On the existence of hyperelliptic curves over $\mathbb{Q}(T)$ with lower Jacobian ranks via generalized Nagao's conjecture

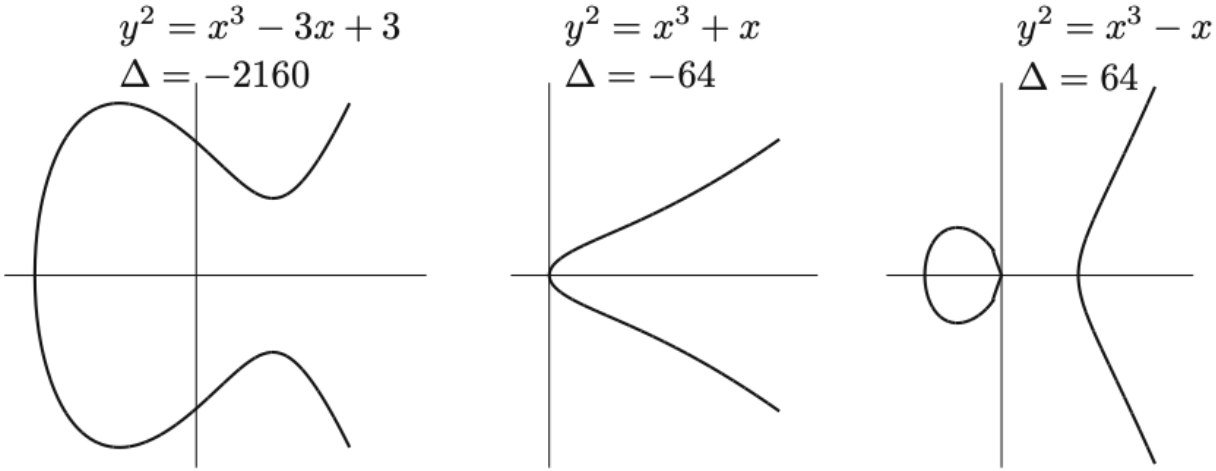
Lucas Chen[1] Joshua Im[2]
Mentor: Steven J. Miller

SMALL REU, Williams College

[1]lucasch@uchicago.edu, [2]jri@tamu.edu

Young Mathematicians Conference
July 30, 2026

Elliptic Curves



$$E/K : y^2 = x^3 + Ax + B, \quad A, B \in K$$

The Group Law

We can associate an **abelian group** to an elliptic curve.

The Group Law

We can associate an **abelian group** to an elliptic curve.

Definition

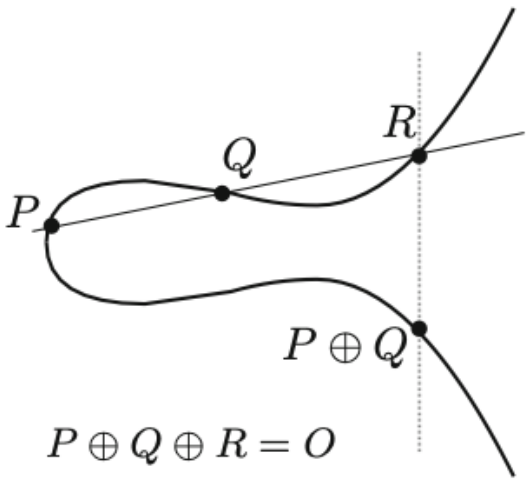
Let $P, Q \in E(K)$ be points on the curve. Define R to be the third point that the line passing through P and Q passes. Define $P + Q$ to be the reflection of R w.r.t the y-axis. Define

$$P + Q + R = O := \mathrm{id}_E.$$

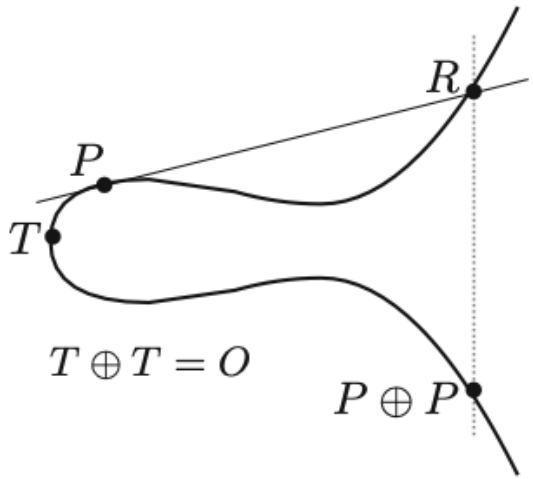
Theorem

$(E(K), +)$ *forms an abelian group.*

The Group Law



Addition of distinct points



Adding a point to itself

Figure: The composition law. (Silverman 2009)

The Mordell-Weil group

For a field extension L/K, $E(K)$ is a subgroup of $E(L)$.

The Mordell-Weil group

For a field extension L/K, $E(K)$ is a subgroup of $E(L)$.

The theorem below is a fundamental result in the field.

Theorem (Mordell-Weil / Lang-Néron)

$E(\mathbb{Q})$ and $E(\mathbb{Q}(T))$ are finitely generated abelian groups. That is for $K = \mathbb{Q}$ or $\mathbb{Q}(T)$,

$$E(K) \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{k_r}\mathbb{Z},$$

where each p_i is prime.

The number of free generators r is called the **rank** of E.

