Abelian varieties, torsion and local arithmetic

Mohammad Sadek

Sabanci University, Istanbul

Representation Theory XIX
Dubrovnik, Croatia, June 22-June 28, 2025

June 26, 2025

What are Diophantine problems?

What are Diophantine problems?

Arithmetic on Curves, Barry Mazur, Bulletin of the American Mathematical Society, Volume 14, Number 2, 1986, 207–259

What are Diophantine problems?

Arithmetic on Curves, Barry Mazur, Bulletin of the American Mathematical Society, Volume 14, Number 2, 1986, 207–259

I. WHAT ARE DIOPHANTINE PROBLEMS?

What are Diophantine problems?

Arithmetic on Curves, Barry Mazur, Bulletin of the American Mathematical Society, Volume 14, Number 2, 1986, 207–259

I. WHAT ARE DIOPHANTINE PROBLEMS?

I don't know the answer.

What are Diophantine problems?

Arithmetic on Curves, Barry Mazur, Bulletin of the American Mathematical Society, Volume 14, Number 2, 1986

I. WHAT ARE DIOPHANTINE PROBLEMS?

I don't know the answer. To feel our way around the question, let us first consider some miscellaneous problems that have been labelled "Diophantine" and then review some attempts towards a systematic organization of these "Diophantine problems".

Diophantine Problems

- List all right-angle triangles all of whose sides are integral, i.e., find all integral solutions (x, y, z) of

$$x^2 + y^2 = z^2.$$

Diophantine Problems

- List all right-angle triangles all of whose sides are integral, i.e., find all integral solutions (x, y, z) of

$$x^2 + y^2 = z^2.$$

- Determine for a given natural number n whether there exists a right-angle triangle with all three sides rational and area equal to n

$$y^2 = x^3 - n^2 x.$$

Diophantine Problems

- List all right-angle triangles all of whose sides are integral, i.e., find all integral solutions (x, y, z) of

$$x^2 + y^2 = z^2.$$

- Determine for a given natural number n whether there exists a right-angle triangle with all three sides rational and area equal to n

$$y^2 = x^3 - n^2 x.$$

- Is it possible that there are infinitely many points on an algebraic planar curve all expressible as rational linear combinations of a finite number of points in the plane?

$$F(x, y) = 0$$

Mordell-Weil Theorem

Theorem

For an abelian variety A over a number field K, the group $A(K)$ of K-rational points of A is a finitely-generated abelian group; so it is of the form

$$T \oplus \mathbb{Z}^r$$

where T is the torsion group and r is the rank of A.

Torsion Subgroups of Elliptic Curves

Proposition

Let $E/\mathbb{Q}_p$ be an elliptic curve and let $m \geq 1$ be an integer that is relatively prime to p. If the reduced curve $\tilde{E}_p/\mathbb{F}_p$ is nonsingular, then the reduction map $E(\mathbb{Q}_p)[m] \longrightarrow \tilde{E}_p(\mathbb{F}_p)$ is injective, where $E(\mathbb{Q}_p)[m]$ denotes the set of points of order m in $E(\mathbb{Q}_p)$.

Torsion Subgroups of Elliptic Curves

Proposition

Let $E/\mathbb{Q}_p$ be an elliptic curve and let $m \geq 1$ be an integer that is relatively prime to p. If the reduced curve $\tilde{E}_p/\mathbb{F}_p$ is nonsingular, then the reduction map $E(\mathbb{Q}_p)[m] \longrightarrow \tilde{E}_p(\mathbb{F}_p)$ is injective, where $E(\mathbb{Q}_p)[m]$ denotes the set of points of order m in $E(\mathbb{Q}_p)$.

In paticular, if E is an elliptic curve over $\mathbb{Q}$, then

$$E(\mathbb{Q})_{tors} \hookrightarrow \tilde{E}_p(\mathbb{F}_p)$$

for all but finitely many primes p.

Torsion Subgroups of Elliptic Curves

Proposition

Let $E/\mathbb{Q}_p$ be an elliptic curve and let $m \geq 1$ be an integer that is relatively prime to p. If the reduced curve $\tilde{E}_p/\mathbb{F}_p$ is nonsingular, then the reduction map $E(\mathbb{Q}_p)[m] \longrightarrow \tilde{E}_p(\mathbb{F}_p)$ is injective, where $E(\mathbb{Q}_p)[m]$ denotes the set of points of order m in $E(\mathbb{Q}_p)$.

In paticular, if E is an elliptic curve over $\mathbb{Q}$, then

$$E(\mathbb{Q})_{tors} \hookrightarrow \tilde{E}_p(\mathbb{F}_p)$$

for all but finitely many primes p.

$$\#E(\mathbb{Q})_{tors} \mid \#\tilde{E}_p(\mathbb{F}_p)$$

for all but finitely many primes p.

Torsion Subgroups of Elliptic Curves

Proposition

Let $E/\mathbb{Q}_p$ be an elliptic curve and let $m \geq 1$ be an integer that is relatively prime to p. If the reduced curve $\tilde{E}_p/\mathbb{F}_p$ is nonsingular, then the reduction map $E(\mathbb{Q}_p)[m] \longrightarrow \tilde{E}_p(\mathbb{F}_p)$ is injective, where $E(\mathbb{Q}_p)[m]$ denotes the set of points of order m in $E(\mathbb{Q}_p)$.

In paticular, if E is an elliptic curve over $\mathbb{Q}$, then

$$E(\mathbb{Q})_{tors} \hookrightarrow \tilde{E}_p(\mathbb{F}_p)$$

for all but finitely many primes p.

$$\#E(\mathbb{Q})_{tors} \mid \#\tilde{E}_p(\mathbb{F}_p)$$

for all but finitely many primes p.
Mazur: $\#E(\mathbb{Q})_{tors} \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 16\}$.

Torsion Subgroups of Elliptic Curves

Theorem

Let $m \geq 2$ be an integer. Let E be an elliptic curve defined over $\mathbb{Q}$. The following statements are equivalent:

a) $\#\widetilde{E}_p(\mathbb{F}_p) \equiv 0 \mod m$ *for a set of primes p of density 1.*

b) *There exists an elliptic curve E' over $\mathbb{Q}$ such that:*

   i) *E is $\mathbb{Q}$-isogenous to E'; and*

   ii) $\#E'(\mathbb{Q})_{\text{tors}} \equiv 0 \mod m$.

Torsion Subgroups of Elliptic Curves

- If $m \nmid \#E'(\mathbb{Q})_{tors}$ for any $\mathbb{Q}$-isogenous elliptic curve E' to E, then there are at least two distinct $a_1, a_2 \mod m$ such that the density of primes p for which $\#\tilde{E}_p(\mathbb{F}_p) \equiv a_i \mod m$ is positive.

Torsion Subgroups of Elliptic Curves

- If $m \nmid \#E'(\mathbb{Q})_{tors}$ for any $\mathbb{Q}$-isogenous elliptic curve E' to E, then there are at least two distinct $a_1, a_2 \mod m$ such that the density of primes p for which $\#\tilde{E}_p(\mathbb{F}_p) \equiv a_i \mod m$ is positive.
- If $2 \nmid \#E'(\mathbb{Q})_{tors}$ for any $\mathbb{Q}$-isogenous elliptic curve E' to E, then the density of primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is odd/even is positive.

