Isogenies, Polarisations and Real Multiplication

2015/10/06 — **Journées C2** — La Londe-Les-Maures

Gaëtan Bisson, Romain Cosset, Alina Dudeanu, Sorina Ionica, Dimitar Jetchev, David Lubicz, Chloe Martindale, Enea Milio, **Damien Robert**, Marco Streng

Outline

Isogenies between elliptic curves

Definition

An isogeny is a (non trivial) algebraic map $f: E_1 \to E_2$ between two elliptic curves such that $f(P+Q) = f(P) + f(Q)$ for all geometric points $P, Q \in E_1$.

Theorem

An algebraic map $f: E_1 \to E_2$ is an isogeny if and only if $f(0_{E_1}) = 0_{E_2}$

Corollary

An algebraic map between two elliptic curves is either

- *trivial (i.e. constant)*
- *or the composition of a translation with an isogeny.*

Remark

- Isogenies are surjective (on the geometric points). In particular, if E is ordinary, any curve isogenous to E is also ordinary.
- Two elliptic curves over $\mathbb{F}_q$ are isogenous if and only if they have the same number of points (Tate).

Algorithmic aspect of isogenies

- Given a kernel $K \subset E(\overline{k})$ compute the isogenous elliptic curve E/K ;
- Given a kernel $K \subset E(\overline{k})$ and $P \in E(k)$ compute the image of P under the isogeny $E \to E/K$;
- Given a kernel $K \subset E(\overline{k})$ compute the map $E \to E/K$;
- Given an elliptic curve E/k compute all isogenous (of a certain degree d) elliptic curves E' ;
- Given two elliptic curves E_1 and E_2 check if they are d-isogenous and if so compute the kernel $K \subset E_1(\overline{k})$.

Algorithmic aspect of isogenies

- Given a kernel $K \subset E(\overline{k})$ compute the isogenous elliptic curve E/K (Vélu's formulae [Vél71]);
- Given a kernel $K \subset E(\overline{k})$ and $P \in E(k)$ compute the image of P under the isogeny $E \to E/K$ (Vélu's formulae [Vél71]);
- Given a kernel $K \subset E(\overline{k})$ compute the map $E \to E/K$ (formal version of Vélu's formulae [Koh96]);
- Given an elliptic curve E/k compute all isogenous (of a certain degree d) elliptic curves E' (Modular polynomial [Eng09; BLS12]);
- Given two elliptic curves E_1 and E_2 check if they are d-isogenous and if so compute the kernel $K \subset E_1(\overline{k})$ (Elkie's method via a differential equation [Elk92; Bos+08]).

$\Rightarrow$ We have quasi-linear algorithms for all these aspects of isogeny computation over elliptic curves.

Destructive cryptographic applications

- An isogeny $f : E_1 \to E_2$ transports the DLP from E_1 to E_2. This can be used to attack the DLP on E_1 if there is a weak curve on its isogeny class (and an efficient way to compute an isogeny to it).

Example

- Extend attacks using Weil descent [GHS02]
- Transfert the DLP from the Jacobian of an hyperelliptic curve of genus 3 to the Jacobian of a quartic curve [Smi09].

Constructive cryptographic applications

- One can recover informations on the elliptic curve E modulo ℓ by working over the ℓ-torsion.
- But by computing isogenies, one can work over a cyclic subgroup of cardinal ℓ instead.
- Since thus a subgroup is of degree ℓ, whereas the full ℓ-torsion is of degree ℓ^2, we can work faster over it.

Example

- The SEA point counting algorithm [Sch95; Mor95; Elk97];
- The CRT algorithms to compute class polynomials [Sut11; ES10];
- The CRT algorithms to compute modular polynomials [BLS12].

Further applications of isogenies

- Splitting the multiplication using isogenies can improve the arithmetic [DIK06; Gau07];
- The isogeny graph of a supersingular elliptic curve can be used to construct secure hash functions [CLG09];
- Construct public key cryptosystems by hiding vulnerable curves by an isogeny (the trapdoor) [Tes06], or by encoding informations in the isogeny graph [RS06];
- Take isogenies to reduce the impact of side channel attacks [Sma03];
- Construct a normal basis of a finite field [CL09];
- Improve the discrete logarithm in $\mathbb{F}_q^*$ by finding a smoothness basis invariant by automorphisms [CL08].

Computing explicit isogenies

- If E_1 and E_2 are two elliptic curves given by short Weierstrass equations $y^2 = x^3 + a_i x + b_i$ an isogeny $f : E_1 \to E_2$ is of the form

$$f(x,y) = (R_1(x), yR_2(x))$$

where R_1 and R_2 are rational functions. (Exercice: $f(0_{E_1}) = 0_{E_2}$; what does this implies on the degrees of R_1 and R_2?)

- Let $w_E = dx/2y$ be the canonical differential. Then $f^* w_{E'} = c w_E$, with c in k so

$$f(x,y) = \left(\frac{g(x)}{h(x)}, cy \left(\frac{g(x)}{h(x)} \right)' \right),$$

where $h(x) = \prod_{P \in \operatorname{Ker} f \setminus \{0_E\}} (x - x_P)$.

Theorem ([Vél71])

Given the equation h of the kernel $\operatorname{Ker} f$, Vélu's formula can compute the isogeny f in time linear in $\deg f$.

Modular polynomials

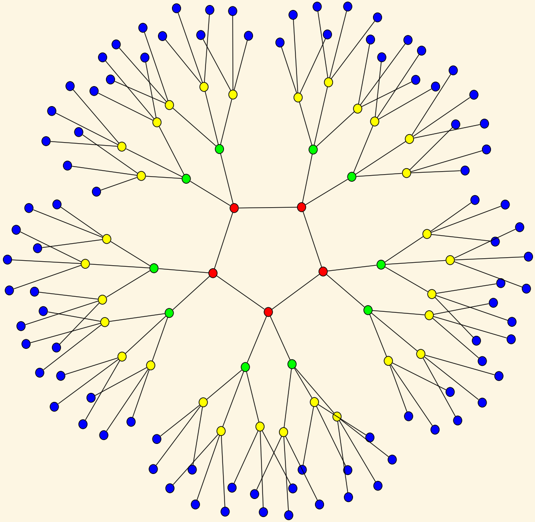
Here $k = \overline{k}$.

