Sato-Tate Groups of Aoki Curves

Rezwan Hoque

Faculty Advisor: Professor Heidi Goodson

Brooklyn College, City University of New York
On the traditional and unceded territory of the Lenape

Brooklyn College The City University of New York

Tow Mentoring Initiative
Research and Mentoring Program

Some Motivation

Every day, millions of people (including you!) make transactions, store, and interact with data online...

Safeguarding sensitive information is of *extreme* importance...

Some Motivation

Every day, millions of people (including you!) make transactions, store, and interact with data online...

Safeguarding sensitive information is of *extreme* importance...

One way to encrypt online information is through **Elliptic Curve Cryptography** (ECC)!

Some Motivation

Every day, millions of people (including you!) make transactions, store, and interact with data online...

Safeguarding sensitive information is of *extreme* importance...

One way to encrypt online information is through **Elliptic Curve Cryptography** (ECC)!

ECC aims to use the theory behind elliptic (and related) curves to hide data from unauthorized users.

Some Motivation

Every day, millions of people (including you!) make transactions, store, and interact with data online...

Safeguarding sensitive information is of *extreme* importance...

One way to encrypt online information is through **Elliptic Curve Cryptography** (ECC)!

ECC aims to use the theory behind elliptic (and related) curves to hide data from unauthorized users.

In fact, ECC is one of the most efficient ways to encrypt online data!

Elliptic Curves

Elliptic curves are equations of the form

$$y^2 = x^3 + Ax + B,$$

where A and B are constants.

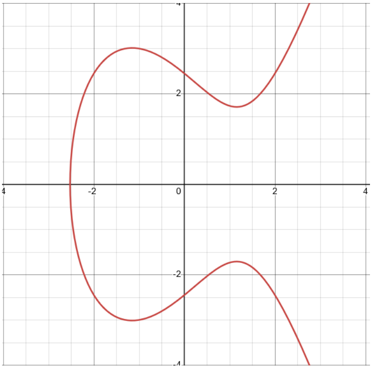

Figure: $y^2 = x^3 - 4x + 6$

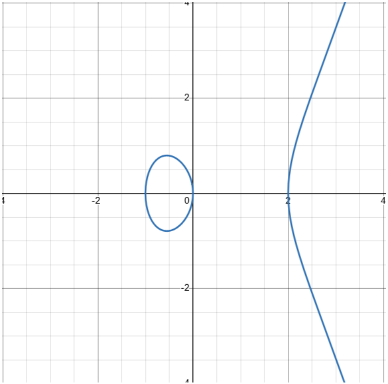

Figure: $y^2 = x(x + 1)(x - 2)$

The Catch

We're interested in curves defined over sets that are ***finite*** in size!

The Catch

We're interested in curves defined over sets that are ***finite*** in size!

More specifically, a finite field $\mathbb{F}_q$.

q is a prime number

So, a curve over $\mathbb{F}_q$ will have finitely many points, rather than infinitely many.

Our Work

Our Work

We are studying the curve

$$y^p = x(x^p - 1),$$

where p is a prime number.

Our Work

We are studying the curve

$$y^p = x(x^p - 1),$$

where p is a prime number.

Goal: Determine the number of points on this curve defined over $\mathbb{F}_q$ as $q \to \infty$.

Our Work

We are studying the curve

$$y^p = x(x^p - 1),$$

where p is a prime number.

Goal: Determine the number of points on this curve defined over $\mathbb{F}_q$ as $q \to \infty$.

I'll be talking about the case $p = 5$, i.e.

$$y^5 = x(x^5 - 1),$$

a *genus* 10 curve.

Stepping Stones

In the 1940s, french mathematician André Weil proved the following (Hasse-Weil bound):

Stepping Stones

In the 1940s, french mathematician André Weil proved the following (Hasse-Weil bound):

$$|q + 1 - \#C(\mathbb{F}_q)| \leq 2g\sqrt{q}.$$

Stepping Stones

In the 1940s, french mathematician André Weil proved the following (Hasse-Weil bound):

$$|q + 1 - \#C(\mathbb{F}_q)| \leq 2g\sqrt{q}.$$

The number of points on a curve C, denoted as $\#C(\mathbb{F}_q)$, is approximately $q + 1$, and differ by at most $2g\sqrt{q}$, where g is the curve's genus.