Torsion Subgroups of Elliptic Curves

- If $m \nmid \#E'(\mathbb{Q})_{tors}$ for any $\mathbb{Q}$-isogenous elliptic curve E' to E, then there are at least two distinct $a_1, a_2 \mod m$ such that the density of primes p for which $\#\tilde{E}_p(\mathbb{F}_p) \equiv a_i \mod m$ is positive.
- If $2 \nmid \#E'(\mathbb{Q})_{tors}$ for any $\mathbb{Q}$-isogenous elliptic curve E' to E, then the density of primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is odd/even is positive.
- The set of integers $m > 1$ such that there is an elliptic curve $E/\mathbb{Q}$ with $m \mid \#\tilde{E}_p(\mathbb{F}_p)$ for all but finitely many primes is

$$\{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 16\}.$$

Orders of Reduction of Elliptic Curves

Fix an elliptic curve $E/\mathbb{Q}$. Given a prime p of good reduction of E, define $a_p := p + 1 - \#\tilde{E}_p(\mathbb{F}_p)$.

Orders of Reduction of Elliptic Curves

Fix an elliptic curve $E/\mathbb{Q}$. Given a prime p of good reduction of E, define $a_p := p + 1 - \#\tilde{E}_p(\mathbb{F}_p)$.

- $|a_p| \leq 2\sqrt{p}$. (Hasse-Weil)

Orders of Reduction of Elliptic Curves

Fix an elliptic curve $E/\mathbb{Q}$. Given a prime p of good reduction of E, define $a_p := p + 1 - \#\tilde{E}_p(\mathbb{F}_p)$.

- $|a_p| \leq 2\sqrt{p}$. (Hasse-Weil)
- Fix an integer n, are there infinitely many primes p such that $a_p(E) = n$?

Orders of Reduction of Elliptic Curves

Fix an elliptic curve $E/\mathbb{Q}$. Given a prime p of good reduction of E, define $a_p := p + 1 - \#\tilde{E}_p(\mathbb{F}_p)$.

- $|a_p| \leq 2\sqrt{p}$. (Hasse-Weil)
- Fix an integer n, are there infinitely many primes p such that $a_p(E) = n$?
- (Elkies) There are infinitely many primes p such that $a_p(E) = 0$.

Orders of Reduction of Elliptic Curves

Fix an elliptic curve $E/\mathbb{Q}$. Given a prime p of good reduction of E, define $a_p := p + 1 - \#\tilde{E}_p(\mathbb{F}_p)$.

- $|a_p| \leq 2\sqrt{p}$. (Hasse-Weil)
- Fix an integer n, are there infinitely many primes p such that $a_p(E) = n$?
- (Elkies) There are infinitely many primes p such that $a_p(E) = 0$.
- **Exercise.** If $E \sim_{\mathbb{Q}} E'$ with $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$, then $a_p(E) \equiv p + 1 \mod 3$ for all but finitely many primes p,

Orders of Reduction of Elliptic Curves

Fix an elliptic curve $E/\mathbb{Q}$. Given a prime p of good reduction of E, define $a_p := p + 1 - \#\tilde{E}_p(\mathbb{F}_p)$.

- $|a_p| \leq 2\sqrt{p}$. (Hasse-Weil)
- Fix an integer n, are there infinitely many primes p such that $a_p(E) = n$?
- (Elkies) There are infinitely many primes p such that $a_p(E) = 0$.
- **Exercise.** If $E \sim_{\mathbb{Q}} E'$ with $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$, then $a_p(E) \equiv p + 1 \mod 3$ for all but finitely many primes p, So $a_p(E) \equiv 0 \text{ or } 2 \mod 3$.

Orders of Reduction of Elliptic Curves

Fix an elliptic curve $E/\mathbb{Q}$. Given a prime p of good reduction of E, define $a_p := p + 1 - \#\tilde{E}_p(\mathbb{F}_p)$.

- $|a_p| \leq 2\sqrt{p}$. (Hasse-Weil)
- Fix an integer n, are there infinitely many primes p such that $a_p(E) = n$?
- (Elkies) There are infinitely many primes p such that $a_p(E) = 0$.
- **Exercise.** If $E \sim_{\mathbb{Q}} E'$ with $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$, then $a_p(E) \equiv p + 1 \mod 3$ for all but finitely many primes p, So $a_p(E) \equiv 0$ or $2 \mod 3$. The set

$$\bigcup_{N \equiv 1 \bmod 3} \{p |\, a_p(E) = N\}$$

is finite.

Orders of Reduction of Elliptic Curves

Theorem (Q. Ji, H. Qin, 2014)

Let $E : y^2 = x^3 + x$. For a prime p, $a_p(E) = 2$ if and only if $p = x^2 + 1$ for some $x \in \mathbb{Z}$.

Orders of Reduction of Elliptic Curves

Theorem (Q. Ji, H. Qin, 2014)

Let $E : y^2 = x^3 + x$. For a prime p, $a_p(E) = 2$ if and only if $p = x^2 + 1$ for some $x \in \mathbb{Z}$. In particular, the polynomial $x^2 + 1$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E) = 2$.

Orders of Reduction of Elliptic Curves

Theorem (Q. Ji, H. Qin, 2014)

Let $E : y^2 = x^3 + x$. For a prime p, $a_p(E) = 2$ if and only if $p = x^2 + 1$ for some $x \in \mathbb{Z}$. In particular, the polynomial $x^2 + 1$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E) = 2$.

Conjecture (Hardy-Littlewood)

Suppose that a, b, c are integers and a is positive; that $\gcd(a, b, c) = 1$; that $a + b$ and c are not both even; and that $b^2 - 4ac$ is not a square. Then, there are infinitely many primes of the form $ax^2 + bx + c$.

Orders of Reduction of Elliptic Curves

Examples. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

Examples. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

$$\#\widetilde{E}_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 12 & \text{if } p \equiv 1, 9, 11, 13, 17, 19 \mod 20 \\ 6 \mod 12 & \text{if } p \equiv 3, 7 \mod 20. \end{cases}$$

Examples. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

$$\#\widetilde{E}_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 12 & \text{if } p \equiv 1, 9, 11, 13, 17, 19 \mod 20 \\ 6 \mod 12 & \text{if } p \equiv 3, 7 \mod 20. \end{cases}$$

$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$,

Examples. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

$$\#\widetilde{E}_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 12 & \text{if } p \equiv 1, 9, 11, 13, 17, 19 \mod 20 \\ 6 \mod 12 & \text{if } p \equiv 3, 7 \mod 20. \end{cases}$$

$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$, but $E \sim_{\mathbb{Q}} E'$ where $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$,

$$E' : y^2 = x^3 - 372x + 2761.$$

Orders of Reduction of Elliptic Curves

Proposition

Let E be an elliptic curve over $\mathbb{Q}$ and $m > 1$ be an integer such that E is not $\mathbb{Q}$-isogenous to an elliptic curve E' with $\#E'(\mathbb{Q})_{\text{tors}} \equiv 0 \mod m$. Then $\#\widetilde{E}_p(\mathbb{F}_p) \equiv 0 \mod m$ for all primes p in a set S of primes of positive density $\delta < 1$.

