Abelian varieties, theta functions and cryptography

Damien Robert[1]

[1] LFANT Team, IMB & Inria Bordeaux Sud-Ouest

10/02/2011 (Luminy)

Outline

1. Public-key cryptography
2. Abelian varieties, Arithmetic and Pairings
3. Isogenies

A brief history of public-key cryptography

- Secret-key cryptography: Vigenère (1553), One time pad (1917), AES (NIST, 2001).
- Public-key cryptography:
  - Diffie–Hellman key exchange (1976).
  - RSA (1978): multiplication/factorisation.
  - ElGamal: exponentiation/discrete logarithm in $G = \mathbb{F}_q^*$.
  - ECC/HECC (1985): discrete logarithm in $G = A(\mathbb{F}_q)$.
  - Lattices, NTRU (1996), Ideal Lattices (2006): perturbate a lattice point/Closest Vector Problem, Bounded Distance Decoding.
  - Polynomial systems, HFE (1996): evaluating polynomials/finding roots.
  - Coding-based cryptography, McEliece (1978): Matrix.vector/decoding a linear code.

  ⇒ Encryption, Signature (+Pseudo Random Number Generator, Zero Knowledge).
- Pairing-based cryptography (2000–2001).
- Homomorphic cryptography (2009).

RSA versus (H)ECC

Security (bits level)	RSA	ECC
72	1008	144
80	1248	160
96	1776	192
112	2432	224
128	3248	256
256	15424	512

Key length comparison between RSA and ECC

- Factorisation of a 768-bit RSA modulus [KAF+10].
- Currently: attempt to attack a 130-bit Koblitz elliptic curve.

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).
- $G = \mathbb{F}_p^*$: sub-exponential attacks.

⇒ Find secure groups with efficient law, compact representation.

Protocol [Diffie–Hellman Key Exchange]

Alice sends g^a, Bob sends g^b, the common key is

$$g^{ab} = (g^b)^a = (g^a)^b.$$

Pairing-based cryptography

Definition

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

- Identity-based cryptography [BF03].
- Short signature [BLS04].
- One way tripartite Diffie–Hellman [Jou04].
- Self-blindable credential certificates [Ver01].
- Attribute based cryptography [SW05].
- Broadcast encryption [GPSW06].

Tripartite Diffie–Helman

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

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

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.

⇒ Use $G = A(k)$ with $k = \mathbb{F}_q$ for the DLP.

Pairings on abelian varieties

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

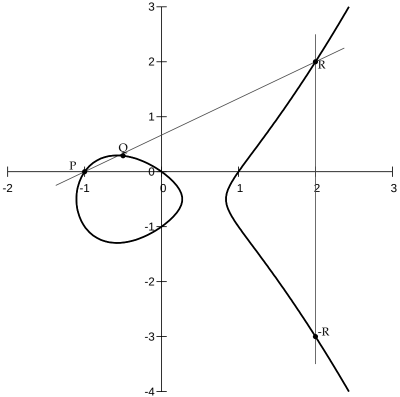
$$e_W : A[\ell] \times A[\ell] \to \mu_\ell \subset \mathbb{F}_{q^k}^*.$$

Elliptic curves

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

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

- An elliptic curve is a plane curve of genus 1.
- Elliptic curves = Abelian varieties of dimension 1.



$$P + Q = -R = (x_R, -y_R)$$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$x_R = \lambda^2 - x_P - x_Q$$

$$y_R = y_P + \lambda(x_R - x_P)$$

Jacobian of hyperelliptic curves

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

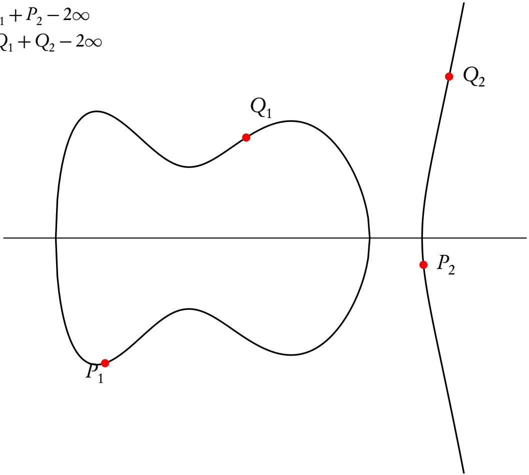
- Divisor: formal sum $D = \sum n_i P_i$, $P_i \in C(\overline{k})$.
  $\deg D = \sum n_i$.
- Principal divisor: $\sum_{P \in C(\overline{k})} v_P(f).P$; $f \in \overline{k}(C)$.
- Jacobian of C = Divisors of degree 0 modulo principal divisors
  + Galois action
  = Abelian variety of dimension g.
- Divisor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

