Gross lattices of supersingular elliptic curves

Algebra and Number Theory Seminar

Gaurish Korpal

University of Arizona

March 25, 2025

Elliptic curves over finite field

Let E be an elliptic curve over finite field $\mathbb{F}_q$ where $q = p^n$ with prime $p > 3$ and $n > 0$.

- $E : y^2 = x^3 + ax + b$ where $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$, along with an extra point 0_E. Points on E form a group with 0_E as the neutral element.
- An $\mathbb{F}_q$-isogeny between $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ is a non-constant rational function $\varphi : E \to E'$ that is compatible with the group law. If φ is a one-to-one polynomial map then it is called $\mathbb{F}_q$-isomorphism.
- The j-invariant $j(E) = 1728\frac{4a^3}{(4a^3+27b^2)}$ identifies isomorphism classes over $\overline{\mathbb{F}}_p$.
- The $\mathbb{F}_q$-endomorphism ring of E, $\mathrm{End}_{\mathbb{F}_q}(E)$, is the set of $\mathbb{F}_q$-isogenies from E to itself, together with the zero map $[0] : E \to E$ given $[0](P) = 0_E$.
- $\#E(\mathbb{F}_q) = q + 1 - \mathrm{tr}(\pi_q)$, where π_q is Frobenius endomorphism $\pi_q(x, y) = (x^q, y^q)$ with $|\mathrm{tr}(\pi_q)| \leq 2\sqrt{q}$. In fact, an $\mathbb{F}_q$-isogeny $\varphi : E \to E'$ exists iff $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.

Supersingular elliptic curves

$\mathrm{End}^0_{\mathbb{F}_q}(E) := \mathrm{End}_{\mathbb{F}_q}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is called endomorphism algebra of E.

- $\mathrm{End}^0_{\mathbb{F}_q}(E)$ is either an imaginary quadratic field $\mathbb{Q}(\sqrt{-\Delta})$ and such a curve is referred to as ordinary elliptic curve, or a definite quaternion $\mathbb{Q}$-algebra B_p ramified at p and ∞ and such a curve is referred to as supersingular elliptic curve.
- If E is supersingular then $j(E) \in \mathbb{F}_{p^2}$ and hence the number of $\overline{\mathbb{F}}_p$-isomorphism classes of such curves is finite and is given by $S_p := \left\lfloor \frac{p}{12} \right\rfloor + \epsilon$ where $\epsilon \in \{0, 1, 2\}$.
- $E/\mathbb{F}_q$ is supersingular iff $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ is isomorphic to a maximal order in B_p.

$$\left\{ \begin{array}{l} \text{isomorphism classes} \\ \text{of supersingular} \\ \text{elliptic curves over } \overline{\mathbb{F}}_p \end{array} \right\} \Big/ \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \longleftrightarrow \left\{ \begin{array}{l} \text{maximal orders} \\ \text{of } B_p \end{array} \right\} /\cong$$

one-to-one correspondence if $j(E) \in \mathbb{F}_p$ & two-to-one correspondence if $j(E) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

Definite quaternion algebras

A quaternion $\mathbb{Q}$-algebra is of the form $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{ij}$, where $\mathbf{i}^2, \mathbf{j}^2 \in \mathbb{Q}^\times$, and $\mathbf{ij} = -\mathbf{ji}$.

Let B_p be a definite quaternion $\mathbb{Q}$-algebra ramified at p and ∞.

$$B_p = \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle := \begin{cases} \mathbf{i}^2 = -1, \mathbf{j}^2 = -1 & \text{if } p = 2 \\ \mathbf{i}^2 = -\ell, \mathbf{j}^2 = -p & \text{if } p \equiv 1 \pmod 4 \\ \mathbf{i}^2 = -1, \mathbf{j}^2 = -p & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

where $\ell \equiv 3 \pmod 4$ is a prime such that $\left(\frac{p}{\ell}\right) = -1$

Maximal quaternion orders

$O \subseteq \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ is called an order if O is a ring whose elements are integral, $\mathbb{Z} \subseteq O$, and contains a basis for $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ as $\mathbb{Q}$-vector space.
An order $O \subsetneq \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ is called maximal if it is not properly contained in another order.