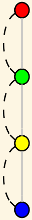
Definition (Modular polynomial)

The modular polynomial $\varphi_\ell(x,y) \in \mathbb{Z}[x,y]$ is a bivariate polynomial such that $\varphi_\ell(x,y) = 0 \Leftrightarrow x = j(E_1)$ and $y = j(E_2)$ with E_1 and E_2 ℓ-isogeneous.

- Roots of $\varphi_\ell(j(E_1),.) \Leftrightarrow$ elliptic curves ℓ-isogeneous to E_1. There are $\ell+1 = \#\mathbb{P}^1(\mathbb{F}_\ell)$ such roots if ℓ is prime.
- φ_ℓ is symmetric;
- The height of φ_ℓ grows as $\widetilde{O}(\ell)$;
- φ_ℓ has total size $\widetilde{O}(\ell^3)$.

A 3-isogeny graph in dimension 1 [Koh96; FM02]





Find elliptic curves with a prescribed number of points

- Let $E/\mathbb{F}_q$ be an ordinary elliptic curve, $\chi_\pi = X^2 - tX + q$ the characteristic polynomial of the Frobenius π;
- $\#E(\mathbb{F}_q) = 1 - t + q$.
- $\Delta_\pi = t^2 - 4q < 0$ (since $t \leqslant 2\sqrt{q}$ by Hasse) so $\mathrm{End}(E) \supset \mathbb{Z}[\pi]$ is an order in $K = \mathbb{Q}(\sqrt{\Delta_\pi})$ a quadratic imaginary field;
- Write $\Delta_\pi = \Delta_0 f^2$, where Δ is the discriminant of K, then f is the conductor of $\mathbb{Z}[\pi] \subset O_K$.

- Conversely fix N in the Hasse-Weil interval, and let $t = 1 + q - N$ and O_K be the maximal order in $\mathbb{Q}(\sqrt{\Delta_\pi})$;
- If $E/\mathbb{F}_q$ has endomorphism ring O_K (or an order in K containing $\mathbb{Z}[\pi]$), then $\#E(\mathbb{F}_q) = N$.

Complex Multiplication

Theorem (Fondamental theorem of Complex Multiplication)

Let K be a quadratic imaginary field, $E/\mathbb{C}$ an elliptic curve with $\mathrm{End}(E) = O_K$.

- *$j(E)$ is algebraic and $K(j(E))$ is the Hilbert class field $\mathfrak{H}_K$ of K (the maximal unramified abelian extension of K).*
- *The minimal polynomial of $j(E)$ is*

$$H_K(X) = \prod_{\sigma \in \mathrm{Gal}(\mathfrak{H}_K/K) \simeq \mathrm{Cl}(K)} (X - \sigma(j(E))) = \prod_{E_i/\mathbb{C} | \mathrm{End}(E_i) = O_K} (X - j(E_i)) \in \mathbb{Z}[X]$$

  where for $\sigma = [I] \in \mathrm{Gal}(\mathfrak{H}_K/K) \simeq \mathrm{Cl}(K)$, $\sigma(j(E)) = j(E/E[I])$;
- *If $p = \mathfrak{p}_1\mathfrak{p}_2$ splits in K, and $\mathfrak{P}$ is a prime above p in $\mathfrak{H}_K$ then E has good reduction at p and $E_{\mathbb{F}_{\mathfrak{P}}}$ is an ordinary elliptic curve over $\mathbb{F}_{\mathfrak{P}}$. The extension $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p$ has degree the order of $[\mathfrak{p}_i] \in \mathrm{Cl}(O_K)$ and $\mathrm{End}(E_{\mathbb{F}_{\mathfrak{P}}}) = O_K$*
- *In particular if p splits completely in $\mathfrak{H}_K$ (or equivalently if $\mathfrak{p}_i$ is principal), then H_K splits over $\mathbb{F}_p$:*

$$H_K \equiv \prod_{E/\mathbb{F}_p | \mathrm{End}(E) = O_K} (X - j(E)) \mod p.$$

The CRT method to compute the class polynomial H_K

1. Find p completely split in $\mathfrak{H}_K$;
2. Find all $\#\mathrm{Cl}(K)$ elliptic curves E over $\mathbb{F}_p$ with $\mathrm{End}(E) = O_K$;
3. Recover $H_K \mod p = \prod_{E/\mathbb{F}_p \mid \mathrm{End}(E) = O_K} (X - j(E))$;
4. Iterate the process for several primes p_i and use the CRT to recover H_K from $H_K \mod p_i$.

Theorem ([Bel+08; Sut11])

Using isogenies in Step 3 to

- *Compute* $\mathrm{End}(E)$ *for a random* $E/\mathbb{F}_p$*;*
- *Go up in the volcano once a curve* E *in the right isogeny class is found;*
- *Once a curve* $E/\mathbb{F}_p$ *is found with* $\mathrm{End}(E) = O_K$ *compute all the others directly from the action of* $\mathrm{Cl}(K)$*;*

yields a quasi-linear algorithm.

Computing $\mathrm{End}(E)$ and going up in the volcano [Koh96; FM02]

- If $E/\mathbb{F}_q$ is ordinary, $\#E(\mathbb{F}_q)$ gives π and so $\mathbb{Z}[\pi] \subset \mathrm{End}(E) \subset O_K$;
- It remains to compute the conductor f of $\mathrm{End}(E)$;
- It suffices to compute $v_\ell(f)$ for ℓ dividing the conductor f_π of $\mathbb{Z}[\pi]$;
- In the ℓ-isogeny graph, following three paths allows to determine the height we are on, and from it the valuation $v_\ell(f)$.
- A similar method is used to go up in the volcano.

Polarised abelian varieties over $\mathbb{C}$

Definition

A complex abelian variety A of dimension g is isomorphic to a compact Lie group V/Λ with

- A complex vector space V of dimension g;
- A $\mathbb{Z}$-lattice Λ in V (of rank $2g$);
- An Hermitian form H on V with $E(\Lambda,\Lambda) \subset \mathbb{Z}$ where $E = \operatorname{Im} H$ is symplectic.

