Gross and Zagier's Fascinating Formula

Mike Daas

Universiteit Leiden

November 23, 2023

Elliptic Curves

Definition

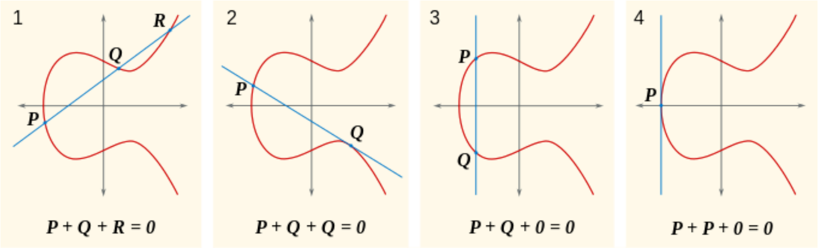
An *elliptic curve* over a field k with $\mathrm{char}(k) = 0$ is given by an equation of the form $y^2 = x^3 + ax + b$ with $a, b \in k$.

Elliptic Curves

Definition

An *elliptic curve* over a field k with $\mathrm{char}(k) = 0$ is given by an equation of the form $y^2 = x^3 + ax + b$ with $a, b \in k$.

The points of an elliptic curve form a *group*:

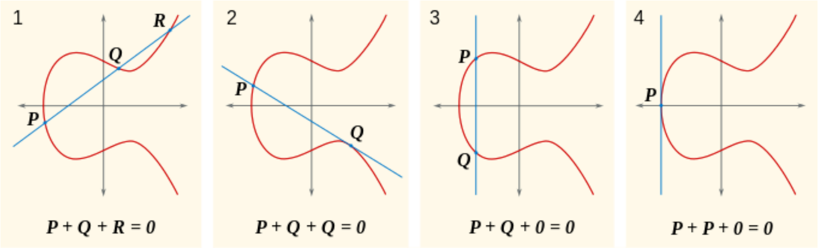


Elliptic Curves

Definition

An *elliptic curve* over a field k with $\mathrm{char}(k) = 0$ is given by an equation of the form $y^2 = x^3 + ax + b$ with $a, b \in k$.

The points of an elliptic curve form a *group*:



- Define the discriminant $\Delta = -16(4a^3 + 27b^2)$.
- An elliptic curve must be *non-singular*: $\Delta \neq 0$.

The j-invariant

Definition

The j-*invariant* of an elliptic curve $E : y^2 = x^3 + ax + b$ is defined as

$$j(E) = -1728\frac{(4a)^3}{\Delta} = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

The j-invariant

Definition

The j-*invariant* of an elliptic curve $E : y^2 = x^3 + ax + b$ is defined as

$$j(E) = -1728\frac{(4a)^3}{\Delta} = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Example

- If $E_1 : y^2 = x^3 + 1$, then $j(E_1) =$

The j-invariant

Definition

The j-*invariant* of an elliptic curve $E : y^2 = x^3 + ax + b$ is defined as

$$j(E) = -1728\frac{(4a)^3}{\Delta} = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Example

- If $E_1 : y^2 = x^3 + 1$, then $j(E_1) = 0$;
- If $E_2 : y^2 = x^3 + x$, then $j(E_2) =$

The j-invariant

Definition

The j-*invariant* of an elliptic curve $E : y^2 = x^3 + ax + b$ is defined as

$$j(E) = -1728 \frac{(4a)^3}{\Delta} = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Example

- If $E_1 : y^2 = x^3 + 1$, then $j(E_1) = 0$;
- If $E_2 : y^2 = x^3 + x$, then $j(E_2) = 1728$.

The j-invariant

Definition

The j-*invariant* of an elliptic curve $E : y^2 = x^3 + ax + b$ is defined as

$$j(E) = -1728\frac{(4a)^3}{\Delta} = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Example

- If $E_1 : y^2 = x^3 + 1$, then $j(E_1) = 0$;
- If $E_2 : y^2 = x^3 + x$, then $j(E_2) = 1728$.

Question

How can we determine whether or not E_1 and E_2 are isomorphic?

