Algorithms on abelian varieties for cryptography

Damien Robert[1]

[1] Microsoft Research

12/01/2012 (Telecom ParisTech++)

Outline

1. Public-key cryptography
2. Abelian varieties
3. Theta functions
4. Isogenies
5. Examples

Discrete logarithm

Definition (DLP)

Let $G = \langle g \rangle$ be a cyclic group of prime order. Let $x \in \mathbb{N}$ and $h = g^x$. The discrete logarithm $\log_g(h)$ is x.

- Exponentiation: $O(\log p)$. DLP: $\widetilde{O}(\sqrt{p})$ (in a generic group). So we can use the DLP for public key cryptography.

$\Rightarrow$ We want to find secure groups with efficient addition law and compact representation.

Pairing-based cryptography

Definition

A pairing is a bilinear application $e : G_1 \times G_1 \to G_2$.

Example

- If the pairing e can be computed easily, the difficulty of the DLP in G_1 reduces to the difficulty of the DLP in G_2.

$\Rightarrow$ MOV attacks on supersingular elliptic curves.

- Identity-based cryptography [BF03].
- Short signature [BLS04].
- One way tripartite Diffie–Hellman [Jou04].
- Self-blindable credential certificates [Ver01].
- Attribute based cryptography [SW05].
- Broadcast encryption [GPS+06].

Example of applications

Tripartite Diffie–Helman

Alice sends g^a, Bob sends g^b, Charlie sends g^c. The common key is

$$e(g,g)^{abc} = e(g^b,g^c)^a = e(g^c,g^a)^b = e(g^a,g^b)^c \in G_2.$$

Example (Identity-based cryptography)

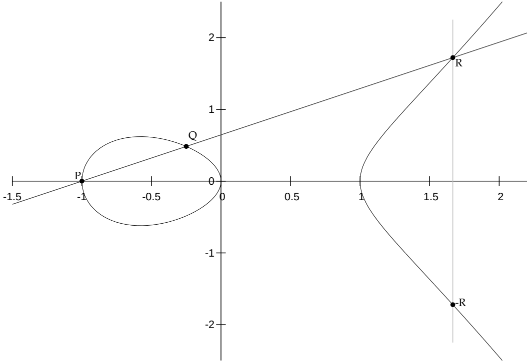
- Master key: (P, sP), s. $\quad s \in \mathbb{N}, P \in G_1$.
- Derived key: Q, sQ. $\quad Q \in G_1$.
- Encryption, $m \in G_2$: $m' = m \oplus e(Q, sP)^r$, rP. $\quad r \in \mathbb{N}$.
- Decryption: $m = m' \oplus e(sQ, rP)$.

Elliptic curves

Definition (car $k \neq 2,3$)

An elliptic curve is a plan curve of equation

$$y^2 = x^3 + ax + b \qquad 4a^3 + 27b^2 \neq 0.$$



Abelian varieties

Definition

An Abelian variety is a complete connected group variety over a base field k.

- Abelian variety = points on a projective space (locus of homogeneous polynomials) + an abelian group law given by rational functions.
- Abelian variety of dimension 1 = elliptic curves.

$\Rightarrow$ Abelian varieties are just the generalization of elliptic curves in higher dimension.

Pairings on abelian varieties

The Weil and Tate pairings on abelian varieties are the only known examples of cryptographic pairings.

$$e_W : A[\ell] \times A[\ell] \rightarrow \mu_\ell \subset \mathbb{F}_{q^k}^*.$$

Abelian surfaces

Abelian varieties of dimension 2 are given by: 5 quadratic equations in $\mathbb{P}^7$.

$$\begin{gathered}
(4a_1a_2+4a_5a_6)X_1X_6+(4a_1a_2+4a_5a_6)X_2X_5 = \\
(4a_3a_44a_4a_3)X_3X_4+(4a_3a_44a_4a_3)X_7X_8; \\
(2a_1a_5+2a_2a_6)X_1^2+(2a_1a_5+2a_2a_6)X_2^2+(-2a_3^2-2a_4^2-2a_3^2-2a_4^2)X_3X_3 = \\
(2a_3^2+2a_4^2+2a_3^2+2a_4^2)X_4X_8+(-2a_1a_5-2a_2a_6)X_5^2+(-2a_1a_5-2a_2a_6)X_6^2; \\
(4a_1a_6+4a_2a_5)X_1X_2+(-4a_3a_4-4a_3a_4)X_3X_8 = \\
(4a_3a_4+4a_3a_4)X_4X_7+(-4a_1a_6-4a_2a_5)X_5X_6; \\
(2a_1^2+2a_2^2+2a_5^2+2a_6^2)X_1X_5+(2a_1^2+2a_2^2+2a_5^2+2a_6^2)X_2X_6+(-2a_3a_3-2a_4a_4)X_3^2 = \\
(2a_3a_3+2a_4a_4)X_4^2+(2a_3a_3+2a_4a_4)X_7^2+(2a_3a_3+2a_4a_4)X_8^2; \\
(2a_1^2-2a_2^2+2a_5^2-2a_6^2)X_1X_5+(-2a_1^2+2a_2^2-2a_5^2+2a_6^2)X_2X_6+(-2a_3a_3+2a_4a_4)X_3^2 = \\
(-2a_3a_3+2a_4a_4)X_4^2+(2a_3a_3-2a_4a_4)X_7^2+(-2a_3a_3+2a_4a_4)X_8^2;
\end{gathered}$$

where the parameters satisfy 2 quartic equations in $\mathbb{P}^5$:

$$\begin{gathered}
a_1^3a_5+a_1^2a_2a_6+a_1a_2^2a_5+a_1a_5^3+a_1a_5a_6^2+a_2^3a_6+a_2a_5^2a_6+a_2a_6^3-2a_3^4-4a_3^2a_4^2-2a_4^4=0; \\
a_1^2a_2a_6+a_1a_2^2a_5+a_1a_5a_6^2+a_2a_5^2a_6-4a_3^2a_4^2=0
\end{gathered}$$

The most general form actually use 72 quadratic equations in 16 variables.