Orders of Reduction of Elliptic Curves

Lemma

Let E be an elliptic curve defined over $\mathbb{Q}$. Let p be a prime of good reduction of E. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square free integer, and $\mathfrak{p} \mid p$ be a prime in K. Then,

$$\#\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}}) = \begin{cases} \#\widetilde{E}_p(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = 1,\ p \neq 2 \\ \#\widetilde{E}_p(\mathbb{F}_p) \cdot \#\widetilde{E}_p^d(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = -1,\ p \neq 2, \end{cases}$$

where $\left(\frac{d}{p}\right)$ is the Legendre symbol of d modulo p.

Orders of Reduction of Elliptic Curves

Lemma

Let E be an elliptic curve defined over $\mathbb{Q}$. Let p be a prime of good reduction of E. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square free integer, and $\mathfrak{p} \mid p$ be a prime in K. Then,

$$\#\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}}) = \begin{cases} \#\widetilde{E}_p(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = 1,\ p \neq 2 \\ \#\widetilde{E}_p(\mathbb{F}_p) \cdot \#\widetilde{E}_p^d(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = -1,\ p \neq 2, \end{cases}$$

where $\left(\frac{d}{p}\right)$ is the Legendre symbol of d modulo p.

Let K be a quadratic number field.

Lemma

Let E be an elliptic curve defined over $\mathbb{Q}$. Let p be a prime of good reduction of E. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square free integer, and $\mathfrak{p} \mid p$ be a prime in K. Then,

$$\#\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}}) = \begin{cases} \#\widetilde{E}_p(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = 1,\ p \neq 2 \\ \#\widetilde{E}_p(\mathbb{F}_p) \cdot \#\widetilde{E}_p^d(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = -1,\ p \neq 2, \end{cases}$$

where $\left(\frac{d}{p}\right)$ is the Legendre symbol of d modulo p.

Let K be a quadratic number field. If $E(\mathbb{Q})_{tors} = G$, Then

Orders of Reduction of Elliptic Curves

Lemma

Let E be an elliptic curve defined over $\mathbb{Q}$. Let p be a prime of good reduction of E. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square free integer, and $\mathfrak{p} \mid p$ be a prime in K. Then,

$$\#\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}}) = \begin{cases} \#\widetilde{E}_p(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = 1,\ p \neq 2 \\ \#\widetilde{E}_p(\mathbb{F}_p) \cdot \#\widetilde{E}_p^d(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = -1,\ p \neq 2, \end{cases}$$

where $\left(\frac{d}{p}\right)$ is the Legendre symbol of d modulo p.

Let K be a quadratic number field. If $E(\mathbb{Q})_{tors} = G$, Then

$$E(K)_{tors}?$$

Orders of Reduction of Elliptic Curves

Lemma

Let E be an elliptic curve defined over $\mathbb{Q}$. Let p be a prime of good reduction of E. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square free integer, and $\mathfrak{p} \mid p$ be a prime in K. Then,

$$\#\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}}) = \begin{cases} \#\widetilde{E}_p(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = 1,\ p \neq 2 \\ \#\widetilde{E}_p(\mathbb{F}_p) \cdot \#\widetilde{E}_p^d(\mathbb{F}_p) & \text{if } \left(\frac{d}{p}\right) = -1,\ p \neq 2, \end{cases}$$

where $\left(\frac{d}{p}\right)$ is the Legendre symbol of d modulo p.

Let K be a quadratic number field. If $E(\mathbb{Q})_{tors} = G$, Then

$$E(K)_{tors}?$$

E. Gonzalez-Jimenez and J. M. Tornero, 2014, 2016.

Orders of Reduction of Elliptic Curves

Given an elliptic curve E defined over a number field K then we define

$$M_K(E) = \sup\{\#E'(K)_{\text{tors}} : E' \text{ is } K\text{-isogenous to } E\}.$$

Orders of Reduction of Elliptic Curves

Given an elliptic curve E defined over a number field K then we define

$$M_K(E) = \sup\{\#E'(K)_{\text{tors}} : E' \text{ is } K\text{-isogenous to } E\}.$$

Theorem (Pajaziti, S-, 2025)

Let $K = \mathbb{Q}(\sqrt{d})$, where d is a square free integer. Let E be an elliptic curve defined over $\mathbb{Q}$ such that $M_K(E) > M_{\mathbb{Q}}(E)$. If $p \nmid 2dM_K(E)$ is a prime of good reduction of E, then

$$\#\widetilde{E}_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod M_K(E) & \text{if } \left(\frac{d}{p}\right) = 1 \\ 2p+2 \mod M_{\mathbb{Q}}(E^d) & \text{if } \left(\frac{d}{p}\right) = -1. \end{cases}$$

In particular, the density of primes p such that $\#\widetilde{E}_p(\mathbb{F}_p) \equiv 0 \mod M_K(E)$ is at least $1/2$.

Orders of Reduction of Elliptic Curves

Example. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

- $E \sim_{\mathbb{Q}} E'$ where $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$, where $E' : y^2 = x^3 - 372x + 2761$.

Orders of Reduction of Elliptic Curves

Example. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

- $E \sim_{\mathbb{Q}} E'$ where $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$, where $E' : y^2 = x^3 - 372x + 2761$.
- For $K = \mathbb{Q}(\sqrt{5})$, $E'(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Orders of Reduction of Elliptic Curves

Example. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

- $E \sim_{\mathbb{Q}} E'$ where $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$, where $E' : y^2 = x^3 - 372x + 2761$.
- For $K = \mathbb{Q}(\sqrt{5})$, $E'(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
- $\#\widetilde{E}_p(\mathbb{F}_p) \equiv 0 \mod 12$ for primes $p \equiv 1, 4 \mod 5$.

Orders of Reduction of Elliptic Curves

Example. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

- $E \sim_{\mathbb{Q}} E'$ where $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$, where $E' : y^2 = x^3 - 372x + 2761$.
- For $K = \mathbb{Q}(\sqrt{5})$, $E'(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
- $\#\widetilde{E}_p(\mathbb{F}_p) \equiv 0 \mod 12$ for primes $p \equiv 1, 4 \mod 5$.
- For the primes $p \equiv 2, 3 \mod 5$, one may have either possibilities for $\#\widetilde{E}_p(\mathbb{F}_p) \mod 12$.
- $(-1, 0) \in E(\mathbb{Q})[2]$,

Orders of Reduction of Elliptic Curves

Example. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

- $E \sim_{\mathbb{Q}} E'$ where $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$, where $E' : y^2 = x^3 - 372x + 2761$.
- For $K = \mathbb{Q}(\sqrt{5})$, $E'(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
- $\#\widetilde{E}_p(\mathbb{F}_p) \equiv 0 \mod 12$ for primes $p \equiv 1, 4 \mod 5$.
- For the primes $p \equiv 2, 3 \mod 5$, one may have either possibilities for $\#\widetilde{E}_p(\mathbb{F}_p) \mod 12$.
- $(-1, 0) \in E(\mathbb{Q})[2]$, $P \in \widetilde{E}_p(\mathbb{F}_p)$ such that $2P = (-1, 0)$ if and only if -1 is a square modulo p.