- Such an Hermitian form H is called a polarisation on A. Conversely, any symplectic form E on V such that $E(\Lambda,\Lambda) \subset \mathbb{Z}$ and $E(ix,iy) = E(x,y)$ for all $x,y \in V$ gives a polarisation H with $E = \operatorname{Im} H$.
- Over a symplectic basis of Λ, E is of the form.

$$\begin{pmatrix} 0 & D_\delta \\ -D_\delta & 0 \end{pmatrix}$$

  where D_δ is a diagonal positive integer matrix $\delta = (\delta_1, \delta_2, \ldots, \delta_g)$ and $\delta_1 \mid \delta_2 | \cdots \mid \delta_g$.
- $\deg H = \prod \delta_i$; H is a principal polarisation if $\deg H = 1$.

Principal polarisations

- If A is principally polarised, $A = \mathbb{C}^g/(\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g)$ where the matrix Ω is in $\mathfrak{H}_g$, the Siegel space of symmetric matrices Ω with $\operatorname{Im}\Omega$ positive definite;
- The principal polarisation H is given by the matrix $(\operatorname{Im}\Omega)^{-1}$.
- The choice of a symplectic basis gives an action of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on $\mathfrak{H}_g$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \Omega = (a\Omega + b)(c\Omega + d)^{-1};$$

- The moduli space of principally polarised abelian varieties is isomorphic to $\mathfrak{H}_g/\mathrm{Sp}_{2g}(\mathbb{Z})$ and has dimension $g(g+1)/2$.

Examples

- In dimension 1 all abelian varieties are principally polarised and are exactly the elliptic curves;
- In dimension 2 the absolutely simple principally polarised abelian surfaces are a Jacobian of an hyperelliptic curve of genus 2;
- In dimension 3 the absolutely simple principally polarised abelian threefold are a Jacobian of a curve of genus 3.

Isogenies

Let $A = V/\Lambda$ and $B = V'/\Lambda'$.

Definition

An isogeny $f : A \to B$ is a bijective linear map $f : V \to V'$ such that $f(\Lambda) \subset \Lambda'$. The kernel of the isogeny is $f^{-1}(\Lambda')/\Lambda \subset A$ and its degree is the cardinal of the kernel.

- Two abelian varieties over a finite field are isogenous iff they have the same zeta function (Tate);
- A morphism of abelian varieties $f : A \to B$ (seen as varieties) is a group morphism iff $f(0_A) = 0_B$.

The dual abelian variety

Definition

If $A=V/\Lambda$ is an abelian variety, its dual is $\widehat{A}=\mathrm{Hom}_{\overline{\mathbb{C}}}(V,\mathbb{C})/\Lambda^*$. Here $\mathrm{Hom}_{\overline{\mathbb{C}}}(V,\mathbb{C})$ is the space of anti-linear forms and $\Lambda^*=\{f \mid f(\Lambda)\subset\mathbb{Z}\}$ is the orthogonal of Λ.

- If H is a polarisation on A, its dual H^* is a polarisation on $\widehat{A}$. Moreover, there is an isogeny $\Phi_H : A\to\widehat{A}$:
$$x\mapsto H(x,\cdot)$$
of degree $\deg H$. We note $K(H)$ its kernel.
- If $f:A\to B$ is an isogeny, then its dual is an isogeny $\widehat{f}:\widehat{B}\to\widehat{A}$ of the same degree.

Remark

The canonical pairing $A\times\widehat{A}\to\mathbb{C}, (x,f)\mapsto f(x)$ induces a canonical principal polarisation on $A\times\widehat{A}$, the Poincaré bundle:
$$E_P((x_1,f_1),(x_2,f_2))=f_1(x_2)-f_2(x_1).$$
The pullback $(\mathrm{Id},\varphi_H)^*E_P=2E$.

Isogenies and polarisations

Definition

- An isogeny $f:(A,H_1)\to(B,H_2)$ between polarised abelian varieties is an isogeny such that
$$f^*H_2 := H_2(f(\cdot),f(\cdot)) = H_1.$$
- f is an ℓ-isogeny between principally polarised abelian varieties if H_1 and H_2 are principal and $f^*H_2=\ell H_1$.

An isogeny $f:(A,H_1)\to(B,H_2)$ respect the polarisations iff the following diagram commutes

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\Phi_{H_1}"] & B \arrow[d, "\Phi_{H_2}"] \\ \widehat{A} & \widehat{B} \arrow[l, "\widehat{f}"] \end{tikzcd}$$

Isogenies and polarisations

Definition

- An isogeny $f:(A,H_1)\to(B,H_2)$ between polarised abelian varieties is an isogeny such that
$$f^*H_2 := H_2(f(\cdot),f(\cdot)) = H_1.$$
- f is an ℓ-isogeny between principally polarised abelian varieties if H_1 and H_2 are principal and $f^*H_2 = \ell H_1$.

$f:(A,H_1)\to(B,H_2)$ is an ℓ-isogeny between principally polarised abelian varieties iff the following diagram commutes

$$\begin{tikzcd}
 & A \arrow[r, "f"] \arrow[dl, "{[\ell]}"'] \arrow[d, "\Phi_{\ell H_1}"] & B \arrow[d, "\Phi_{H_2}"] \\
A \arrow[r, "\Phi_{H_1}"'] & \widehat{A} & \widehat{B} \arrow[l, "\widehat{f}"]
\end{tikzcd}$$

Isogenies and polarisations

Definition

- An isogeny $f:(A,H_1)\to(B,H_2)$ between polarised abelian varieties is an isogeny such that
$$f^*H_2 := H_2(f(\cdot),f(\cdot)) = H_1.$$
- f is an ℓ-isogeny between principally polarised abelian varieties if H_1 and H_2 are principal and $f^*H_2 = \ell H_1$.