Jacobian of hyperelliptic curves

$C: y^2 = f(x)$, hyperelliptic curve of genus g. $(\deg f = 2g+1)$

- Divisor: formal sum $D = \sum n_i P_i$, $P_i \in C(\overline{k})$.
  $\deg D = \sum n_i$.
- Principal divisor: $\sum_{P \in C(\overline{k})} v_P(f).P$; $f \in \overline{k}(C)$.
- Jacobian of C = Divisors of degree 0 modulo principal divisors
  \+ Galois action
  = Abelian variety of dimension g.
- Divisor class $D \Rightarrow$ unique representative (Riemann–Roch):

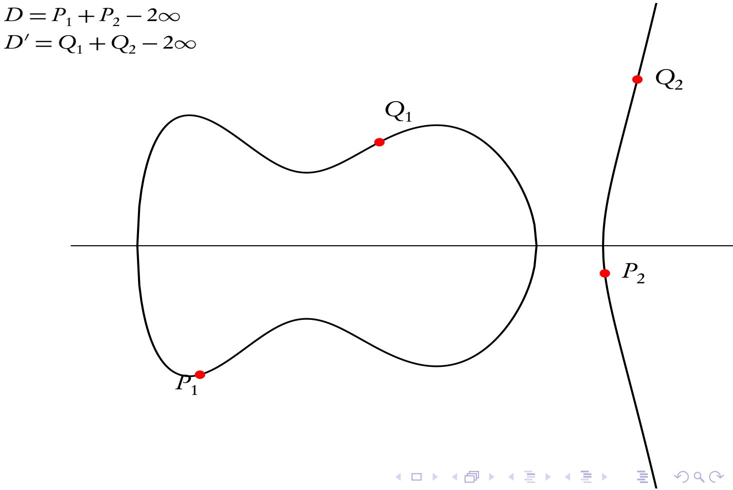
$$D = \sum_{i=1}^{k} (P_i - P_\infty) \qquad k \leqslant g, \quad \text{symmetric } P_i \neq P_j$$

- Mumford coordinates: $D = (u, v) \Rightarrow u = \prod (x - x_i)$, $v(x_i) = y_i$.
- Cantor algorithm: addition law.

Abelian varieties as Jacobians

Dimension 2: Jacobians of hyperelliptic curves of genus 2:

$$y^2 = f(x), \deg f = 5.$$

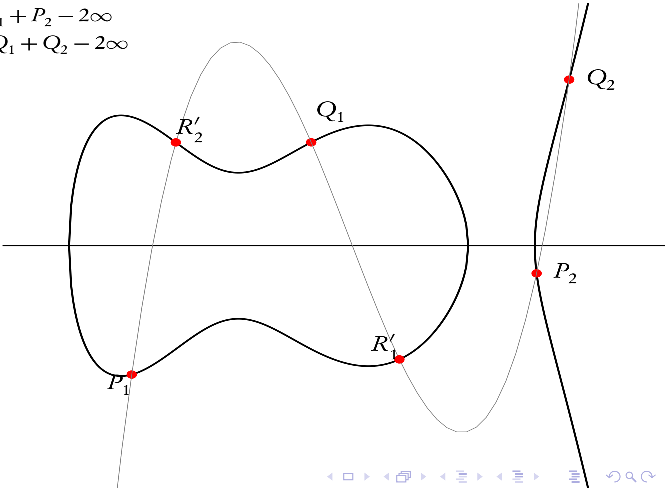


Abelian varieties as Jacobians

Dimension 2: Jacobians of hyperelliptic curves of genus 2:

$$y^2 = f(x), \deg f = 5.$$

$D = P_1 + P_2 - 2\infty$
$D' = Q_1 + Q_2 - 2\infty$

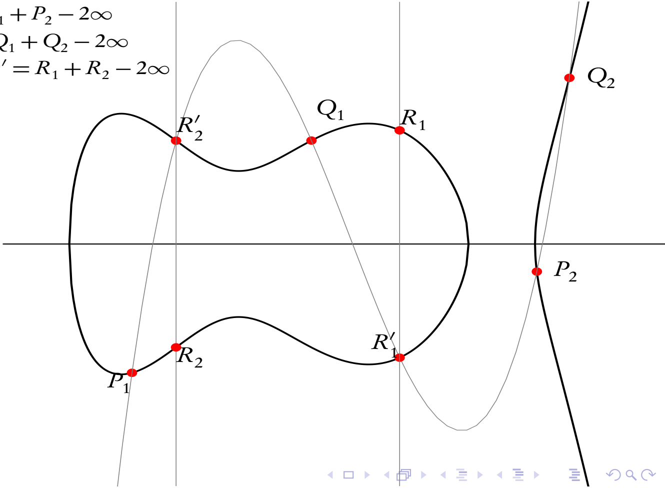


Abelian varieties as Jacobians

Dimension 2: Jacobians of hyperelliptic curves of genus 2:

$$y^2 = f(x), \deg f = 5.$$

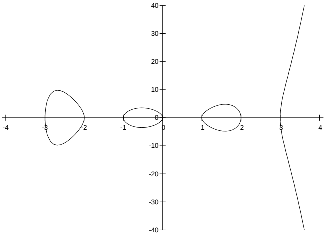
$D = P_1 + P_2 - 2\infty$
$D' = Q_1 + Q_2 - 2\infty$
$D + D' = R_1 + R_2 - 2\infty$



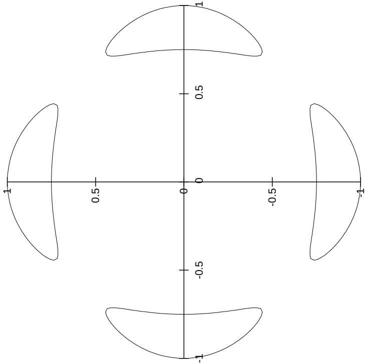
Abelian varieties as Jacobians

Dimension 3

Jacobians of hyperelliptic curves of genus 3.



Jacobians of quartics.



Abelian varieties as Jacobians

Dimension 4

Abelian varieties do not come from a curve generically.

Security of abelian varieties

g	# points	DLP
1	$O(q)$	$\tilde{O}(q^{1/2})$
2	$O(q^2)$	$\tilde{O}(q)$
3	$O(q^3)$	$\tilde{O}(q^{4/3})$ (Jacobian of an hyperelliptic curve) $\tilde{O}(q)$ (Jacobian of a quartic)
g $g > \log(q)$	$O(q^g)$	$\tilde{O}(q^{2-2/g})$ $L_{1/2}(q^g) = \exp(O(1)\log(x)^{1/2}\log\log(x)^{1/2})$

Security of the DLP

- Weak curves (MOV attack, Weil descent, anomal curves).

Complex abelian varieties

- Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, where $\Omega \in \mathcal{H}_g(\mathbb{C})$ the Siegel upper half space.
- The theta functions with characteristic are analytic (quasi periodic) functions on $\mathbb{C}^g$.