The j-invariant

Definition

The j-*invariant* of an elliptic curve $E : y^2 = x^3 + ax + b$ is defined as

$$j(E) = -1728\frac{(4a)^3}{\Delta} = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Example

- If $E_1 : y^2 = x^3 + 1$, then $j(E_1) = 0$;
- If $E_2 : y^2 = x^3 + x$, then $j(E_2) = 1728$.

Question

How can we determine whether or not E_1 and E_2 are isomorphic?

Theorem

It holds that $E_1 \cong E_2$ over $\overline{k}$ if and only if $j(E_1) = j(E_2)$.

Endomorphisms

Observation

We have infinitely many rational maps $E \to E$: namely, for $n \in \mathbb{Z}$, consider $[n] : E \to E$ sending $P \in E$ to $n \cdot P \in E$.

Endomorphisms

Observation

We have infinitely many rational maps $E \to E$: namely, for $n \in \mathbb{Z}$, consider $[n] : E \to E$ sending $P \in E$ to $n \cdot P \in E$.

Example

For $E_1 : y^2 = x^3 + 1$, the map $[2] : E \to E$ is explicitly given by

$$P = (x, y) \mapsto 2 \cdot P = \left(\frac{9x^4}{4y^2} - 2x, \frac{3x^2}{2y} \left(3x - \frac{9x^4}{4y^2} \right) - y \right).$$

Endomorphisms

Observation

We have infinitely many rational maps $E \to E$: namely, for $n \in \mathbb{Z}$, consider $[n] : E \to E$ sending $P \in E$ to $n \cdot P \in E$.

Example

For $E_1 : y^2 = x^3 + 1$, the map $[2] : E \to E$ is explicitly given by

$$P = (x, y) \mapsto 2 \cdot P = \left(\frac{9x^4}{4y^2} - 2x, \frac{3x^2}{2y} \left(3x - \frac{9x^4}{4y^2} \right) - y \right).$$

Question

Are there more such *endomorphisms* $E \to E$?

Endomorphisms

Observation

We have infinitely many rational maps $E \to E$: namely, for $n \in \mathbb{Z}$, consider $[n] : E \to E$ sending $P \in E$ to $n \cdot P \in E$.

Example

For $E_1 : y^2 = x^3 + 1$, the map $[2] : E \to E$ is explicitly given by

$$P = (x, y) \mapsto 2 \cdot P = \left(\frac{9x^4}{4y^2} - 2x, \frac{3x^2}{2y} \left(3x - \frac{9x^4}{4y^2} \right) - y \right).$$

Question

Are there more such *endomorphisms* $E \to E$?
What are all possible structures of the ring $\mathrm{End}(E)$?

Complex Multiplication

Theorem

Let E/k be an elliptic curve with $\mathrm{char}(k) = 0$. Then:

- Either $\mathrm{End}(E) = \mathbb{Z}$;
- Or $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic number field. We say that E *has CM*.

Complex Multiplication

Theorem

Let E/k be an elliptic curve with $\mathrm{char}(k) = 0$. Then:

- Either $\mathrm{End}(E) = \mathbb{Z}$;
- Or $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic number field. We say that E *has CM*.

Example 1

For $E_1 : y^2 = x^3 + 1$, we have a map $[\zeta_3] : E \to E$ given by

$$P = (x, y) \mapsto (\zeta_3 x, y) \implies \mathrm{End}(E) \cong \mathbb{Z}[\zeta_3].$$

Complex Multiplication

Theorem

Let E/k be an elliptic curve with $\text{char}(k) = 0$. Then:

- Either $\text{End}(E) = \mathbb{Z}$;
- Or $\text{End}(E)$ is isomorphic to an order in an imaginary quadratic number field. We say that E *has CM*.