For B_p we know the following explicit examples of maximal orders

$$O = \begin{cases} \mathbb{Z}\left\langle 1, \mathbf{i}, \mathbf{j}, \frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} \right\rangle & \text{if } p = 2 \\ \mathbb{Z}\left\langle 1, \frac{1+\mathbf{i}}{2}, \frac{\mathbf{j}+\mathbf{k}}{2}, \frac{r\mathbf{i}+\mathbf{k}}{\ell} \right\rangle & \text{if } p \equiv 1 \pmod 4 \\ \mathbb{Z}\left\langle 1, \mathbf{i}, \frac{1+\mathbf{j}}{2}, \frac{\mathbf{i}+\mathbf{k}}{2} \right\rangle & \text{if } p = 3 \pmod 4 \end{cases}$$

where $r^2 + p \equiv 0 \pmod{\ell}$.

Difficult and easy problems

Theoretically, it is possible to translate a problem about supersingular curves to a problem about maximal orders in quaternion algebra, and vice versa.

Difficult

Given a supersingular j-invariant, find a maximal quaternion order $O \subsetneq B_p$ such that $O \cong \mathrm{End}_{\overline{\mathbb{F}}_p}(E(j))$.

Easy

Given a maximal quaternion order $O \subsetneq B_p$, find a supersingular j-invariant such that $O \cong \mathrm{End}_{\overline{\mathbb{F}}_p}(E(j))$.

Not so difficult problem when $j \in \mathbb{F}_p$

World of curves

1. If $j \in \mathbb{F}_p$ then $\pi_p^2 - \mathrm{tr}(\pi_p)\pi_p + p = 0$ in $\mathrm{End}_{\overline{\mathbb{F}}_p}(E(j))$.
2. Since $E(j)$ is supersingular, $\mathrm{tr}(\pi_p) = 0$ and hence $\pi_p^2 + p = 0$.
3. Supersingular $E(j)$ is CM by the imaginary quadratic order $\mathbb{Z}[\sqrt{-p}]$ in the field $\mathbb{Q}(\sqrt{-p})$.

World of quaternions

1. ℓ be a prime such that $\left(\frac{p}{\ell}\right) = -1$ and $\ell \equiv 3 \pmod 8$.
2. $\left(\frac{-p}{\ell}\right) = 1$ implies there exists r such that $r^2 + p \equiv 0 \pmod \ell$.
3. If $p \equiv 3 \pmod 4$, then there exists r' such that $r'^2 + p \equiv 0 \pmod{4\ell}$.

A solution to the difficult problem when $j \in \mathbb{F}_p$

Let $B_p = \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ with $\mathbf{i}^2 = -\ell$ and $\mathbf{j}^2 = -p$.

$$\mathrm{End}_{\overline{\mathbb{F}}_p}(E(j)) \cong \begin{cases} O(\ell) \coloneqq \mathbb{Z}\left\langle 1, \frac{1+\mathbf{i}}{2}, \frac{\mathbf{j}+\mathbf{k}}{2}, \frac{r\mathbf{i}+\mathbf{k}}{\ell} \right\rangle & \text{if } \frac{1+\pi_p}{2} \notin \mathrm{End}_{\overline{\mathbb{F}}_p}(E(j)) \\ O'(\ell) \coloneqq \mathbb{Z}\left\langle 1, \mathbf{i}, \frac{1+\mathbf{j}}{2}, \frac{r'\mathbf{i}+\mathbf{k}}{2\ell} \right\rangle & \text{if } \frac{1+\pi_p}{2} \in \mathrm{End}_{\overline{\mathbb{F}}_p}(E(j)) \end{cases}$$

$p \equiv 1 \mod 4$

There are $\frac{h(-4p)}{2}$ supersingular j-invariants where $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$ and $\mathrm{End}_{\overline{\mathbb{F}}_p}(E) \cong O(\ell)$.