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = \sum_{n\in\mathbb{Z}^g} e^{\pi i\, {}^t(n+a)\Omega(n+a) + 2\pi i\, {}^t(n+a)(z+b)} \qquad a,b \in \mathbb{Q}^g$$

Quasi-periodicity:

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z+m_1\Omega+m_2,\Omega) = e^{2\pi i({}^t a\cdot m_2 - {}^t b\cdot m_1) - \pi i\, {}^t m_1\Omega m_1 - 2\pi i\, {}^t m_1\cdot z}\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega).$$

- Projective coordinates:

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{P}_{\mathbb{C}}^{n^g-1} \\ z & \longmapsto & (\vartheta_i(z))_{i\in Z(\overline{n})} \end{array}$$

where $Z(\overline{n}) = \mathbb{Z}^g/n\mathbb{Z}^g$ and $\vartheta_i = \vartheta\left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix}\right](., \frac{\Omega}{n})$.

Theta functions of level n

- Translation by a point of n-torsion:

$$\vartheta_i\left(z+\frac{m_1}{n}\Omega+\frac{m_2}{n}\right)=e^{-\frac{2\pi i}{n}\,{}^t i\cdot m_1}\vartheta_{i+m_2}(z).$$

- $(\vartheta_i)_{i\in Z(\overline{n})}$: basis of the theta functions of level n
$\Leftrightarrow A[n]=A_1[n]\oplus A_2[n]$: symplectic decomposition.

- $(\vartheta_i)_{i\in Z(\overline{n})}=\begin{cases}\text{coordinates system} & n\geqslant 3\\ \text{coordinates on the Kummer variety } A/\pm 1 & n=2\end{cases}$

- Theta null point: $\vartheta_i(0)_{i\in Z(\overline{n})}=$ modular invariant.

The differential addition law ($k=\mathbb{C}$)

$$\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big)=$$

$$\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big).$$

where $\chi\in\hat{Z}(\overline{2}), i,j,k,l\in Z(\overline{n})$

$$(i',j',k',l')=A(i,j,k,l)$$

$$A=\frac{1}{2}\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}$$

Example: addition in genus 1 and in level 2

Differential Addition Algorithm:
Input: $P = (x_1 : z_1)$, $Q = (x_2 : z_2)$
and $R = P - Q = (x_3 : z_3)$ with $x_3 z_3 \neq 0$.
Output: $P + Q = (x' : z')$.

1. $x_0 = (x_1^2 + z_1^2)(x_2^2 + z_2^2)$;
2. $z_0 = \frac{A^2}{B^2}(x_1^2 - z_1^2)(x_2^2 - z_2^2)$;
3. $x' = (x_0 + z_0)/x_3$;
4. $z' = (x_0 - z_0)/z_3$;
5. Return $(x' : z')$.

Cost of the arithmetic with low level theta functions (car $k \neq 2$)

	Mumford	Level 2	Level 4
Doubling	$34M + 7S$	$7M + 12S + 9m_0$	$49M + 36S + 27m_0$
Mixed Addition	$37M + 6S$		

Multiplication cost in genus 2 (one step).

	Montgomery	Level 2	Jacobians coordinates
Doubling	$5M + 4S + 1m_0$	$3M + 6S + 3m_0$	$3M + 5S$
Mixed Addition			$7M + 6S + 1m_0$

Multiplication cost in genus 1 (one step).

The Weil pairing on elliptic curves

- Let $E: y^2 = x^3 + ax + b$ be an elliptic curve over k ($\operatorname{car} k \neq 2, 3$).
- Let $P, Q \in E[\ell]$ be points of ℓ-torsion.
- Let f_P be a function associated to the principal divisor $\ell(P-0)$, and f_Q to $\ell(Q-0)$. We define:

$$e_{W,\ell}(P,Q) = \frac{f_Q(P-0)}{f_P(Q-0)}.$$

- The application $e_{W,\ell}: E[\ell] \times E[\ell] \to \mu_\ell(\overline{k})$ is a non degenerate pairing: the Weil pairing.

The Weil and Tate pairing with theta coordinates

P and Q points of ℓ-torsion.

$$\begin{array}{ccccc}
0_A & P & 2P & \ldots & \ell P = \lambda_P^0 0_A \\
Q & P \oplus Q & 2P+Q & \ldots & \ell P + Q = \lambda_P^1 Q \\
2Q & P+2Q & & & \\
\ldots & \ldots & & & \\
\ell Q = \lambda_Q^0 0_A & P + \ell Q = \lambda_Q^1 P & & &
\end{array}$$

- $e_{W,\ell}(P,Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_P^0 \lambda_Q^1}$.
  If $P = \Omega x_1 + x_2$ and $Q = \Omega y_1 + y_2$, then $e_{W,\ell}(P,Q) = e^{-2\pi i \ell ({}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2)}$.
- $e_{T,\ell}(P,Q) = \frac{\lambda_P^1}{\lambda_P^0}$.

Why does it works?

$$\begin{array}{ccccc}
0_A & \alpha P & \alpha^4(2P) & \dots & \alpha^{\ell^2}(\ell P) = \lambda'^0_P 0_A \\
\beta Q & \gamma(P \oplus Q) & \frac{\gamma^2\alpha^2}{\beta}(2P+Q) & \dots & \frac{\gamma^\ell \alpha^{\ell(\ell-1)}}{\beta^{\ell-1}}(\ell P + Q) = \lambda'^1_P \beta Q \\
\beta^4(2Q) & \frac{\gamma^2\beta^2}{\alpha}(P+2Q) & & & \\
\dots & \dots & & & \\
\beta^{\ell^2}(\ell Q) = \lambda'^0_Q 0_A & \frac{\gamma^\ell \beta^{\ell(\ell-1)}}{\alpha^{\ell-1}}(P+\ell Q) = \lambda'^1_Q \alpha P & & &
\end{array}$$

We then have

$$\lambda'^0_P = \alpha^{\ell^2}\lambda^0_P, \quad \lambda'^0_Q = \beta^{\ell^2}\lambda^0_Q, \quad \lambda'^1_P = \frac{\gamma^\ell \alpha^{(\ell(\ell-1))}}{\beta^\ell}\lambda^1_P, \quad \lambda'^1_Q = \frac{\gamma^\ell \beta^{(\ell(\ell-1))}}{\alpha^\ell}\lambda^1_Q,$$

$$e'_{W,\ell}(P,Q) = \frac{\lambda'^1_P \lambda'^0_Q}{\lambda'^0_P \lambda'^1_Q} = \frac{\lambda^1_P \lambda^0_Q}{\lambda^0_P \lambda^1_Q} = e_{W,\ell}(P,Q),$$

$$e'_{T,\ell}(P,Q) = \frac{\lambda'^1_P}{\lambda'^0_P} = \frac{\gamma^\ell}{\alpha^\ell \beta^\ell}\frac{\lambda^1_P}{\lambda^0_P} = \frac{\gamma^\ell}{\alpha^\ell \beta^\ell} e_{T,\ell}(P,Q).$$

Isogenies

Definition

A (separable) isogeny is a finite surjective (separable) morphism between two Abelian varieties.

