Elliptic Curves

Thesis Defense

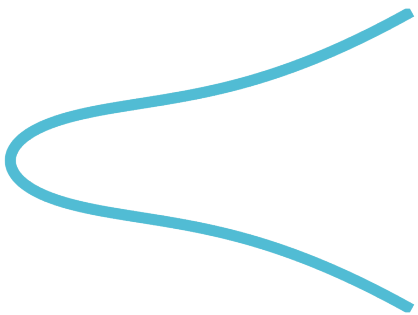
Tufts University

April 2017

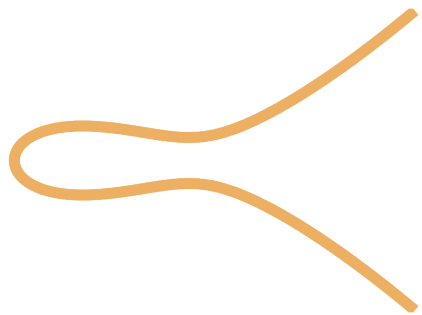
Table of Contents

Definition

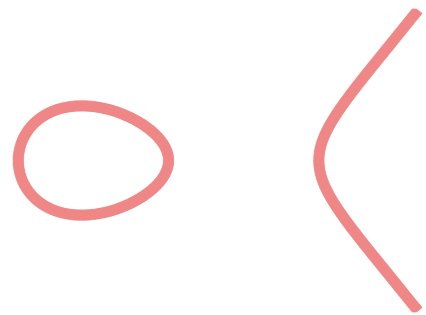
An elliptic curve is a nonsingular cubic plane curve with at least one rational point.



$y^2 = x^3 + x + 1$

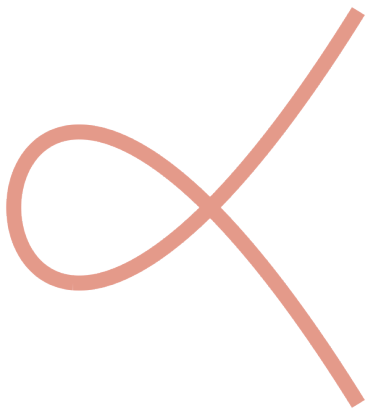


$y^2 = x^3 - x + 1$

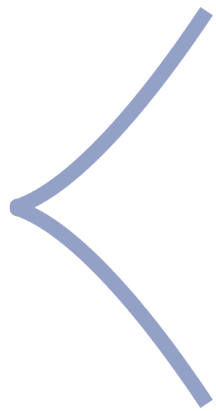


$y^2 = x^3 - x$

Singular Curves



Crunode:
$y^2 = x^3 + x^2$



Ordinary Cusp:
$y^2 = x^3$

Acnode:
$y^2 = x^3 - x^2$

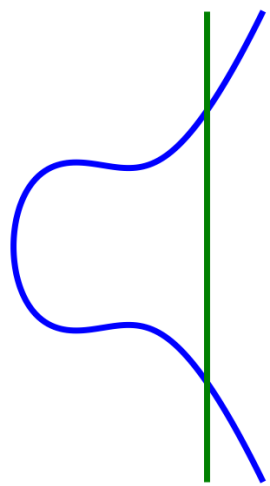
Timeline

285 a.d.	Diophantus publishes *Arithmetica*
...	
1637	Fermat states Fermat's Last Theorem
1669	Newton expresses arc-lenghts of ellipses as infinite series
1750	Euler states a group law for Elliptic Integrals
1779	Bezout's Theorem is Stated
...	Gauss, Fagnano, Bernoulli, Legendre, Jacobi, Eisenstein, Abel, and others work on elliptic functions
1862	Weierstraß Parametrizes $\wp$
1916	Ramanujan conjectures τ congruences
1922	Mordell's Theorem
1928	Mordell-Weil Theorem
1933	Hasse's Bound
1973	Deligne Proves Weil's Riemann Hypothesis
1977	Mazur's Torsion Theorem
1985	Elliptic Curve Cryptography is born
1987	Lenstra's Integer Factorization Algorithm
1995	Wiles' Modularity Theorem
2006	Elkies' Discovery of a Rank ≥ 28 Curve
2006	Proof of the Sato-Tate Conjecture is Finished

Bezout's Theorem in the Plane

Theorem

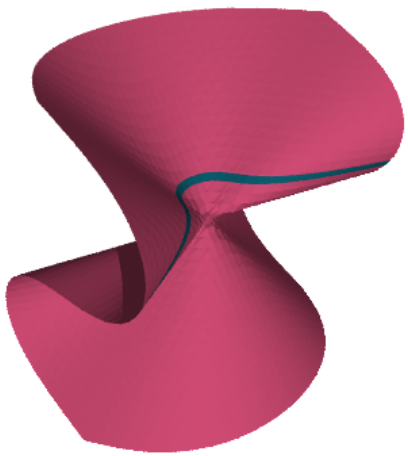
Let k be a field, and let $P, Q \in k[x, y]$ be non-zero polynomials in two variables x, y with no common factor. Then the two curves $\{(x, y) \in k^2 : P(x, y) = 0\}$ and $\{(x, y) \in k^2 : Q(x, y) = 0\}$ intersect at most $deg(P)deg(Q)$ times.

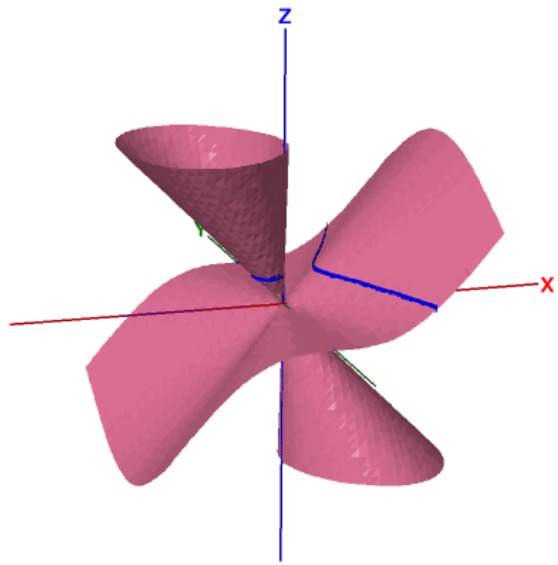


$y^2 = x^3 + x^2 + 1$ and $x = 1$

Projective Geometry

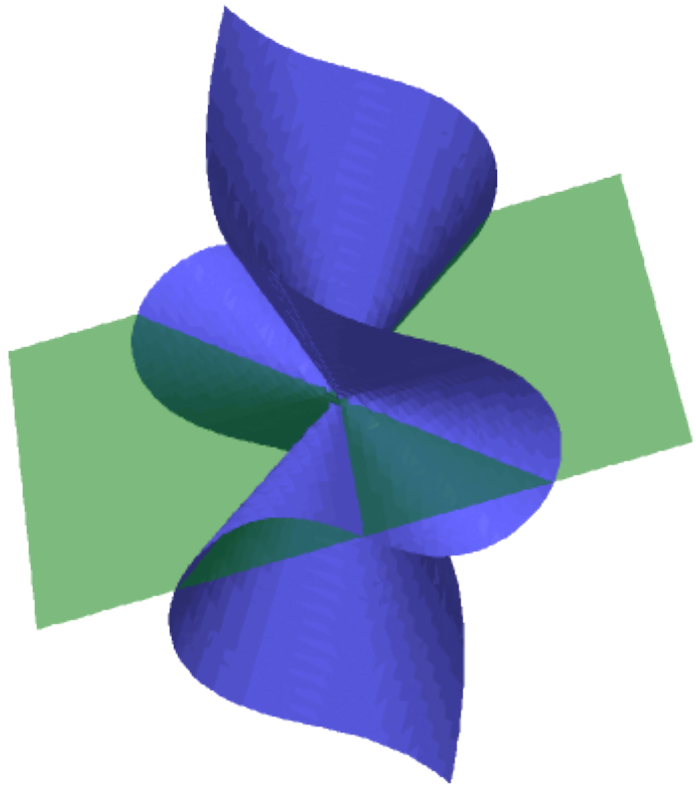
$\mathbb{A}^2(k) = k^2$ and $\mathbb{P}^2(k) = \{(x, y, z) \in k^3 : (x, y, z) \neq (0, 0, 0)\}/\sim$ where $\sim$ is the equivalence relation where $(x, y, z) \sim (x', y', z')$ if and only if there is a scaling factor $c \neq 0$ such that $(x, y, z) = (cx', cy', cz')$.





Bezout's Theorem in Projective Geometry

Let P and Q be homogeneous polynomials in the projective plane with no common factor. Then their projective solutions have $\deg(P)\deg(Q)$ intersection points counting multiplicity.



$$y^2z = x^3 + x^2z + z^3 \text{ and } x = z$$

Groups

Definition

A group is a set G with a binary operation $\cdot$ with the following properties

i. There exists an identity, 1, such that $1 \cdot g = g$ for every g in G.

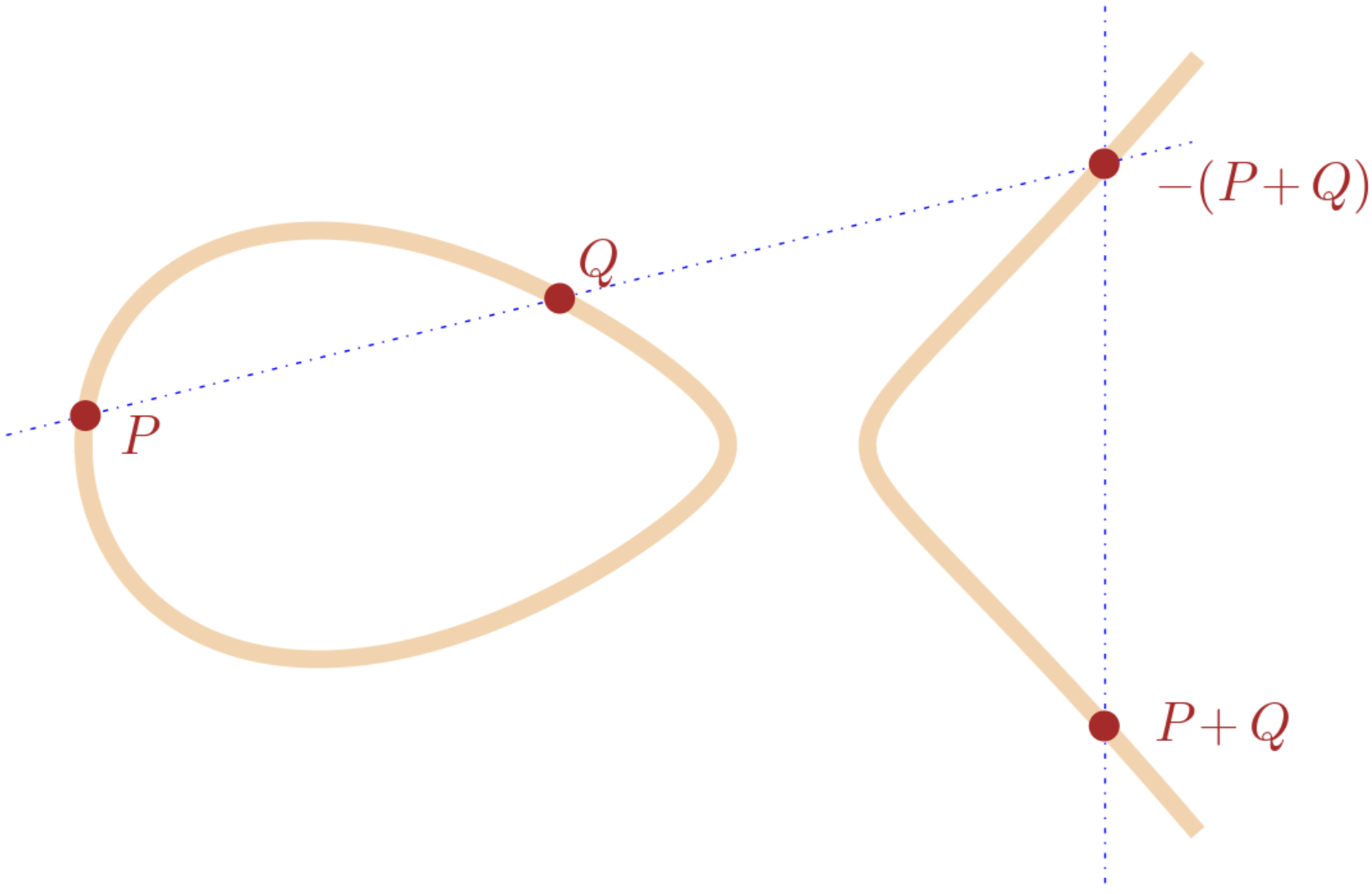
ii. Inverses exist for every element such that $g^{-1}g = gg^{-1} = 1$ for every g in G.