Example of the addition law in genus 2

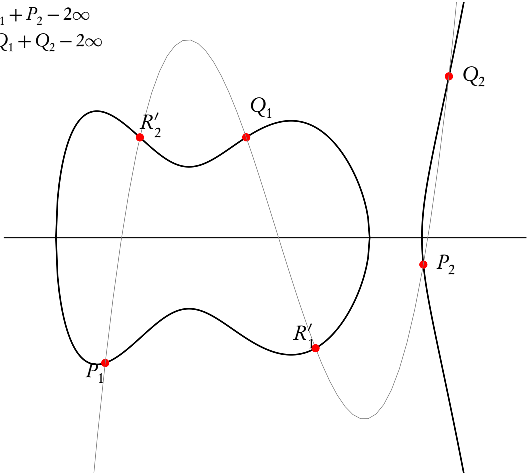
$$D = P_1 + P_2 - 2\infty$$
$$D' = Q_1 + Q_2 - 2\infty$$



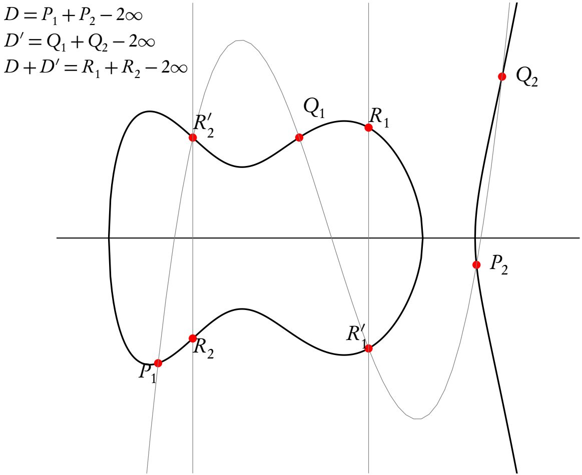
Example of the addition law in genus 2

$D = P_1 + P_2 - 2\infty$

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



Example of the addition law in genus 2



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

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 hyperelliptic curve)
		$\tilde{O}(q)$ (Jacobian of non hyperelliptic curve)
g	$O(q^g)$	$\tilde{O}(q^{2-2/g})$
$g > \log(q)$		$L_{1/2}(q^g) = \exp(O(1)\log(x)^{1/2}\log\log(x)^{1/2})$

Security of the DLP

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

⇒ Public-key cryptography with the DLP: Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

⇒ Pairing-based cryptography: Abelian varieties of dimension $g \leqslant 4$.

Security of abelian varieties

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

Security of the DLP

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

⇒ Public-key cryptography with the DLP: Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

⇒ Pairing-based cryptography: Abelian varieties of dimension $g \leqslant 4$.

Complex abelian varieties

- Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, where $\Omega \in \mathscr{H}_g(\mathbb{C})$ the Siegel upper half space.
- The theta functions with characteristic give a lot of 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:

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

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:

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

- $(\vartheta_i)_{i\in Z(\overline{n})}$: 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 $\chi\in\hat{Z}(\overline{2}), i,j,k,l\in Z(\overline{n})$

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

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

Arithmetic with low level theta functions (car $k \neq 2$)

	Mumford [Lan05]	Level 2 [Gau07]	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	Level 4
Doubling	$5M+4S+1m_0$	$3M+6S+3m_0$	$3M+5S$	$9M+10S+5$
Mixed Addition			$7M+6S+1m_0$	

Multiplication cost in genus 1 (one step).

Arithmetic with high level theta functions [LR10a]

- Algorithms for
  - Additions and differential additions in level 4.
  - Computing $P \pm Q$ in level 2 (need one square root). [LR10b]
  - Fast differential multiplication.
- Compressing coordinates $O(1)$:
  - Level $2n$ theta null point $\Rightarrow 1+g(g+1)/2$ level 2 theta null points.
  - Level $2n \Rightarrow 1+g$ level 2 theta functions.
- Decompression: n^g differential additions.

The Weil and Tate pairing with theta coordinates [LR10b]

P and Q points of ℓ-torsion.

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

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

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) ⇒ Verify a curve is secure.
- Compute the class field polynomials (CM-method) ⇒ Construct a secure curve.
- Compute the modular polynomials ⇒ Compute isogenies.
- Determine $\mathrm{End}(A)$ ⇒ 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

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

- 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 $g = 1$, $n = 2$, $\ell = 3$

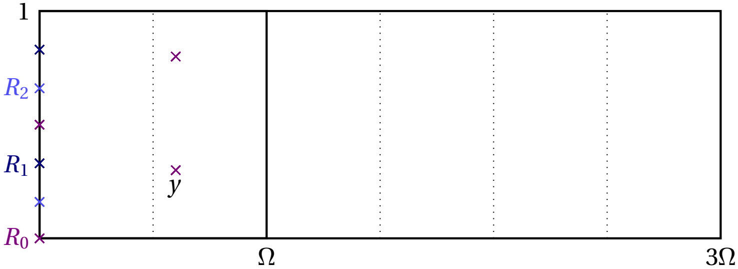
$$\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level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