Hyperelliptic Curves

A **hyperelliptic curve** of genus g is a natural generalization of the elliptic curve. For a polynomial $f(x) \in K[x]$, it is cut out by the equation

$$\mathcal{X}/K : y^2 = f(x), \qquad \deg f(x) = 2g+1 \text{ or } 2g+2$$

Hyperelliptic Curves

A **hyperelliptic curve** of genus g is a natural generalization of the elliptic curve. For a polynomial $f(x) \in K[x]$, it is cut out by the equation

$$\mathcal{X}/K : y^2 = f(x), \qquad \deg f(x) = 2g + 1 \text{ or } 2g + 2$$

$\mathcal{X}$ generates a **Jacobian variety** denoted $J(\mathcal{X})$, a geometric object which is an abelian group.

The Jacobian satisfies Mordell-Weil and has an equivalent notion of rank.

Frobenius Trace

(Hyper)Elliptic curve $\mathcal{X} : y^2 = f(x)$ over $\mathbb{F}_p$:

$$\#\mathcal{X}(\mathbb{F}_p) = \#\{(x, y) \in \mathbb{F}_p^2 \mid y^2 \equiv f(x) \pmod{p}\}$$

Theorem (Hasse, 1933)

In the case of elliptic curves E, $|(p+1) - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$.

Definition (Frobenius Trace)

We call $a_{\mathcal{X}}(p) = (p+1) - \#\mathcal{X}(\mathbb{F}_p)$ the **Frobenius trace** of $\mathcal{X}$ at a prime p.

(This is legitimately the trace of a Frobenius operator on a very specific module!)

Our research focuses on hyperelliptic curves $\mathcal{X}$ over $\mathbb{Q}(T)$. Then the elliptic curve obtained by the specialization $T = t$ is well-defined over $\mathbb{Q}$, which we call $\mathcal{X}_t/\mathbb{Q}$.

Definition (rth Moment)

Fix a prime p. Let $a_{\mathcal{X}_t}(p)$ be the Frobenius trace of $\mathcal{X}_t$ at p. The **rth moment** of $\mathcal{X}$ is defined by

$$A_{\mathcal{X},r}(p) = \frac{1}{p}\sum_{t=0}^{p-1} a_{\mathcal{X}_t}(p)^r.$$

Nagao's Conjecture

Nagao conjectured on the relationships between the first moment and the rank.

Conjecture (Nagao)

For an elliptic curve $E/\mathbb{Q}(T)$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{p\leq N} -A_{E,1}(p) \log p = \operatorname{rank}(E/\mathbb{Q}(T)).$$

Conjecture (Nagao, Generalized)

For a hyperelliptic curve $\mathcal{X}/\mathbb{Q}(T)$ such that the Jacobian variety of $\mathcal{X}$ has no subvariety over $\mathbb{Q}$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{p\leq N} -A_{\mathcal{X},1}(p) \log p = \operatorname{rank} J_{\mathcal{X}}(\mathbb{Q}(T)).$$

Nagao - Why do we care?

It is generally hard to find an (hyper)elliptic curve with

- high rank, and
- a fixed, given rank.

Nagao - Why do we care?

It is generally hard to find an (hyper)elliptic curve with

- high rank, and
- a fixed, given rank.

Nagao's conjecture lets us construct (hyper)elliptic curves with a specific rank.

Nagao - Why do we care?

It is generally hard to find an (hyper)elliptic curve with

- high rank, and
- a fixed, given rank.

Nagao's conjecture lets us construct (hyper)elliptic curves with a specific rank.

Known results on existence of (hyper)elliptic curves over $\mathbb{Q}(T)$:

- For any g, there exists infinitely many hyperelliptic curves of rank 0, 1, 2.
- Rank could be arbitrarily large (genus is not fixed!)

In general, it is not known if there exists an hyperelliptic curve for a specific (g, r).

Main Results

We state our main results.

Theorem

Assume generalized Nagao's conjecture. Then there exists infinitely many hyperelliptic curves $\mathcal{X}/\mathbb{Q}(T) : y^2 = f(x, T)$ *of genus* g *with* $\operatorname{rank} J_{\mathcal{X}}(\mathbb{Q}(T)) = r$ *if*

- $1 \leq r \leq 2g + 1$,
- $2g + 2 \leq r \leq 4g + 4$.

So, with the assumption of generalized Nagao, we can find infinitely many hyperelliptic curves with a fixed genus and rank, in the given range.

Constructions

1. $1 \leq r \leq 2g$.

Proof mainly uses character sums and Galois theory.

Constructions

1. $1 \leq r \leq 2g$.

Proof mainly uses character sums and Galois theory.

- Consider $\mathcal{X} : y^2 = a(x)T + b(x)$.
- Let $a(x)$ have degree r and splits completely over $\mathbb{Q}$, and $b(x) = x^{2g+1}$ (resp. x^{2g+2}).
- Use Hilbert's irreducibility theorem to verify that for infinitely many choices of $a(x)$, the Galois group of $a(x)T + b(x)$ over $\mathbb{Q}(T)$ is S_{2g+1} (resp. S_{2g+2}).
- Use linear Legendre sums to compute the first moment.

2. $2g + 1 \leq r \leq 4g + 2$.

Proof mainly uses character sums, Galois theory, and algebraic geometry.

Constructions

2. $2g + 1 \leq r \leq 4g + 2$.

Proof mainly uses character sums, Galois theory, and algebraic geometry.

- Consider $\mathcal{X} : y^2 = a(x)T^2 + b(x)T + c(x)$.
- Construct $a(x)$, $b(x)$, $c(x)$ so that $b(x)^2 - 4a(x)c(x)$ have square roots.
- Verify that the geometric monodromy group of $c(x)$ is S_{2g+1} (resp. S_{2g+2}).
- Use quadratic Legendre sums to compute the first moment.

Thank you for listening!