iii. Group operation associates $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in G$.

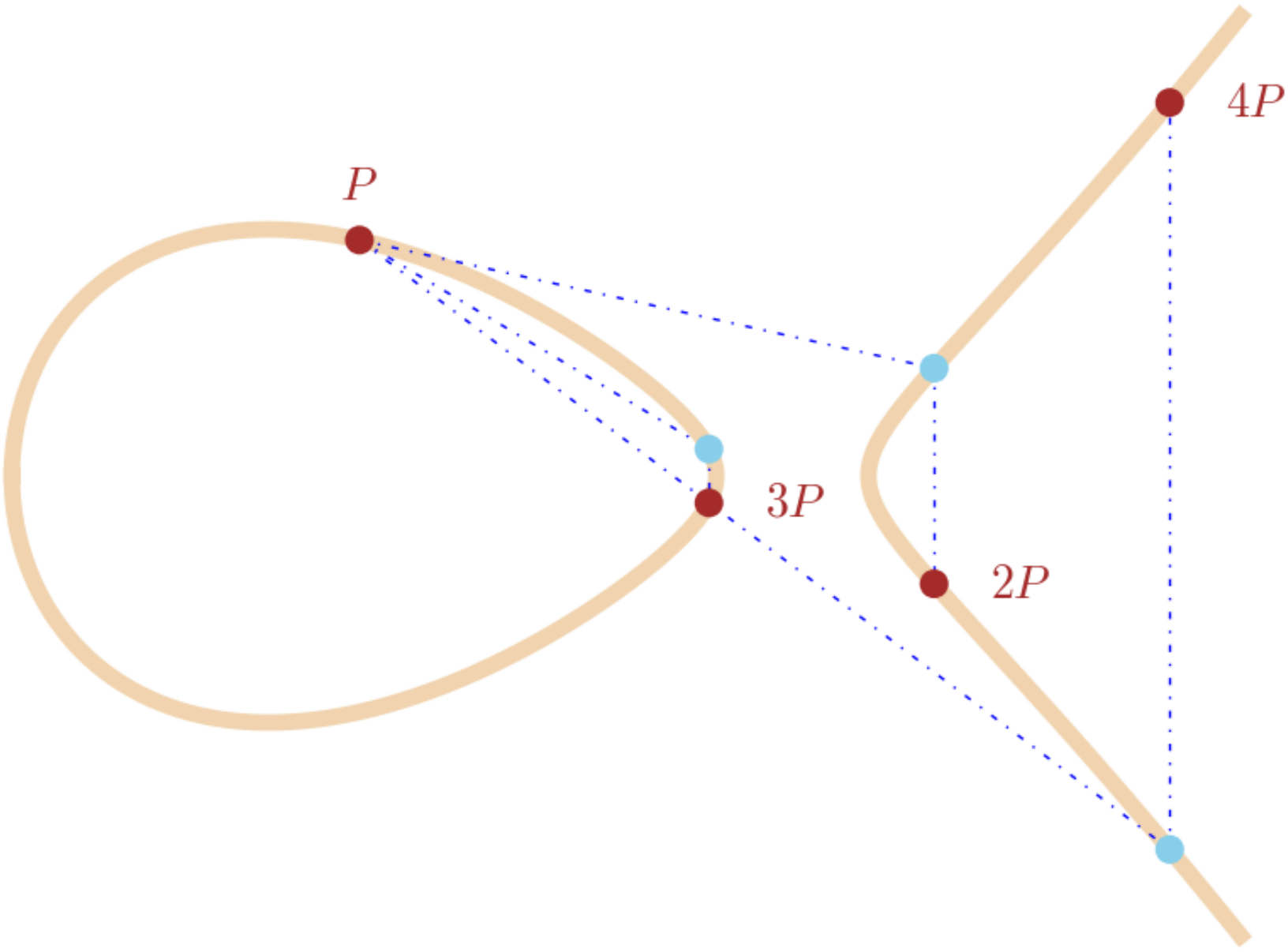
iv. A group is abelian if $a \cdot b = b \cdot a$ for all $a, b \in G$.

v. A group is finitely generated if for some finite subset $S \subseteq G$ every element in G can be written as a group operation done unto elements of S.

Elliptic Curve Addition



Elliptic Curve Multiplication (by $\mathbb{Z}$)



Mordell's Theorem

The rational points of an elliptic curve are a finitely generated abelian group.

$$E(\mathbb{Q}) = \underbrace{\mathbb{Z} + \mathbb{Z} + \cdots + \mathbb{Z}}_{r<\infty \text{ times}} + \underbrace{\text{Torsion}}_{\text{a finite subgroup}}$$

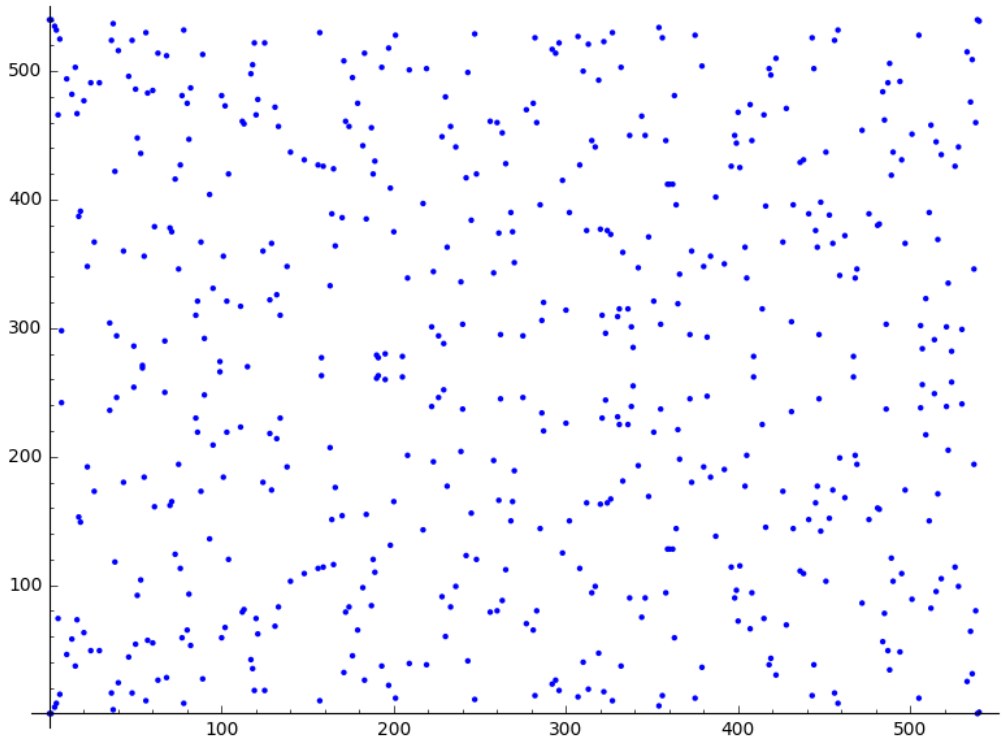
Mazur's Theorem

The torsion subgroups of elliptic curves are the following fifteen groups.

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } 1 \leq n \leq 10 \text{ or } n = 12, \text{ or}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \text{ where } n \in \{2, 4, 6, 8\}.$$

Finite Field Elliptic Curves

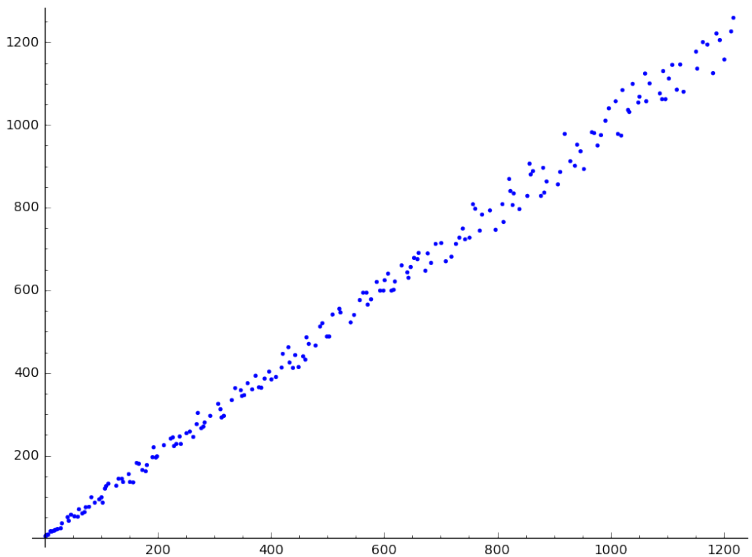


$y^2 + y = x^3 + x^2 - 2x$ over $\mathbb{F}_{541}$

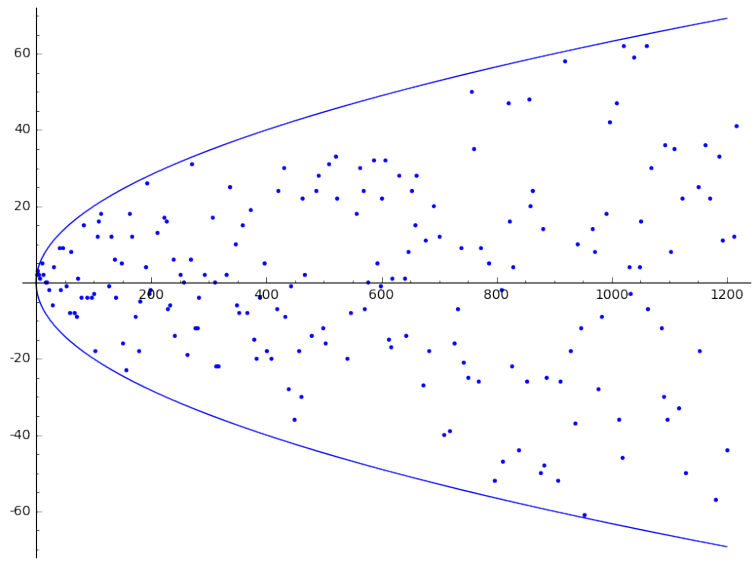
Hasse's Bound

Hasse showed the size of a finite field elliptic curve is bounded.