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

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

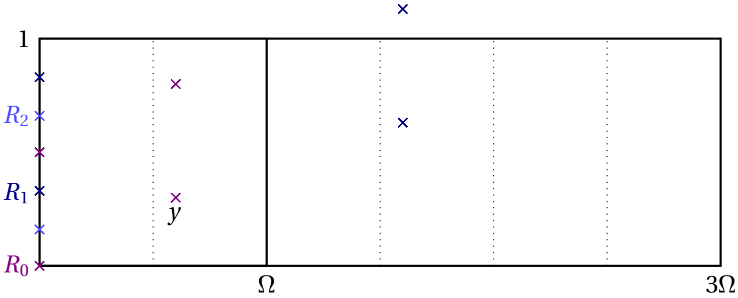
An example with $g = 1$, $n = 2$, $\ell = 3$

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



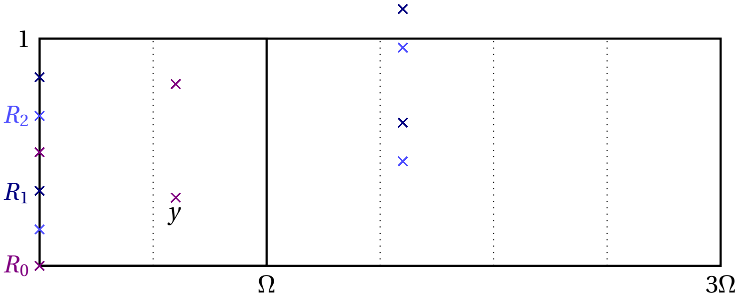
An example with $g=1$, $n=2$, $\ell=3$

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



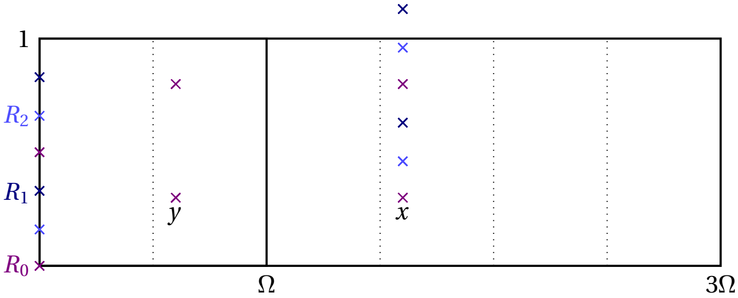
An example with $g = 1$, $n = 2$, $\ell = 3$

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



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

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



Changing level

Theorem (Koizumi–Kempf)

Let F be a matrix of rank r such that ${}^t F F = \ell \,\mathrm{Id}_r$. 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

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

- If $\ell = a^2 + b^2$, we take $F = \left(\begin{smallmatrix} a & b \\ -b & a\end{smallmatrix}\right)$, 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 $r = 4$.

Computing isogenies [Cosset, Lubicz, R.]

- Let A/k be an abelian variety of dimension g over k given in theta coordinates. Let $K \subset A$ be a maximal isotropic subgroup of $A[\ell]$ (ℓ prime to 2 and the characteristic). Then we have an algorithm to compute the isogeny $A \mapsto A/K$.
- Need $O(\#K)$ differential additions in A + $O(\ell^g)$ or $O(\ell^{2g})$ multiplications $\Rightarrow$ fast.
- The formulas are rational if the kernel K is rational.

$\Rightarrow$ Work in level 2.

$\Rightarrow$ Convert back and forth to Mumford coordinates:

$$\begin{tikzcd}
A \arrow[r, "\widehat{\pi}"] \arrow[d, equal] & B \arrow[d, equal] \\
\mathrm{Jac}(C_1) \arrow[r, dotted] & \mathrm{Jac}(C_2)
\end{tikzcd}$$

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, $2\ell \wedge \operatorname{car} k = 1$. 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 $k = \mathbb{F}_q$, $J = \operatorname{Jac}(H)$, ℓ odd prime, $2\ell \wedge \operatorname{car} k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \operatorname{Jac}(H')$ (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 $k = \mathbb{F}_q$, $J = \operatorname{Jac}(H)$, ℓ odd prime, $2\ell \wedge \operatorname{car} k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \operatorname{Jac}(H')$ (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 $J \longmapsto \mathrm{Jac}(H')$ (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, $2\ell \wedge \operatorname{car} k = 1$. 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.

Timings for isogenies computations $(\ell = 7)$

```
Jacobian of Hyperelliptic Curve defined by y^2 = t^254*x^6 + t^223*
  t^255*x^4 + t^318*x^3 + t^668*x^2 + t^543*x + t^538 over GF(3^6)
> time RationallyIsogenousCurvesG2(J,7);
** Computing  7 -rationnal isotropic subgroups
  -- Computing the 7 -torsion over extension of deg 4
  !! Basis: 2 points in Finite field of size 3^24
  -- Listing subgroups
  1 subgroups over Finite field of size 3^24
  -- Convert the subgroups to theta coordinates
  Time: 0.060
Computing the 1 7 -isogenies
  ** Precomputations for l= 7 Time: 0.180
  ** Computing the 7 -isogeny
    Computing the l-torsion Time: 0.030
    Changing level Time: 0.210
  Time: 0.430
Time: 0.490
[ <[ t^620, t^691, t^477 ], Jacobian of Hyperelliptic Curve defined
y^2 = t^615*x^6 + t^224*x^5 + t^37*x^4 + t^303*x^3 + t^715*x^2 + t^
```

