}, \frac{(r + r^{-1})(rs + r^{-1}s^{-1})}{r - r^{-1}} \right)$$

for some $r, s \in \mathbb{F}_{p^2}^{\times}$.

Parametrizing Markoff Triples

– A triple $(a, b, c) \in \mathbb{F}_p$ with $a \neq 0, \pm\frac{2}{3}$ solves $x^2 + y^2 + z^2 = 3xyz$ if and only if it is of the form

$$\left(r + r^{-1}, \frac{(r + r^{-1})(s + s^{-1})}{r - r^{-1}}, \frac{(r + r^{-1})(rs + r^{-1}s^{-1})}{r - r^{-1}} \right)$$

for some $r, s \in \mathbb{F}_{p^2}^\times$.
– The orbit of this triple under R_2 and R_3 consists precisely of triples of the form

$$\left(r + r^{-1}, \frac{(r + r^{-1})(r^{2n}s + r^{-2n}s^{-1})}{r - r^{-1}}, \frac{(r + r^{-1})(r^{2n\pm1}s + r^{2n\pm1}s^{-1})}{r - r^{-1}} \right)$$

for some $n \in \mathbb{Z}$

Order of a Triple and the Cage

- The Order of Markoff mod p triple (a, b, c), denoted $\mathrm{Ord}((a, b, c))$, is

$$\max(\mathrm{ord}_p(a), \mathrm{ord}_p(b), \mathrm{ord}_p(c))$$

where $\mathrm{ord}_p(a)$ is the multiplicative order of r in $\mathbb{F}_{p^2}^{\times}$ and $a = r + r^{-1}$

Order of a Triple and the Cage

- The Order of Markoff mod p triple (a, b, c), denoted $\mathrm{Ord}((a, b, c))$, is

$$\max(\mathrm{ord}_p(a), \mathrm{ord}_p(b), \mathrm{ord}_p(c))$$

  where $\mathrm{ord}_p(a)$ is the multiplicative order of r in $\mathbb{F}_{p^2}^\times$ and $a = r + r^{-1}$
- Define the Cage $\mathcal{C}_p$ to be the connected component in $\mathcal{G}_p$ of triples of maximal order

Order of a Triple and the Cage

- The Order of Markoff mod p triple (a, b, c), denoted $\mathrm{Ord}((a, b, c))$, is

$$\max(\mathrm{ord}_p(a), \mathrm{ord}_p(b), \mathrm{ord}_p(c))$$

  where $\mathrm{ord}_p(a)$ is the multiplicative order of r in $\mathbb{F}_{p^2}^\times$ and $a = r + r^{-1}$
- Define the Cage $\mathcal{C}_p$ to be the connected component in $\mathcal{G}_p$ of triples of maximal order

To show connectivity, it suffices to show $\mathcal{G}_p \backslash \mathcal{C}_p$ is empty (which by Chen has size divisible by p)

Connectivity Proof Sketch

- Suppose (a, b, c) is not in the Cage and is of maximal Order d among all non-Cage elements, with a the coordinate of order d

Connectivity Proof Sketch

- Suppose (a, b, c) is not in the Cage and is of maximal Order d among all non-Cage elements, with a the coordinate of order d
- This triple is connected to those whose other entries are of the form $\frac{(r+r^{-1})(sr^n+(sr^n)^{-1})}{r-r^{-1}}$ for some n

Connectivity Proof Sketch

- Suppose (a, b, c) is not in the Cage and is of maximal Order d among all non-Cage elements, with a the coordinate of order d
- This triple is connected to those whose other entries are of the form $\frac{(r+r^{-1})(sr^n+(sr^n)^{-1})}{r-r^{-1}}$ for some n
- Since d is maximal, the order of $\frac{(r+r^{-1})(sr^n+(sr^n)^{-1})}{r-r^{-1}} = f + f^{-1}$ (call it d') must satisfy $d' \leq d$, $d'|p \pm 1$