Proposition

If $K\subset A(\overline{k})$, H_1 descends to a polarisation H_2 on A/K (ie $f^*H_2 = H_1$) if and only if $\operatorname{Im} H_1(K+\Lambda_1, K+\Lambda_1)\subset\mathbb{Z}$ *iff K is isotropic for the E_1-pairing. The degree of H_2 is then* $\deg H_1/\deg f^2$.

Example

Let $\Lambda_1 = \Omega_1\mathbb{Z}^g + \mathbb{Z}^g$, $H_1 = \ell(\operatorname{Im}\Omega_1)^{-1}$, then A/K is principally polarised ($A/K = \mathbb{C}^g/(\Omega_2\mathbb{Z}^g+\mathbb{Z}^g)$) if $K = \frac{1}{\ell}\mathbb{Z}^g$ or $K = \frac{1}{\ell}\Omega\mathbb{Z}^g$.

Theta functions

- Let (A, H_0) be a principally polarised abelian variety over $\mathbb{C}$;
- $A = \mathbb{C}^g / (\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ with $\Omega \in \mathfrak{H}_g$ and $H_0 = (\Im\Omega)^{-1}$.
- All automorphic forms corresponding to a multiple of H_0 come from the theta functions with characteristics:

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

- Automorphic property:

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

- Define $\vartheta_i = \vartheta\left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix}\right](., \frac{\Omega}{n})$ for $i \in Z(\overline{n}) = \mathbb{Z}^g / n\mathbb{Z}^g$
- $(\vartheta_i)_{i \in Z(\overline{n})} = \begin{cases} \text{coordinates system} & n \geqslant 3 \\ \text{coordinates on the Kummer variety } A/\pm 1 & n = 2 \end{cases}$

Computing isogenies in dimension 2

- Richelot formuluae [Ric36; Ric37] allows to compute 2-isogenies between Jacobians of hyperelliptic curves of genus 2 (ie maximal isotropic kernels in $A[2]$);
- The duplication formulae for theta functions

$$\vartheta\left[\begin{smallmatrix}\chi\\0\end{smallmatrix}\right](0, 2\frac{\Omega}{n})^2 = \frac{1}{2^g} \sum_{t \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} e^{-2i\pi 2\, {}^t\chi \cdot t} \vartheta\left[\begin{smallmatrix}0\\t\end{smallmatrix}\right](0, \frac{\Omega}{n})^2$$

$$\vartheta\left[\begin{smallmatrix}0\\i/2\end{smallmatrix}\right](0, 2\Omega)^2 = \frac{1}{2^g} \sum_{i_1+i_2=0 \pmod 2} \vartheta\left[\begin{smallmatrix}0\\i_1/2\end{smallmatrix}\right](0,\Omega)\vartheta\left[\begin{smallmatrix}0\\i_2/2\end{smallmatrix}\right](0,\Omega) \quad \text{(for all } \chi \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g\text{);}$$

  allows to generalize Richelot formulae to any dimension;
- Dupont compute modular polynomials of level 2 in [Dup06] and started the computation of modular polynomials of level 3.
- Low degree formulae [DL08] effective for $\ell = 3$ and made explicit in [Smi12];
- Via constructing functions on the Jacobian from functions on the curve [CE14].

The isogeny formula

$$\ell \wedge n = 1, \quad A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \quad B = \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g)$$

$$\vartheta_b^A := \vartheta\begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix}\left(\cdot, \frac{\Omega}{n}\right), \quad \vartheta_b^B := \vartheta\begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix}\left(\cdot, \frac{\ell\Omega}{n}\right)$$

Theorem ([CR14; LR15])

Let F be a matrix of rank r such that ${}^tFF = \ell \,\mathrm{Id}_r$, $X = (\ell x, 0, \ldots, 0)$ in $(\mathbb{C}^g)^r$ and $Y = YF^{-1} = (x, 0, \ldots, 0)F^T \in (\mathbb{C}^g)^r$, $i \in (Z(\overline{n}))^r$ and $j = iF^{-1}$.

$$\vartheta_{i_1}^A(\ell z)\ldots\vartheta_{i_r}^A(0) = \sum_{\substack{t_1,\ldots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ F(t_1,\ldots,t_r)=(0,\ldots,0)}} \vartheta_{j_1}^B(Y_1+t_1)\ldots\vartheta_{j_r}^B(Y_r+t_r),$$

This can be computed given only the equations (in a suitable form) of the kernel K. When K is rational, the complexity is $\widetilde{O}(\ell^g)$ or $\widetilde{O}(\ell^{2g})$ operations in $\mathbb{F}_q$ according to whether $\ell \equiv 1$ or 3 modulo 4.

- “Record” isogeny computation: $\ell = 1321$.

Birational invariants for $\mathfrak{H}_g/\mathrm{Sp}_4(\mathbb{Z})$

Definition

- The Igusa invariants are Siegel modular functions j_1, j_2, j_3 for $\Gamma = \mathrm{Sp}_4(\mathbb{Z})$ defined by

$$j_1 := \frac{h_{12}^5}{h_{10}^6}, \quad j_2 := \frac{h_4 h_{12}^3}{h_{10}^4}, \quad j_3 := \frac{h_{16} h_{12}^2}{h_{10}^4}$$

  where the h_i are modular forms of weight i given by explicit polynomials in terms of theta constants.

- Invariants derived by Streng are better suited for computations:

$$i_1 := \frac{h_4 h_6}{h_{10}}, \quad i_2 := \frac{h_4^2 h_{12}}{h_{10}^2}, \quad i_3 := \frac{h_4^5}{h_{10}^2}.$$

- The three invariants $j_{i,\ell}(\Omega) = j_i(\ell\Omega)$ encode a principally polarised abelian surface ℓ-isogeneous to $A = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$;
- All others ppav ℓ-isogenous to A comes from the action of $\Gamma/\Gamma_0(\ell)$ on Ω. The index is $\ell^3 + \ell^2 + \ell + 1$.