$$|E(\mathbb{F}_q)| - q - 1 \leq 2\sqrt{q}.$$



$|E(\mathbb{F}_p)|$



$|E(\mathbb{F}_p)| - p - 1$

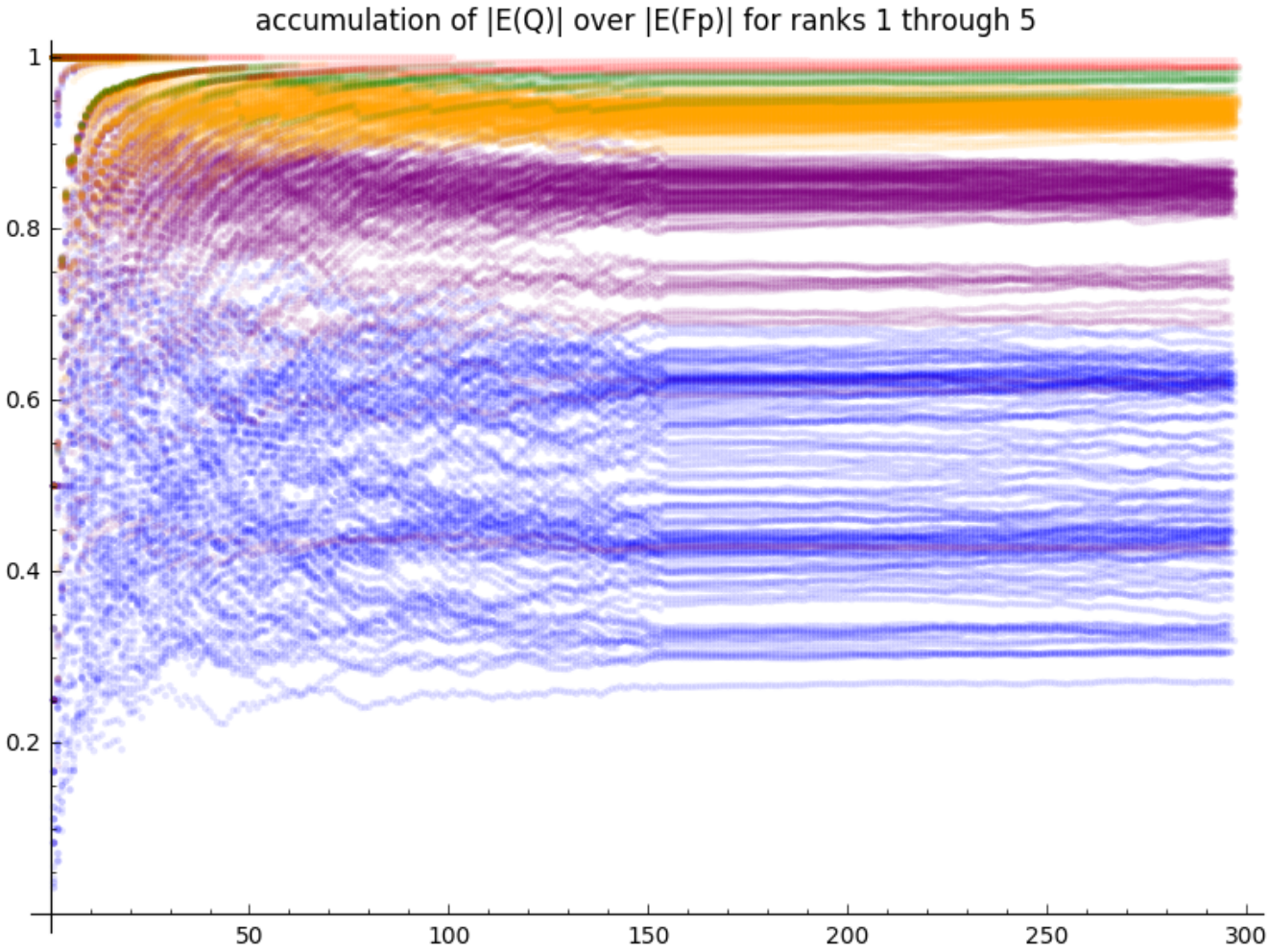
Lenstra's Factorization Algorithm

0. Let $n \geq 2$ be a composite integer to be factored.
1. Check that $\gcd(n, 6) = 1$ and that n is not a perfect power.
2. Choose random integers b, x_1, and y_1 modulo n.
3. Set $P = (x_1, y_1)$ and $c = y_1^2 - x_1^3 - bx_1 \pmod{n}$.
4. Let E be the elliptic curve $E : y^2 = x^3 + bx + c$.
5. Repeat Step 6 through 9 for $d = 2, 3, 4, \ldots$ up to a specified bound.
6. Compute $Q = dP \pmod{n}$ and set $P = Q$.
7. If the computation of Step 6 fails then we have found a divisor, $g = \gcd(x(Q) - x(P), n)$.
8. If $g < n$, then we find g is a factor of n.
9. If $g = n$, go back to step 2 and pick a different curve and point.
10. If all factors have not yet been found, go back to step 2 and try again.

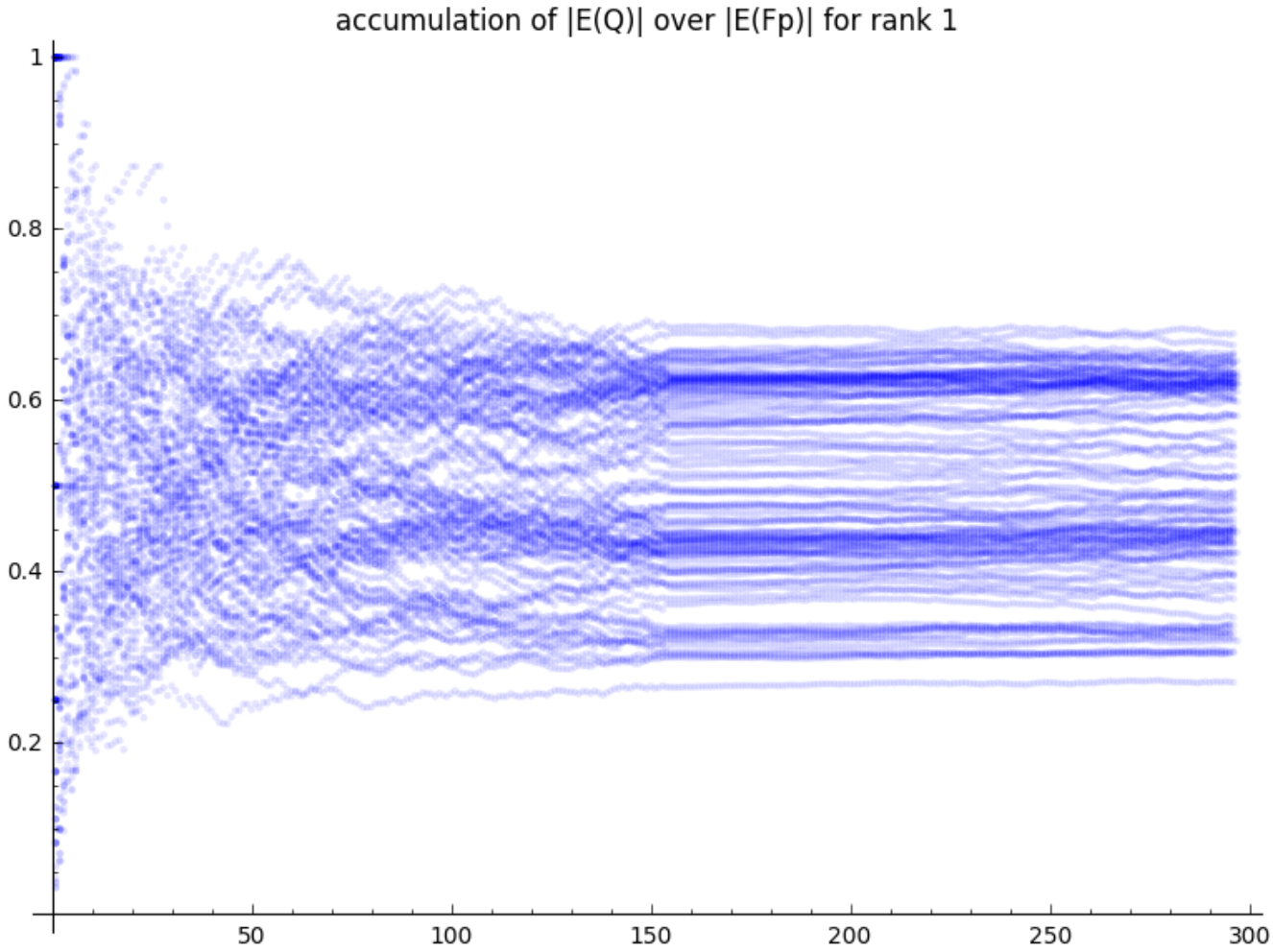
How Does $E(\mathbb{Q})$ Reduce into $E(\mathbb{F}_p)$

$$F_E(p) = \frac{\sum_{\text{primes} \leq p} |\langle \text{free-generators}(E(\mathbb{Q})) \rangle|}{\sum_{\text{primes} \leq p} |E(\mathbb{F}_p)|}$$