Orders of Reduction of Elliptic Curves

Example. (Conjecture by Z.H. Sun, 2006, D. Kim, J.K. Koo, Y.K. Park, 2008)

$$E : y^2 = x^3 - 12x - 11$$

- $E \sim_{\mathbb{Q}} E'$ where $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$, where $E' : y^2 = x^3 - 372x + 2761$.
- For $K = \mathbb{Q}(\sqrt{5})$, $E'(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
- $\#\widetilde{E}_p(\mathbb{F}_p) \equiv 0 \mod 12$ for primes $p \equiv 1, 4 \mod 5$.
- For the primes $p \equiv 2, 3 \mod 5$, one may have either possibilities for $\#\widetilde{E}_p(\mathbb{F}_p) \mod 12$.
- $(-1, 0) \in E(\mathbb{Q})[2]$, $P \in \widetilde{E}_p(\mathbb{F}_p)$ such that $2P = (-1, 0)$ if and only if -1 is a square modulo p. Therefore, one has

$$\#\widetilde{E}_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 12 & \text{if } p \equiv 1, 9, 11, 13, 17, 19 \mod 20 \\ 6 \mod 12 & \text{if } p \equiv 3, 7 \mod 20. \end{cases}$$

$\#\widetilde{E}_p(\mathbb{F}_p) \equiv 0 \mod 12$ for primes of density $3/4$, $\#\widetilde{E}_p(\mathbb{F}_p) \equiv 6 \mod 12$ for primes of density $1/4$.

Orders of Reduction of Elliptic Curves

Example.

- $E : y^2 = x^3 + 20148x + 586096$

Example.

- $E : y^2 = x^3 + 20148x + 586096$
- $E(\mathbb{Q}(\sqrt{-6}))_{\text{tors}} \cong \mathbb{Z}/8\mathbb{Z}$

Example.

- $E : y^2 = x^3 + 20148x + 586096$
- $E(\mathbb{Q}(\sqrt{-6}))_{\text{tors}} \cong \mathbb{Z}/8\mathbb{Z}$
-

$$\#\widetilde{E}_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 8 & \text{if } p \equiv 1, 5, 7, 11, 19, 23 \mod 24 \\ 4 \mod 8 & \text{if } p \equiv 13, 17 \mod 24. \end{cases}$$

Orders of Reduction of Elliptic Curves

Theorem (Pajaziti, S-, 2025)

Let E_T be the elliptic curve described by

$$E_T : y^2 = x^3 - 7T\ x^2 + 96T^2\ x + 256\ T^3.$$

For any $T = t \in \mathbb{Z} \setminus \mathbb{Z}^2$ and any prime $p \neq 2, 3, 29$ with $\nu_p(t) = 0$ such that $\left(\frac{t}{p}\right) = 1$, one has $\#\widetilde{E}_{t,p}(\mathbb{F}_p) \equiv 0 \mod 5$.

Orders of Reduction of Elliptic Curves

Theorem (Pajaziti, S-, 2025)

Let E_T be the elliptic curve described by

$$E_T : y^2 = x^3 - 7T\ x^2 + 96T^2\ x + 256\ T^3.$$

For any $T = t \in \mathbb{Z} \setminus \mathbb{Z}^2$ and any prime $p \neq 2, 3, 29$ with $\nu_p(t) = 0$ such that $\left(\frac{t}{p}\right) = 1$, one has $\#\widetilde{E}_{t,p}(\mathbb{F}_p) \equiv 0 \mod 5$.
There are infinitely many values $T = t$ such that

$$\#\widetilde{E}_{t,p}(\mathbb{F}_p) \equiv 0 \mod 10$$

for a set S of primes p of density at least $1/6$;

Orders of Reduction of Elliptic Curves

Theorem (Pajaziti, S-, 2025)

Let E_T be the elliptic curve described by

$$E_T : y^2 = x^3 - 7T\ x^2 + 96T^2\ x + 256\ T^3.$$

For any $T = t \in \mathbb{Z} \setminus \mathbb{Z}^2$ and any prime $p \neq 2, 3, 29$ with $\nu_p(t) = 0$ such that $\left(\frac{t}{p}\right) = 1$, one has $\#\widetilde{E}_{t,p}(\mathbb{F}_p) \equiv 0 \mod 5$.
There are infinitely many values $T = t$ such that

$$\#\widetilde{E}_{t,p}(\mathbb{F}_p) \equiv 0 \mod 10$$

for a set S of primes p of density at least $1/6$; and

$$\#\widetilde{E}_{t,p}(\mathbb{F}_p) \equiv 0 \mod 20$$

for a positive proportion of the primes in S.

Torsion Points

Torsion Points, or Exceptional Points

Torsion Points, or Exceptional Points

On Exceptional Points on Cubic Curves, G. Billing , K. Mahler, Journal of the London Mathematical Society, Volume s1–15, Issue 1, 1940, Pages 32–43

ON EXCEPTIONAL POINTS ON CUBIC CURVES

G. BILLING *and* K. MAHLER†.

Introduction.

1. Let C be a cubic curve of genus one and let P_0 be any point on it. The tangent at P_0 cuts C in a point P_1, the tangent at P_1 cuts C in a point P_2, and so on. If this construction leads to only a finite number of different points, then P_0 is called an exceptional point. Otherwise P_0 is called an ordinary point.

Torsion Points-Revisited

14. THEOREM. *There is no cubic of genus* 1 *with a group of* 11 *rational exceptional points.*

Torsion Points-Revisited

14. THEOREM. *There is no cubic of genus* 1 *with a group of* 11 *rational exceptional points.*

Proof.

The case $n = 11$.

13. LEMMA 2. *The curve*

(1) $$x_1^2 x_2 - x_1 x_2^2 - x_1 x_3^2 + x_2^2 x_3 = 0$$

has five and only five rational points (x_1, x_2, x_3), *namely*

(X) $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 0)$, *and* $(1, 1, 1)$.

Torsion Points-Revisited

G. Bergman, On the exceptional points of cubic curves, Ark. Mat. 2 (1953), 489–535.

Torsion Points-Revisited

G. Bergman, On the exceptional points of cubic curves, Ark. Mat. 2 (1953), 489–535.

In the case $\Omega = k(1)$ the following result has been obtained by LEVI [7], HURWITZ [6], NAGELL [10], [15], BILLING [1]–[4], MAHLER [9] and LIND [8]:

Theorem 1. *There exist curves (1), whose exceptional groups in $k(1)$ are of the following types: (1), (2), (3), (2, 2), (4), (5), (2, 3), (7), (4, 2), (8), (9), (2, 5), (2, 2, 3), (4, 3) and (8, 2). There does not exist any curve (1), whose exceptional group in $k(1)$ contains a sub-group of the type (11), (2, 7), (3, 5), (16), (2, 2, 5), (4, 5), (4, 2, 3) or (8, 3).*

Torsion Points-Revisited

Points of Order 13 on Elliptic Curves, B. Mazur and J. Tate, Inventiones math. 22 (1973), 41–49.