- Isogenies = Rational map + group morphism + finite kernel.
- Isogenies $\Leftrightarrow$ Finite subgroups.

$$(f : A \to B) \mapsto \operatorname{Ker} f$$
$$(A \to A/H) \leftarrow H$$

- *Example:* Multiplication by ℓ ($\Rightarrow \ell$-torsion), Frobenius (non separable).

Cryptographic usage of isogenies

- Transfer the DLP from one Abelian variety to another.
- Point counting algorithms (ℓ-adic or p-adic) $\Rightarrow$ Verify a curve is secure.
- Compute the class field polynomials (CM-method) $\Rightarrow$ Construct a secure curve.
- Compute the modular polynomials $\Rightarrow$ Compute isogenies.
- Determine $\mathrm{End}(A)$ $\Rightarrow$ CRT method for class field polynomials.

Vélu's formula

Theorem

Let $E : y^2 = f(x)$ be an elliptic curve and $G \subset E(k)$ a finite subgroup. Then E/G is given by $Y^2 = g(X)$ where

$$X(P) = x(P) + \sum_{Q \in G \setminus \{0_E\}} (x(P+Q) - x(Q))$$

$$Y(P) = y(P) + \sum_{Q \in G \setminus \{0_E\}} (y(P+Q) - y(Q)).$$

- Uses the fact that x and y are characterised in $k(E)$ by

$$\begin{array}{rll} v_{0_E}(x) = -2 & v_P(x) \geqslant 0 & \text{if } P \neq 0_E \\ v_{0_E}(y) = -3 & v_P(y) \geqslant 0 & \text{if } P \neq 0_E \\ y^2/x^3(0_E) = 1 & & \end{array}$$

- No such characterisation in genus $g \geqslant 2$ for Mumford coordinates.

The isogeny theorem

Theorem

- *Let* $\varphi : Z(\overline{n}) \to Z(\overline{\ell n}), x \mapsto \ell.x$ *be the canonical embedding.* *Let* $K = A_2[\ell] \subset A_2[\ell n]$.
- *Let* $(\vartheta_i^A)_{i \in Z(\overline{\ell n})}$ *be the theta functions of level* ℓn *on* $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$.
- *Let* $(\vartheta_i^B)_{i \in Z(\overline{n})}$ *be the theta functions of level* n *of* $B = A/K = \mathbb{C}^g / (\mathbb{Z}^g + \frac{\Omega}{\ell} \mathbb{Z}^g)$.
- *We have:*

$$(\vartheta_i^B(x))_{i \in Z(\overline{n})} = (\vartheta_{\varphi(i)}^A(x))_{i \in Z(\overline{n})}$$

Example

$\pi : (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}) \mapsto (x_0, x_3, x_6, x_9)$ is a 3-isogeny between elliptic curves.

An example with $g = 1$, $n = 2$, $\ell = 3$

$$\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$

An example with $g=1$, $n=2$, $\ell=3$

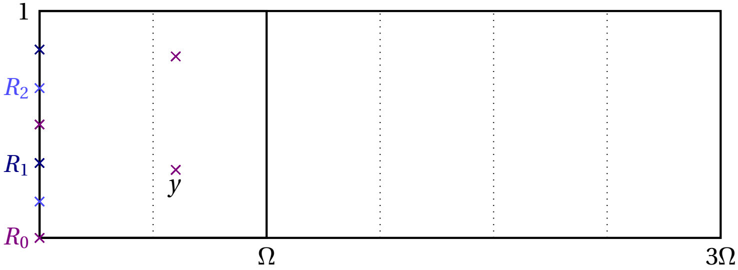
$$
\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}
$$

An example with $g=1$, $n=2$, $\ell=3$

$$
\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}
$$

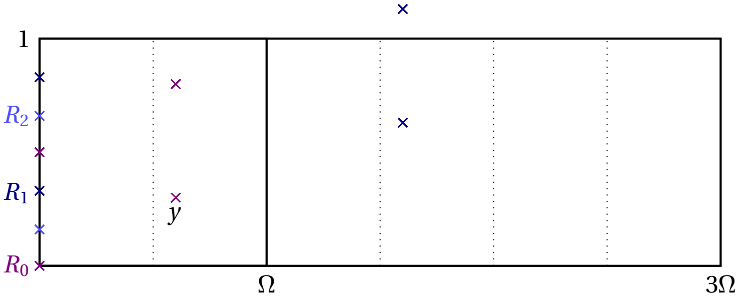
An example with $g=1$, $n=2$, $\ell=3$

$$
\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g),\ \text{level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g),\ \text{level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g),\ \text{level } n \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}
$$



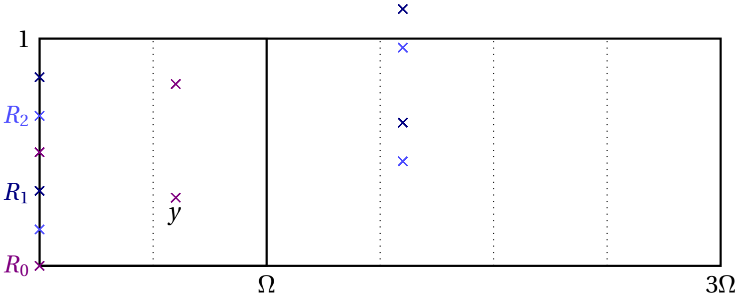
An example with $g=1$, $n=2$, $\ell=3$

$$\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$



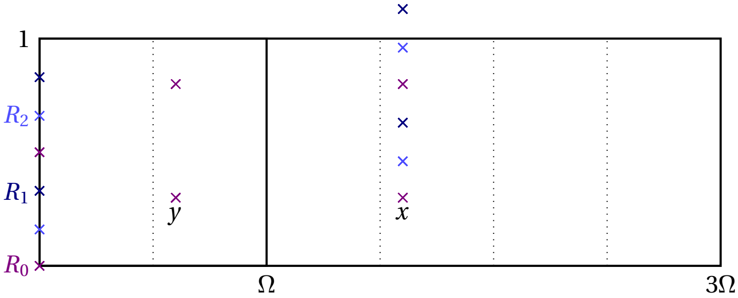
An example with $g = 1$, $n = 2$, $\ell = 3$

$$\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$



An example with $g=1$, $n=2$, $\ell=3$

$$\begin{tikzcd}[column sep=small]
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$