Timings for isogenies computations $(\ell = 5)$

```
Jacobian of Hyperelliptic Curve defined by y^2 = 39*x^6 + 4*x^5 + 8
  + 10*x^3 + 31*x^2 + 39*x + 2 over GF(83)
> time RationallyIsogenousCurvesG2(J,5);
** Computing  5 -rationnal isotropic subgroups
  -- Computing the 5 -torsion over extension of deg 24
  Time: 0.940
  !! Basis: 4 points in Finite field of size 83^24
  -- Listing subgroups
  Time: 1.170
  6 subgroups over Finite field of size 83^24
  -- Convert the subgroups to theta coordinates
  Time: 0.360
Time: 2.630
Computing the 6 5 -isogenies
Time: 0.820
Time: 3.460
 [ <[ 36, 69, 38 ], Jacobian of Hyperelliptic Curve defined by
 y^2 = 27*x^6 + 63*x^5 + 5*x^4 + 24*x^3 + 34*x^2 + 6*x + 76 over GF
   ...]
```

Timings for isogeny graphs $(\ell = 3)$

```
Jacobian of Hyperelliptic Curve defined by y^2 = 41*x^6 + 131*x^5 +
  55*x^4 + 57*x^3 + 233*x^2 + 225*x + 51 over GF(271)
time isograph,jacobians:=IsoGraphG2(J,{3}: save_mem:=-1);
Computed 540 isogenies and found 135 curves.
Time: 14.410
```

- Core 2 with 4BG of RAM.
- Computing kernels: $\approx 5s$.
- Computing isogenies: $\approx 7s$ (Torsion: $\approx 2s$, Changing level: $\approx 3.5s$.)

Going further $(\ell = 53)$

```
Jacobian of Hyperelliptic Curve defined by y^2 = 97*x^6 + 77*x^5 +
  62*x^4 + 14*x^3 + 33*x^2 + 18*x + 40 over GF(113)
> time RationallyIsogenousCurvesG2(J,53);
** Computing  53 -rationnal isotropic subgroups
  -- Computing the 53 -torsion over extension of deg 52 Time: 8.610
  !! Basis: 3 points in Finite field of size 113^52
  -- Listing subgroups Time: 1.210
  2 subgroups over Finite field of size 113^52
  -- Convert the subgroups to theta coordinates Time: 0.100
  Time: 9.980
Computing the 2 53 -isogenies
  ** Precomputations for l= 53 Time: 0.240
  ** Computing the 53 -isogeny
    Computing the l-torsion Time: 7.570
    Changing level Time: 1.170
  Time: 8.840
  ** Computing the 53 -isogeny
  Time: 8.850
Time: 27.950
```

Going further $(\ell = 19)$

```
  Jacobian of Hyperelliptic Curve defined by y^2 = 194*x^6 + 554*x^
  606*x^4 + 523*x^3 + 642*x^2 + 566*x + 112 over GF(859)
  > time RationallyIsogenousCurvesG2(J,19);
  ** Computing  19 -rationnal isotropic subgroups (extension degree
  Time: 0.760
Computing the 2 19 -isogenies
  ** Precomputations for l= 19 Time: 11.160
  ** Computing the 19 -isogeny
    Computing the l-torsion Time: 0.250
    Changing level Time: 18.590
  Time: 18.850
  ** Computing the 19 -isogeny
    Computing the l-torsion Time: 0.250
    Changing level Time: 18.640
  Time: 18.900
Time: 51.060
[ <[ 341, 740, 389 ], Jacobian of Hyperelliptic Curve defined by y^
    680*x^5 + 538*x^4 + 613*x^3 + 557*x^2 + 856*x + 628 over GF(859
  ... ]
```

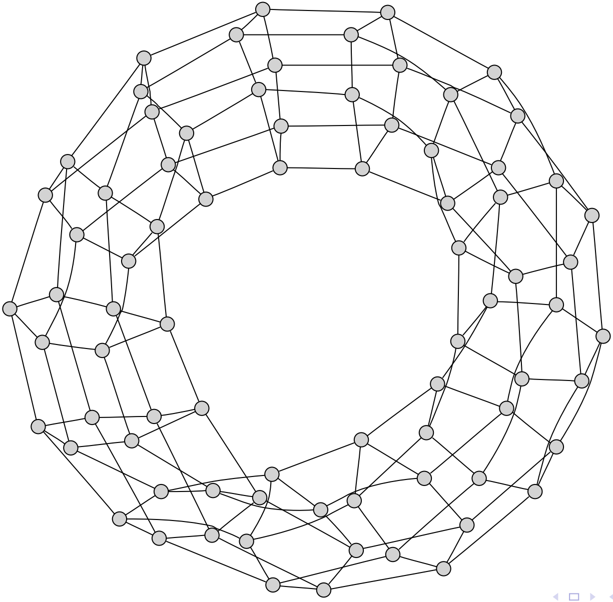
A record isogeny computation! $(\ell = 1321)$

- J Jacobian of $y^2 = x^5 + 41691x^4 + 24583x^3 + 2509x^2 + 15574x$ over $\mathbb{F}_{42179}$.
- $\#J = 2^{10}1321^2$.

