Supersingular Isogeny Graphs and Quaternion Algebras.

1. Isogeny Graphs: Background and Motivation.

Outline / Motivation:
This minicourse will consist of four lectures:

1) Background. Isogeny graphs. Applications.
2) Supersingular Isogeny Graphs in Cryptography.
   * post-quantum cryptography.
3) Introduction to Quaternion Algebras.
4) The Deuring correspondence:
   \[
   \{ \text{maximal orders} \} \quad \overset{\sim}{\longleftrightarrow} \quad \{ \text{supersingular} \} \quad \mathbb{F}_p^2 / \text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)
   \]
   * applications to SIG cryptography.

Background

- **Elliptic Curves.**
  Let \( k = \mathbb{F}_q \) be a finite field of characteristic \( p \neq 2,3 \).
  
  **Definition.**
  - An **elliptic curve** \( E/k \) is a smooth projective curve of genus 1 over \( k \), together with a distinguished \( k \)-rational point \( 0 \).
  - \( E \) is isomorphic over \( k \) to the projective curve associated to an affine Weierstrass equation
    \[
    E: y^2 = x^3 + ax + b, \quad a, b \in k.
    \]
  - We define the **j-invariant** \( j(E) \) of \( E \) to be
    \[
    j(E) := j(a, b) := 1728 \frac{4a^3}{4a^3 + 27b^2}
    \]
    for any Weierstrass model of \( E \).
FACTS:

1) Elliptic curves $E, E'$ are isomorphic over $\bar{k} \iff j(E) = j(E')$.

2) There is a 1-1 correspondence

$$\bar{k} \leftrightarrow \text{ set of } \bar{k}\text{-isomorphism classes of elliptic curves over } \bar{k}.$$ 

Isogenies,

DEFINITION.

- Let $E, E'$ be elliptic curves over $\bar{k}$. An isogeny $\varphi : E \to E'$ is a nonzero morphism of pointed curves.

- The degree of an isogeny is its degree as a rational map.

- An isogeny of degree $n$ is called an $n$-isogeny.

$E, E'$ are $n$-isogenous if they are related by a degree $n$ isogeny, and if $j, j' \in \bar{k}$ are $n$-isogenous over $\bar{k}$ if there are $n$-isogenous $E, E'/\bar{k}$ such that $j(E) = j$ and $j(E') = j'$.

- The kernel of $\varphi$ is the kernel of the induced map

$$\varphi : E(\bar{k}) \to E'(\bar{k}).$$

FACTS:

1) If $p | n$, then the kernel of an $n$-isogeny $\varphi$ has size $n$ (we say $\varphi$ is separable).

2) Every finite subgroup of $E(\bar{k})$ is the kernel of a separable isogeny over $\bar{k}$ which is uniquely determined up to isomorphism. (This isogeny can be explicitly computed using Vélu's formulas).
3) Every \( n \)-isogeny \( \varphi : E \to E' \) has a unique dual isogeny \( \hat{\varphi} : E' \to E \) such that \( \varphi \circ \hat{\varphi} = \hat{\varphi} \circ \varphi = \text{Id} \), where \([n]\) is the multiplication-by-\( n\) map.

4) The kernel of \([n]\) is the \( n \)-torsion subgroup
\[
E[n] = \left\{ P \in E(\bar{k}) \mid nP = 0 \right\},
\]
and when \( p \nmid n \),
\[
E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.
\]

**Lemma**

Let \( E \) be an elliptic curve with \( j(E) \neq 0, 1728 \), and let \( l \neq p = \text{char}(k) \) be prime. Up to isomorphism, the number of \( k \)-rational \( l \)-isogenies from \( E \) is 0, 1, 2 or \( l+1 \).

**Proof**

- \( E[l] \) contains \( l+1 \) subgroups of order \( l \), each of which is the kernel of a separable \( l \)-isogeny over \( \bar{k} \). Every \( l \)-isogeny \( \varphi \) from \( E \) arises in this way, since \( \ker(\varphi) \subseteq \ker(\hat{\varphi} \circ \varphi) = E[l] \). So there are \( l+1 \) isogenies of degree \( l \) defined over \( \bar{k} \).
- \( \varphi \) is defined over \( k \) \( \iff \) \( \ker(\varphi) \) is invariant under the action of the group \( G = \text{Gal}(k(E[l])/k) \), which acts linearly on \( E[l] \cong \mathbb{F}_l^2 \), in which order- \( l \) subgroups are linear subspaces. But if \( G \) fixes more than 2 linear subspaces, then it must fix everything.
• **Note:** The hypothesis that \( j(E) \neq 0, 1728 \) guarantees that 
\( E \) doesn't have extra automorphisms.