Torsion Points-Revisited

Points of Order 13 on Elliptic Curves, B. Mazur and J. Tate, Inventiones math. 22 (1973), 41–49.

1. Introduction

The main object of this note is to show that an elliptic curve defined over $\mathbb{Q}$ cannot have a rational point of order 13. Equivalently, $X_1(13)$, the curve that classifies elliptic curves with a chosen point of order 13, has no non-cuspidal points rational over $\mathbb{Q}$. This has also been announced by Blass who uses a method somewhat different from ours [1][1].

Torsion Points-Revisited

Points of Order 13 on Elliptic Curves, B. Mazur and J. Tate, Inventiones math. 22 (1973), 41–49.

1. Introduction

The main object of this note is to show that an elliptic curve defined over $\mathbb{Q}$ cannot have a rational point of order 13. Equivalently, $X_1(13)$, the curve that classifies elliptic curves with a chosen point of order 13, has no non-cuspidal points rational over $\mathbb{Q}$. This has also been announced by Blass who uses a method somewhat different from ours [1][1].

1. Blass, J.: Points of order 13 on elliptic curves. (A. M. S. Announcement)

Torsion Points-Revisited

Theorem (Mazur, 1978)

$\mathbb{T}$ is one of the following fifteen groups:

$$\mathbb{Z}/n\mathbb{Z},\ 1 \leq n \leq 12,\ n \neq 11;$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ 1 \leq n \leq 4.$$

Mordell-Weil Theorem

Theorem

For an abelian variety A over a number field K, the group $A(K)$ of K-rational points of A is a finitely-generated abelian group; so it is of the form

$$T \oplus \mathbb{Z}^r$$

where T is the torsion group and r is the rank of A.

Mordell-Weil Theorem

Theorem

For an abelian variety A over a number field K, the group $A(K)$ of K-rational points of A is a finitely-generated abelian group; so it is of the form

$$T \oplus \mathbb{Z}^r$$

where T is the torsion group and r is the rank of A.

- Kamienny, 1992, $\dim A = 1$, $[K : \mathbb{Q}] = 2 : 11, 13$ ✓

Mordell-Weil Theorem

Theorem

For an abelian variety A over a number field K, the group $A(K)$ of K-rational points of A is a finitely-generated abelian group; so it is of the form

$$T \oplus \mathbb{Z}^r$$

where T is the torsion group and r is the rank of A.

- Kamienny, 1992, $\dim A = 1$, $[K : \mathbb{Q}] = 2 :$ 11, 13 ✓
- Parent, 2003, $\dim A = 1$, $[K : \mathbb{Q}] = 3:$ 11, 13 ✓

Mordell-Weil Theorem

Theorem

For an abelian variety A over a number field K, the group $A(K)$ of K-rational points of A is a finitely-generated abelian group; so it is of the form

$$T \oplus \mathbb{Z}^r$$

where T is the torsion group and r is the rank of A.

- Kamienny, 1992, $\dim A = 1$, $[K : \mathbb{Q}] = 2$: 11, 13 ✓
- Parent, 2003, $\dim A = 1$, $[K : \mathbb{Q}] = 3$: 11, 13 ✓
- M. Derickx, S. Kamienny, W. Stein and M. Stoll, 2023, $\dim A = 1$, $[K : \mathbb{Q}] = 4, 5, 6, 7$: 11, 13 ✓

Torsion Points on Abelian Varieties

- Flynn, 1990: The Jacobian of

$$y^2 = x^6+2x^5+(2t+3)x^4+2x^3+(t^2+1)x^2+2t(1-t)x+t^2, \quad t \neq 0$$

has a $\mathbb{Q}$-rational point of order 11.

Torsion Points on Abelian Varieties

- Flynn, 1990: The Jacobian of

$$y^2 = x^6+2x^5+(2t+3)x^4+2x^3+(t^2+1)x^2+2t(1-t)x+t^2, \quad t \neq 0$$

has a $\mathbb{Q}$-rational point of order 11.

- Flynn, 1991: The Jacobian of

$$y^2 + \left(x^3 - t(x-1)^2 - x^2(x-1)\right) y = -tx^2(x-1)^3, \quad t \neq 0$$

has a $\mathbb{Q}$-rational point of order 13.

Torsion Points on Abelian Varieties

- Flynn, 1990: The Jacobian of

$$y^2 = x^6+2x^5+(2t+3)x^4+2x^3+(t^2+1)x^2+2t(1-t)x+t^2, \quad t \neq 0$$

has a $\mathbb{Q}$-rational point of order 11.

- Flynn, 1991: The Jacobian of

$$y^2 + \left(x^3 - t(x-1)^2 - x^2(x-1)\right) y = -tx^2(x-1)^3, \quad t \neq 0$$

has a $\mathbb{Q}$-rational point of order 13.

- Daowsud, 2013: There is a 1-parameter family of hyperelliptic curves of genus 3 whose Jacobian has a $\mathbb{Q}$-rational point of order 11.

Torsion Points on Abelian Varieties

$\dim A = 3$, rational point of order 13?

Continued fractions

- Every real number x has a *continued fraction* representation of the form

$$\begin{aligned} x &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \\ &= [a_0; a_1, a_2, a_3, \ldots]. \end{aligned}$$

Continued fractions

- Every real number x has a *continued fraction* representation of the form

$$\begin{aligned} x &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \\ &= [a_0; a_1, a_2, a_3, \ldots]. \end{aligned}$$

- A real number x has a *finite* continued fraction representation if and only if x is rational.

Continued fractions

- Every real number x has a *continued fraction* representation of the form

$$\begin{aligned} x &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \\ &= [a_0; a_1, a_2, a_3, \ldots]. \end{aligned}$$

- A real number x has a *finite* continued fraction representation if and only if x is rational.
- x has a **periodic** continued fraction representation if and only if x is a quadratic irrational.

Continued fractions

- Every real number x has a *continued fraction* representation of the form

$$\begin{aligned} x &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \\ &= [a_0; a_1, a_2, a_3, \ldots]. \end{aligned}$$

- A real number x has a *finite* continued fraction representation if and only if x is rational.
- x has a **periodic** continued fraction representation if and only if x is a quadratic irrational. Moreover,

$$\sqrt{N} = \left[N_0, \overline{a_1, a_2, \ldots, a_{k-2} = a_2, a_{k-1} = a_1, a_k = 2N_0}\right]$$

where $N_0 = \lfloor N \rfloor$.

Continued fractions and formal power series

Let $K = \mathbb{Q}((X^{-1}))$ be the field of formal Laurent series in X^{-1} over $\mathbb{Q}$.

Continued fractions and formal power series

Let $K = \mathbb{Q}((X^{-1}))$ be the field of formal Laurent series in X^{-1} over $\mathbb{Q}$.

Theorem (Artin, 1924)

Let n be an integer. Any formal power series

$$f(x) = \sum_{-\infty < i \leq n} b_i X^i \in \mathbb{Q}((X^{-1}))$$

can be expressed uniquely as a continued fraction

$$\begin{aligned} f(x) &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}} \\ &= [a_0; a_1, a_2, \ldots] \end{aligned}$$

where $a_i \in \mathbb{Q}[x]$ for $i \geq 0$ and $\deg a_i > 0$ for $i > 0$.