$p \equiv 3 \mod 4$ and $j \neq 1728$

- $\frac{h(-4p)-1}{2}$ supersingular j-invariants where $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$ and $\mathrm{End}_{\overline{\mathbb{F}}_p}(E) \cong O(\ell)$.
- $\frac{h(-p)-1}{2}$ supersingular j-invariants where $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ and $\mathrm{End}_{\overline{\mathbb{F}}_p}(E) \cong O'(\ell)$.

Successive minima

The quaternion algebra $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ is equipped with an inner product $(x, y) = \frac{1}{2}\,\mathrm{trd}(x\overline{y})$ and norm $\|x\|^2 = (x, x) = \mathrm{nrd}(x)$.

For Λ a free $\mathbb{Z}$-module (or a lattice) in $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ of rank n and $1 \leq i \leq n$, the *i*th successive minimum of Λ is the smallest value D_i such that the rank of the $\mathbb{Z}$-submodule of Λ generated by $\{x \in \Lambda : \|x\|^2 \leq D_i\}$ is greater than or equal to i. An ordered list of elements $x_1, \ldots, x_n \in \Lambda$ attains the successive minima of Λ if $\|x_i\|^2 = D_i$.

Lemma

A lattice Λ of rank at most 3 always has a basis that attains its successive minima, we call this ordered basis a successive minimal basis of Λ.

Gram matrix

A lattice in $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ with a $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\}$ is denoted by $\langle b_1, \ldots, b_n \rangle$.

Let Λ be a rank-n lattice in $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ with a basis $\{b_1, b_2, \ldots, b_n\}$. The Gram matrix for this basis is the symmetric matrix $G_\Lambda = ((b_i, b_j))_{i,j} = (\frac{1}{2}\operatorname{trd}(b_i \bar{b}_j))_{i,j}$, and the determinant of Λ, denoted by $\det(\Lambda) := \det(G_\Lambda)$, is the square of the volume of Λ.

Lemma

There is a minimal constant γ_n (called the n-th Hermite constant) such that

$$\det(\Lambda) \leq \prod_{i=1}^{n} D_i \leq \gamma_n^n \det(\Lambda)$$

Moreover, $\gamma_2^2 = \frac{4}{3}$ and $\gamma_3^3 = 2$.

Size reduction

Given a basis $b_1, b_2, \cdots, b_m$ of a lattice Λ, we can apply the Gram–Schmidt process to obtain an orthogonal basis $b_1, b_2^*, \cdots, b_m^*$ for $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$, which we call the Gram-Schmidtification of $b_1, b_2, \cdots, b_m$, and the Gram-Schmidt coefficients $\mu_{i,j} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)}$ for $i > j$. The ordered pair $\{b_i, b_j\}$ for $i > j$ is called size-reduced if $|\mu_{i,j}| \leq \frac{1}{2}$.

Lemma

If a pair $\{b_i, b_j\}$ is not size-reduced, then we can obtain a new size-reduced pair $\{b_i', b_j\}$ by replacing b_i with $b_i' = b_i - \lfloor \mu_{i,j} \rceil b_j$, where $\lfloor \mu_{i,j} \rceil$ denotes the integer closest to $\mu_{i,j}$. Moreover, $\langle b_i, b_j \rangle = \langle b_i', b_j \rangle$, i.e., they generate the same lattice.

Gross lattice

Let O be a maximal order in B_p.

If $\mathrm{End}_{\overline{\mathbb{F}}_p}(E) \cong O$, then $O^T := \{2\alpha - \mathrm{trd}(\alpha) : \alpha \in O\}$ is called the Gross lattice of E.

Lemma

O^T is a free $\mathbb{Z}$-module of rank 3.

Lemma (Kohel, Corollary 71, PhD thesis, 1996)

$\det(O^T) = 4p^2$ and hence $4p^2 \leq D_1 D_2 D_3 \leq 8p^2$ using the Hermite constants.

In late 1980s, Gross defined this lattice, Elkies showed that $D_1 \leq 2p^{2/3}$, and Kaneko improved it to $D_1 \leq \frac{4}{\sqrt{3}} p^{1/2}$ when $j(O) \in \mathbb{F}_p$.