Connectivity Proof Sketch

- Suppose (a, b, c) is not in the Cage and is of maximal Order d among all non-Cage elements, with a the coordinate of order d
- This triple is connected to those whose other entries are of the form $\frac{(r+r^{-1})(sr^n+(sr^n)^{-1})}{r-r^{-1}}$ for some n
- Since d is maximal, the order of $\frac{(r+r^{-1})(sr^n+(sr^n)^{-1})}{r-r^{-1}} = f + f^{-1}$ (call it d') must satisfy $d' \leq d$, $d'|p \pm 1$
- So our aim is to bound the number of possible exponents n for which $\mathrm{ord}_p(\frac{(r+r^{-1})(sr^n+(sr^n)^{-1})}{r-r^{-1}}) = d'$ divides d

Bounding Solutions

Lemma (Eddy–Fuchs–L.–Martin–Tripeny ('23))

If $r \in \mathbb{F}_{p^2}^\times$ has order $t > 2$, then the number of congruence classes $n \pmod{t}$ for which $ord_p((r + r^{-1})(sr^n + (sr^n)^{-1})/(r - r^{-1}))$ divides d is at most $\frac{3}{2}\max((6td)^{1/3}, 4td/p)$.

Bounding Solutions

Lemma (Eddy–Fuchs–L.–Martin–Tripeny ('23))

If $r \in \mathbb{F}_{p^2}^{\times}$ has order $t > 2$, then the number of congruence classes $n \pmod{t}$ for which $ord_p((r + r^{-1})(sr^n + (sr^n)^{-1})/(r - r^{-1}))$ divides d is at most $\frac{3}{2}\max((6td)^{1/3}, 4td/p)$.

If we consider d to be the largest order of any element not in the cage and $\mathcal{T}_d$ to be the number of divisors of $p \pm 1$ which do not exceed d, then

Bounding Solutions

Lemma (Eddy–Fuchs–L.–Martin–Tripeny ('23))

If $r \in \mathbb{F}_{p^2}^{\times}$ has order $t > 2$, then the number of congruence classes $n \pmod t$ for which $\mathrm{ord}_p((r + r^{-1})(sr^n + (sr^n)^{-1})/(r - r^{-1}))$ divides d is at most $\frac{3}{2}\max((6td)^{1/3}, 4td/p)$.

If we consider d to be the largest order of any element not in the cage and $\mathcal{T}_d$ to be the number of divisors of $p \pm 1$ which do not exceed d, then

$$d \leq \sum_{d' \in \mathcal{T}_d} \frac{3}{2} \max\left((6dd')^{1/3}, \frac{4dd'}{p}\right) < \frac{3T_d}{2} \max\left((6d^2)^{1/3}, \frac{4d^2}{p}\right).$$

Bounding Solutions

Lemma (Eddy–Fuchs–L.–Martin–Tripeny ('23))

If $r \in \mathbb{F}_{p^2}^{\times}$ has order $t > 2$, then the number of congruence classes $n \pmod{t}$ for which $ord_p((r + r^{-1})(sr^n + (sr^n)^{-1})/(r - r^{-1}))$ divides d is at most $\frac{3}{2}\max((6td)^{1/3}, 4td/p)$.

If we consider d to be the largest order of any element not in the cage and $\mathcal{T}_d$ to be the number of divisors of $p \pm 1$ which do not exceed d, then

$$d \leq \sum_{d' \in \mathcal{T}_d} \frac{3}{2} \max\left((6dd')^{1/3}, \frac{4dd'}{p}\right) < \frac{3T_d}{2} \max\left((6d^2)^{1/3}, \frac{4d^2}{p}\right).$$

Considering both cases separately and rearranging yields...