Changing level

Theorem (Koizumi–Kempf)

Let F be a matrix of rank r such that ${}^tFF = \ell \operatorname{Id}_r$. Let $X \in (\mathbb{C}^g)^r$ and $Y = F(X) \in (\mathbb{C}^g)^r$. Let $j \in (\mathbb{Q}^g)^r$ and $i = F(j)$. Then we have

$$\vartheta\left[\begin{smallmatrix}0\\ i_1\end{smallmatrix}\right](Y_1, \frac{\Omega}{n}) \dots \vartheta\left[\begin{smallmatrix}0\\ i_r\end{smallmatrix}\right](Y_r, \frac{\Omega}{n}) = \sum_{\substack{t_1,\dots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ F(t_1,\dots,t_r)=(0,\dots,0)}} \vartheta\left[\begin{smallmatrix}0\\ j_1\end{smallmatrix}\right](X_1 + t_1, \frac{\Omega}{\ell n}) \dots \vartheta\left[\begin{smallmatrix}0\\ j_r\end{smallmatrix}\right](X_r + t_r, \frac{\Omega}{\ell n}),$$

(This is the isogeny theorem applied to $F_A : A^r \to A^r$.)

- If $\ell = a^2 + b^2$, we take $F = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, so $r = 2$.
- In general, $\ell = a^2 + b^2 + c^2 + d^2$, we take F to be the matrix of multiplication by $a + bi + cj + dk$ in the quaternions, so $r = 4$.

$\Rightarrow$ We have a complete algorithm to compute the isogeny $A \mapsto A/K$ given the kernel K [Cosset, Lubicz, R.].

AVIsogenies

- AVIsogenies: Magma code written by Bisson, Cosset and R.
  http://avisogenies.gforge.inria.fr
- Released under LGPL 2+.
- Implement isogeny computation (and applications thereof) for abelian varieties using theta functions.
- Current release 0.2: isogenies in genus 2.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k=\mathbb{F}_q$, $J=\mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \operatorname{car} k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k=\mathbb{F}_q$, $J=\mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \operatorname{car} k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \operatorname{car} k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k=\mathbb{F}_q$, $J=\mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Computing the right extension

- $J = \mathrm{Jac}(H)$ abelian variety of dimension 2. $\chi(X)$ the corresponding zeta function.
- Degree of a point of ℓ-torsion | the order of X in $\mathbb{F}_\ell[X]/\chi(X)$.
- If K rational, $K(\overline{k}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, the degree of a point in K | the LCM of orders of X in $\mathbb{F}_\ell[X]/P(X)$ for $P \mid \chi$ of degree two.
- Since we are looking to K maximal isotropic, $J[\ell] \simeq K \oplus K'$ and we know that $P \mid \chi$ is such that $\chi(X) \equiv P(X)P(\overline{X}) \mod \ell$ where $\overline{X} = q/X$ represents the Verschiebung.

Remark

The degree n is $\leqslant \ell^2 - 1$. If ℓ is totally split in $\mathbb{Z}[\pi, \overline{\pi}]$ then $n \mid \ell - 1$.

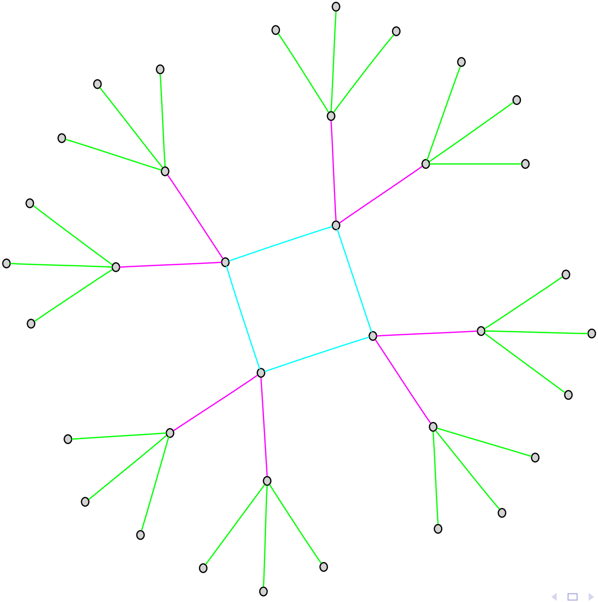
Computing the ℓ-torsion

- We want to compute $J(\mathbb{F}_{q^n})[\ell]$.
- From the zeta function $\chi(X)$ we can compute random points in $J(\mathbb{F}_{q^n})[\ell^\infty]$ uniformly.
- If P is in $J(\mathbb{F}_{q^n})[\ell^\infty]$, $\ell^m P \in J(\mathbb{F}_{q^n})[\ell]$ for a suitable m. This does not give uniform points of ℓ-torsion but we can correct the points obtained.

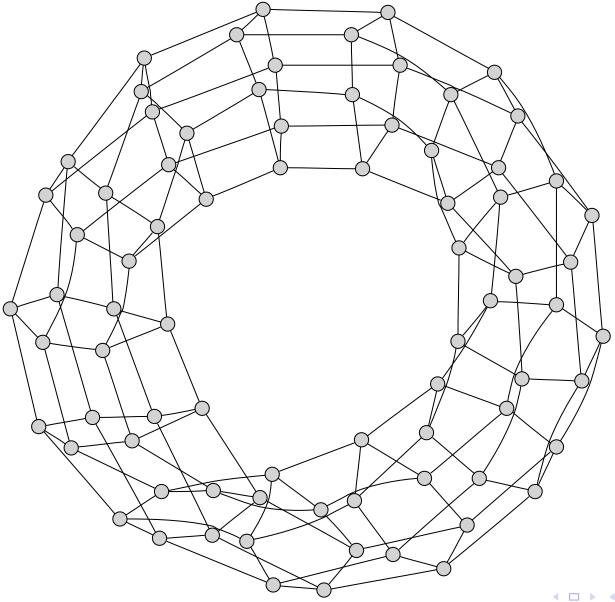
Example

- Suppose $J(\mathbb{F}_{q^n})[\ell^\infty] = < P_1, P_2 >$ with P_1 of order ℓ^2 and P_2 of order ℓ.
- First random point $Q_1 = P_1 \Rightarrow$ we recover the point of ℓ-torsion: $\ell.P_1$.
- Second random point $Q_2 = \alpha P_1 + \beta P_2$. If $\alpha \neq 0$ we recover the point of ℓ-torsion $\alpha \ell P_1$ which is not a new generator.
- We correct the original point: $Q_2' = Q_2 - \alpha Q_1 = \beta P_2$.