Continued fractions algorithm

- Set $f_0(x) = f(x) = \sum_{n=-m}^{\infty} b_i x^{-i}$.

Continued fractions algorithm

- Set $f_0(x) = f(x) = \sum_{n=-m}^{\infty} b_i x^{-i}$.
- Let $a_0(x) = \lfloor f(x) \rfloor$

Continued fractions algorithm

- Set $f_0(x) = f(x) = \sum_{n=-m}^{\infty} b_i x^{-i}$.
- Let $a_0(x) = \lfloor f(x) \rfloor = \sum_{n=-m}^{0} b_i x^{-i}$.

Continued fractions algorithm

- Set $f_0(x) = f(x) = \sum_{n=-m}^{\infty} b_i x^{-i}$.
- Let $a_0(x) = \lfloor f(x) \rfloor = \sum_{n=-m}^{0} b_i x^{-i}$. In other words, $a_0(x)$ is the polynomial part of $f(x)$.

Continued fractions algorithm

- Set $f_0(x) = f(x) = \sum_{n=-m}^{\infty} b_i x^{-i}$.
- Let $a_0(x) = \lfloor f(x) \rfloor = \sum_{n=-m}^{0} b_i x^{-i}$. In other words, $a_0(x)$ is the polynomial part of $f(x)$.
- Set $f_1(x) = 1/(f(x) - a_0(x))$.

Continued fractions algorithm

- Set $f_0(x) = f(x) = \sum_{n=-m}^{\infty} b_i x^{-i}$.
- Let $a_0(x) = \lfloor f(x) \rfloor = \sum_{n=-m}^{0} b_i x^{-i}$. In other words, $a_0(x)$ is the polynomial part of $f(x)$.
- Set $f_1(x) = 1/(f(x) - a_0(x))$.
- Continue in this fashion:

$$\begin{aligned} a_k(x) &= \lfloor f_k(x) \rfloor, \ k \geq 1, \\ f_{k+1}(x) &= 1/(f_k(x) - a_k(x)). \end{aligned}$$

Continued fractions algorithm

- Set $f_0(x) = f(x) = \sum_{n=-m}^{\infty} b_i x^{-i}$.
- Let $a_0(x) = \lfloor f(x) \rfloor = \sum_{n=-m}^{0} b_i x^{-i}$. In other words, $a_0(x)$ is the polynomial part of $f(x)$.
- Set $f_1(x) = 1/(f(x) - a_0(x))$.
- Continue in this fashion:

$$\begin{aligned} a_k(x) &= \lfloor f_k(x) \rfloor, \ k \geq 1, \\ f_{k+1}(x) &= 1/(f_k(x) - a_k(x)). \end{aligned}$$

- $f(x) \in \mathbb{Q}((X^{-1}))$ has a finite continued fraction representation if and only if $f(x)$ is a rational function.

Continued fractions algorithm

- Set $f_0(x) = f(x) = \sum_{n=-m}^{\infty} b_i x^{-i}$.
- Let $a_0(x) = \lfloor f(x) \rfloor = \sum_{n=-m}^{0} b_i x^{-i}$. In other words, $a_0(x)$ is the polynomial part of $f(x)$.
- Set $f_1(x) = 1/(f(x) - a_0(x))$.
- Continue in this fashion:

$$\begin{aligned} a_k(x) &= \lfloor f_k(x) \rfloor, \ k \geq 1, \\ f_{k+1}(x) &= 1/(f_k(x) - a_k(x)). \end{aligned}$$

- $f(x) \in \mathbb{Q}((X^{-1}))$ has a finite continued fraction representation if and only if $f(x)$ is a rational function. Long Division!

Continued fractions of square roots of polynomials

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. We will discuss the continued fraction representation of $\sqrt{f(x)}$.

Continued fractions of square roots of polynomials

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. We will discuss the continued fraction representation of $\sqrt{f(x)}$.
- We will assume that $f(x)$ is of even degree.

Continued fractions of square roots of polynomials

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. We will discuss the continued fraction representation of $\sqrt{f(x)}$.
- We will assume that $f(x)$ is of even degree. We also assume that the leading coefficient is a square in $\mathbb{Z}$.

Continued fractions of square roots of polynomials

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. We will discuss the continued fraction representation of $\sqrt{f(x)}$.
- We will assume that $f(x)$ is of even degree. We also assume that the leading coefficient is a square in $\mathbb{Z}$.
- If $\deg f(x) = 2$, when is the continued fraction expansion of $\sqrt{f(x)}$ periodic?

Continued fractions of square roots of polynomials

Let $f(x) = x^2 + 1$. Let's see the continued fraction algorithm implemented on $\sqrt{x^2 + 1}$.

Continued fractions of square roots of polynomials

Let $f(x) = x^2 + 1$. Let's see the continued fraction algorithm implemented on $\sqrt{x^2+1}$.

- $a_0(x) = \lfloor \sqrt{x^2+1} \rfloor = x$.

Continued fractions of square roots of polynomials

Let $f(x) = x^2 + 1$. Let's see the continued fraction algorithm implemented on $\sqrt{x^2+1}$.

- $a_0(x) = \lfloor \sqrt{x^2+1} \rfloor = x$.
- $f_1(x) = \dfrac{1}{\sqrt{x^2+1} - x} = \dfrac{\sqrt{x^2+1}+x}{x^2+1-x^2} = \sqrt{x^2+1} + x.$

Continued fractions of square roots of polynomials

Let $f(x) = x^2 + 1$. Let's see the continued fraction algorithm implemented on $\sqrt{x^2+1}$.

- $a_0(x) = \lfloor \sqrt{x^2+1} \rfloor = x$.
- $f_1(x) = \dfrac{1}{\sqrt{x^2+1} - x} = \dfrac{\sqrt{x^2+1}+x}{x^2+1-x^2} = \sqrt{x^2+1} + x$.
- $a_1(x) = \lfloor f_1(x) \rfloor = 2x$.

Continued fractions of square roots of polynomials

Let $f(x) = x^2 + 1$. Let's see the continued fraction algorithm implemented on $\sqrt{x^2+1}$.

- $a_0(x) = \lfloor \sqrt{x^2+1} \rfloor = x$.
- $f_1(x) = \dfrac{1}{\sqrt{x^2+1} - x} = \dfrac{\sqrt{x^2+1}+x}{x^2+1-x^2} = \sqrt{x^2+1} + x$.
- $a_1(x) = \lfloor f_1(x) \rfloor = 2x$.
- $f_2(x) = \dfrac{1}{f_1(x) - a_1(x)} = \dfrac{1}{\sqrt{x^2+1} - x} = \sqrt{x^2+1} + x$.

Continued fractions of square roots of polynomials

Let $f(x) = x^2 + 1$. Let's see the continued fraction algorithm implemented on $\sqrt{x^2+1}$.