Example 1

For $E_1 : y^2 = x^3 + 1$, we have a map $[\zeta_3] : E \to E$ given by

$$P = (x, y) \mapsto (\zeta_3 x, y) \implies \text{End}(E) \cong \mathbb{Z}[\zeta_3].$$

Example 2

For $E_1 : y^2 = x^3 + x$, we have a map $[i] : E \to E$ given by

$$P = (x, y) \mapsto (-x, iy) \implies \text{End}(E) \cong \mathbb{Z}[i].$$

Gross and Zagier's discovery (1/2)

Most curves do *not* have CM. Examples:

$$E_3 : y^2 = x^3 - 2835x - 71442 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right];$$

$$E_4 : y^2 = x^3 - 9504x + 365904 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right];$$

$$E_5 : y^2 = x^3 - 608x + 5776 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right].$$

Gross and Zagier's discovery (1/2)

Most curves do *not* have CM. Examples:

$$E_3 : y^2 = x^3 - 2835x - 71442 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right];$$

$$E_4 : y^2 = x^3 - 9504x + 365904 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right];$$

$$E_5 : y^2 = x^3 - 608x + 5776 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right].$$

We compute that

$$j(E_3) = -3^3 5^3, \quad j(E_4) = -2^{15}, \quad \text{and} \quad j(E_5) = -2^{15} 3^3.$$

Gross and Zagier's discovery (1/2)

Most curves do *not* have CM. Examples:

$$E_3 : y^2 = x^3 - 2835x - 71442 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right];$$

$$E_4 : y^2 = x^3 - 9504x + 365904 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right];$$

$$E_5 : y^2 = x^3 - 608x + 5776 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right].$$

We compute that

$$j(E_3) = -3^3 5^3, \quad j(E_4) = -2^{15}, \quad \text{and} \quad j(E_5) = -2^{15} 3^3.$$

However, the following is striking:

$$j(E_3) - j(E_4) = 7 \cdot 13 \cdot 17 \cdot 19;$$
$$j(E_3) - j(E_5) = 3^7 \cdot 13 \cdot 31;$$
$$j(E_4) - j(E_5) = 2^{16} \cdot 13.$$

Gross and Zagier's discovery (2/2)

More examples:

$$E_6 : y^2 = x^3 - 13760x + 621264 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right];$$

$$E_7 : y^2 = x^3 - 117920x + 15585808 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right];$$

$$E_8 : y^2 = x^3 - 34790720x + 78984748304 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right].$$

Gross and Zagier's discovery (2/2)

More examples:

$$E_6 : y^2 = x^3 - 13760x + 621264 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right];$$

$$E_7 : y^2 = x^3 - 117920x + 15585808 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right];$$

$$E_8 : y^2 = x^3 - 34790720x + 78984748304 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right].$$

We compute that

$$j(E_6) = -2^{18}3^3 5^3, \quad j(E_7) = -2^{15}3^3 5^3 11^3, \text{ and } j(E_8) = -2^{18}3^3 5^3 23^3 29^3.$$

Gross and Zagier's discovery (2/2)

More examples:

$$E_6 : y^2 = x^3 - 13760x + 621264 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right];$$

$$E_7 : y^2 = x^3 - 117920x + 15585808 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right];$$

$$E_8 : y^2 = x^3 - 34790720x + 78984748304 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right].$$

We compute that

$$j(E_6) = -2^{18}3^3 5^3, \quad j(E_7) = -2^{15}3^3 5^3 11^3, \text{ and } j(E_8) = -2^{18}3^3 5^3 23^3 29^3.$$

The following is even more striking:

$$j(E_6) - j(E_7) = 2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2;$$
$$j(E_6) - j(E_8) = 2^{19} \cdot 3^6 \cdot 5^3 \cdot 7^3 \cdot 37 \cdot 433;$$
$$j(E_7) - j(E_8) = 2^{15} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 139 \cdot 331.$$

An unexpected connection

Recall the curves

$$E_3 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \text{ and } j(E_3) = -3^3 5^3;$$

$$E_4 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right] \text{ and } j(E_4) = -2^{15};$$

$$E_5 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \text{ and } j(E_5) = -2^{15} 3^3.$$

An unexpected connection

Recall the curves

$$E_3 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \text{ and } j(E_3) = -3^3 5^3;$$

$$E_4 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right] \text{ and } j(E_4) = -2^{15};$$

$$E_5 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \text{ and } j(E_5) = -2^{15}3^3.$$

Recall that $j(E_3) - j(E_4) = 7 \cdot 13 \cdot 17 \cdot 19$. Let $D = 7 \cdot 11$.