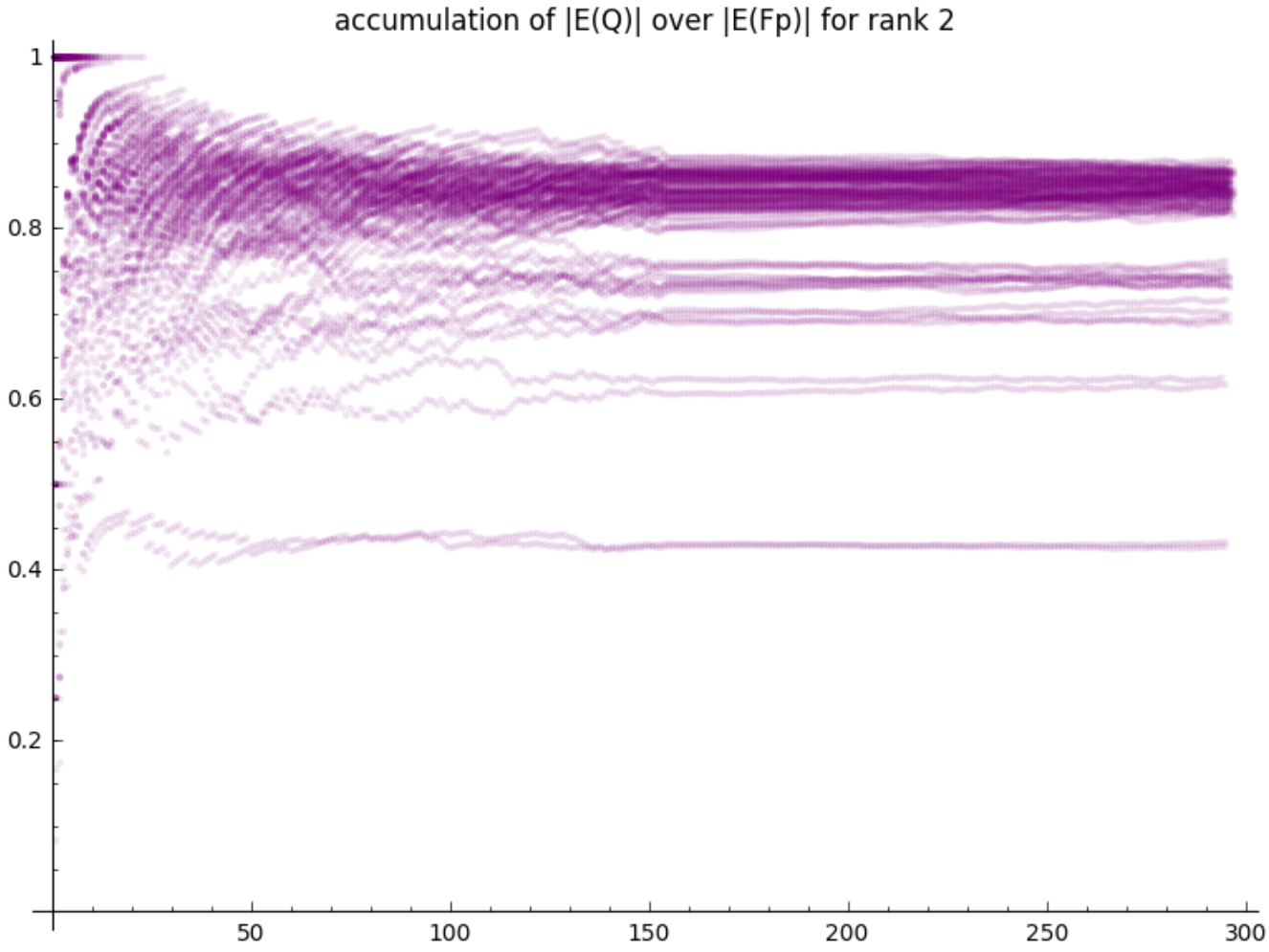
How Does $E(\mathbb{Q})$ Reduce into $E(\mathbb{F}_p)$



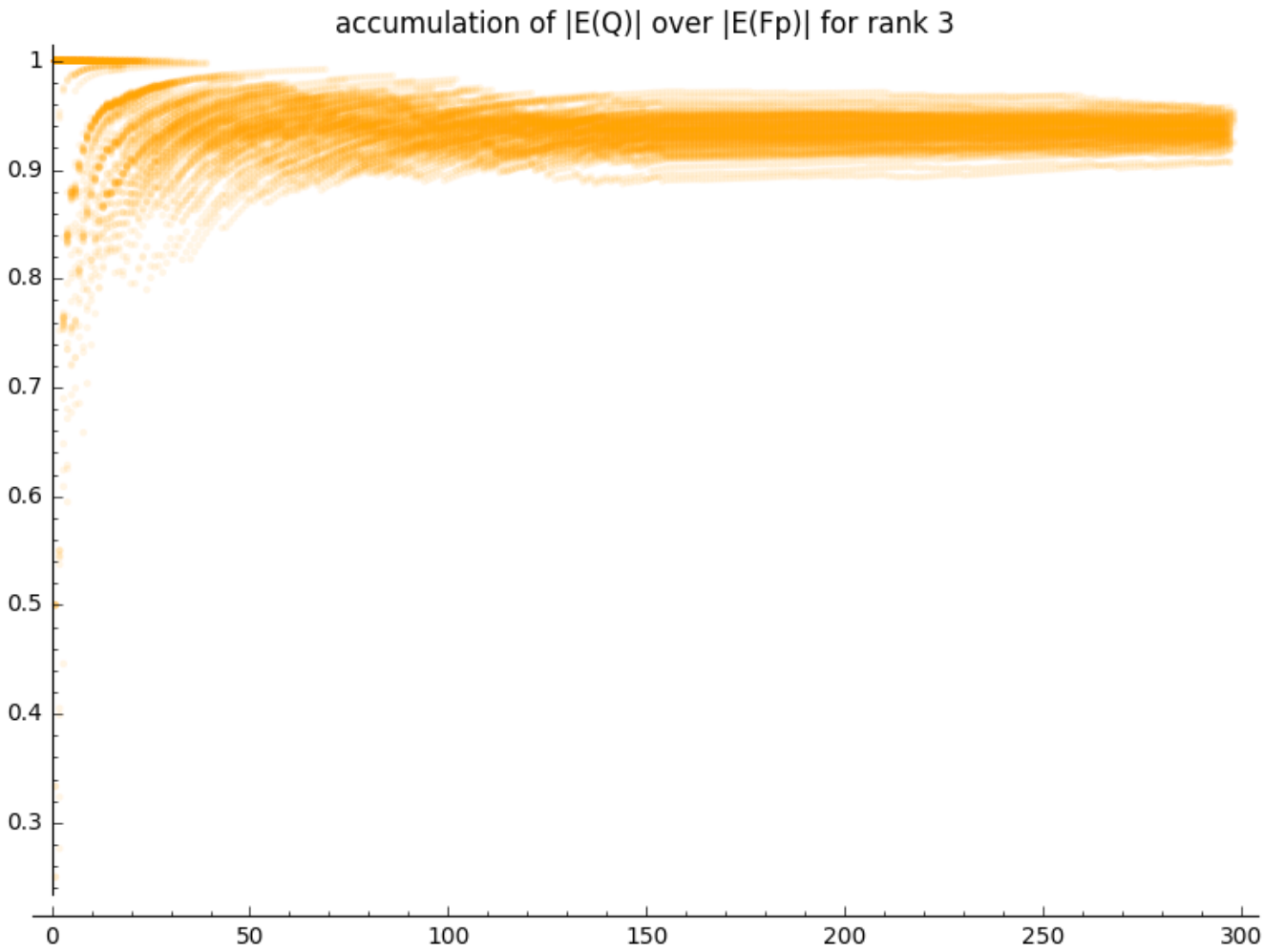
How Does $E(\mathbb{Q})$ Reduce into $E(\mathbb{F}_p)$



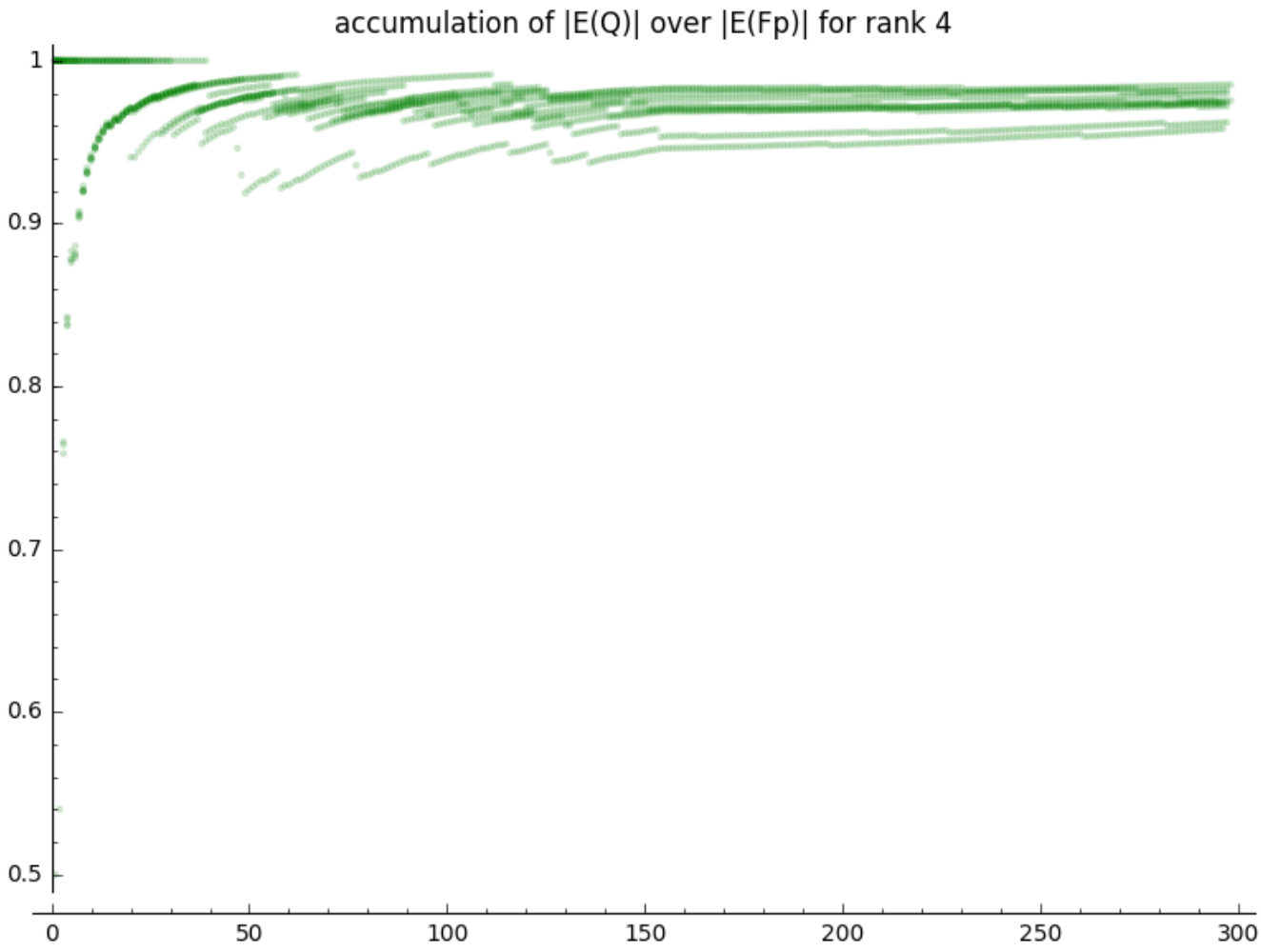
How Does $E(\mathbb{Q})$ Reduce into $E(\mathbb{F}_p)$