**The Modular Equation.**

Let \( j(\tau) \) be the modular \( j \)-function. For each \( N \in \mathbb{N} \), the minimal polynomial \( \phi_N \) of \( j(N\tau) \) over \( \mathbb{C}(j(\tau)) \) is the modular polynomial

\[
\phi_N \in \mathbb{Z}[j(\tau)][y] \subset \mathbb{Z}[x,y].
\]

**FACTS:**

1) \( \phi_N \) is symmetric in \( x \) and \( y \).

2) When \( \ell \) is prime, \( \phi_\ell \) has degree \( \ell+1 \) in both variables.

3) The modular equation \( \phi_N(x,y) = 0 \) is a canonical equation for the modular curve \( Y_0(N) = \Gamma_0(N)\backslash \mathcal{H} \). It parametrizes pairs of elliptic curves over \( \mathbb{C} \) related by a cyclic \( N \)-isogeny.

   In particular, when \( N = \ell \) is prime,

   \[
   \phi_\ell(j(E), j(E')) = 0 \iff j(E) \text{ and } j(E') \text{ are } \ell \text{-isogenous.}
   \]

   This moduli interpretation remains true over any field \( \mathbb{F} \) with \( \text{char}(\mathbb{F}) \neq \ell \).

4) Let \( m_\ell(j, j') := \text{ord}_{t=j'} \phi_\ell(j, t) \). Whenever \( j, j' \neq 0, 1728 \),

   \[
   m_\ell(j, j') = m_\ell(j', j).
   \]
The Endomorphism Ring.

**Definition.**
An endomorphism of an elliptic curve $E$ is either the zero map or an isogeny from $E$ to itself.

The endomorphisms of $E$ form a ring $\text{End}(E)$ in which

$$ (\phi + \psi)(P) = \phi(P) + \psi(P) $$

$$ (\phi \circ \psi)(P) = \phi(\psi(P)) $$

for all $P \in E(\overline{K})$.

- For each integer $n$, $[n] \in \text{End}(E)$, so $\mathbb{Z} \subseteq \text{End}(E)$.
- Over a finite field $k = \mathbb{F}_q$, $\text{End}(E)$ is always larger than $\mathbb{Z}$:
  $$ \text{End}(E) \cong \begin{cases} 
  \text{an order } 0 \text{ in an imaginary quadratic field (E ordinary).} \\
  \text{an order } 0 \text{ in a definite quaternion algebra (E supersingular).}
\end{cases} $$

We say that $E$ has complex multiplication (CM) by $0$, and we'll fix an isomorphism $0 \rightarrow \text{End}(E)$.

**Proposition**
Let $E/\mathbb{k} = \mathbb{F}_p^n$ be an elliptic curve. The following are equivalent:

a) $E$ is supersingular.

b) $E[p]$ is trivial.

c) The map $[p] : E \rightarrow E$ is purely inseparable and $j(E) \in \mathbb{F}_p^2$.

**Note:** if $E$ and $E'$ are isogenous, then $\text{End}(E) \otimes \mathbb{Q} \cong \text{End}(E') \otimes \mathbb{Q}$. Hence, supersingularity is preserved under isogeny.
Isogeny graphs of elliptic curves.

Let $k = \mathbb{F}_q$ be a field with $\text{char}(k) = p$ and $l \neq p$ be prime.

**Definition.**

The $l$-isogeny graph $G_e(k)$ is the directed graph with vertex set $k$ and edges $(j, j')$ present with multiplicity $m_e(j, j') := \text{ord}_{t = j} \phi_e(j, t)$.

- The vertices of $G_e(k)$ represent $l$-invariants and its edges correspond to (isomorphism classes of) $l$-isogenies defined over $k$.
- Since $m_e(j, j') = m_e(j', j)$ when $j, j' \neq 0, 1728$, we can regard the subgraph of $G_e(k)$ on $k \setminus \{0, 1728\}$ as an undirected graph.
- By the last remark, $G_e(k)$ consists of ordinary and supersingular components. We'll see that they have different properties.

**Supersingular Isogeny Graphs.**

- Since every supersingular $j$-invariant in $k$ lies in $\mathbb{F}_{p^2}$, if $E$ is supersingular then all roots of $\phi_e(j(E), y)$ lie in $\mathbb{F}_{p^2}$. Hence every vertex in a supersingular component of $G_e(\mathbb{F}_{p^2})$ has out-degree $l + 1$.
- Moreover, by a result of Kohel, $G_e(\mathbb{F}_{p^2})$ has just one supersingular component.
- By the above, if \( p \equiv 1 \mod 12 \), then the single supersingular component of \( G_{\ell}(\mathbb{F}_p) \) is an undirected \((l+1)\)-regular graph, with \( N_p \approx \frac{p}{12} \) vertices. Moreover:

- **Theorem (Pizer)**
  The supersingular component of \( G_{\ell}(\mathbb{F}_p) \) is a Ramanujan graph.