- $a_0(x) = \lfloor \sqrt{x^2+1} \rfloor = x$.
- $f_1(x) = \dfrac{1}{\sqrt{x^2+1} - x} = \dfrac{\sqrt{x^2+1}+x}{x^2+1-x^2} = \sqrt{x^2+1} + x$.
- $a_1(x) = \lfloor f_1(x) \rfloor = 2x$.
- $f_2(x) = \dfrac{1}{f_1(x) - a_1(x)} = \dfrac{1}{\sqrt{x^2+1} - x} = \sqrt{x^2+1} + x$.
-

$$\begin{aligned} \sqrt{x^2+1} &= x + \cfrac{1}{2x + \cfrac{1}{2x + \ddots}} \\ &= [x; 2x, 2x, \ldots] \end{aligned}$$

Continued fractions of square roots of polynomials

Let $f(x) = x^2 + 1$. Let's see the continued fraction algorithm implemented on $\sqrt{x^2+1}$.

- $a_0(x) = \lfloor \sqrt{x^2+1} \rfloor = x$.
- $f_1(x) = \dfrac{1}{\sqrt{x^2+1} - x} = \dfrac{\sqrt{x^2+1}+x}{x^2+1-x^2} = \sqrt{x^2+1} + x$.
- $a_1(x) = \lfloor f_1(x) \rfloor = 2x$.
- $f_2(x) = \dfrac{1}{f_1(x) - a_1(x)} = \dfrac{1}{\sqrt{x^2+1} - x} = \sqrt{x^2+1} + x$.
-

$$\begin{aligned} \sqrt{x^2+1} &= x + \cfrac{1}{2x + \cfrac{1}{2x + \ddots}} \\ &= [x; 2x, 2x, \ldots] = [x; \overline{2x}]. \end{aligned}$$

Continued fractions of square roots of polynomials

Let $f(x) = x^2 + 1$. Let's see the continued fraction algorithm implemented on $\sqrt{x^2+1}$.

- $a_0(x) = \lfloor \sqrt{x^2+1} \rfloor = x$.
- $f_1(x) = \dfrac{1}{\sqrt{x^2+1} - x} = \dfrac{\sqrt{x^2+1}+x}{x^2+1-x^2} = \sqrt{x^2+1} + x$.
- $a_1(x) = \lfloor f_1(x) \rfloor = 2x$.
- $f_2(x) = \dfrac{1}{f_1(x) - a_1(x)} = \dfrac{1}{\sqrt{x^2+1} - x} = \sqrt{x^2+1} + x$.
-

$$\begin{aligned} \sqrt{x^2+1} &= x + \cfrac{1}{2x + \cfrac{1}{2x + \ddots}} \\ &= [x; 2x, 2x, \ldots] = [x; \overline{2x}]. \end{aligned}$$

- If $\deg(f(x)) = 2$, then the continued fraction expansion of $\sqrt{f(x)}$ is periodic.

Continued fractions of square roots of polynomials

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$.

Continued fractions of square roots of polynomials

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$.
- We will assume that $f(x)$ is of even degree.

Continued fractions of square roots of polynomials

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$.
- We will assume that $f(x)$ is of even degree. We also assume that the leading coefficient is a square in $\mathbb{Z}$.

Continued fractions of square roots of polynomials

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$.
- We will assume that $f(x)$ is of even degree. We also assume that the leading coefficient is a square in $\mathbb{Z}$.
- If $\deg f(x) \geq 4$, when is the continued fraction expansion of $y = \sqrt{f(x)}$ periodic?

Continued fractions of square roots of polynomials

- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$.
- We will assume that $f(x)$ is of even degree. We also assume that the leading coefficient is a square in $\mathbb{Z}$.
- If $\deg f(x) \geq 4$, when is the continued fraction expansion of $y = \sqrt{f(x)}$ periodic?
- The curve

$$y^2 = f(x)$$

has two rational points at infinity $\infty_{\pm} := (1 : \pm\sqrt{a_n} : 0)$

Continued fractions of square roots of polynomials

Theorem (Adams, Razar, 1980)

Let $C : y^2 = f(x)$ be a hyperelliptic curve described as above. The divisor $D_\infty = (\infty_+) - (\infty_-)$ is torsion if and only if the continued fraction of y is periodic.

Theorem (Adams, Razar, 1980)

Let $C : y^2 = f(x)$ be a hyperelliptic curve described as above. The divisor $D_\infty = (\infty_+) - (\infty_-)$ is torsion if and only if the continued fraction of y is periodic.

In the latter case, the following statements hold:

a) $y = [a_0; \overline{a_1, a_2, \cdots, a_{m-1}, 2\gamma a_0, a_{m-1}, \cdots, a_2, a_1, 2a_0}]$, *where* $(a_1, a_2, \cdots, a_{m-1})$ *is skew symmetric of skew value* γ^{-1}.

b) $\deg a_0 = g + 1$, *and* $1 \leq \deg a_i \leq g$ *for* $1 \leq i \leq m - 1$.

c) *The order of* D_∞ *is* $g + 1 + \sum_{i=1}^{m-1} \deg a_i$.

Theorem (Kuru, S-, 2025)

Fix an integer $g \geq 3$. Let $\alpha, \beta \geq 1, \gamma \geq 0$ be integers such that $2\alpha + 2\beta + \gamma = g + 1$. Let $a_1(x), r(x), u(x) \in \mathbb{Q}[x]$ be of degrees α, β, γ, respectively. If the affine equation

$$y^2 = r(x)^2 \left(u(x)(a_1(x)^2 r(x) + 1) + a_1(x)\right)^2 + 4\left(u(x)a_1(x)r^2(x) + r(x)\right)$$

describes a hyperelliptic curve C, then the divisor at infinity is torsion of order $g + 1 + 6\alpha + 3\beta + \gamma$.

Theorem (Kuru, S-, 2025)

Fix an integer $g \geq 3$. Let $\alpha, \beta \geq 1, \gamma \geq 0$ be integers such that $2\alpha + 2\beta + \gamma = g + 1$. Let $a_1(x), r(x), u(x) \in \mathbb{Q}[x]$ be of degrees α, β, γ, respectively. If the affine equation

$$y^2 = r(x)^2 \left(u(x)(a_1(x)^2 r(x) + 1) + a_1(x)\right)^2 + 4\left(u(x)a_1(x)r^2(x) + r(x)\right)$$

describes a hyperelliptic curve C, then the divisor at infinity is torsion of order $g + 1 + 6\alpha + 3\beta + \gamma$. In addition, if $\beta = 1$, and the Galois group of the polynomial

$$r(x)\left(u(x)(a_1(x)^2 r(x) + 1) + a_1(x)\right)^2 + 4\left(u(x)a_1(x)r(x) + 1\right)$$

is either the full symmetric group $\mathbf{S}_{2g+1}$ or the alternating group $\mathbf{A}_{2g+1}$, then the Jacobian J_C of C satisfies that $\mathrm{End}(J_C) = \mathbb{Z}$, in particular, J_C is an absolutely simple abelian variety

Torsion on Jacobian Varieties

Theorem

There exists infinitely many hyperelliptic curves of genus 3 *over* $\mathbb{Q}$ *whose Jacobians posses a rational point of order* 13.

Theorem

There exists infinitely many hyperelliptic curves of genus 3 *over* $\mathbb{Q}$ *whose Jacobians posses a rational point of order* 13.

Proof.