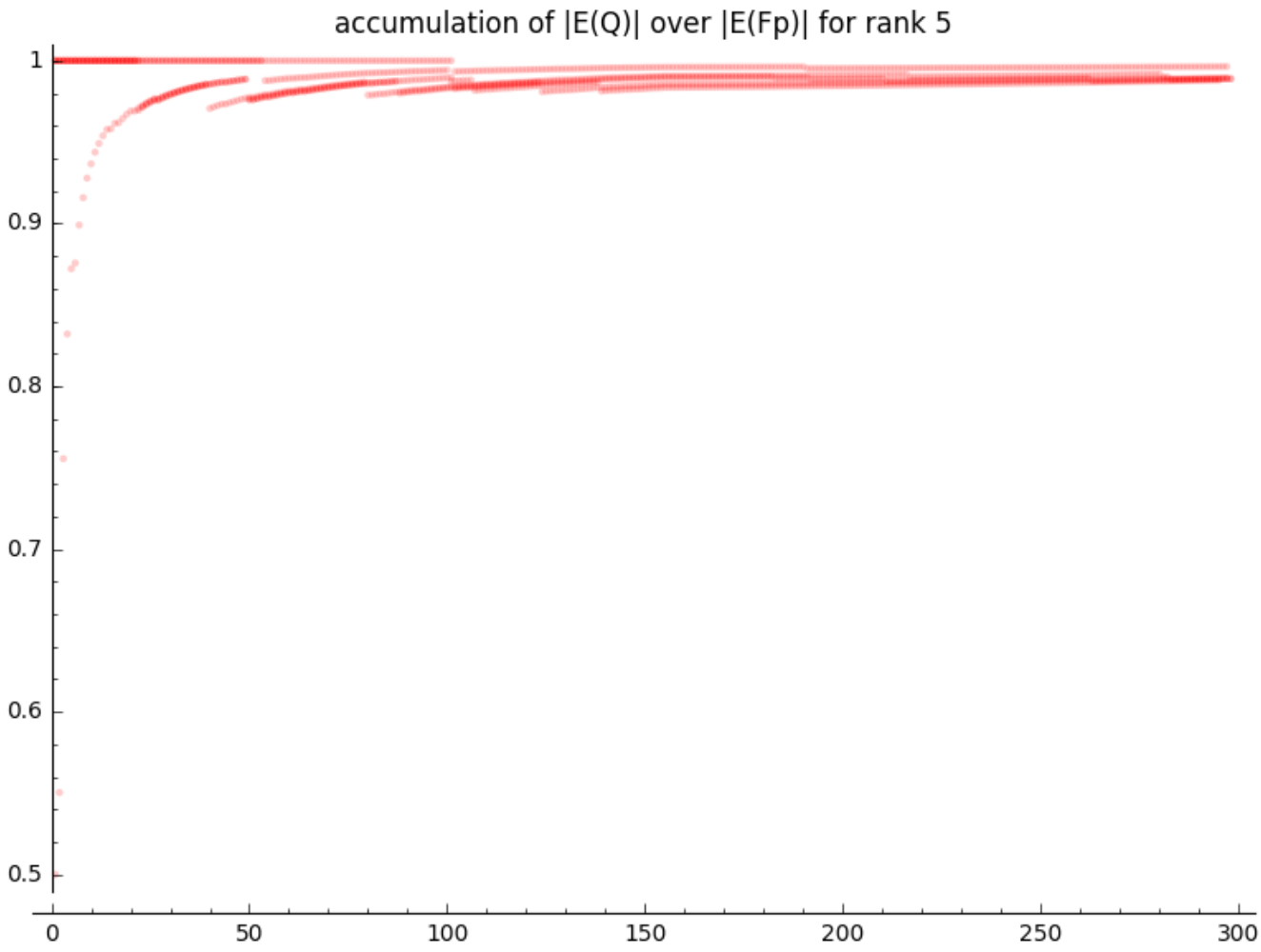
How Does $E(\mathbb{Q})$ Reduce into $E(\mathbb{F}_p)$



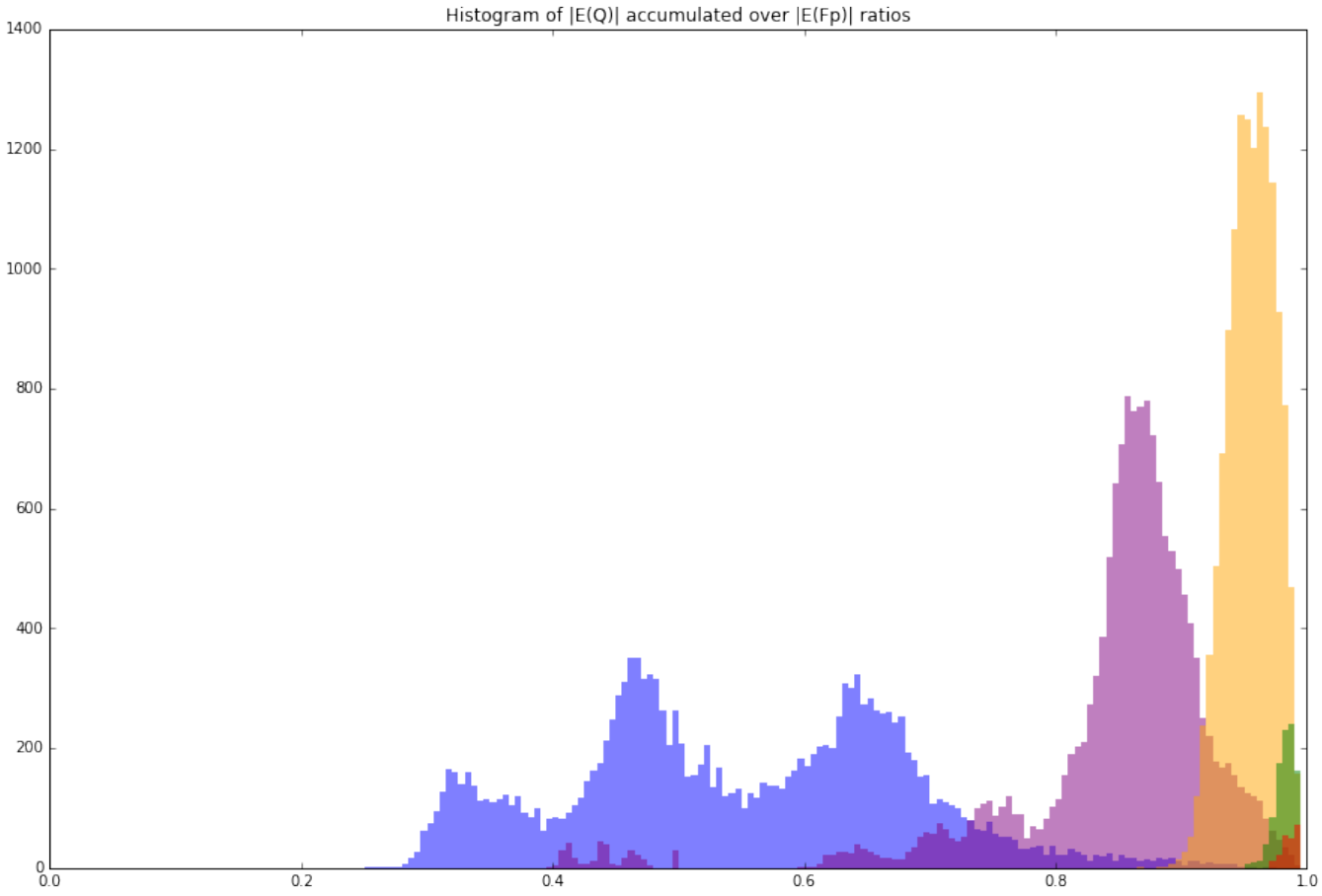
How Does $E(\mathbb{Q})$ Reduce into $E(\mathbb{F}_p)$



How Does $E(\mathbb{Q})$ Reduce into $E(\mathbb{F}_p)$



How Does $E(\mathbb{Q})$ Reduce into $E(\mathbb{F}_p)$



Generating a Subgroup with $(0, 0)$

Check it out! (0,0) is always on

$$E_{A,B} : y^2 + y = x^3 + Ax^2 + Bx$$

Generating a Subgroup with $(0, 0)$

We define a set for each prime of elliptic curves

$$S_p = \{E_{A,B} : \Delta(E) \neq 0 \text{ and } A, B \in \mathbb{F}_p\}.$$

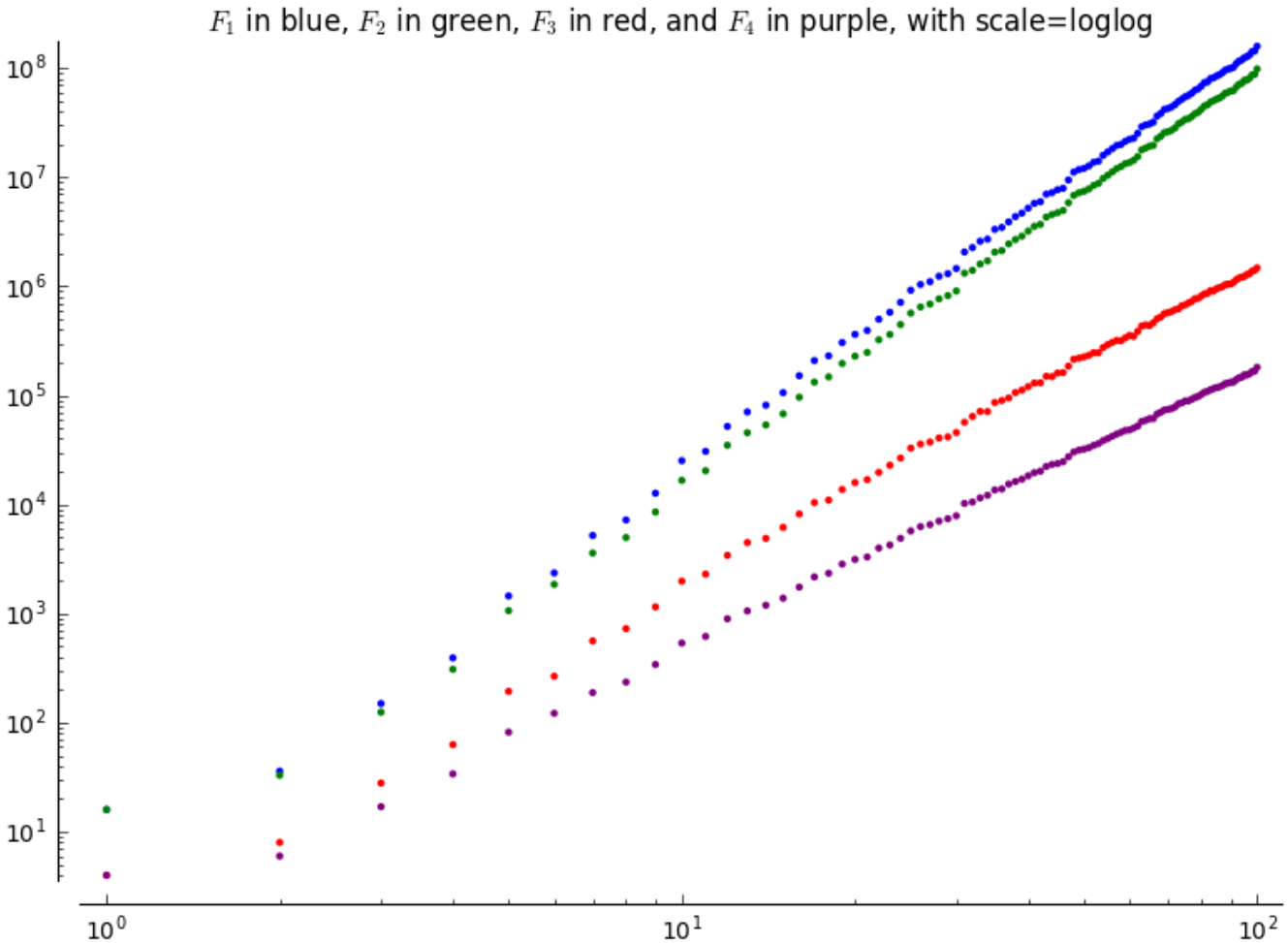
And we define the following functions at each prime as a sum over this set.