An unexpected connection

Recall the curves

$$E_3 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \text{ and } j(E_3) = -3^3 5^3;$$

$$E_4 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right] \text{ and } j(E_4) = -2^{15};$$

$$E_5 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \text{ and } j(E_5) = -2^{15} 3^3.$$

Recall that $j(E_3) - j(E_4) = 7 \cdot 13 \cdot 17 \cdot 19$. Let $D = 7 \cdot 11$.

x	± 1	± 3	± 5	± 7
$(D - x^2)/4$	19	17	13	7

An unexpected connection

Recall the curves

$$E_3 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \text{ and } j(E_3) = -3^3 5^3;$$

$$E_4 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right] \text{ and } j(E_4) = -2^{15};$$

$$E_5 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \text{ and } j(E_5) = -2^{15} 3^3.$$

Recall that $j(E_3) - j(E_4) = 7 \cdot 13 \cdot 17 \cdot 19$. Let $D = 7 \cdot 11$.

x	± 1	± 3	± 5	± 7
$(D - x^2)/4$	19	17	13	7

Recall that $j(E_3) - j(E_5) = 3^7 \cdot 13 \cdot 31$. Let $D = 7 \cdot 19$.

An unexpected connection

Recall the curves

$$E_3 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \text{ and } j(E_3) = -3^3 5^3;$$

$$E_4 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right] \text{ and } j(E_4) = -2^{15};$$

$$E_5 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \text{ and } j(E_5) = -2^{15} 3^3.$$

Recall that $j(E_3) - j(E_4) = 7 \cdot 13 \cdot 17 \cdot 19$. Let $D = 7 \cdot 11$.

x	± 1	± 3	± 5	± 7
$(D - x^2)/4$	19	17	13	7

Recall that $j(E_3) - j(E_5) = 3^7 \cdot 13 \cdot 31$. Let $D = 7 \cdot 19$.

x	± 1	± 3	± 5	± 7	± 9	± 11
$(D - x^2)/4$	$3 \cdot 11$	31	3^3	$3 \cdot 7$	13	3

Three colours of primes

Suppose we have E_1 and E_2 with CM by $\mathbb{Z}\left[\frac{1+\sqrt{D_1}}{2}\right]$ and $\mathbb{Z}\left[\frac{1+\sqrt{D_2}}{2}\right]$.

Three colours of primes

Suppose we have E_1 and E_2 with CM by $\mathbb{Z}\left[\frac{1+\sqrt{D_1}}{2}\right]$ and $\mathbb{Z}\left[\frac{1+\sqrt{D_2}}{2}\right]$.
Many things can happen to primes in larger orders. For example:

$$(2) = (1+i)^2 \in \mathbb{Z}[i], \quad 3 \in \mathbb{Z}[i] \text{ is prime, and } 5 = (2+i)(2-i) \in \mathbb{Z}[i].$$

Three colours of primes

Suppose we have E_1 and E_2 with CM by $\mathbb{Z}\left[\frac{1+\sqrt{D_1}}{2}\right]$ and $\mathbb{Z}\left[\frac{1+\sqrt{D_2}}{2}\right]$.
Many things can happen to primes in larger orders. For example:

$$(2) = (1+i)^2 \in \mathbb{Z}[i], \quad 3 \in \mathbb{Z}[i] \text{ is prime, and } 5 = (2+i)(2-i) \in \mathbb{Z}[i].$$

Let $D = D_1 D_2$. Three types of primes dividing $(D - x^2)/4 > 0$:

- Blue primes: primes that are no longer prime in both $\mathbb{Z}\left[\frac{1+\sqrt{D_i}}{2}\right]$;