Utility of Gross lattice

Let O_1 and O_2 be two maximal orders of B_p. We say that O_1 and O_2 are of the same type if there exists non-zero $c \in B_p$ such that $cO_1c^{-1} = O_2$, in which case we write $O_1 \sim O_2$.

Theorem (Chevyrev-Galbraith, 2013)

O_1 and O_2 are of the same type if

- $p > 286$
- O_1^T and O_2^T have the same successive minima $D_1 \leq D_2 \leq D_3$
- $D_1 D_2 < 16p/3$

If $j(O) \in \mathbb{F}_p$, then $D_1 D_2 < 16p/3$.

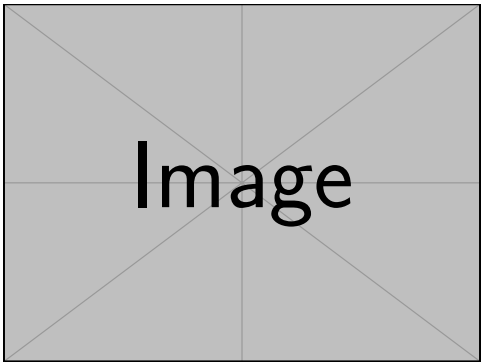
Theorem (Goren-Love, 2023)

O_1 and O_2 are of the same type if O_1^T and O_2^T have the same successive minima $D_1 \leq D_2 \leq D_3$.

(Their theorem is a bit stronger.)

Joint work with

Chenfeng He, Ha Tran, and Christelle Vincent.



Thanks to BIRS and SLMath!

No Gross lattice is orthogonal or well-rounded

A lattice is said to be orthogonal if it has an orthogonal basis, i.e., every pair of distinct vectors in this basis is orthogonal, and a lattice of rank n is well-rounded if it has n linearly-independent shortest vectors, i.e., all of its n successive minima are equal.

Theorem

If $p \neq 2$, then there is no supersingular elliptic curve over $\overline{\mathbb{F}}_p$ for which the Gross lattice is orthogonal or well-rounded.

Orthogonality will lead to $D_1 = 4$ and contradict our results about $j = 1728$.
Well-roundedness will contradict Goren-Love's Lemma 4.4.

Is $j(O) \in \mathbb{F}_p$?

Theorems

Any one of the following conditions is necessary and sufficient for $j(O) \in \mathbb{F}_p$:

1. O^T has a rank-2 sublattice of determinant $4p$.
2. A rank-2 sublattice of O^T with a basis consisting of two elements attaining the first two successive minima of O^T is of determinant $4p$.
3. For $p \geq 37$, the third successive minimum of O^T is bounded by $p \leq D_3 \leq \frac{8p}{7} + \frac{7}{4}$.

Tight bounds on D_3

1. For $p \geq 11$, $\frac{1+\pi_p}{2} \in \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ iff $D_3 = p$ (or $j = 1728$).
2. If $j = -15^3$, $p \equiv 5 \pmod 7$, and $p \geq 13$, then $D_3 = \frac{8p+9}{7} \approx \left(\frac{8p}{7} + \frac{7}{4}\right) - 0.46$.

Is $j(O) \in \mathbb{F}_p^2 \setminus \mathbb{F}_p$?

Theorem

$j(O) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ iff the third successive minimum of O^T is bounded by $D_3 \leq \frac{3p}{5} + 5$.

The proof uses the following key ideas:

1. $\max_{[\sqrt{a},b]} \left\{x + \frac{a}{x}\right\} = b + \frac{a}{b}$
2. Size-reducedness property of a basis attaining the successive minima of O^T.
3. O^T is an integral, rank-3 lattice of determinant $4p^2$.

Tight bound on D_3

If $j = -565760a + 914880 \in \mathbb{Q}(a) = \mathbb{Q}[t]/\langle t^2 - t - 1\rangle \cong \mathbb{Q}(\sqrt{5})$ and $p \equiv 17 \pmod{20}$ then $D_3 = \frac{3p+9}{5}$ (or $\frac{3p+4}{5}$).