Modular polynomials in dimension 2

Definition (ℓ-modular polynomials)

$$\Phi_{1,\ell}(X, j_1, j_2, j_3) = \prod_{\gamma \in \Gamma/\Gamma_0(\ell)} (X - j_{1,\ell}^{\gamma})$$

$$\Psi_{i,\ell}(X, j_1, j_2, j_3) = \sum_{\gamma \in \Gamma/\Gamma_0(\ell)} j_{i,\ell}^{\gamma} \prod_{\gamma' \in \Gamma/\Gamma_0(\ell) \setminus \{\gamma\}} (X - j_{1,\ell}^{\gamma'}) \quad (i = 2, 3)$$

$$\Phi_{1,\ell}, \Psi_{2,\ell}, \Psi_{3,\ell} \in \mathbb{Q}(j_1, j_2, j_3)[X].$$

- Computed via an evaluation–interpolation approach;
- Evaluation requires evaluating the modular invariants on Ω at high precision;

⇒ Uses a generalized version of the AGM to compute theta functions in quasi-linear time in the precision [Dup06];

⇒ Need to interpolate rational functions;

- Denominator describes the Humbert surface of discriminant ℓ^2 [BL09; Gru10];
- Quasi-linear algorithm [Dup06; Mil14];
- Can be generalized to smaller modular invariants [Mil14].

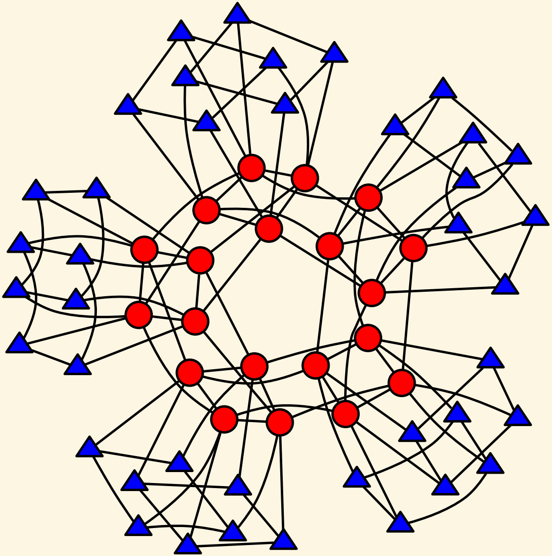
Example of modular polynomials in dimension 2 [Mil14]

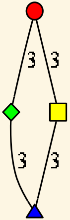
Invariant	ℓ	Size
Igusa	2	57 MB
Streng	2	2.1 MB
Streng	3	890 MB
Theta	3	175 KB
Theta	5	200 MB
Theta	7	29 GB

Example

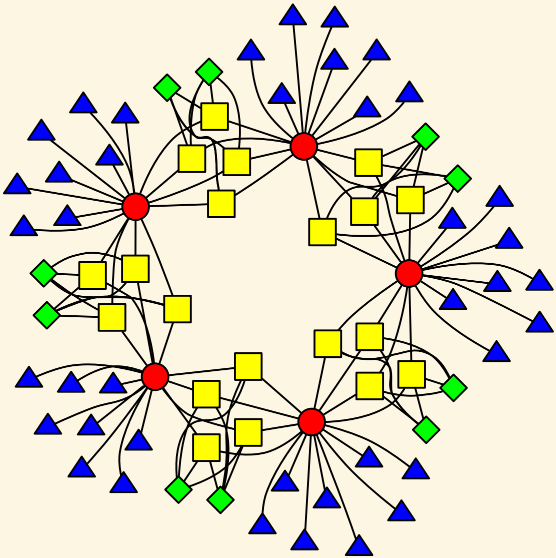
The denominator of $\Phi_{1,3}$ for modular functions b_1, b_2, b_3 derived from theta constant of level 2 is:
$1024b_3^6b_2^6b_1^{10} - ((768b_3^8 + 1536b_3^4 - 256)b_3^8 + 1536b_3^8b_3^4 - 256b_3^8)b_1^8 + (1024b_3^6b_2^{10} + (1024b_3^{10} + 2560b_3^6 - 512b_3^2)b_2^6 - (512b_3^6 - 64b_3^2)b_2^2)b_1^6 - (1536b_3^8b_2^8 + (-416b_3^4 + 32)b_2^4 + 32b_3^4)b_1^4 - ((512b_3^6 - 64b_3^2)b_2^6 - 64b_3^6b_2^2)b_1^2 + 256b_3^8b_2^8 - 32b_3^4b_2^4 + 1.$

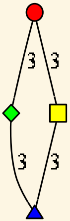
Isogeny graphs in dimension 2 ($\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$)



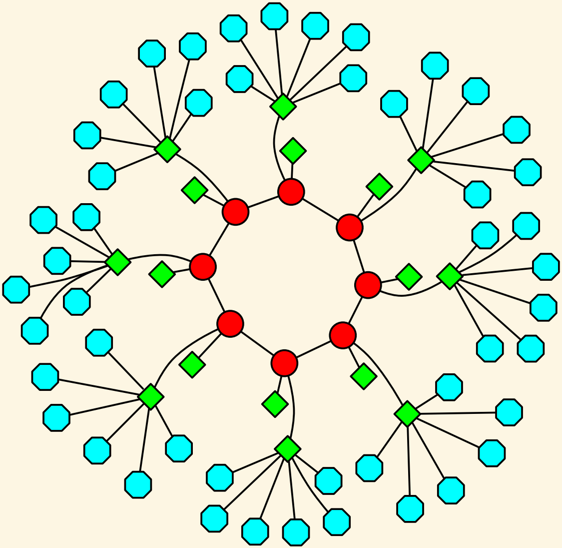


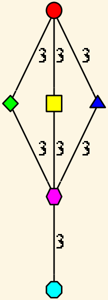
Isogeny graphs in dimension 2 ($\ell = q = Q\overline{Q}$)



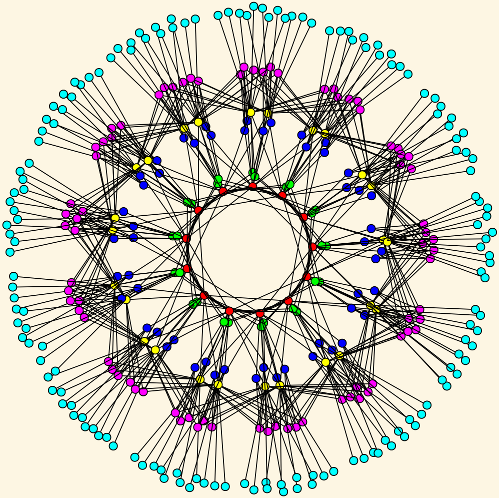


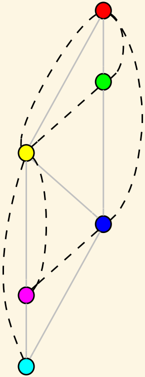
Isogeny graphs in dimension 2 ($\ell = q = Q\overline{Q}$)





Isogeny graphs and lattice of orders [Bisson, Cosset, R.]