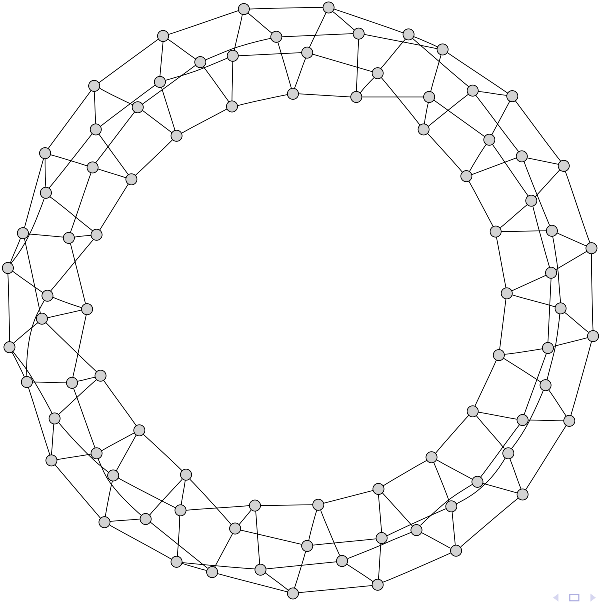
```
> time RationallyIsogenousCurvesG2(J,1321:ext_degree:=1);
** Computing  1321 -rationnal isotropic subgroups
Time: 0.350
Computing the 1 1321 -isogenies
  ** Precomputations for l= 1321
  Time: 1276.950
  ** Computing the 1321 -isogeny
    Computing the l-torsion
    Time: 1200.270
    Changing level
    Time: 1398.780
  Time: 5727.250
Time: 7004.240
Time: 7332.650
[ <[ 9448, 15263, 31602 ], Jacobian of Hyperelliptic Curve defined
  y^2 = 33266*x^6 + 20155*x^5 + 31203*x^4 + 9732*x^3 +
  4204*x^2 + 18026*x + 29732 over GF(42179)> ]
```

- Computed with [illegible]GB of RAM

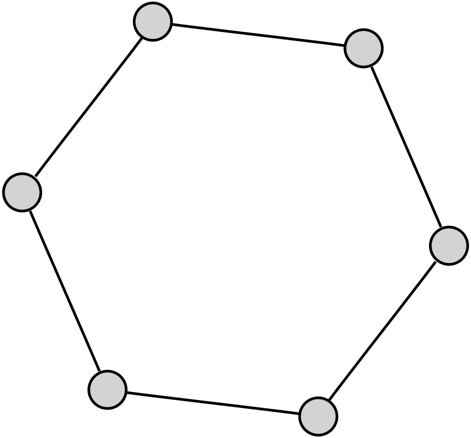
Isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



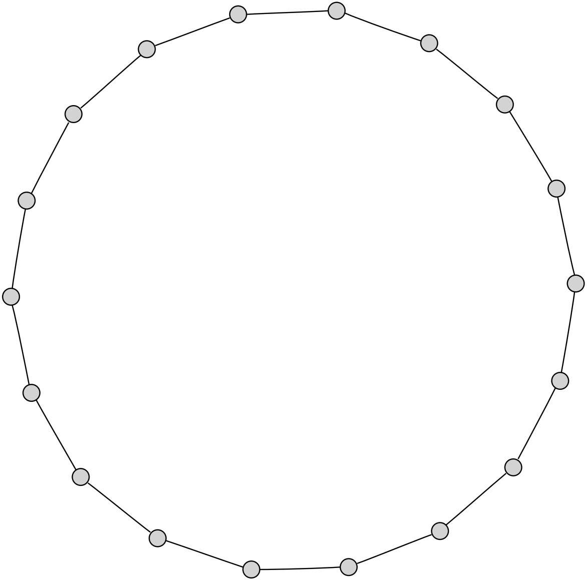
Isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



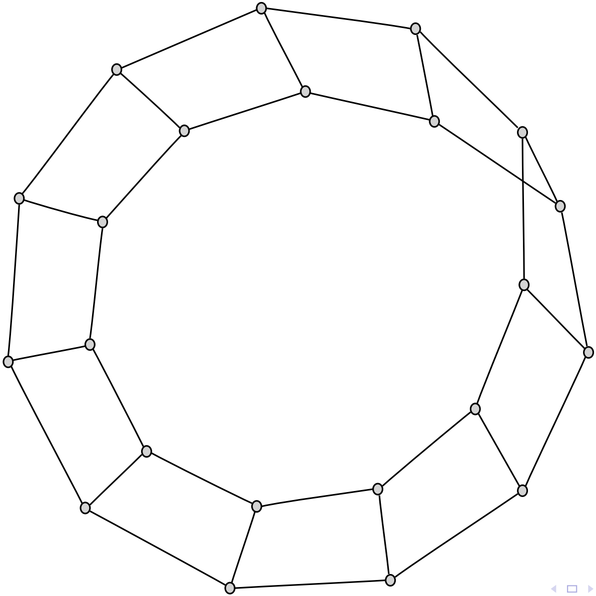
Isogeny graphs: $\ell = q = Q\overline{Q}$ $(\mathbb{Q} \longmapsto K_0 \longmapsto K)$



Isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2^2$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$

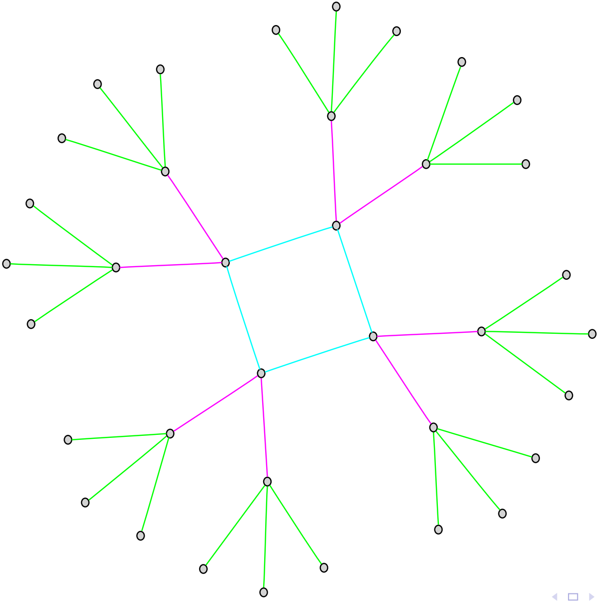


Isogeny graphs: $\ell = q^2 = Q^2\overline{Q}^2$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$

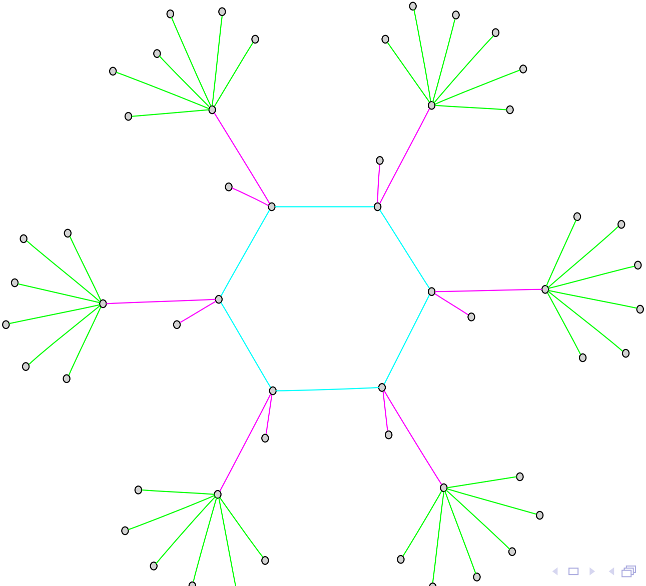


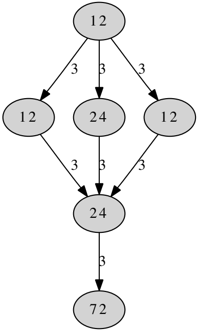
Isogeny graphs: $\ell = q^2 = Q^4$ $(\mathbb{Q} \longmapsto K_0 \longmapsto K)$

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

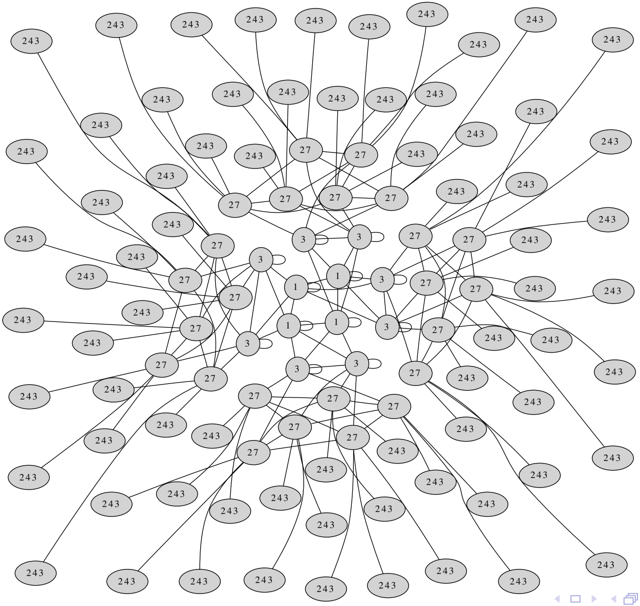


Non maximal isogeny graphs ($\ell = q = Q\overline{Q}$)