In

$$y^2 = r(x)^2 \left(u(x)(a_1(x)^2 r(x) + 1) + a_1(x)\right)^2 + 4\left(u(x)a_1(x)r^2(x) + r(x)\right),$$

choose $r(x) = ax + b \in \mathbb{Q}[x]$, $a \neq 0$, $u(x) = u \in \mathbb{Q} \setminus \{0\}$, and $a_1(x) = cx + d \in \mathbb{Q}[x]$, $c \neq 0$. □

What is

$$\int \frac{6x}{\sqrt{x^4 + 4x^3 - 6x^2 + 4x + 1}}\, dx?$$

What is

$$\int \frac{6x}{\sqrt{x^4+4x^3-6x^2+4x+1}}\,dx?$$

$$\int \frac{6x}{\sqrt{x^4+4x^3-6x^2+4x+1}}\,dx$$

What is

$$\int \frac{6x}{\sqrt{x^4+4x^3-6x^2+4x+1}}\,dx?$$

$$\int \frac{6x}{\sqrt{x^4+4x^3-6x^2+4x+1}}\,dx =$$

$$\log\Big[x^6 + 12x^5+45x^4+44x^3-33x^2+43+ (x^4+10x^3+30x^2+22x-11)\sqrt{x^4+4x^3-6x^2+4x+1}\Big].$$

Periodic continued fractions

Let $f(x)$ be a degree 4 polynomial with integer coefficients, no double roots, and a square leading coefficient.

Periodic continued fractions

Let $f(x)$ be a degree 4 polynomial with integer coefficients, no double roots, and a square leading coefficient.
Recall $C : y^2 = f(x)$ is an elliptic curve with two rational points ∞^+ and ∞^-.

Periodic continued fractions

Let $f(x)$ be a degree 4 polynomial with integer coefficients, no double roots, and a square leading coefficient.
Recall $C : y^2 = f(x)$ is an elliptic curve with two rational points ∞^+ and ∞^-.

Theorem (Adams, Razar, 1983)

The following statements are equivalent.

(1) $y = \sqrt{f(x)}$ *has a* **periodic** *continued fraction expansion.*

Periodic continued fractions

Let $f(x)$ be a degree 4 polynomial with integer coefficients, no double roots, and a square leading coefficient.
Recall $C : y^2 = f(x)$ is an elliptic curve with two rational points ∞^+ and ∞^-.

Theorem (Adams, Razar, 1983)

The following statements are equivalent.

(1) $y = \sqrt{f(x)}$ *has a* **periodic** *continued fraction expansion.*

(2) *The point* $(\infty^+) - (\infty^-)$ *is a torsion point in* $C(\mathbb{Q})$

Periodic continued fractions

Let $f(x)$ be a degree 4 polynomial with integer coefficients, no double roots, and a square leading coefficient.
Recall $C : y^2 = f(x)$ is an elliptic curve with two rational points ∞^+ and ∞^-.

Theorem (Adams, Razar, 1983)

The following statements are equivalent.

(1) $y = \sqrt{f(x)}$ *has a* **periodic** *continued fraction expansion.*

(2) *The point* $(\infty^+) - (\infty^-)$ *is a torsion point in* $C(\mathbb{Q})$*, i.e., a point of finite order.*

Periodic continued fractions

Let $f(x)$ be a degree 4 polynomial with integer coefficients, no double roots, and a square leading coefficient.
Recall $C : y^2 = f(x)$ is an elliptic curve with two rational points ∞^+ and ∞^-.

Theorem (Adams, Razar, 1983)

The following statements are equivalent.

(1) $y = \sqrt{f(x)}$ *has a* **periodic** *continued fraction expansion.*

(2) *The point* $(\infty^+) - (\infty^-)$ *is a torsion point in* $C(\mathbb{Q})$*, i.e., a point of finite order.*

(3) *There exist* $W(x), Z(x) \in \mathbb{Q}[x]$ *such that* $W(x)^2 - f(x)Z(x)^2 \in \mathbb{Q}^\times$ *with* $Z(x) \neq 0$.

$$\int \frac{6x}{\sqrt{x^4 + 4x^3 - 6x^2 + 4x + 1}}\, dx$$

$$\int \frac{6x}{\sqrt{x^4 + 4x^3 - 6x^2 + 4x + 1}}\, dx$$

- Set $D(x) = x^4 + 4x^3 - 6x^2 + 4x + 1$,

$$\int \frac{6x}{\sqrt{x^4+4x^3-6x^2+4x+1}}\,dx$$

- Set $D(x) = x^4+4x^3-6x^2+4x+1$, $\sqrt{D(x)}$ is periodic.

$$\int \frac{6x}{\sqrt{x^4+4x^3-6x^2+4x+1}}\,dx$$

- Set $D(x) = x^4 + 4x^3 - 6x^2 + 4x + 1$, $\sqrt{D(x)}$ is periodic. So, there is a solution to the equation $p(x)^2 - D(x)q(x)^2 \in \mathbb{Q}^\times$.

$$\int \frac{6x}{\sqrt{x^4+4x^3-6x^2+4x+1}}\,dx$$

- Set $D(x) = x^4 + 4x^3 - 6x^2 + 4x + 1$, $\sqrt{D(x)}$ is periodic. So, there is a solution to the equation $p(x)^2 - D(x)q(x)^2 \in \mathbb{Q}^\times$.
- In fact, the solution is

$$\begin{aligned} p(x) &= x^6 + 12x^5 + 45x^4 + 44x^3 - 33x^2 + 43 \\ q(x) &= x^4 + 10x^3 + 30x^2 + 22x - 11. \end{aligned}$$

$$\int \frac{6x}{\sqrt{x^4+4x^3-6x^2+4x+1}}\,dx$$

- Set $D(x) = x^4 + 4x^3 - 6x^2 + 4x + 1$, $\sqrt{D(x)}$ is periodic. So, there is a solution to the equation $p(x)^2 - D(x)q(x)^2 \in \mathbb{Q}^\times$.
- In fact, the solution is

$$\begin{aligned} p(x) &= x^6 + 12x^5 + 45x^4 + 44x^3 - 33x^2 + 43 \\ q(x) &= x^4 + 10x^3 + 30x^2 + 22x - 11. \end{aligned}$$

and nicely enough $6x = p'(x)/q(x) =: f(x)$.

$$\int \frac{6x}{\sqrt{x^4+4x^3-6x^2+4x+1}}\,dx$$

- Set $D(x) = x^4 + 4x^3 - 6x^2 + 4x + 1$, $\sqrt{D(x)}$ is periodic. So, there is a solution to the equation $p(x)^2 - D(x)q(x)^2 \in \mathbb{Q}^\times$.
- In fact, the solution is

$$\begin{aligned} p(x) &= x^6 + 12x^5 + 45x^4 + 44x^3 - 33x^2 + 43 \\ q(x) &= x^4 + 10x^3 + 30x^2 + 22x - 11. \end{aligned}$$

  and nicely enough $6x = p'(x)/q(x) =: f(x)$.

- $$\int \frac{f(x)}{\sqrt{D(x)}}dx = \log\left(p(x) + q(x)\sqrt{D(x)}\right).$$

Thank you!