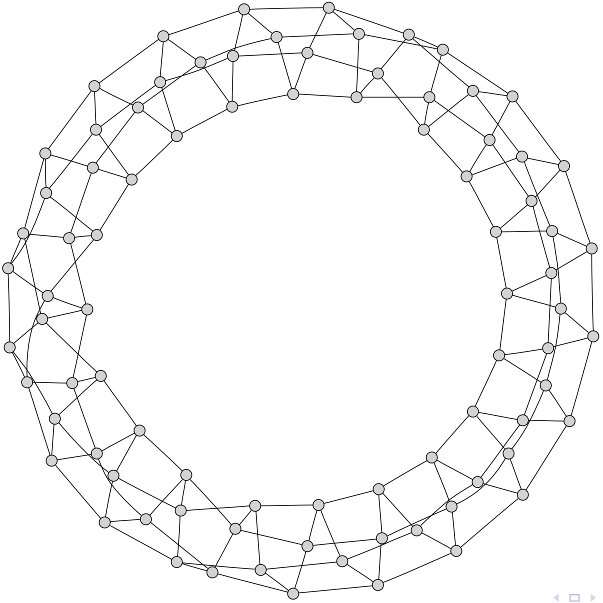
Isogeny graphs for elliptic curves



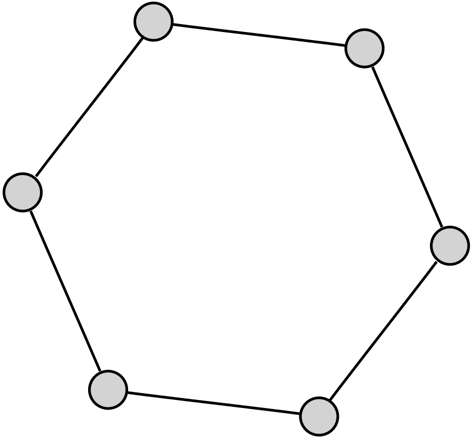
Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$



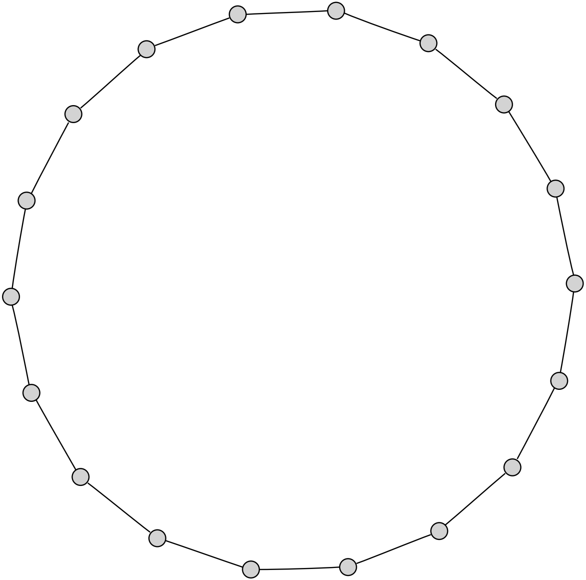
Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2 \overline{Q}_2$



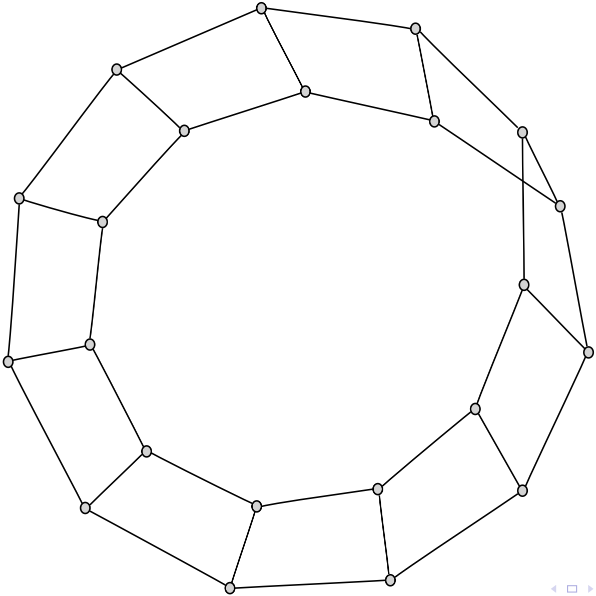
Horizontal isogeny graphs: $\ell = q = Q\overline{Q}$ $(\mathbb{Q} \longmapsto K_0 \longmapsto K)$



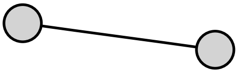
Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2^2$



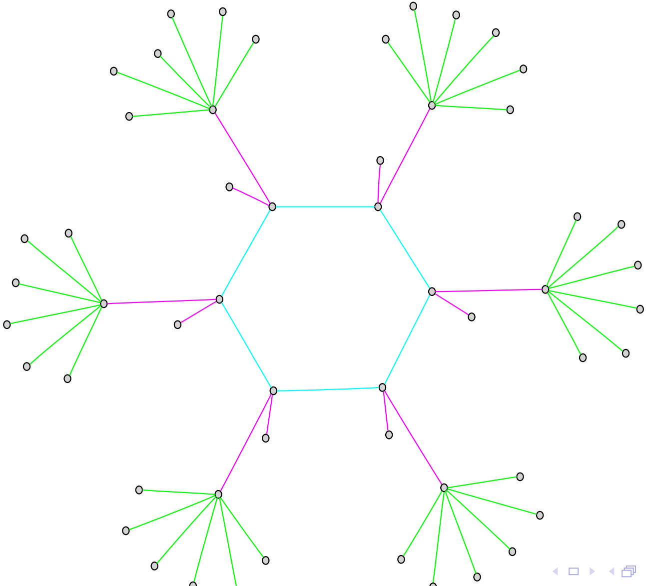
Horizontal isogeny graphs: $\ell = q^2 = Q^2\overline{Q}^2$