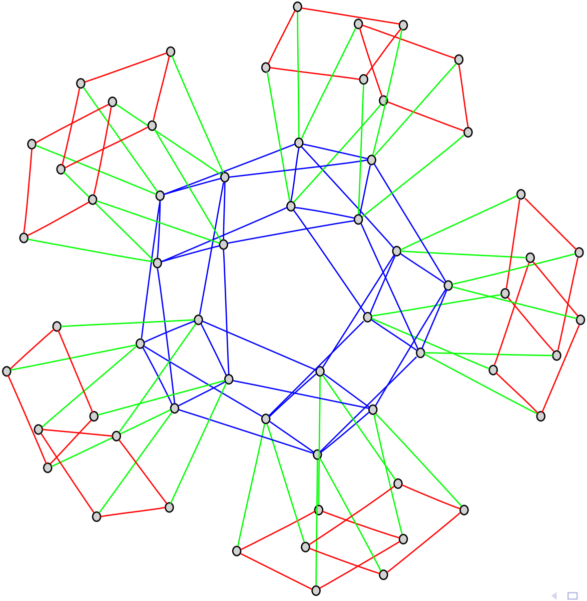




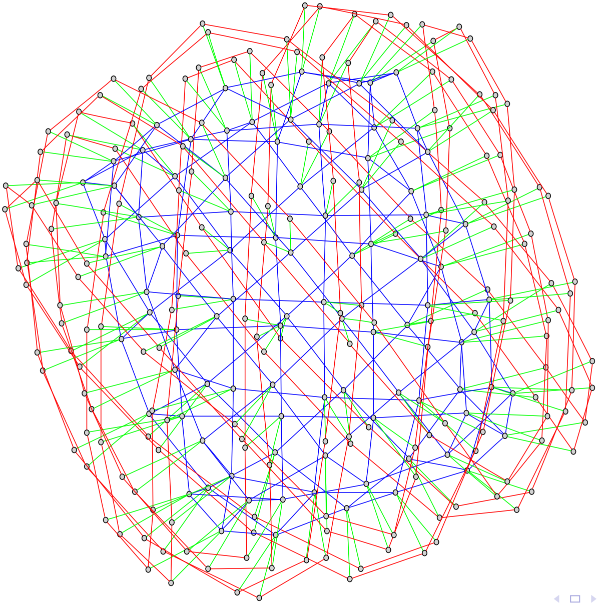
Non maximal isogeny graphs ($\ell = q = Q\overline{Q}$)



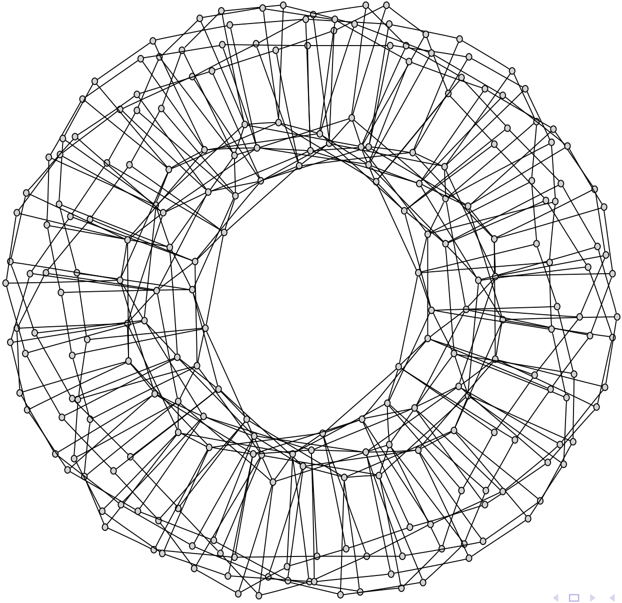
Non maximal isogeny graphs $(\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2})$



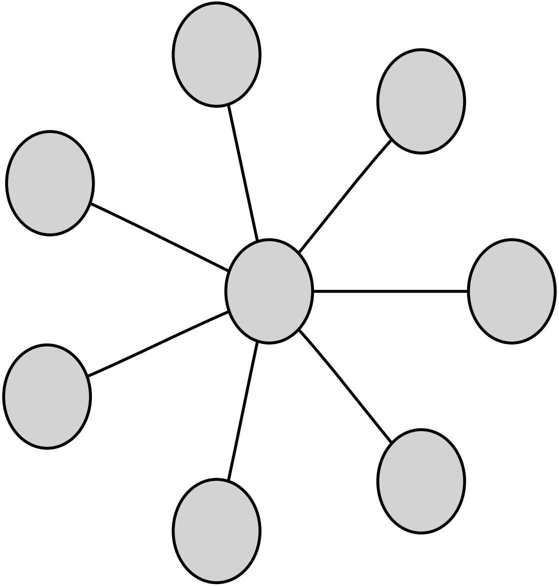
Non maximal isogeny graphs ($\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$)