First Connectivity Criterion

Proposition (Eddy–Fuchs–L.–Martin–Tripeny ('23))

Let $\tau_d(n)$ denote the number of divisors of n that are $\leq d$. For d dividing $p-1$ or $p+1$, let $T_d = \tau_d(p-1) + \tau_d(p+1)$. If no such divisor satisfies either inequality

$$\frac{2\sqrt{2p}}{T_d} < d < \frac{81T_d^3}{4} \quad \text{or} \quad \frac{p}{6T_d} < d < \frac{8\sqrt{p}(p \pm 1)\tau(p \pm 1)}{\phi(p \pm 1)}$$

(where the $\pm$ is $+$ when $d|p+1$ and $-$ if $d|p-1$), then $\mathcal{G}_p$ is connected.

First Connectivity Criterion

Proposition (Eddy–Fuchs–L.–Martin–Tripeny ('23))

Let $\tau_d(n)$ denote the number of divisors of n that are $\leq d$. For d dividing $p-1$ or $p+1$, let $T_d = \tau_d(p-1) + \tau_d(p+1)$. If no such divisor satisfies either inequality

$$\frac{2\sqrt{2p}}{T_d} < d < \frac{81\,T_d^3}{4} \quad \text{or} \quad \frac{p}{6\,T_d} < d < \frac{8\sqrt{p}(p \pm 1)\tau(p \pm 1)}{\phi(p \pm 1)}$$

(where the $\pm$ is $+$ when $d|p+1$ and $-$ if $d|p-1$),
then $\mathcal{G}_p$ is connected.

Applying standard bounds for τ and ϕ yields our 10^{532} bound

Maximal Divisors

Definition

For a natural number n and real ℓ, let $\mathcal{M}_\ell(n)$ denote the set of divisors d of n less than or equal to ℓ such that no other divisor d' of n less than or equal to ℓ divides d

As ℓ increases, $\mathcal{M}_\ell(n)$ is constant between any two consecutive divisors of n, so we only need to check $\mathcal{M}_d(n)$ at $d|n$

Maximal Divisors

Definition

For a natural number n and real ℓ, let $\mathcal{M}_\ell(n)$ denote the set of divisors d of n less than or equal to ℓ such that no other divisor d' of n less than or equal to ℓ divides d

As ℓ increases, $\mathcal{M}_\ell(n)$ is constant between any two consecutive divisors of n, so we only need to check $\mathcal{M}_d(n)$ at $d|n$

$\star$ In our previous sum, we can replace all divisors of $p \pm 1$ less than d, $\mathcal{T}_d$, with $\mathcal{M}_d(p \pm 1)$ to lessen the overcounting of solutions $\star$

Updated Connectivity Criterion using Maximal Divisors

Theorem (Eddy–Fuchs–L.–Martin–Tripeny ('23))

For d dividing $p-1$ or $p+1$, let $M_d = |\mathcal{M}_d(p-1)| + |\mathcal{M}_d(p+1)|$. If no such divisor satisfies either inequality

$$\frac{2\sqrt{2p}}{M_d} < d < \frac{81 M_d^3}{4} \quad \text{or} \quad \frac{p}{6M_d} < d < \frac{8\sqrt{p}(p\pm 1)\tau(p\pm 1)}{\phi(p\pm 1)}$$

(where the $\pm$ is determined by whether d divides $p-1$ or $p+1$), then $\mathcal{G}_p$ is connected.

Updated Connectivity Criterion using Maximal Divisors

Theorem (Eddy–Fuchs–L.–Martin–Tripeny ('23))

For d dividing $p-1$ or $p+1$, let $M_d = |\mathcal{M}_d(p-1)| + |\mathcal{M}_d(p+1)|$. If no such divisor satisfies either inequality

$$\frac{2\sqrt{2p}}{M_d} < d < \frac{81M_d^3}{4} \quad \text{or} \quad \frac{p}{6M_d} < d < \frac{8\sqrt{p}(p\pm 1)\tau(p\pm 1)}{\phi(p\pm 1)}$$

(where the $\pm$ is determined by whether d divides $p-1$ or $p+1$), then $\mathcal{G}_p$ is connected.