Three colours of primes

Suppose we have E_1 and E_2 with CM by $\mathbb{Z}\left[\frac{1+\sqrt{D_1}}{2}\right]$ and $\mathbb{Z}\left[\frac{1+\sqrt{D_2}}{2}\right]$. Many things can happen to primes in larger orders. For example:

$$(2) = (1+i)^2 \in \mathbb{Z}[i], \quad 3 \in \mathbb{Z}[i] \text{ is prime, and } 5 = (2+i)(2-i) \in \mathbb{Z}[i].$$

Let $D = D_1 D_2$. Three types of primes dividing $(D - x^2)/4 > 0$:

- Blue primes: primes that are no longer prime in both $\mathbb{Z}\left[\frac{1+\sqrt{D_i}}{2}\right]$;
- Green primes: primes that stay prime with even exponent;

Three colours of primes

Suppose we have E_1 and E_2 with CM by $\mathbb{Z}\left[\frac{1+\sqrt{D_1}}{2}\right]$ and $\mathbb{Z}\left[\frac{1+\sqrt{D_2}}{2}\right]$. Many things can happen to primes in larger orders. For example:

$$(2) = (1+i)^2 \in \mathbb{Z}[i], \quad 3 \in \mathbb{Z}[i] \text{ is prime, and } 5 = (2+i)(2-i) \in \mathbb{Z}[i].$$

Let $D = D_1 D_2$. Three types of primes dividing $(D - x^2)/4 > 0$:

- Blue primes: primes that are no longer prime in both $\mathbb{Z}\left[\frac{1+\sqrt{D_i}}{2}\right]$;
- Green primes: primes that stay prime with even exponent;
- Red primes: primes that stay prime with odd exponent.

Three colours of primes

Suppose we have E_1 and E_2 with CM by $\mathbb{Z}\left[\frac{1+\sqrt{D_1}}{2}\right]$ and $\mathbb{Z}\left[\frac{1+\sqrt{D_2}}{2}\right]$. Many things can happen to primes in larger orders. For example:

$$(2) = (1+i)^2 \in \mathbb{Z}[i], \quad 3 \in \mathbb{Z}[i] \text{ is prime, and } 5 = (2+i)(2-i) \in \mathbb{Z}[i].$$

Let $D = D_1 D_2$. Three types of primes dividing $(D - x^2)/4 > 0$:

- Blue primes: primes that are no longer prime in both $\mathbb{Z}\left[\frac{1+\sqrt{D_i}}{2}\right]$;
- Green primes: primes that stay prime with even exponent;
- Red primes: primes that stay prime with odd exponent.

Example: let $D_1 = -7$ and $D_2 = -43$. Then:

x	± 1	± 3	± 5	± 7	± 9	± 11	± 13	± 15	± 17
$\frac{D-x^2}{4}$	$3 \cdot 5^2$	73	$3 \cdot 23$	$3^2 \cdot 7$	$5 \cdot 11$	$3^2 \cdot 5$	$3 \cdot 11$	19	3

The Fascinating Formula

Recipe

- For each integer $(D - x^2)/4 > 0$, colour its primes.

The Fascinating Formula

Recipe

- For each integer $(D - x^2)/4 > 0$, colour its primes.
- If there is *not* exactly 1 red prime p, skip.

The Fascinating Formula

Recipe

- For each integer $(D - x^2)/4 > 0$, colour its primes.
- If there is *not* exactly 1 red prime p, skip.
- Otherwise, add 1 to its exponent and those of all blue primes.

The Fascinating Formula

Recipe

- For each integer $(D - x^2)/4 > 0$, colour its primes.
- If there is *not* exactly 1 red prime p, skip.
- Otherwise, add 1 to its exponent and those of all blue primes.
- Multiply these numbers together to get k; then obtain $p^{k/2}$.

The Fascinating Formula

Recipe

- For each integer $(D - x^2)/4 > 0$, colour its primes.
- If there is *not* exactly 1 red prime p, skip.
- Otherwise, add 1 to its exponent and those of all blue primes.
- Multiply these numbers together to get k; then obtain $p^{k/2}$.