$j = 0$ and $j = 1728$

$j = 0$, $p \equiv 2 \mod 3$, $B_p = \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ such that $\mathbf{i}^2 = -3, \mathbf{j}^2 = -p$, $O := O(3)$

O^T has a successive minimal basis given by $\{\mathbf{i}, \frac{\mathbf{i}+3\mathbf{j}-\mathbf{k}}{3}, \frac{-\mathbf{i}-2\mathbf{k}}{3}\}$ and the Gram matrix of this basis is

$$G_{O^T} = \begin{pmatrix} 3 & 1 & 1 \\ 1 & \frac{4p+1}{3} & -\left(\frac{2p-1}{3}\right) \\ 1 & -\left(\frac{2p-1}{3}\right) & \frac{4p+1}{3} \end{pmatrix}.$$

$j = 12^3$, $p \equiv 3 \mod 4$, $B_p = \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ with $\mathbf{i}^2 = -1, \mathbf{j}^2 = -p$, $O := O'(1)$

For $p > 3$, O^T has a successive minimal basis given by $\{2\mathbf{i}, \mathbf{j}, \mathbf{i} - \mathbf{k}\}$ and the Gram matrix of this basis Is

$$G_{O^T} = \begin{pmatrix} 4 & 0 & 2 \\ 0 & p & 0 \\ 2 & 0 & p+1 \end{pmatrix}.$$

$j = 1728 \iff D_2 = p \iff D_3 = p + 1.$

The 13 CM curves over $\mathbb{Q}$

Lemma

Let E be a CM-elliptic curve defined over $\mathbb{Q}$ with $\mathcal{O} := \mathrm{End}_{\overline{\mathbb{Q}}}(E) \subseteq \mathbb{Q}(\sqrt{-\Delta})$ and $\mathrm{disc}(\mathcal{O}) = -d$. Let p be a prime of supersingular reduction and $\widetilde{E} := E \pmod{p}$ with $O := \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \subseteq B_p$.There exists a positive integer N_E, which depends on $j(E)$, such that for $p \geq N_E$ we have $D_1 = d$.

It is a consequence of Gross-Zagier formula.

j-invariant	0	1728	-15^3	20^3	-32^3	$2 \cdot 30^3$	66^3	-96^3
$D_1 = d$	3	4	7	8	11	12	16	19
N_E	5	7	13	23	29	41	67	79

j-invariant	$-3 \cdot 160^3$	255^3	-960^3	-5280^3	-640320^3
$D_1 = d$	27	28	43	67	163
N_E	167	181	433	1103	6691

Sign of j-invariant for the 13 CM curves over $\mathbb{Q}$

For $p \geq N_E$, we have the following four types of Gram matrix of a successive minimal basis of the Gross lattice of $\widetilde{E}/\mathbb{F}_p$.

Theorem

For $j(E) > 0$.

1. if $O = O'(\ell)$ then
$$G_{O^T} = \begin{pmatrix} d & 2t & 0 \\ 2t & \frac{4(p+t^2)}{d} & 0 \\ 0 & 0 & p \end{pmatrix} \text{ with}$$
$0 \leq t \leq d/4$, or
2. if $O = O(\ell)$ then
$$G_{O^T} = \begin{pmatrix} d & 2m & 2n \\ 2m & \frac{4(p+m^2)}{d} & m \\ 2n & m & p+n \end{pmatrix} \text{ with}$$
$0 \leq m, n \leq d/4$

For $j(E) \leq 0$, we have $O = O(\ell)$.

3. $$G_{O^T} = \begin{pmatrix} d & 2u & u \\ 2u & \frac{4\left(p+u^2\right)}{d} & \frac{2\left(p+u^2\right)}{d} \\ u & \frac{2\left(p+u^2\right)}{d} & p+\frac{p+u^2}{d} \end{pmatrix} \text{ with}$$
$0 \leq u \leq d/4$, or
4. $$G_{O^T} = \begin{pmatrix} d & a & b \\ a & \frac{4p+a^2}{d} & -\left(\frac{2p-ab}{d}\right) \\ b & -\left(\frac{2p-ab}{d}\right) & p+\frac{p+b^2}{d} \end{pmatrix}$$
with $0 < a, b \leq d/2$

Thank you!