$$F_1(p) = \sum_{E \in S_p} |E(\mathbb{F}_p)|,$$

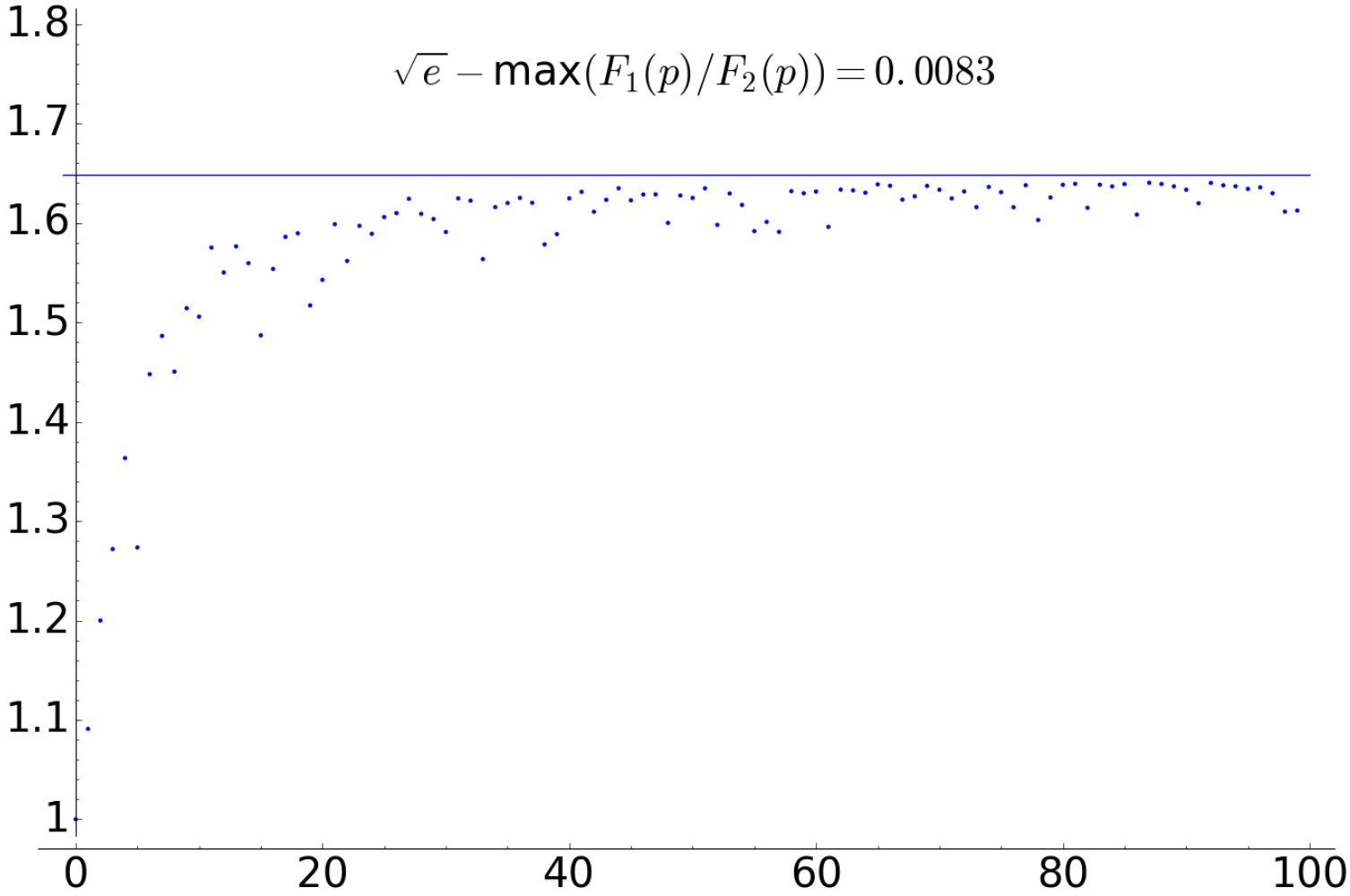
$$F_2(p) = \sum_{E \in S_p} |\langle (0,0) \rangle|,$$

