Nico's Numerical Nightmare: An upper bound on p for disconnected G_p

Nico Tripeny

August 11, 2021

The Cage

Definition (The Cage)

Recall *the cage* is the set of maximal triples. The elements of the cage are connected in G_p (BGS).

The Cage

Definition (The Cage)

Recall *the cage* is the set of maximal triples. The elements of the cage are connected in G_p (BGS).

Our goal is to show all elements are connected to the cage.

The Cage

Definition (The Cage)

Recall *the cage* is the set of maximal triples. The elements of the cage are connected in G_p (BGS).

Our goal is to show all elements are connected to the cage.

Theorem

If p is greater than 10^{1310}, then G_p is connected.

Order of an Element

Definition

The *order* of an element a in a group G is the smallest positive integer n such that $a^n = 1$.

Order of an Element

Definition

The *order* of an element a in a group G is the smallest positive integer n such that $a^n = 1$.

Definition

The *order of an element* x in a Markoff triple is the order of $\begin{pmatrix} 0 & 1 \\ -1 & x \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)$

Order of an Element

Definition

The *order* of an element a in a group G is the smallest positive integer n such that $a^n = 1$.

Definition

The *order of an element* x in a Markoff triple is the order of $\begin{pmatrix} 0 & 1 \\ -1 & x \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)$

Definition

The *order of a triple* (x, y, z) is the maximum of the order of its elements x, y, and z.

Order of an Element (Continued)

Lemma

If $x = h + h^{-1}$ with $h \in \mathbb{F}_p$ or $h \in \mathbb{F}_{p^2}$, then the order of x is the order of h in $\mathbb{F}_p^*$ or $\mathbb{F}_{p^2}^*$ (BGS)

Order of an Element (Continued)

Lemma

If $x = h + h^{-1}$ with $h \in \mathbb{F}_p$ or $h \in \mathbb{F}_{p^2}$, then the order of x is the order of h in $\mathbb{F}_p^*$ or $\mathbb{F}_{p^2}^*$ (BGS)

Example

$h \in \mathbb{F}_p$ Let $p = 7$ and $x = 6$. We want to find h such that $h + h^{-1} = 6$.
Subtracting 4 and multiplying by h we get $h^2 - 6h + 1 = 0$

Order of an Element (Continued)

Lemma

If $x = h + h^{-1}$ with $h \in \mathbb{F}_p$ or $h \in \mathbb{F}_{p^2}$, then the order of x is the order of h in $\mathbb{F}_p^*$ or $\mathbb{F}_{p^2}^*$ (BGS)

Example

$h \in \mathbb{F}_p$ Let $p = 7$ and $x = 6$. We want to find h such that $h + h^{-1} = 6$.
Subtracting 4 and multiplying by h we get $h^2 - 6h + 1 = 0$ We see
$h = \frac{6 \pm \sqrt{36-4}}{2} = \frac{6 \pm 2}{2} = 4, 2$.
Since $4^{-1} = 2$ in $\mathbb{F}_p$, we see this is the correct solution for h.

Order of an Element (Continued)

Lemma

If $x = h + h^{-1}$ with $h \in \mathbb{F}_p$ or $h \in \mathbb{F}_{p^2}$, then the order of x is the order of h in $\mathbb{F}_p^*$ or $\mathbb{F}_{p^2}^*$ (BGS)

Example

$h \in \mathbb{F}_p$ Let $p = 7$ and $x = 6$. We want to find h such that $h + h^{-1} = 6$.
Subtracting 4 and multiplying by h we get $h^2 - 6h + 1 = 0$ We see
$h = \frac{6 \pm \sqrt{36-4}}{2} = \frac{6 \pm 2}{2} = 4, 2$.
Since $4^{-1} = 2$ in $\mathbb{F}_p$, we see this is the correct solution for h.

Example

$h \in \mathbb{F}_{p^2}$ Let $p = 7$ and $x = 4$.
Similar to above we get $h = \frac{4 \pm \sqrt{16-4}}{2} = \frac{4 \pm \sqrt{5}}{2}$.