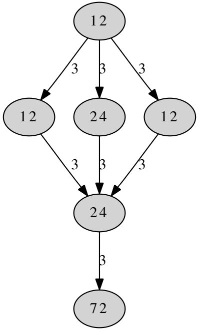


Horizontal isogeny graphs: $\ell = q^2 = Q^4$

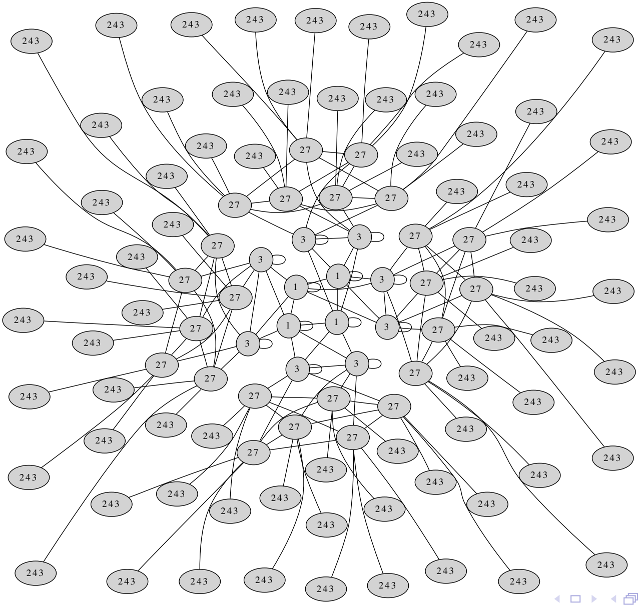


General isogeny graphs ($\ell = q = Q\overline{Q}$)

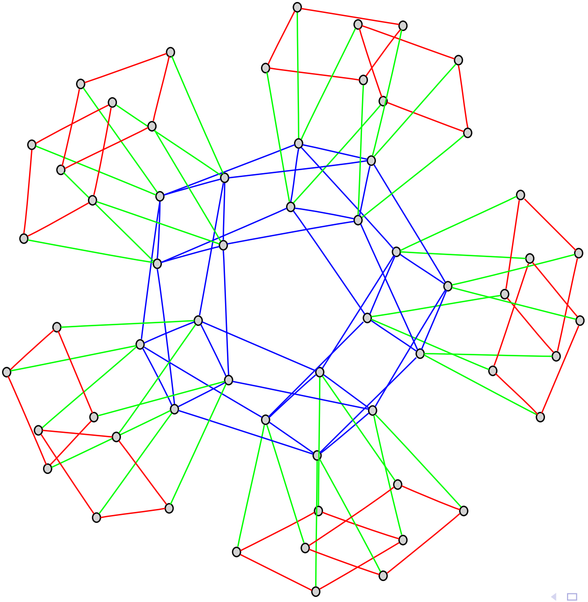




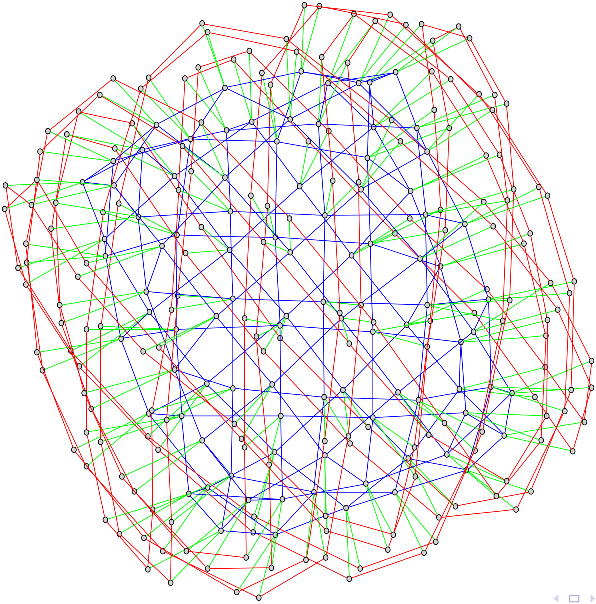
General isogeny graphs ($\ell = q = Q\overline{Q}$)



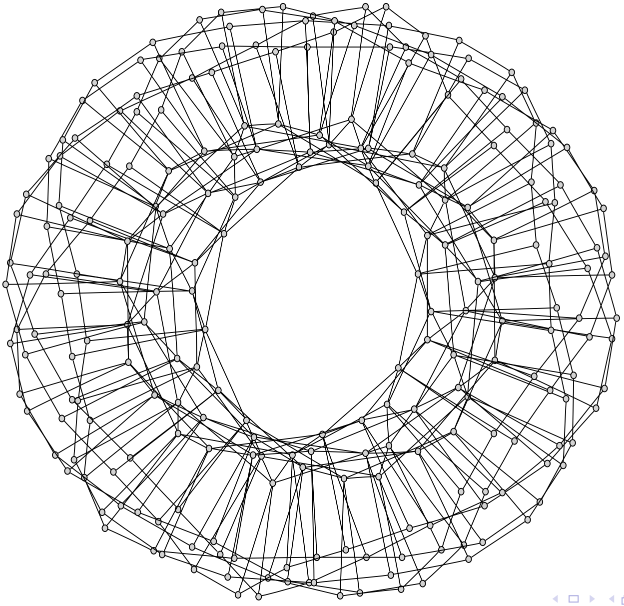
General isogeny graphs ($\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$)



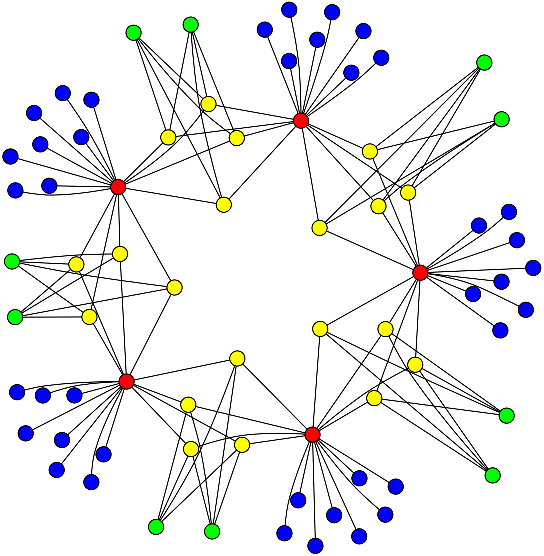
General isogeny graphs ($\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$)



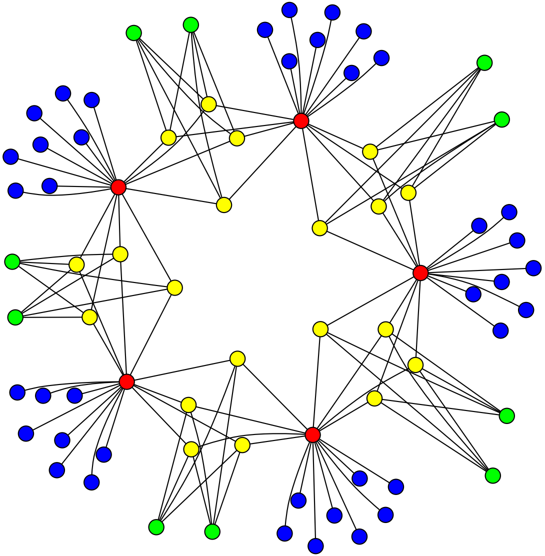
General isogeny graphs ($\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$)