$$F_3(p) = \sum_{E \in S_p} [E(\mathbb{F}_p) : \langle (0,0) \rangle].$$

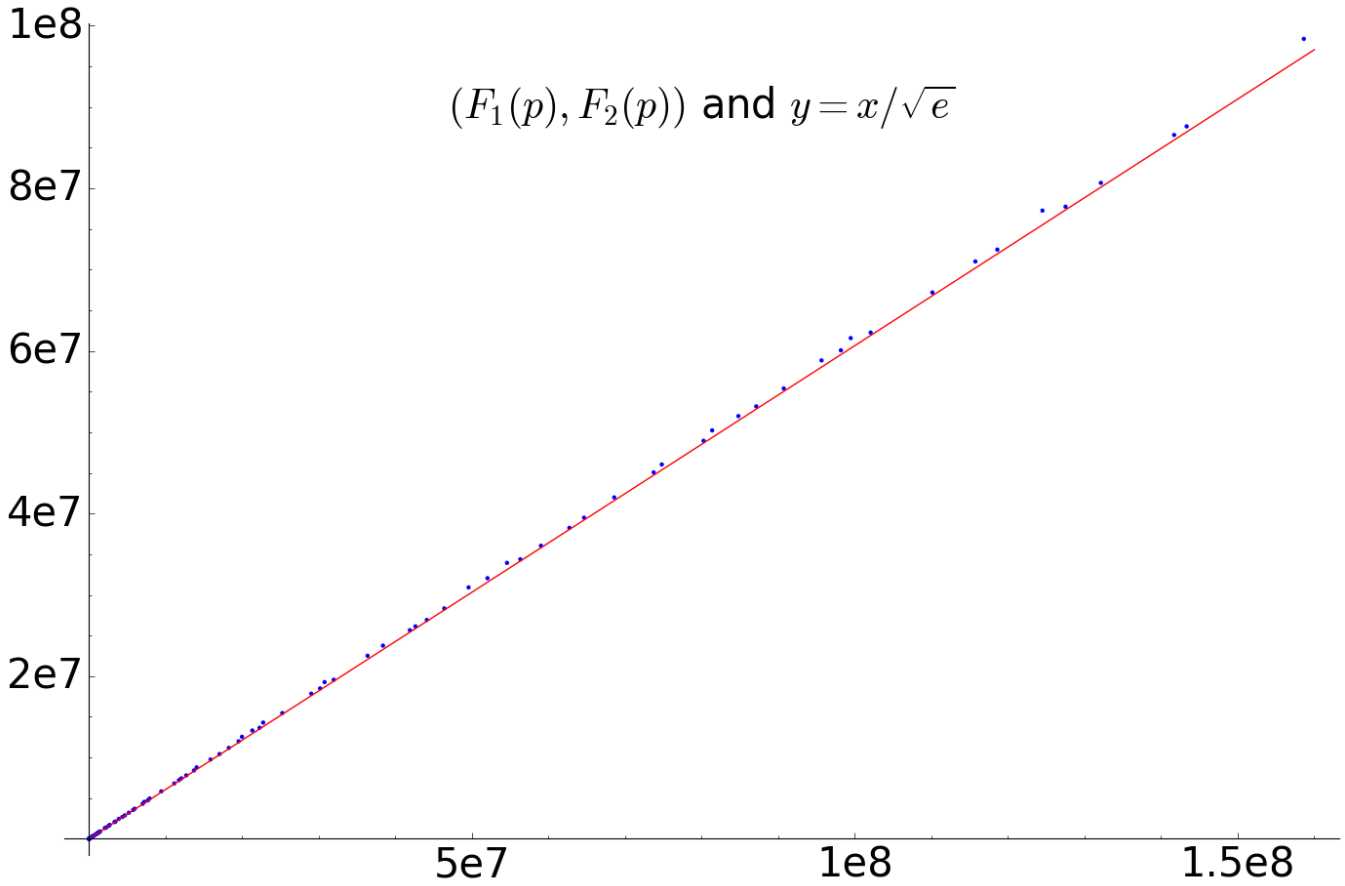
Generating a Subgroup with $(0, 0)$



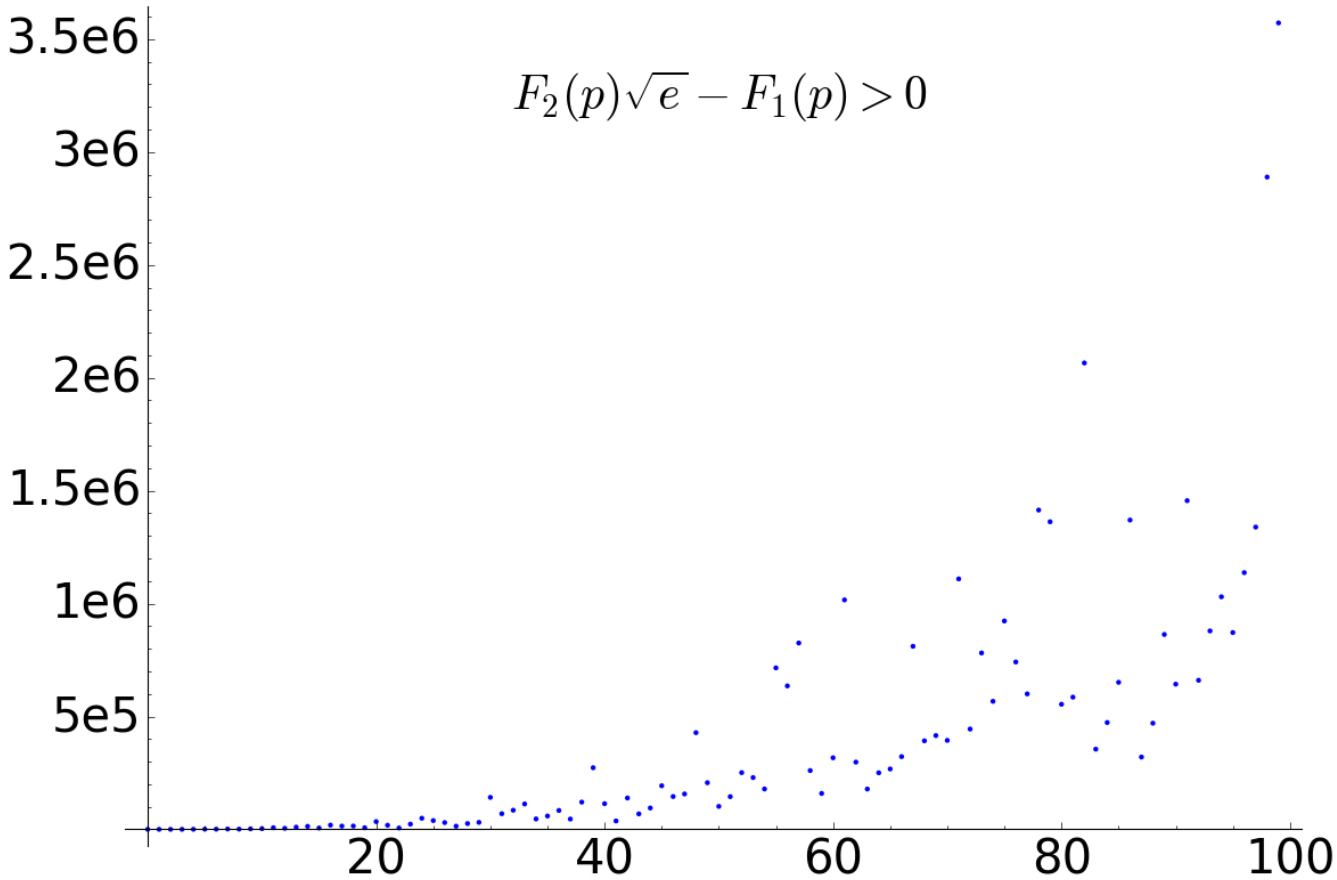
Generating a Subgroup with $(0, 0)$



Generating a Subgroup with $(0, 0)$



Generating a Subgroup with $(0, 0)$

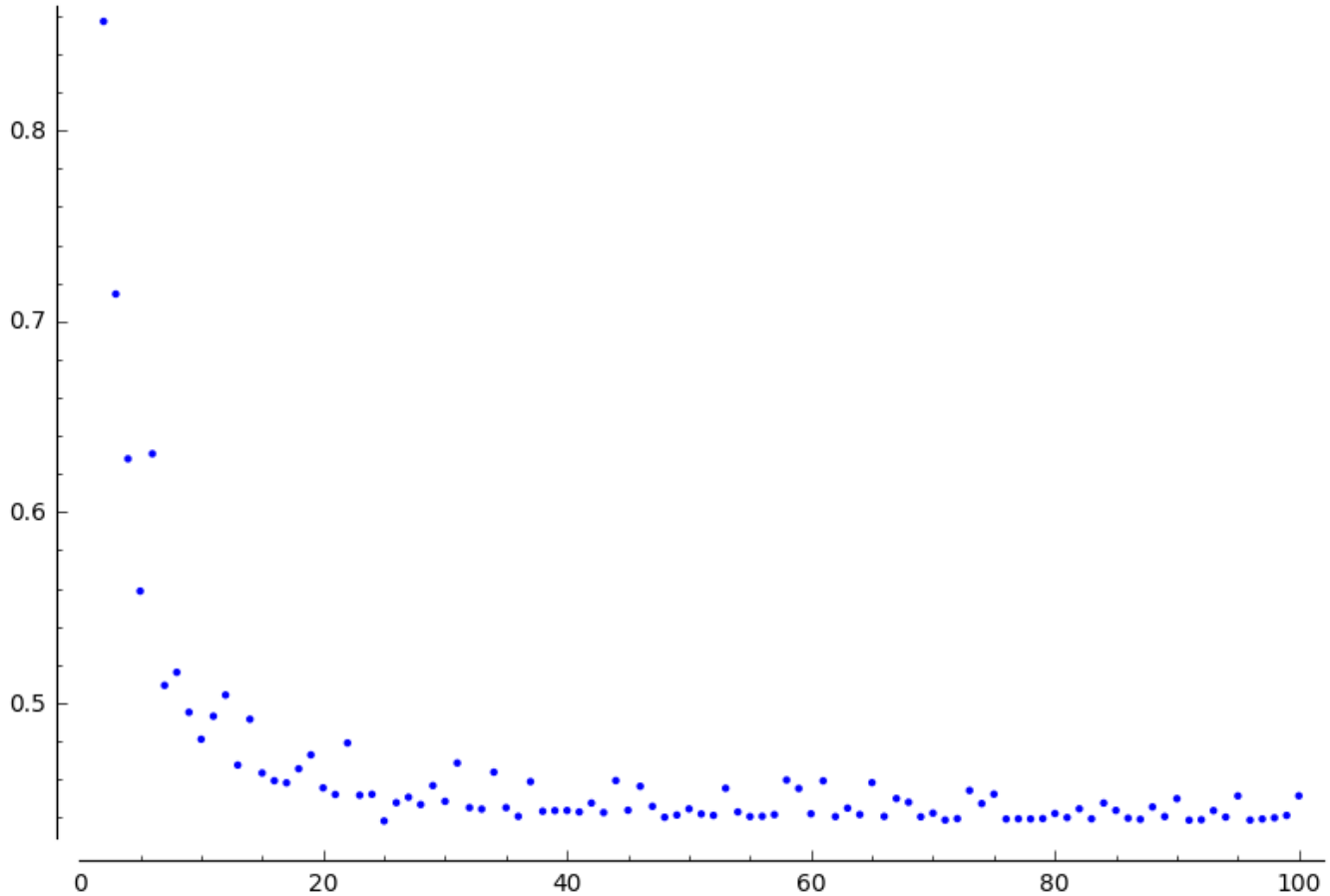


How Often is the Subgroup the Group?

Now, we're investigating the divisibility of the index $[E(\mathbb{F}_p) : \langle(0,0)\rangle] = |E(\mathbb{F}_p)|/|\langle(0,0)\rangle|$.
How often is it one? How often is it even? How often is it divisible by n?

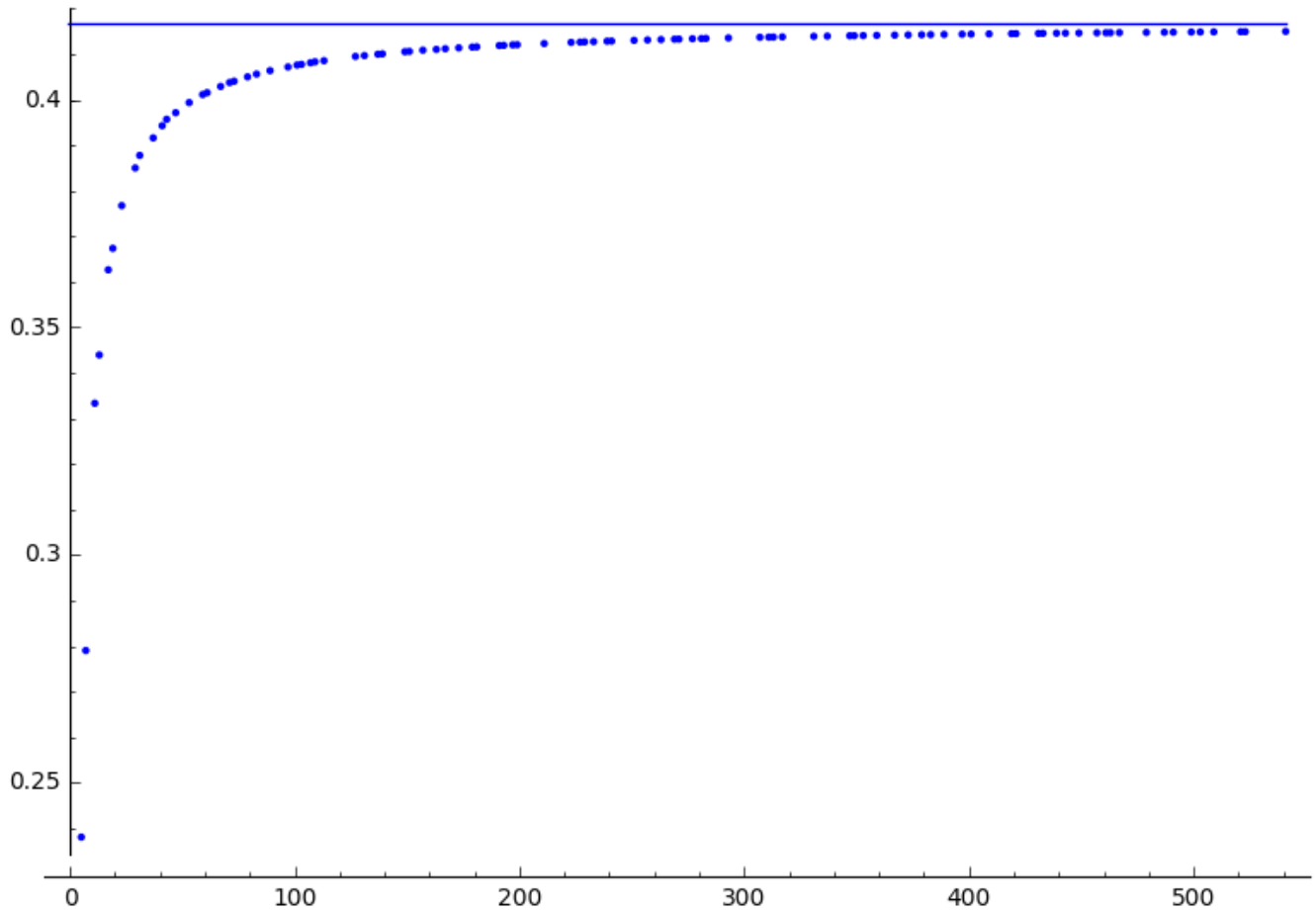
How Often is the Subgroup the Group?

How often is $\frac{|E(F_p)|}{|\langle(0,0)\rangle|}$ one? About 44% of the time.