Order of an Element (Continued)

Lemma

If $x = h + h^{-1}$ with $h \in \mathbb{F}_p$ or $h \in \mathbb{F}_{p^2}$, then the order of x is the order of h in $\mathbb{F}_p^*$ or $\mathbb{F}_{p^2}^*$ (BGS)

Example

$h \in \mathbb{F}_p$ Let $p = 7$ and $x = 6$. We want to find h such that $h + h^{-1} = 6$.
Subtracting 4 and multiplying by h we get $h^2 - 6h + 1 = 0$ We see
$h = \frac{6 \pm \sqrt{36-4}}{2} = \frac{6 \pm 2}{2} = 4, 2$.
Since $4^{-1} = 2$ in $\mathbb{F}_p$, we see this is the correct solution for h.

Example

$h \in \mathbb{F}_{p^2}$ Let $p = 7$ and $x = 4$.

Similar to above we get $h = \frac{4 \pm \sqrt{16-4}}{2} = \frac{4 \pm \sqrt{5}}{2}$. Since 5 is not a quadratic residue mod 7, this is in $\mathbb{F}_{p^2}$ but is still a solution to $h + h^{-1} = 4$

Order of an Element Continued

Lemma

If $x = h + h^{-1}$ with $h \in \mathbb{F}_{p^2}$ then the order of h divides $p + 1$ or $p - 1$

Order of an Element Continued

Lemma

If $x = h + h^{-1}$ with $h \in \mathbb{F}_{p^2}$ then the order of h divides $p + 1$ or $p - 1$

Example

Notice that the order of 2 is 3 and 3 divides 6 as expected.

Order of an Element Continued

Lemma

If $x = h + h^{-1}$ with $h \in \mathbb{F}_{p^2}$ then the order of h divides $p+1$ or $p-1$

Example

Notice that the order of 2 is 3 and 3 divides 6 as expected.

Also, the order of $\frac{4 \pm \sqrt{5}}{2}$ is 8.

Order of an Element Continued

Lemma

If $x = h + h^{-1}$ with $h \in \mathbb{F}_{p^2}$ then the order of h divides $p+1$ or $p-1$

Example

Notice that the order of 2 is 3 and 3 divides 6 as expected.
Also, the order of $\frac{4 \pm \sqrt{5}}{2}$ is 8.

Proof.

Since $x \in \mathbb{F}_p^*$, $x^{p-1} = 1$, we have $x^p = (h + h^{-1})^p = h^p + h^{-p} = x$.
Since h and h^{-1} are the only solutions to $x = y + y^{-1}$, we see $h^p = h$ or $h^p = h^{-1}$.
So, $h^{p+1} = 1$ or $h^{p-1} = 1$ giving the desired result. □

Orbit of a Triple

Definition

The orbit of a triple (x, y, z) with respect to x is all triples obtained by applying the matrix $\begin{pmatrix} 0 & 1 \\ -1 & x \end{pmatrix}$ to the triple.

Orbit of a Triple

Definition

The orbit of a triple (x, y, z) with respect to x is all triples obtained by applying the matrix $\begin{pmatrix} 0 & 1 \\ -1 & x \end{pmatrix}$ to the triple.

Lemma

All elements of the triples in the orbit of (x, y, z) *with respect to* x *are of the form* $h + \frac{\sigma}{h}$ *where* $h + h^{-1} = x$ *and* $\sigma \neq 1$ *(BGS)*

The End Game

Definition (The End Game)

We are in *The End Game* when a triple has order greater than $p^{1/2+\delta}$ for $\delta > 0$.

The End Game

Definition (The End Game)

We are in *The End Game* when a triple has order greater than $p^{1/2+\delta}$ for $\delta > 0$.

Theorem

All triples in the end game have a triple of maximal order in their orbits (BGS).

Smaller Order

What if the order of a triple is smaller than $p^{1/2+\delta}$?

Smaller Order

What if the order of a triple is smaller than $p^{1/2+\delta}$?

We can no longer guarantee there is an element of maximal order in the orbit.

Smaller Order

What if the order of a triple is smaller than $p^{1/2+\delta}$?

We can no longer guarantee there is an element of maximal order in the orbit.

Can we show there is an order of larger (not maximal) order in the orbit?

Smaller Order

What if the order of a triple is smaller than $p^{1/2+\delta}$?

We can no longer guarantee there is an element of maximal order in the orbit.

Can we show there is an order of larger (not maximal) order in the orbit?

Definition (The Middle Game)

We are in *The Middle Game* when a triple has order less than $p^{1/2+\delta}$.

An Important Result

Theorem

Every component of G_p has a size divisible by p (Chen).