Non principal polarisations

- Let $f : (A, H_1) \rightarrow (B, H_2)$ be an isogeny between principally polarised abelian varieties;
- When $\operatorname{Ker} f$ is not maximal isotropic in $A[\ell]$ then $f^* H_2$ is not of the form ℓH_1;
- How can we go from the principal polarisation H_1 to $f^* H_1$?

Non principal polarisations

Theorem (Birkenhake-Lange, Th. 5.2.4)

Let A be an abelian variety with a principal polarisation H_1;

- *Let $O_0 = \mathrm{End}(A)^s$ be the real algebra of endomorphisms symmetric under the Rosati involution;*
- *Let $\mathrm{NS}(A)$ be the Néron-Severi group of line bundles modulo algebraic equivalence.*

Then

- *$\mathrm{NS}(A)$ is isomorphic to O_0 via*

$$\beta \in O_0 \mapsto H_\beta = \beta H_1 = H_1(\beta\cdot,\cdot);$$

- *This induces a bijection between polarisations of degree d in $\mathrm{NS}(A)$ and totally positive symmetric endomorphisms of norm d in O_0^{++};*
- *The isomorphic class of a polarisation $H_\beta \in \mathrm{NS}(A)$ for $f \in O_0^{++}$ correspond to the action $\varphi \mapsto \varphi^* \beta \varphi$ of the automorphisms of A.*

Cyclic isogeny

- Let $f:(A,H_1)\to(B,H_2)$ be an isogeny between principally polarised abelian varieties with cyclic kernel of degree ℓ;
- There exists β such that the following diagram commutes:

$$\begin{tikzcd}
 & A \arrow[r, "f"] \arrow[dl, "\beta"'] \arrow[d, "\Phi_{f^*H_2}"] & B \arrow[d, "\Phi_{H_2}"] \\
A \arrow[r, "\Phi_{H_1}"'] & \widehat{A} & \widehat{B} \arrow[l, "\widehat{f}"]
\end{tikzcd}$$

- β is an $(\ell,0,\dots,\ell,0,\dots)$-isogeny whose kernel is not isotropic for the H_1-Weil pairing on $A[\ell]$!
- β commutes with the Rosatti involution so is a real endomorphism (β is H_1-symmetric). Since H_1 is Hermitian, β is totally positive.
- $\operatorname{Ker} f$ is maximal isotropic for βH_1; conversely if K is a maximal isotropic kernel in $A[\beta]$ then $f: A\to A/K$ fits in the diagram above.

β-isogenies

Theorem ([Dudeanu, Jetchev, R.])

- *Let $(A, \mathscr{L})$ be a ppav and $\beta \in \mathrm{End}(A)^{++}$ be a totally positive real element of degree ℓ. Let $K \subset \mathrm{Ker}\,\beta$ be cyclic of degree ℓ (note that it is automatically isotropic). Then A/K is principally polarised.*
- *Conversely if there is a cyclic isogeny $f : A \to B$ of degree ℓ between ppav then there exists $\beta \in \mathrm{End}(A)^{++}$ such that $\mathrm{Ker}\, f \subset \mathrm{Ker}\,\beta$.*
- *Given the kernel $\ker f$ we have a polynomial time algorithm in $\deg f$ for computing the isogeny f.*

Corollary

- *If $NS(A) = \mathbb{Z}$ there are no cyclic isogenies to a ppav;*
- *For an ordinary abelian surface, if there is a cyclic isogeny of degree ℓ then ℓ splits into totally positive principal ideals in the real quadratic order which is locally maximal at ℓ. A cyclic isogeny does not change the real multiplication.*

Cyclic modular polynomials in dimension 2 [Milio-R.]

- Given $\beta \in O_{K_0}$ one can define the β-modular polynomial in terms of symmetric invariants of the Hilbert space $\mathfrak{H}_1^g/(\mathrm{Sl}_2(O_{K_0}) \oplus \mathrm{Sl}_2(O_{K_0})^\sigma)$;
- If $D=2$ or $D=5$ the symmetric Hilbert moduli space is rational and parametrized by two invariants: the Gundlach invariants;
- Use an evaluation–interpolation approach via the action of $\mathrm{Sl}_2(O_{K_0})/\Gamma_0(\beta_i)$ which give all the $\ell+1$ β_i-isogenies;

- For general D the Hilbert space is not unirational $\Rightarrow$ we need to interpolate three invariants (the pull back of three Siegel invariants);
- There is an algebraic relation between the invariants we interpolate $\Rightarrow$ need to normalise the modular polynomials by fixing a Gröbner basis.

Example of cyclic modular polynomials in dimension 2 [Milio-R.]