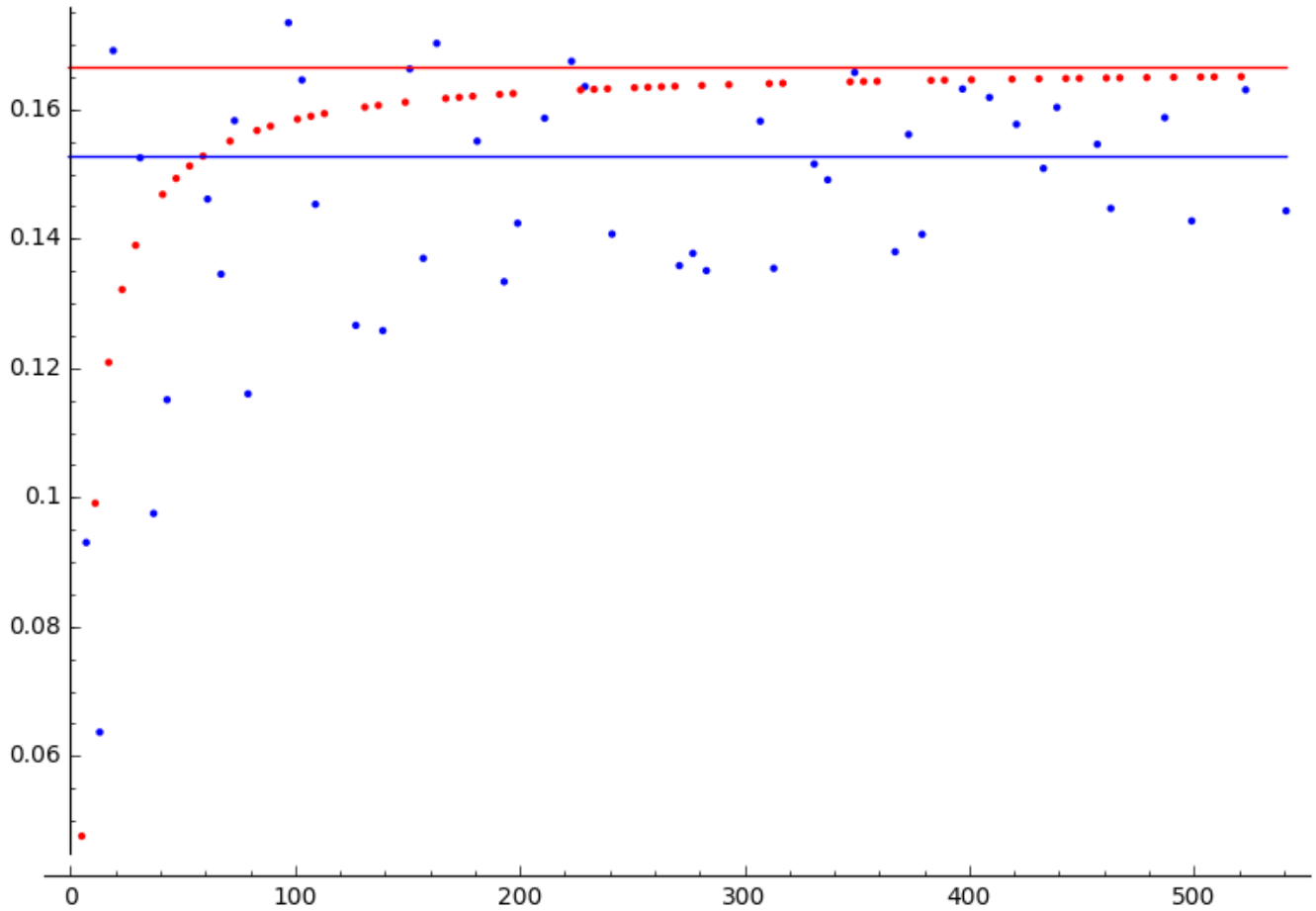
How Often is the Index Even?

We believe that it's 10/24 probability in the limit.



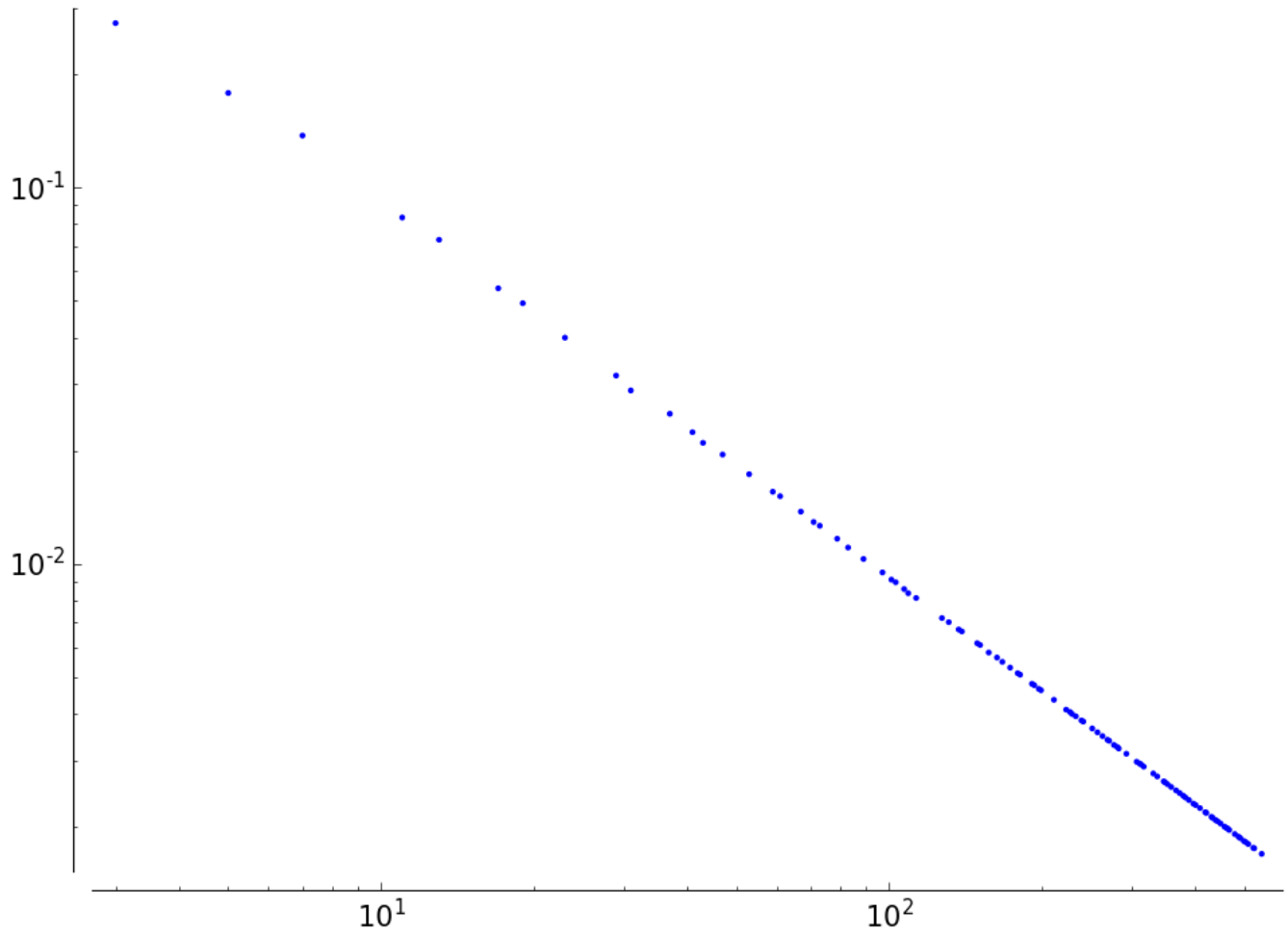
How Often is the Index Three Divisible?

If $p = 1 \pmod{p}$, then the probability is $33/216$.
If $p = 2 \pmod{p}$, then the probability is $36/216$.



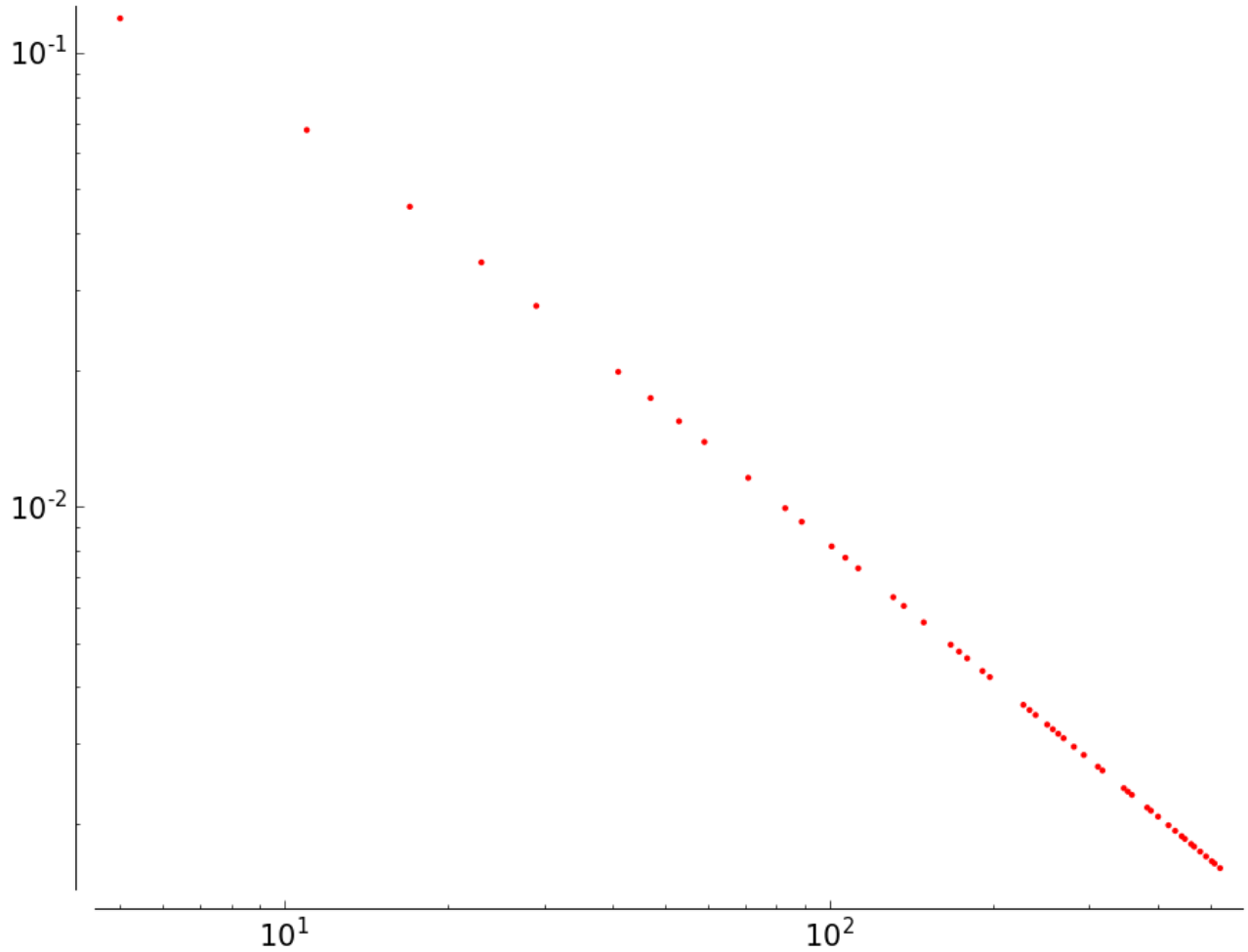
Error Analysis

For our claim that 10/24 is the probability the index is even in the limit, we find that error from our conjectural bound decays exponentially.



Error Analysis

And a similar story for 36/216



Conclusions

Questions?