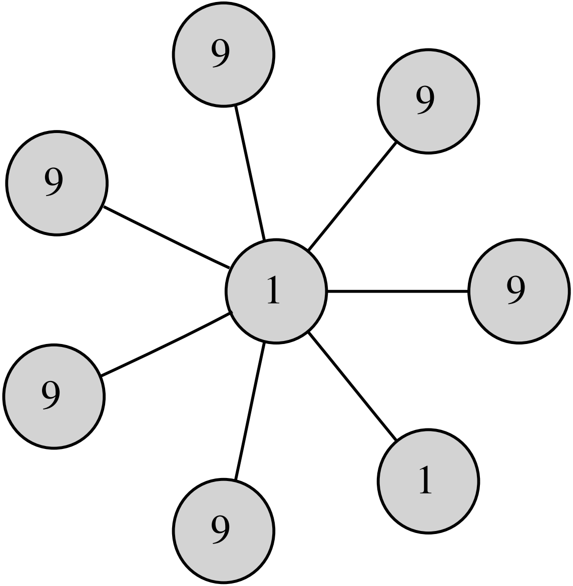
Non maximal isogeny graphs ($\ell = q_1 q_2 = Q_1\overline{Q_1}Q_2\overline{Q_2}$)



Non maximal isogeny graphs ($\ell = q = Q^2$)



Non maximal isogeny graphs ($\ell = q = Q^2$)

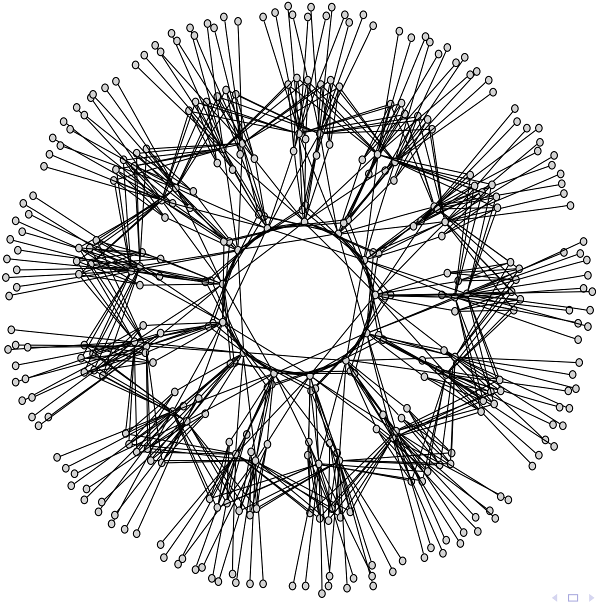


Applications and perspectives

- Computing endomorphism ring. Generalize [BS09] to higher genus, work by Bisson.
- Class polynomials in genus 2 using the CRT. If K is a CM field and $J/\mathbb{F}_p$ is such that $\mathrm{End}(J) \otimes_{\mathbb{Z}} \mathbb{Q} = K$, use isogenies to find the Jacobians whose endomorphism ring is O_K. Work by Lauter+R.

- Modular polynomials in genus 2 using theta null points: computed by Gruenewald using analytic methods for $\ell = 3$.
- Isogenies using rational coordinates? Work by Smith using the geometry of Kummer surfaces for $\ell = 3$ $(g = 2)$. Cassels and Flynn: modification of theta coordinates to have rational coordinates on hyperelliptic curves of genus 2.
- How to compute $(\ell, 1)$-isogenies in genus 2?
- Look at $g = 3$ (associate theta coordinates to the Jacobian of a non hyperelliptic curve).

Thank you for your attention!



Bibliography

[BS09] G. Bisson and A. Sutherland. “Computing the endomorphism ring of an ordinary elliptic curve over a finite field”. In: *Journal of Number Theory* (2009) (cit. on p. 64).

[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. 6).

[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. 6).

[Gau07] P. Gaudry. “Fast genus 2 arithmetic based on Theta functions”. In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 18).

[GPSW06] 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. 6).

[Jou04] A. Joux. “A one round protocol for tripartite Diffie–Hellman”. In: *Journal of Cryptology* 17.4 (2004), pp. 263–276 (cit. on p. 6).

[KAF+10] T. Kleinjung, K. Aoki, J. Franke, et al. “Factorization of a 768-bit RSA modulus”. In: (2010) (cit. on p. 4).

[Lan05] T. Lange. “Formulae for arithmetic on genus 2 hyperelliptic curves”. In: *Applicable Algebra in Engineering, Communication and Computing* 15.5 (2005), pp. 295–328 (cit. on p. 18).

[LR10a] D. Lubicz and D. Robert. *Computing isogenies between abelian varieties*. 2010. arXiv:1001.2016. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf. HAL: hal-00446062.

[LR10b] D. Lubicz and D. Robert. "Efficient pairing computation with theta functions". In: *Algorithmic Number Theory*. Lecture Notes in Comput. Sci. 6197 (July 2010). Ed. by G. Hanrot, F. Morain, and E. Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. DOI: 10.1007/978-3-642-14518-6_21. URL: http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. Slides http://www.normalesup.org/~robert/publications/slides/2010-07-ants.pdf.

[SW05] A. Sahai and B. Waters. "Fuzzy identity-based encryption". In: *Advances in Cryptology–EUROCRYPT 2005* (2005), pp. 457–473 (cit. on p. 6).

[Ver01] E. Verheul. "Self-blindable credential certificates from the Weil pairing". In: *Advances in Cryptology—ASIACRYPT 2001* (2001), pp. 533–551 (cit. on p. 6).