The first few primes for which this theorem guarantees connectivity of $\mathcal{G}_p$ are $p = 3, 7, 101$ and $1,327,363$ (a gap on the order of 10^6)

A Bound on Maximal Divisors

Theorem (Eddy–Fuchs–L.–Martin–Tripeny ('23))

For any $\varepsilon > 0$*, if* $\alpha \in [\varepsilon, 1-\varepsilon]$ *then*

$$\log|\mathcal{M}_{n^\alpha}(n)| = \log\left(\frac{1}{\alpha^\alpha(1-\alpha)^{1-\alpha}}\right)\frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right).$$

The implied constant depends only on ε*.*

A Bound on Maximal Divisors

Theorem (Eddy–Fuchs–L.–Martin–Tripeny ('23))

For any $\varepsilon > 0$*, if* $\alpha \in [\varepsilon, 1-\varepsilon]$ *then*

$$\log |\mathcal{M}_{n^\alpha}(n)| = \log\left(\frac{1}{\alpha^\alpha(1-\alpha)^{1-\alpha}}\right)\frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right).$$

The implied constant depends only on ε*.*

We can now apply this to our connectivity criterion to deduce the following...

A Stronger Bound on p_0 from Maximal Divisors

Theorem

$\mathcal{G}_p$ is connected for all primes

$$p > 863\#53\#13\#7\#5\#3^3 2^5 \approx 3.448 \cdot 10^{392}$$

where $n\#$ denotes the product of primes less than or equal to n.

A Stronger Bound on p_0 from Maximal Divisors

Theorem

$\mathcal{G}_p$ is connected for all primes

$$p > 863\#53\#13\#7\#5\#3^3 2^5 \approx 3.448 \cdot 10^{392}$$

where $n\#$ denotes the product of primes less than or equal to n.

$p = 863\#53\#13\#7\#5\#3^3 2^5 - 1471$ is the largest prime for which we do not know if $\mathcal{G}_p$ is connected.

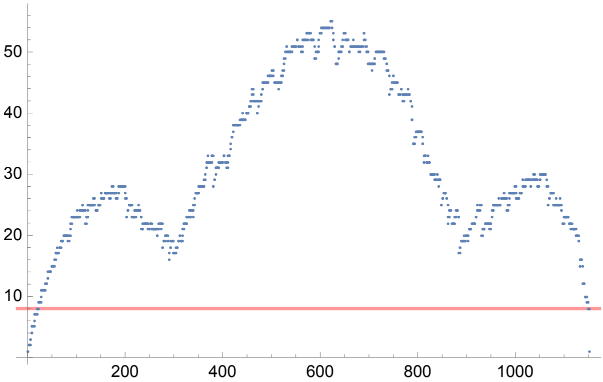
Testing for Smaller Values of 10^n

n	$q_{10000}(10^n)$	$r_{10000}(10^n)$
8	20.22%	38.12%
9	49.04%	67.46%
10	76.41%	87.05%
11	90.78%	95.33%
12	97.10%	98.29%
13	98.65%	99.11%
14	99.44%	99.52%
15	99.74%	99.83%
16	99.88%	99.88%
17	99.93%	99.95%
18	99.97%	100%
19	99.97%	99.97%
20	99.97%	100%
21	99.99%	99.99%

n	$q_{10000}(10^n)$	$r_{10000}(10^n)$
22	100%	100%
23	100%	100%
24	100%	100%
25	100%	100%
26	100%	100%
27	100%	100%
28	100%	100%
29	100%	100%
30	100%	100%
31	100%	100%
32	100%	100%
33	100%	100%
34	100%	100%
35	100%	100%

$q_m(10^n) =$ the percentage of the first m primes after 10^n for which the Connectivity Criterion guarantees connectivity of $\mathcal{G}_p$
$r_m(10^n) =$ the percentage of m random primes between 10^n and 10^{n+1} for which the Connectivity Criterion guarantees connectivity of $\mathcal{G}_p$.

Thank You!



Plot of $|\mathcal{M}_{d_i}(n)|$ as i ranges from 1 to the number of divisors of $n = 32323232323232323232$