Example: let $D_1 = -7$ and $D_2 = -43$. Then:

x	± 1	± 3	± 5	± 7	± 9	± 11	± 13	± 15	± 17
$\frac{D-x^2}{4}$	$3 \cdot 5^2$	73	$3 \cdot 23$	$3^2 \cdot 7$	$5 \cdot 11$	$3^2 \cdot 5$	$3 \cdot 11$	19	3
$p^{k/2}$	3	73	3^2	7	5^2	5	3^2	19	3

The Fascinating Formula

Recipe

- For each integer $(D - x^2)/4 > 0$, colour its primes.
- If there is *not* exactly 1 red prime p, skip.
- Otherwise, add 1 to its exponent and those of all blue primes.
- Multiply these numbers together to get k; then obtain $p^{k/2}$.

Example: let $D_1 = -7$ and $D_2 = -43$. Then:

x	± 1	± 3	± 5	± 7	± 9	± 11	± 13	± 15	± 17
$\frac{D-x^2}{4}$	$3 \cdot 5^2$	73	$3 \cdot 23$	$3^2 \cdot 7$	$5 \cdot 11$	$3^2 \cdot 5$	$3 \cdot 11$	19	3
$p^{k/2}$	3	73	3^2	7	5^2	5	3^2	19	3

Final step: multiplying all these $p^{k/2}$ together gives the right answer!

Example

x	± 1	± 3	± 5	± 7	± 9	± 11	± 13	± 15	± 17
$\frac{D-x^2}{4}$	$3 \cdot 5^2$	73	$3 \cdot 23$	$3^2 \cdot 7$	$5 \cdot 11$	$3^2 \cdot 5$	$3 \cdot 11$	19	3
$p^{k/2}$	3	73	3^2	7	5^2	5	3^2	19	3

Recall the curves

$$E_3 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \text{ and } j(E_3) = -3^3 5^3;$$

$$E_6 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right] \text{ and } j(E_6) = -2^{18} 3^3 5^3.$$

Example

x	± 1	± 3	± 5	± 7	± 9	± 11	± 13	± 15	± 17
$\frac{D-x^2}{4}$	$3 \cdot 5^2$	73	$3 \cdot 23$	$3^2 \cdot 7$	$5 \cdot 11$	$3^2 \cdot 5$	$3 \cdot 11$	19	3
$p^{k/2}$	3	73	3^2	7	5^2	5	3^2	19	3

Recall the curves

$$E_3 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \text{ and } j(E_3) = -3^3 5^3;$$

$$E_6 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right] \text{ and } j(E_6) = -2^{18} 3^3 5^3.$$

Then indeed,

$$j(E_3) - j(E_6) = 2^{18} 3^3 5^3 - 3^3 5^3 = 884732625$$

Example

x	± 1	± 3	± 5	± 7	± 9	± 11	± 13	± 15	± 17
$\frac{D-x^2}{4}$	$3 \cdot 5^2$	73	$3 \cdot 23$	$3^2 \cdot 7$	$5 \cdot 11$	$3^2 \cdot 5$	$3 \cdot 11$	19	3
$p^{k/2}$	3	73	3^2	7	5^2	5	3^2	19	3

Recall the curves

$$E_3 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \text{ and } j(E_3) = -3^3 5^3;$$

$$E_6 \text{ with CM by } \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right] \text{ and } j(E_6) = -2^{18} 3^3 5^3.$$

Then indeed,

$$j(E_3) - j(E_6) = 2^{18}3^3 5^3 - 3^3 5^3 = 884732625 = 3^6 \cdot 5^3 \cdot 7 \cdot 19 \cdot 73.$$

More generally, when $j(E) \notin \mathbb{Z}$ but in a bigger number field, then it still holds for the *absolute norm* of the difference between j-values.

What is the j-function really?

Theorem

The $\mathbb{C}$-points of an elliptic curve are given by $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ for some $\tau \in \mathcal{H}$. Now CM-curves correspond to actual CM-points:

$$\tau \in \{i, \sqrt{-3}, (1 + \sqrt{-7})/2, \ldots\}.$$

What is the j-function really?