ℓ $(D=2)$	Size (Gundlach)	Theta	ℓ $(D=5)$	Size (Gundlach)	Theta
2	8.5KB		5	22KB	45KB
7	172KB		11	3.5MB	308KB
17	5.8MB	221KB	19	33MB	3.6MB
23	21 MB		29	188MB	
31	70 MB		31	248 MB	
41	225 MB	7.2MB			

Example

For $D=2$, $\beta = 5+2\sqrt{2} \,|\, 17$, using b_1, b_2, b_3 pullback of level 2 theta functions on the Hilbert space, the denominator of $\Phi_{1,\beta}$ is $b_3^6 b_2^{18} + (6b_3^8 6b_3^4 + 1)b_2^{16} + (15b_3^{10} 24b_3^6 + 7b_3^2)b_2^{14} + (20b_3^{12} 42b_3^8 + 9b_3^4 + 2)b_2^{12} + (15b_3^{14} 48b_3^{10} + 37b_3^6 + 4b_3^2)b_2^{10} + (6b_3^{16} 42b_3^{12} + 68b_3^8 26b_3^4 + 3)b_2^8 + (b_3^{18} 24b_3^{14} + 37b_3^{10} + 8b_3^6 b_3^2)b_2^6 + (6b_3^{16} + 9b_3^{12} 26b_3^8 24b_3^4 + 2)b_2^4 + (7b_3^{14} + 4b_3^{10} b_3^6)b_2^2 + (b_3^{16} + 2b_3^{12} + 3b_3^8 + 2b_3^4 + 1)$.

Abelian varieties with real and complex multiplication

- Let K be a CM field (a totally imaginary quadratic extension of a totally real field K_0 of dimension g);
- An abelian variety with RM by K_0 is of the form $\mathbb{C}^g/(\Lambda_1 \oplus \Lambda_2 \tau)$ where Λ_i is a lattice in K_0, K_0 is embedded into $\mathbb{C}^g$ via $K_0 \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^g \subset \mathbb{C}^g$, and $\tau \in \mathfrak{H}_1^g$;
- The polarisations are of the form

$$H(z_1, z_2) = \sum_{\varphi_i : K \to \mathbb{C}} \varphi_i(\lambda z_1 \overline{z_2}) / \Im \tau_i$$

  for a totally positive element $\lambda \in K_0^{++}$. In other words if $x_i, y_i \in K_0$, then $E(x_1 + y_1 \tau, x_2 + y_2 \tau) = \mathrm{Tr}_{K_0/\mathbb{Q}}(\lambda(x_2 y_1 - x_1 y_2))$.
- An abelian variety with CM by K is of the form $\mathbb{C}^g/\Phi(\Lambda)$ where Λ is a lattice in K and Φ is a CM-type.
- The polarisations are of the form

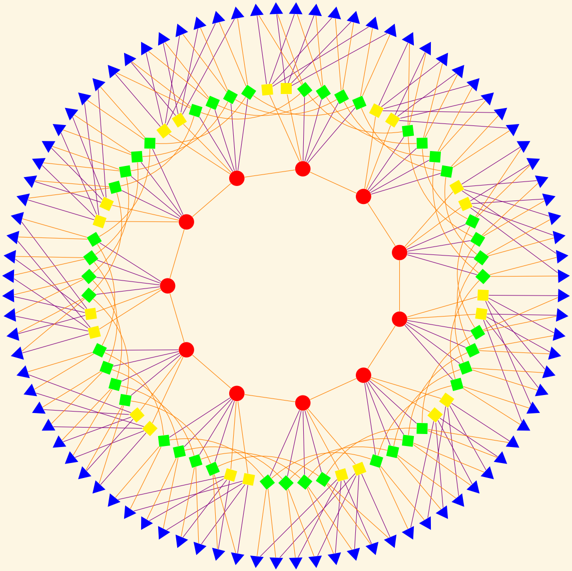
$$E(z_1, z_2) = \mathrm{Tr}_{K/Q}(\xi z_1 \overline{z_2})$$

  for a totally imaginary element $\xi \in K$. The polarisation is principal iff $\xi \overline{\Lambda} = \Lambda^\star$ where $\Lambda^\star$ is the dual of Λ for the trace.

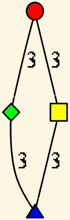
Cyclic isogeny graph in dimension 2 [IT14]

- Let A be a principally polarised abelian surface over $\mathbb{F}_q$ with CM by $O \subset O_K$ and RM by $O_0 \subset O_{K_0}$;
- If O_0 is maximal (locally at ℓ) and that we are in the split case: $(\ell) = (\beta_1)(\beta_2)$ in O_0, then $A[\ell] = A[\beta_1] \oplus A[\beta_2]$. Assume that β_i is totally positive.
- There are two kind of cyclic isogenies: β_1-isogenies ($K \subset A[\beta_1]$) and β_2-isogenies.
- Looking at β_1 isogenies, we recover the volcano structure: $O = O_0 + \mathfrak{f} O_K$ for a certain O_0-ideal $\mathfrak{f}$ such that the conductor of O is $\mathfrak{f} O_K$.
  - If $\mathfrak{f}$ is prime to β_1, there are 2, 1, or 0 horizontal isogenies according to whether β_1 splits, is ramified or is inert in O. The others are descending to $O_0 + \mathfrak{f}\beta_1 O_K$;
  - If $\mathfrak{f}$ is not prime to β_1 there is one ascending isogeny (to $O_0 + \mathfrak{f}/\beta_1 O_K$) and ℓ descending ones;
  - We are at the bottom when the β_1-valuation of $\mathfrak{f}$ is equal to the valuation of the conductor of $\mathbb{Z}[\pi, \overline{\pi}]$.
- ℓ-isogenies preserving O_0 are a composition of a β_1-isogeny with a β_2-isogeny.
- When ℓ is inert, ℓ-isogenies preserving the RM O_0 form a volcano.

Cyclic isogeny graph in dimension 2 [IT14]



β_1 is inert and β_2 is split in K.



Changing the real multiplication in dimension 2: moving between pancakes

Cyclic isogenies (that preserve principal polarisations) conserve real multiplication; so we need to look at ℓ-isogenies.