- **Definition.**
  A d-regular graph is a Ramanujan graph if \( \lambda_2 \leq \sqrt{d+1} \), where \( \lambda_2 \) is the 2\(^{nd}\) largest eigenvalue of its adjacency matrix.

- **Remark:** Pizer proved an analogous result in the context of orders in a quaternion algebra; it translates to our setting by the Deuring correspondence.

  We'll come back to this next week.

- **Ordinary Isogeny Graphs.**

  Let \( E / \mathbb{F}_q \) be ordinary. Then \( \text{End}(E) \cong 0 \) with \( \mathbb{Z}[\pi] \subset 0 \subset 0_K \), where \( \pi \) is the Frobenius endomorphism and \( K = \mathbb{Q}(\sqrt{\text{tr}(\pi)^2 - 4q}) \).

  By a theorem of Tate, isogenous elliptic curves have the same \( \text{tr}(\pi) \).

  We can separate the vertices of the connected component of \( G_{\ell}(\mathbb{F}_q) \) containing \( j(E) \) into levels \( V_0, \ldots, V_d \), so that a vertex \( j(E') \) belongs to the level \( V_i \) with \( i = \nu_E([0_K : 0]) \).

(We'll check below that \( \bigcup_{i=0}^d V_i \) is in fact a connected graph).
Let \( \varphi : E \to E' \) be an \( \ell \)-isogeny of elliptic curves with CM by imaginary orders \( \mathcal{O} = \mathbb{Z} + \tau \mathbb{Z} \) and \( \mathcal{O}' = \mathbb{Z} + \tau' \mathbb{Z} \), for some \( \tau, \tau' \in \mathbb{H} \). Then \( \varphi \circ \tau' \cdot \varphi \in \text{End}(E) \Rightarrow \ell \tau' \in \mathcal{O} \); similarly, \( \ell \tau \in \mathcal{O}' \). Hence there are three possibilities:

1) \( \mathcal{O} = \mathcal{O}' \) (\( \varphi \) is horizontal)

2) \([\mathcal{O} : \mathcal{O}'] = \ell \) (\( \varphi \) is descending)

3) \([\mathcal{O}' : \mathcal{O}] = \ell \) (\( \varphi \) is ascending)

Both \( \mathcal{O} \) and \( \mathcal{O}' \) lie in the ring of integers \( \mathcal{O}_k \) of the same field \( k \).

### Horizontal Isogenies

Let \( E/k \) be an elliptic curve with CM by an imaginary quadratic order \( \mathcal{O} \). Let \( \mathfrak{a} \) be an invertible \( \mathcal{O} \)-ideal. The \( \mathfrak{a} \)-torsion subgroup

\[
E[\mathfrak{a}] = \{ P \in E(\overline{k}) | \mathfrak{a}(P) = 0 \text{ for all } \mathfrak{a} \in \mathfrak{a} \}
\]

is the kernel of a separable isogeny \( \varphi_\mathfrak{a} : E \to E' \).

- If \( \mathfrak{p} \not| \text{Norm}(\mathfrak{a}) \), then \( \deg(\varphi_\mathfrak{a}) = \text{Norm}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}] \).
- \( \mathfrak{a} \) invertible \( \Rightarrow \text{End}(E) \cong \text{End}(E') \) (exercise), so \( \varphi_\mathfrak{a} \) is a horizontal isogeny.

If \( \mathfrak{a}, \mathfrak{b} \) are invertible \( \mathcal{O} \)-ideals, then \( \varphi_{\mathfrak{a} \mathfrak{b}} = \varphi_\mathfrak{a} \varphi_\mathfrak{b} \). So the group of invertible \( \mathcal{O} \)-ideals acts on the set of elliptic curves with endomorphism ring \( \mathcal{O} \).

When \( \mathfrak{a} \) is principal, \( E \cong E' \). Hence there is an induced action of \( \text{Cl}(\mathcal{O}) \) on the set

\[
\text{Ell}_{\mathcal{O}}(k) = \{ j(E) \mid E/k \text{ with } \text{End}(E) \cong \mathcal{O} \}.
\]
- This action is faithful and transitive, so if $E(k) \neq \emptyset$, it is a torsor for the group $\text{Cl}(O)$.
- The cardinality of $E(k)$ is either 0 or $h = \#\text{Cl}(O)$, so either every $E/\bar{k}$ with CM by $O$ can be defined over $k$, or none of them can.
- Each horizontal $l$-isogeny $\Phi$ arises from the action of an invertible $O$-ideal $l$ of norm $l$ (the ideal of endomorphisms $x \in O$ whose kernels contain the kernel of $\Phi$).
- If $l \mid [O_k:O]$, then no such ideals exist.
- Otherwise we say that $O$ is maximal at $l$, and in this case the number of invertible ideals of norm $l$ equals

$$1 + \left(\frac{\text{disc}(k)}{l}\right) = \begin{cases} 0, & \text{if } l \text{ is inert in } k \\ 1, & \text{if } l \text{ is ramified in } k \\ 2, & \text{if } l \text{ splits in } k. \end{cases}$$

### Vertical Isogenies

Let $O$ be an imaginary quadratic order with discriminant $D$, and let $O' = \mathbb{Z} + lO$ be the order of index $l$ in $O$.