An Important Result

Theorem

Every component of G_p has a size divisible by p (Chen).

So, we do not have to show every triple is connected to the cage, only that all but at most $p - 1$ are.

An Important Result

Theorem

Every component of G_p has a size divisible by p (Chen).

So, we do not have to show every triple is connected to the cage, only that all but at most $p - 1$ are.

Our goal is to show for what values of p we can guarantee this for.

Connecting to Triple of Larger Order

Let a triple (x_1, x_2, x_3) have order $n < p^{1/2+\delta}$ with x_1 being the coordinate of largest order.

Connecting to Triple of Larger Order

Let a triple (x_1, x_2, x_3) have order $n < p^{1/2+\delta}$ with x_1 being the coordinate of largest order.

We need the orbit to have less than n elements of order at most n to guarantee it has a triple of larger order.

Connecting to Triple of Larger Order

Let a triple (x_1, x_2, x_3) have order $n < p^{1/2+\delta}$ with x_1 being the coordinate of largest order.

We need the orbit to have less than n elements of order at most n to guarantee it has a triple of larger order.

Example

If a triple (x_1, x_2, x_3) has order 12 and we know there are 10 triples in the orbit of order at most 12, there must be a triple of order greater than 12.

What to Bound

Theorem

Let $x_1 = h_1 + h_1^{-1}$ with the order of x_1 being n. The number of elements in the orbit of (x_1, x_2, x_3) of the form $h_2 + h_2^{-1}$ where $ord(h_2) = m \leq n$ is at most

$$20 \cdot \max\{(n \cdot m)^{\frac{1}{3}}, \frac{(n \cdot m)}{p}\}$$

(Corvaja and Zannier)

What to Bound

Theorem

Let $x_1 = h_1 + h_1^{-1}$ with the order of x_1 being n. The number of elements in the orbit of (x_1, x_2, x_3) of the form $h_2 + h_2^{-1}$ where $ord(h_2) = m \leq n$ is at most

$$20 \cdot \max\{(n \cdot m)^{\frac{1}{3}}, \frac{(n \cdot m)}{p}\}$$

(Corvaja and Zannier)

Since n and m in the middle game are less than $p^{1/2+\delta}$ the second part is irrelevant so we get an upper bound of $20 \cdot (n \cdot m)^{\frac{1}{3}}$

Summation we are After

To show the triple of order y as an element of larger order in its orbit, it suffices to show

$$20 \cdot n^{\frac{1}{3}} \sum_{\substack{d \leq n \\ d \mid p \pm 1}} d^{\frac{1}{3}} < n$$

Summation we are After

To show the triple of order y as an element of larger order in its orbit, it suffices to show

$$20 \cdot n^{\frac{1}{3}} \sum_{\substack{d \leq n \\ d \mid p \pm 1}} d^{\frac{1}{3}} < n$$

Unfortunately, this doesn't always hold, so we want to find the smallest value of n where it fails. This will depend on the prime p.

Bounding the Sum

Let $\tau(p \pm 1)$ be the number of divisors of both $p + 1$ and $p - 1$.

Bounding the Sum

Let $\tau(p \pm 1)$ be the number of divisors of both $p+1$ and $p-1$.

We know $\tau(p \pm 1) < C \cdot p^{\frac{1}{\log\log(p)}}$

$$20 \cdot n^{\frac{1}{3}} \cdot \sum_{\substack{d \leq n \\ d \mid p \pm 1}} d^{\frac{1}{3}} \cdot \leq 20 \cdot n^{\frac{2}{3}} \sum_{\substack{d \leq n \\ d \mid p \pm 1}} 1 \leq 20 \cdot n^{\frac{2}{3}} \cdot \tau(p \pm 1) \leq 20 \cdot C \cdot p^{\frac{1}{\log\log(p)}} \cdot n^{\frac{2}{3}}$$

Bounding the Sum

Let $\tau(p \pm 1)$ be the number of divisors of both $p+1$ and $p-1$.