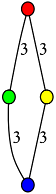


Isogeny graph and lattice of orders in genus 2

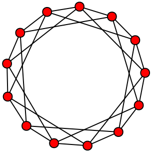


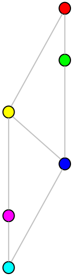
Isogeny graph and lattice of orders in genus 2



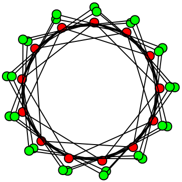


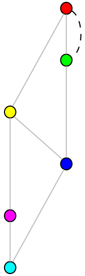
Isogeny graph and lattice of orders in genus 2



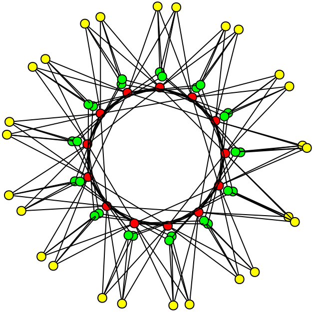


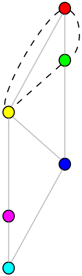
Isogeny graph and lattice of orders in genus 2



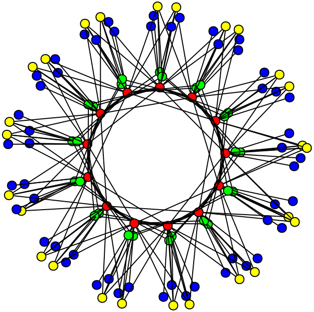


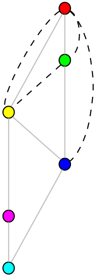
Isogeny graph and lattice of orders in genus 2



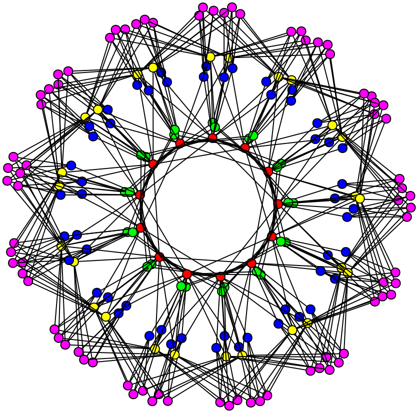


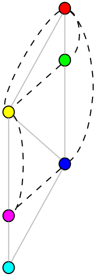
Isogeny graph and lattice of orders in genus 2



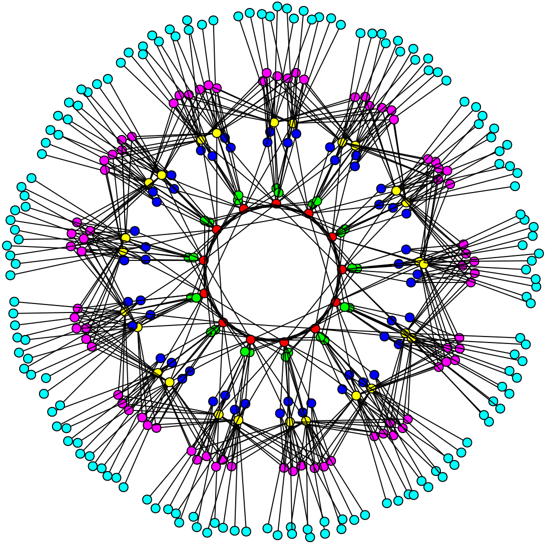


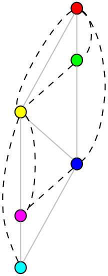
Isogeny graph and lattice of orders in genus 2





Isogeny graph and lattice of orders in genus 2

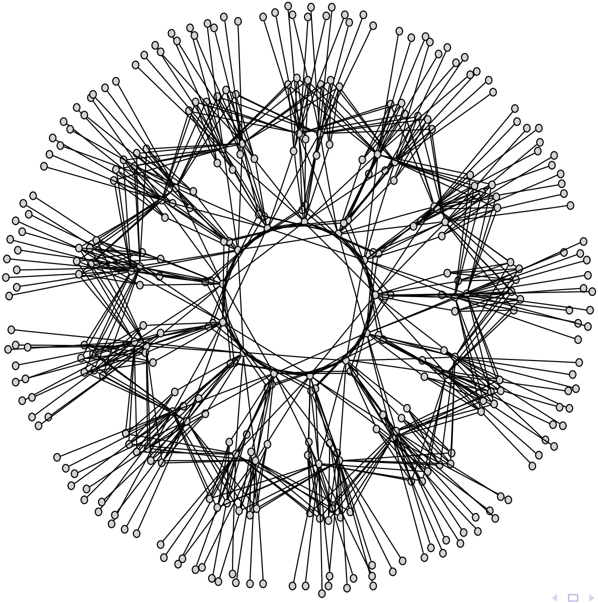




Applications and perspectives

- Modular polynomials in genus 2.
- Isogenies using rational coordinates?
- How to compute cyclic isogenies in genus 2?
- Dimension 3.

Thank you for your attention!



Bibliography

[BF03] D. Boneh and M. Franklin. "Identity-based encryption from the Weil pairing". In: *SIAM Journal on Computing* 32.3 (2003), pp. 586–615 (cit. on p. 4).

[BLS04] D. Boneh, B. Lynn, and H. Shacham. "Short signatures from the Weil pairing". In: *Journal of Cryptology* 17.4 (2004), pp. 297–319 (cit. on p. 4).

[GPS+06] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-based encryption for fine-grained access control of encrypted data". In: *Proceedings of the 13th ACM conference on Computer and communications security*. ACM. 2006, p. 98 (cit. on p. 4).

[Jou04] A. Joux. "A one round protocol for tripartite Diffie–Hellman". In: *Journal of Cryptology* 17.4 (2004), pp. 263–276 (cit. on p. 4).

[SW05] A. Sahai and B. Waters. "Fuzzy identity-based encryption". In: *Advances in Cryptology–EUROCRYPT 2005* (2005), pp. 457–473 (cit. on p. 4).

[Ver01] E. Verheul. "Self-blindable credential certificates from the Weil pairing". In: *Advances in Cryptology—ASIACRYPT 2001* (2001), pp. 533–551 (cit. on p. 4).