Stepping Stones

In the 1940s, french mathematician André Weil proved the following (Hasse-Weil bound):

$$|q + 1 - \#C(\mathbb{F}_q)| \leq 2g\sqrt{q}.$$

The number of points on a curve C, denoted as $\#C(\mathbb{F}_q)$, is approximately $q + 1$, and differ by at most $2g\sqrt{q}$, where g is the curve's genus.

Let $t_q = |q + 1 - \#C(\mathbb{F}_q)|$. Dividing both sides by $\sqrt{q}$ gives

$$a_1 = \frac{t_q}{\sqrt{q}} \implies -2g \leq a_1 \leq 2g \implies -20 \leq a_1 \leq 20.$$

Stepping Stones

In the 1940s, french mathematician André Weil proved the following (Hasse-Weil bound):

$$|q + 1 - \#C(\mathbb{F}_q)| \leq 2g\sqrt{q}.$$

The number of points on a curve C, denoted as $\#C(\mathbb{F}_q)$, is approximately $q + 1$, and differ by at most $2g\sqrt{q}$, where g is the curve's genus.

Let $t_q = |q + 1 - \#C(\mathbb{F}_q)|$. Dividing both sides by $\sqrt{q}$ gives

$$a_1 = \frac{t_q}{\sqrt{q}} \implies -2g \leq a_1 \leq 2g \implies -20 \leq a_1 \leq 20.$$

Aim: Determine the distribution of a_1 as $q \to \infty$

The Sato-Tate Conjecture

Proposed by Mikio Sato and John Tate in the 1960s.

The Sato-Tate Conjecture

Proposed by Mikio Sato and John Tate in the 1960s.

Conjecture (Generalized Sato-Tate Conjecture)

As $p \to \infty$*, the distribution converges to the distribution of traces in the Sato-Tate group, a compact subgroup of* $\mathrm{USp}(2g)$ *associated to the Jacobian of the curve.*

The Sato-Tate Conjecture

Proposed by Mikio Sato and John Tate in the 1960s.

Conjecture (Generalized Sato-Tate Conjecture)

As $p \to \infty$, the distribution converges to the distribution of traces in the Sato-Tate group, a compact subgroup of $\mathrm{USp}(2g)$ *associated to the Jacobian of the curve.*

These curves have an associated *Sato-Tate group*, which is a set of matrices. Computing the characteristic polynomial of each element gives the element's trace, which reveals certain behaviors about the number of points on the curve!

The Sato-Tate Group for $p = 5$

Theorem (Goodson, Hoque)

Let C_5 be the genus $g = 10$ curve $y^5 = x(x^5 - 1)$. Then, up to conjugation in $\mathrm{USp}(2g)$, the Sato-Tate group of the Jacobian is

$$\mathrm{ST}(\mathrm{Jac}(C_5)) = \langle \mathrm{U}(1)^{10}, \gamma \rangle,$$

where γ is the 10×10 block matrix

$$\left(\begin{array}{c|c|c|c|c|c|c|c|c|c}
 & & I & & & & & & & \\ \hline
 & & & & & & I & & & \\ \hline
 & & & & & & & & & I \\ \hline
 & & & & J & & & & & \\ \hline
 & & & & & J & & & & \\ \hline
 & I & & & & & & & & \\ \hline
J & & & & & & & & & \\ \hline
 & & & & & & & & I & \\ \hline
 & & & I & & & & & & \\ \hline
 & & & & & & & I & &
\end{array}\right).$$

What is the a_1 Distribution?

Now that we have the ST group for our curve, we can compute the traces of each $\mathrm{U}(1)^{10} \cdot \gamma^i$, where $0 \leq i \leq 19$.

What is the a_1 Distribution?

Now that we have the ST group for our curve, we can compute the traces of each $\mathrm{U}(1)^{10} \cdot \gamma^i$, where $0 \leq i \leq 19$.

This leads us to compute *moment statistics*, a statistical tool used to numerically describe a data set through its average value, variance, skewness, and more!

$$[1, 0, 1, 0, 57, 0, 5140]$$

What is the a_1 Distribution?

Now that we have the ST group for our curve, we can compute the traces of each $\mathrm{U}(1)^{10} \cdot \gamma^i$, where $0 \leq i \leq 19$.

This leads us to compute *moment statistics*, a statistical tool used to numerically describe a data set through its average value, variance, skewness, and more!