Theorem

The $\mathbb{C}$-points of an elliptic curve are given by $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ for some $\tau \in \mathcal{H}$. Now CM-curves correspond to actual CM-points:

$$\tau \in \{i, \sqrt{-3}, (1 + \sqrt{-7})/2, \ldots\}.$$

So instead of $j(E)$, we can consider $j : \mathcal{H} \to \mathbb{C}$ and study $j(\tau)$.

What is the j-function really?

Theorem

The $\mathbb{C}$-points of an elliptic curve are given by $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ for some $\tau \in \mathcal{H}$. Now CM-curves correspond to actual CM-points:

$$\tau \in \{i, \sqrt{-3}, (1 + \sqrt{-7})/2, \ldots\}.$$

So instead of $j(E)$, we can consider $j : \mathcal{H} \to \mathbb{C}$ and study $j(\tau)$. Changing the basis of a lattice gives the same elliptic curve. This means that even

$$j : \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H} \to \mathbb{C}$$

where $\mathrm{SL}_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid \det(A) = 1\}$ acts on $\mathcal{H}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

What is the j-function really?

Theorem

The $\mathbb{C}$-points of an elliptic curve are given by $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ for some $\tau \in \mathcal{H}$. Now CM-curves correspond to actual CM-points:

$$\tau \in \{i, \sqrt{-3}, (1 + \sqrt{-7})/2, \ldots\}.$$

So instead of $j(E)$, we can consider $j : \mathcal{H} \to \mathbb{C}$ and study $j(\tau)$. Changing the basis of a lattice gives the same elliptic curve. This means that even

$$j : SL_2(\mathbb{Z}) \setminus \mathcal{H} \to \mathbb{C}$$

where $SL_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid \det(A) = 1\}$ acts on $\mathcal{H}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

The quotient $SL_2(\mathbb{Z}) \setminus \mathcal{H}$ is called a *modular curve*.

Shimura curves

How did we obtain the modular curve $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$?

Shimura curves

How did we obtain the modular curve $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$?

- Start with matrix algebra $M_2(\mathbb{Q})$;
- Take a maximal order inside it: $M_2(\mathbb{Z})$;
- Take the subgroup of units of norm 1: $\mathrm{SL}_2(\mathbb{Z})$.

Shimura curves

How did we obtain the modular curve $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$?

- Start with matrix algebra $M_2(\mathbb{Q})$;
- Take a maximal order inside it: $M_2(\mathbb{Z})$;
- Take the subgroup of units of norm 1: $\mathrm{SL}_2(\mathbb{Z})$.

Let B denote an indefinite quaternion algebra. Let $R \subset B$ be a maximal order and let $R_1^\times$ be the subgroup of units of norm 1. Define

$$X_B(\mathbb{C}) = R_1^\times \setminus \mathcal{H};$$

this is known as a Shimura curve.

Shimura curves

How did we obtain the modular curve $SL_2(\mathbb{Z}) \backslash \mathcal{H}$?

- Start with matrix algebra $M_2(\mathbb{Q})$;
- Take a maximal order inside it: $M_2(\mathbb{Z})$;
- Take the subgroup of units of norm 1: $SL_2(\mathbb{Z})$.

Let B denote an indefinite quaternion algebra. Let $R \subset B$ be a maximal order and let $R_1^\times$ be the subgroup of units of norm 1. Define

$$X_B(\mathbb{C}) = R_1^\times \backslash \mathcal{H};$$

this is known as a Shimura curve. Sometimes, there exists a generator J of the function field. This choice is not unique, but the *cross-ratio* is:

$$\frac{J(x) - J(z)}{J(x) - J(w)} \frac{J(y) - J(z)}{J(y) - J(w)}.$$

My research

Theorem, D. (2023)

For *CM-points* τ_1, τ_1', τ_2, τ_2', the algebraic norm of the cross-ratio

$$\frac{J(\tau_1) - J(\tau_2)}{J(\tau_1) - J(\tau_2')} \frac{J(\tau_1') - J(\tau_2)}{J(\tau_1') - J(\tau_2')}$$

obeys a similarly fascinating formula.