Assume $D < -4$, so that the only units in $O$, $O'$ are $\pm 1, i$ (this excludes $O = \mathbb{Z}[i]$ and $O = \mathbb{Z}[\sqrt{3}]$, corresponding to $j = 1728$ and $0$, respectively).

### Lemma

Let $E'/k$ be an elliptic curve with CM by $O'$. Then there is a unique ascending $l$-isogeny from $E'$ to an elliptic curve $E/k$ with CM by $O$. 
PROOF (Sketch)
First, show that if any $E'/\mathbb{K}$ with CM by $\mathcal{O}'$ admits an ascending $\ell$-isogeny, then so does every such elliptic curve. Then use induction on $d = v_\ell([\mathcal{O}_k : \mathcal{O}])$, plus the fact that the number of horizontal $\ell$-isogenies and $\# \Ell_{\mathbb{G}}(\mathbb{K})$ are known. (See Lemma 6 in Sutherland’s “Isogeny Volcanoes” for details).

Now we are ready to describe the ordinary components of $\mathbb{G}_\ell(F_q)$. First, we need a definition:

**DEFINITION.**
An $\ell$-volcano $V$ is a connected undirected graph whose vertices are partitioned into levels $V_0, \ldots, V_d$ such that:

1) The subgraph on $V_0$ (the surface) is a regular graph of degree at most 2.

2) For $i > 0$, each vertex in $V_i$ has exactly one neighbour in level $V_{i-1}$, and this accounts for every edge not on the surface.

3) For $i < d$, each vertex in $V_i$ has degree $\ell + 1$.

The integer $d$ is the depth of the volcano.
Theorem (Kohel). Let $V$ be an ordinary component of $G_{e}(F_q)$ that does not contain $0$ or $1728$. Then $V$ is an $l$-volcano for which:

1. The vertices in level $V_{i}$ all have the same endomorphism ring $O_{i}$.
2. The subgraph on $V_{0}$ has degree $1 + \left( \frac{\text{disc}(k)}{l} \right)$, where $K$ is the fraction field of $O_{0}$.
3. If $\left( \frac{\text{disc}(k)}{l} \right) \geq 0$, then $\#V_{0}$ is the order of $[l]$ in $\mathcal{O}(O_{0})$; otherwise $\#V_{0} = 1$.
4. The depth of $V$ is $d = \nu_{e}(\left[ O_{k} : \mathbb{Z}[\pi] \right])$, where $\pi$ is the Frobenius endomorphism of any $E$ with $j(E) \in V$.
5. We have $e \mid \left[ O_{k} : O_{0} \right]$ and $\left[ O_{i} : O_{i+1} \right] = l$ for $0 \leq i < d$.

Proof

Exercise.

Remark: The theorem can be easily extended to the case where $V$ contains $0$ or $1728$, modifying the claim that $V$ is an $l$-volcano appropriately.
Applications

- **Identifying Supersingular Curves.**
  
  We can exploit the differences between ordinary and supersingular isogeny graphs to determine whether an elliptic curve $E/k$ is supersingular.

- **Algorithm:** (Sutherland).
  
  **Input:** an elliptic curve $E/k$, with $\text{char}(k) = p$.
  
  **Output:** whether $E$ is ordinary or supersingular.

  - **Step 1:** if $j(E) \notin \mathbb{F}_p$, return "ordinary".
  
  - **Step 2:** if $p \leq 3$ return "supersingular," if $j(E) = 0$ "ordinary," if $j(E) \neq 0$.
  
  - **Step 3:** Find 3 roots of $\zeta_2(j(E), y)$ in $\mathbb{F}_p$.
    
    If this is not possible, return "ordinary".

  - **Step 4:** Walk 3 paths in parallel, for up to $\lceil \log_2 p \rceil + 1$ steps.
    
    If any of these paths hits $V_d$, return "ordinary".

  - **Step 5:** Return "supersingular".

- **Remark:** It's a Las Vegas algorithm with expected time $\tilde{O}(\log^3 p)$, and $O(\log p)$ space. These complexity bounds significantly improve existing methods.

- **Other Applications.**
  
  - Computing endomorphism rings of ordinary elliptic curves (Bisson, Sutherland)
  
  - Computing Hilbert class polynomials (Sutherland/Belding, Bröker, Enge, Lauter)
  
  - Computing modular polynomials (Bröker, Lauter, Sutherland).