We know $\tau(p \pm 1) < C \cdot p^{\frac{1}{\log\log(p)}}$

$$20 \cdot n^{\frac{1}{3}} \cdot \sum_{\substack{d \leq n \\ d \mid p \pm 1}} d^{\frac{1}{3}} \cdot \leq 20 \cdot n^{\frac{2}{3}} \sum_{\substack{d \leq n \\ d \mid p \pm 1}} 1 \leq 20 \cdot n^{\frac{2}{3}} \cdot \tau(p \pm 1) \leq 20 \cdot C \cdot p^{\frac{1}{\log\log(p)}} \cdot n^{\frac{2}{3}}$$

It suffices to show $20 \cdot C \cdot p^{\frac{1}{\log\log(p)}} \cdot n^{\frac{2}{3}} < n$ or $(20 \cdot C \cdot p^{\frac{1}{\log\log(p)}})^3 < n$.

Bounding the Sum

Let $\tau(p \pm 1)$ be the number of divisors of both $p+1$ and $p-1$.

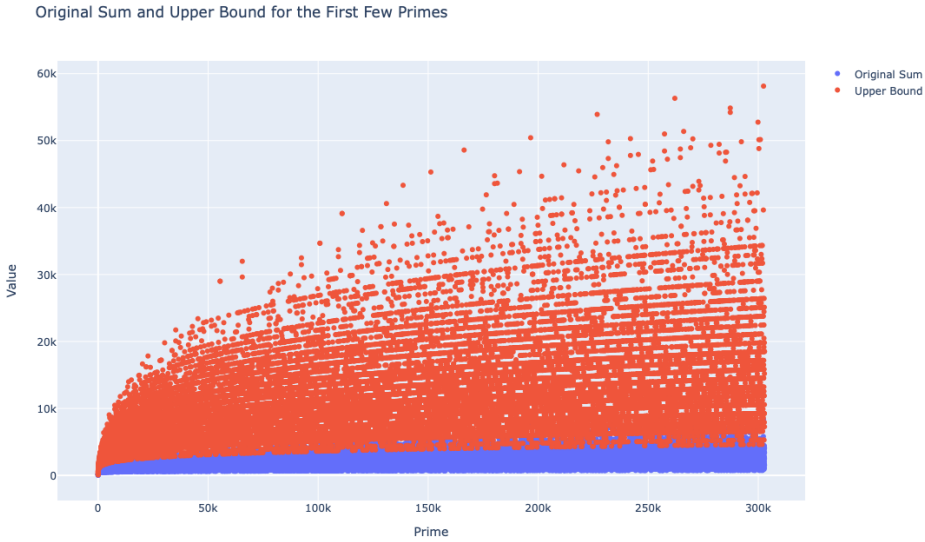
We know $\tau(p \pm 1) < C \cdot p^{\frac{1}{\log\log(p)}}$

$$20 \cdot n^{\frac{1}{3}} \cdot \sum_{\substack{d \leq n \\ d \mid p \pm 1}} d^{\frac{1}{3}} \cdot \leq 20 \cdot n^{\frac{2}{3}} \sum_{\substack{d \leq n \\ d \mid p \pm 1}} 1 \leq 20 \cdot n^{\frac{2}{3}} \cdot \tau(p \pm 1) \leq 20 \cdot C \cdot p^{\frac{1}{\log\log(p)}} \cdot n^{\frac{2}{3}}$$

It suffices to show $20 \cdot C \cdot p^{\frac{1}{\log\log(p)}} \cdot n^{\frac{2}{3}} < n$ or $(20 \cdot C \cdot p^{\frac{1}{\log\log(p)}})^3 < n$.

Notice if we just had the order of a triple divides $p^2 - 1$ instead of $p \pm 1$ we would have roughly the square of this for our answer.

Graph for Upper Bound



Defining y_p

We want to find the largest divisor such that the inequality fails.

Defining y_p

We want to find the largest divisor such that the inequality fails.

This will allow us to bound the number of triples not connected to the cage.

Defining y_p

We want to find the largest divisor such that the inequality fails.

This will allow us to bound the number of triples not connected to the cage.

So, let $y_p \leq (20 \cdot C \cdot p^{\frac{1}{\log\log(p)}})^3$ be the greatest divisor with this property.

Another Summation

Let $y_p \leq (20 \cdot C \cdot p^{\frac{1}{\log \log(p)}})^3$. Triples with order less than y_p may not be connected to the cage.

Another Summation

Let $y_p \leq (20 \cdot C \cdot p^{\frac{1}{\log \log(p)}})^3$. Triples with order less than y_p may not be connected to the cage.

How many such triples are there? For the first coordinate, there are $\sum_{\substack{d \leq y_p \\ d \mid p \pm 1}} d$ possibilities, since each divisor d contributes no more than d elements of that order.