My research

Theorem, D. (2023)

For *CM-points* $\tau_1, \tau_1', \tau_2, \tau_2'$, the algebraic norm of the cross-ratio

$$\frac{J(\tau_1) - J(\tau_2)}{J(\tau_1) - J(\tau_2')} \frac{J(\tau_1') - J(\tau_2)}{J(\tau_1') - J(\tau_2')}$$

obeys a similarly fascinating formula.

Main ideas of proof:

- Relate the above to a p-adic quantity involving Θ-functions.

My research

Theorem, D. (2023)

For *CM-points* $\tau_1, \tau_1', \tau_2, \tau_2'$, the algebraic norm of the cross-ratio

$$\frac{J(\tau_1) - J(\tau_2)}{J(\tau_1) - J(\tau_2')} \frac{J(\tau_1') - J(\tau_2)}{J(\tau_1') - J(\tau_2')}$$

obeys a similarly fascinating formula.

Main ideas of proof:

- Relate the above to a p-adic quantity involving Θ-functions.
- Compute the derivative of a family of p-adic Hilbert mod. forms.

My research

Theorem, D. (2023)

For *CM-points* $\tau_1, \tau_1', \tau_2, \tau_2'$, the algebraic norm of the cross-ratio

$$\frac{J(\tau_1) - J(\tau_2)}{J(\tau_1) - J(\tau_2')} \frac{J(\tau_1') - J(\tau_2)}{J(\tau_1') - J(\tau_2')}$$

obeys a similarly fascinating formula.

Main ideas of proof:

- Relate the above to a p-adic quantity involving Θ-functions.
- Compute the derivative of a family of p-adic Hilbert mod. forms.
- Splits into two parts: the cross-ratio and the fascinating formula.

My research

Theorem, D. (2023)

For *CM-points* $\tau_1, \tau_1', \tau_2, \tau_2'$, the algebraic norm of the cross-ratio

$$\frac{J(\tau_1) - J(\tau_2)}{J(\tau_1) - J(\tau_2')} \frac{J(\tau_1') - J(\tau_2)}{J(\tau_1') - J(\tau_2')}$$

obeys a similarly fascinating formula.

Main ideas of proof:

- Relate the above to a p-adic quantity involving Θ-functions.
- Compute the derivative of a family of p-adic Hilbert mod. forms.
- Splits into two parts: the cross-ratio and the fascinating formula.
- For abstract reasons this gives zero so these parts must be equal.

My research

Theorem, D. (2023)

For *CM-points* $\tau_1, \tau_1', \tau_2, \tau_2'$, the algebraic norm of the cross-ratio

$$\frac{J(\tau_1) - J(\tau_2)}{J(\tau_1) - J(\tau_2')} \frac{J(\tau_1') - J(\tau_2)}{J(\tau_1') - J(\tau_2')}$$

obeys a similarly fascinating formula.

Main ideas of proof:

- Relate the above to a p-adic quantity involving Θ-functions.
- Compute the derivative of a family of p-adic Hilbert mod. forms.
- Splits into two parts: the cross-ratio and the fascinating formula.
- For abstract reasons this gives zero so these parts must be equal.
- Compute family by deforming its associated Galois representation infinitesimally ($\epsilon^2 = 0$) and prove an $R = T$-theorem.

My research

Theorem, D. (2023)

For *CM-points* $\tau_1, \tau_1', \tau_2, \tau_2'$, the algebraic norm of the cross-ratio

$$\frac{J(\tau_1) - J(\tau_2)}{J(\tau_1) - J(\tau_2')} \frac{J(\tau_1') - J(\tau_2)}{J(\tau_1') - J(\tau_2')}$$

obeys a similarly fascinating formula.

Main ideas of proof:

- Relate the above to a p-adic quantity involving Θ-functions.
- Compute the derivative of a family of p-adic Hilbert mod. forms.
- Splits into two parts: the cross-ratio and the fascinating formula.
- For abstract reasons this gives zero so these parts must be equal.
- Compute family by deforming its associated Galois representation infinitesimally ($\epsilon^2 = 0$) and prove an $R = T$-theorem.

Thank you for your attention!