[1, 0, 1, 0, 57, 0, 5140]

The numerical moments calculated from $\frac{t_q}{\sqrt{q}}$, up to $q<2^{22}$, get close to the moments generated by the group, validating the ST conjecture!

[-0.00050968, 0.993906, 0.00368233, 14.8362, 0.25881, 304.502, 7.78995]

Visualizing a_1

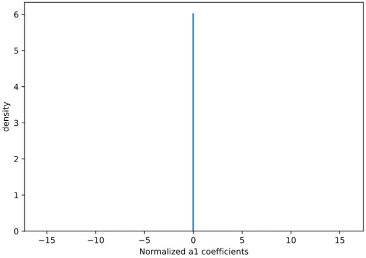

Figure: All primes q

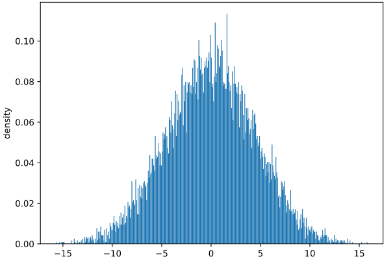

Figure: Primes $q \equiv 1 \pmod{25}$

Future Work

- Work on other curves of the form $y^p = x(x^p - 1)$.
  - Can we generalize the behavior?
- What happens when we vary the first x term?
  - i.e. $y^p = x^a(x^p - 1)$
- Find moment statistics for $a_2, a_3, \ldots, a_n$!

Bonus Slide: More Distributions!

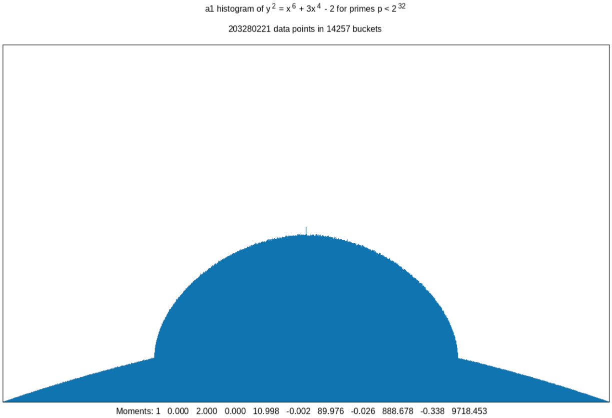

Figure: a_1 distribution of a genus 2 curve

(image credit: Goodson)

Bonus Slide: More Distributions!

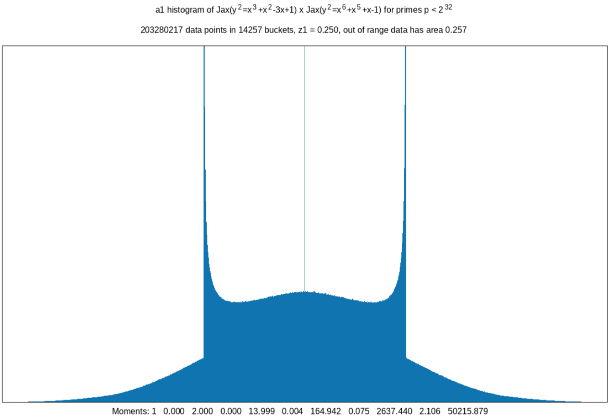

Figure: a_1 distribution of a genus 3 curve

(image credit: Goodson)

Bonus Slide: More Distributions!

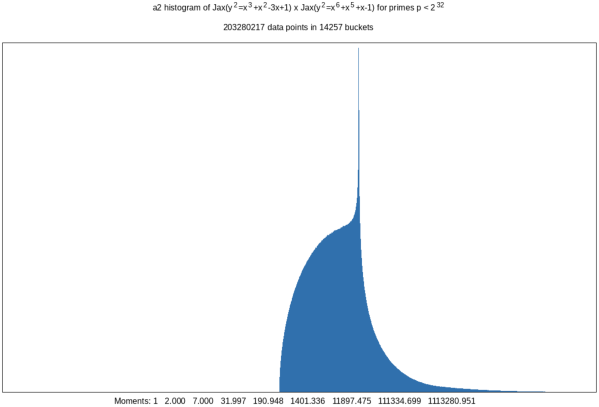

Figure: a_2 distribution of a genus 3 curve

(image credit: Goodson)