Another Summation

Let $y_p \leq (20 \cdot C \cdot p^{\frac{1}{\log\log(p)}})^3$. Triples with order less than y_p may not be connected to the cage.

How many such triples are there? For the first coordinate, there are $\sum_{\substack{d \leq y_p \\ d \mid p \pm 1}} d$ possibilities, since each divisor d contributes no more than d elements of that order.

This is bounded by

$$\sum_{\substack{d \leq y_p \\ d \mid p \pm 1}} d < C \cdot y_p \cdot \tau(p \pm 1) < C' \cdot p^{\frac{4}{\log\log(p)}}$$

where C' is a "small" constant.

Wait, So How Many Triples?

The number of options for the first and second coordinates is $C' \cdot p^{\frac{4}{\log\log(p)}}$.

Wait, So How Many Triples?

The number of options for the first and second coordinates is $C' \cdot p^{\frac{4}{\log \log(p)}}$.

When two of the coordinates x_1, x_2, x_3 are fixed, you get a quadratic. So, there are 2 or fewer options for the third coordinate.

Wait, So How Many Triples?

The number of options for the first and second coordinates is $C' \cdot p^{\frac{4}{\log \log(p)}}$.

When two of the coordinates x_1, x_2, x_3 are fixed, you get a quadratic. So, there are 2 or fewer options for the third coordinate.

To see this, set x and y in the Markoff equation $x^2 + y^2 + z^2 - xyz = 0$
This becomes a quadratic equation in z and we see the solutions are
$z = \frac{xy \pm \sqrt{(xy)^2 - 4(x^2+y^2)}}{2}$.

Wait, So How Many Triples?

The number of options for the first and second coordinates is $C' \cdot p^{\frac{4}{\log\log(p)}}$.

When two of the coordinates x_1, x_2, x_3 are fixed, you get a quadratic. So, there are 2 or fewer options for the third coordinate.

To see this, set x and y in the Markoff equation $x^2 + y^2 + z^2 - xyz = 0$
This becomes a quadratic equation in z and we see the solutions are
$z = \frac{xy \pm \sqrt{(xy)^2 - 4(x^2+y^2)}}{2}$.

In total, there are at most $2 \cdot (C' \cdot p^{\frac{4}{\log\log(p)}})^2 = C'' p^{\frac{8}{\log\log(p)}}$ triples where C'' is again "small".

The Big Reveal

G_p is always connected for $p >$

The Big Reveal

G_p is always connected for $p >$ 4107755233619240794081891241325317263085341759
778723028478029962515056329124940339482377262029843699491740209019599507 4
764278924146828007731544482763379155961141934795025409753585615716697500 9
715862054070385885890407256164306329639747674844354460740765235438477716 7
189640548684489494730037739507146679205451890469249475313147581853040378 6
654145914492761866648928529388522730962619761498189146474154836008923333 1
153990964718521055274072303404185621395503593635586410334008672363420700 5
756824060036944090986824615297683576839940432743918405356113923746755901 6
848400134120134839122437807493547350751471670845891206182881681157828264 6
183788548679668610088377523447271737992932879635394209191864501116624141 8
179541186350753840363503175504435455454587760343971373596083791231984836 6
484621071843691388061748711031487988894605574185946058749746168982746720 4
846541733910697855443647667366594246594658924472033451058433211926176550 0
155994040725573349156139051471886153256899589463035385531328977972996492 6
916557323898805522495309928997176786028671515186668325162418941983940547 5
629357164064301381442067386476447346811644111880777167699738440721620320 1
192469921150700376530100803846148063357320085125625005776642512847253483 6

How'd We Get That?

Want to know when is $C'' p^{\frac{8}{\log \log(p)}} < p$?

How'd We Get That?

Want to know when is $C''p^{\frac{8}{\log\log(p)}} < p$?

When p is slightly larger than e^{e^8}, then $p^{\frac{8}{\log\log(p)}} < p$ and the "small" C'' has little effect.

How'd We Get That?

Want to know when is $C'' p^{\frac{8}{\log\log(p)}} < p$?

When p is slightly larger than e^{e^8}, then $p^{\frac{8}{\log\log(p)}} < p$ and the "small" C'' has little effect.

This, with the theorem of Chen from earlier, shows if $p > e^{e^8} \approx 10^{1300}$ then G_p is connected.

Thank You!