Proposition

- *Let O_ℓ be the order of conductor ℓ inside O_{K_0}. ℓ-isogenies going from O_ℓ to O_{K_0} are of the form*

$$\mathbb{C}^g/(O_\ell \oplus O_\ell^\vee \tau) \to \mathbb{C}^g/(O_{K_0} \oplus O_{K_0}^\vee \tau).$$

- $\mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee)/\mathrm{Sl}_2(O_\ell \oplus O_\ell^\vee)$ *acts on such isogenies;*
- *When ℓ splits in O_{K_0}, $\mathrm{Sl}_2(O_{K_0} \oplus O_{K_0}^\vee)/\mathrm{Sl}_2(O_\ell \oplus O_\ell^\vee) \simeq \mathrm{Sl}_2(O_{K_0}/\ell O_{K_0})/\mathrm{Sl}_2(O_\ell/\ell O_\ell) \simeq \mathrm{SL}_2(\mathbb{F}_l^2)/\mathrm{Sl}_2(\mathbb{F}_l) \simeq \mathrm{Sl}_2(\mathbb{F}_l)$, so we find $\ell^3 - \ell$ ℓ-isogenies changing the real multiplication.*
- *On the other hand there is $(\ell+1)^2$ ℓ-isogenies preserving the real multiplication*
- *In total we find all $\ell^3 + \ell^2 + \ell + 1$ ℓ-isogenies.*

Changing the real multiplication in dimension 2: moving between pancakes

Corollary ([Ionica, Martindale, R., Streng])

If O is maximal at ℓ,

- *If ℓ is split there are $\ell^2+2\ell+1$ RM-horizontal ℓ-isogenies and $\ell^3-\ell$ RM-descending ℓ-isogenies;*
- *If ℓ is inert there are ℓ^2+1 RM-horizontal ℓ-isogenies and $\ell^3+\ell$ RM-descending ℓ-isogenies;*
- *If ℓ is ramified there are $\ell^2+\ell+1$ RM-horizontal ℓ-isogenies and ℓ^3 RM-descending ℓ-isogenies;*

If O is not maximal at ℓ, there are 1 RM-ascending ℓ-isogeny, $\ell^2+\ell$ RM-horizontal ℓ-isogenies and ℓ^3 RM-descending ℓ-isogenies.

AVIsogenies [Bisson, Cosset, R.]

- 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.

Bibliography

J. Belding, R. Bröker, A. Enge, and K. Lauter. "Computing Hilbert Class Polynomials". In: *ANTS*. Ed. by A. J. van der Poorten and A. Stein. Vol. 5011. Lecture Notes in Computer Science. Springer, 2008, pp. 282–295. ISBN: 978-3-540-79455-4 (cit. on p. 14).

A. Bostan, F. Morain, B. Salvy, and E. Schost. "Fast algorithms for computing isogenies between elliptic curves". In: *Mathematics of Computation* 77.263 (2008), pp. 1755–1778 (cit. on p. 5).

R. Bröker and K. Lauter. "Modular polynomials for genus 2". In: *LMS J. Comput. Math.* 12 (2009), pp. 326–339. ISSN: 1461-1570. arXiv: 0804.1565 (cit. on p. 27).

R. Bröker, K. Lauter, and A. Sutherland. "Modular polynomials via isogeny volcanoes". In: *Mathematics of Computation* 81.278 (2012), pp. 1201–1231. arXiv: 1001.0402 (cit. on pp. 5, 7).

D. Charles, K. Lauter, and E. Goren. "Cryptographic hash functions from expander graphs". In: *Journal of Cryptology* 22.1 (2009), pp. 93–113. ISSN: 0933-2790 (cit. on p. 8).

R. Cosset and D. Robert. "An algorithm for computing (ℓ,ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". In: *Mathematics of Computation* (Nov. 2014). DOI: 10.1090/S0025-5718-2014-02899-8. URL: http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL: hal-00578991, eprint: 2011/143. (Cit. on p. 25).

J.-M. Couveignes and T. Ezome. "Computing functions on Jacobians and their quotients". In: (2014). arXiv: 1409.0481 (cit. on p. 24).

J. Couveignes and R. Lercier. "Galois invariant smoothness basis". In: *Algebraic geometry and its applications* (2008) (cit. on p. 8).

J. Couveignes and R. Lercier. “Elliptic periods for finite fields”. In: *Finite fields and their applications* 15.1 (2009), pp. 1–22 (cit. on p. 8).

C. Doche, T. Icart, and D. Kohel. “Efficient scalar multiplication by isogeny decompositions”. In: *Public Key Cryptography-PKC 2006* (2006), pp. 191–206 (cit. on p. 8).

I. Dolgachev and D. Lehavi. “On isogenous principally polarized abelian surfaces”. In: *Curves and abelian varieties* 465 (2008), pp. 51–69 (cit. on p. 24).

A. Dudeanu, jetchev, and D. Robert. “Computing cyclic isogenies in genus 2”. Sept. 2013. In preparation.

R. Dupont. “Moyenne arithmetico-geometrique, suites de Borchardt et applications”. In: *These de doctorat, Ecole polytechnique, Palaiseau* (2006) (cit. on pp. 24, 27).

N. Elkies. “Explicit isogenies”. In: *manuscript, Boston MA* (1992) (cit. on p. 5).

N. Elkies. “Elliptic and modular curves over finite fields and related computational issues”. In: *Computational perspectives on number theory: proceedings of a conference in honor of AOL Atkin, September 1995, University of Illinois at Chicago*. Vol. 7. Amer Mathematical Society. 1997, p. 21 (cit. on p. 7).

A. Enge. “Computing modular polynomials in quasi-linear time”. In: *Math. Comp* 78.267 (2009), pp. 1809–1824 (cit. on p. 5).

A. Enge and A. Sutherland. “Class invariants by the CRT method, ANTS IX: Proceedings of the Algorithmic Number Theory 9th International Symposium”. In: *Lecture Notes in Computer Science* 6197 (July 2010), pp. 142–156 (cit. on p. 7).

M. Fouquet and F. Morain. “Isogeny volcanoes and the SEA algorithm”. In: *Algorithmic Number Theory* (2002), pp. 47–62 (cit. on pp. 11, 15).

S. Galbraith, F. Hess, and N. Smart. “Extending the GHS Weil descent attack”. In: *Advances in Cryptology—EUROCRYPT 2002*. Springer. 2002, pp. 29–44 (cit. on p. 6).

P. Gaudry. “Fast genus 2 arithmetic based on Theta functions”. In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 8).

D. Gruenewald. “Computing Humbert surfaces and applications”. In: *Arithmetic, Geometry, Cryptography and Codint Theory 2009* (2010), pp. 59–69 (cit. on p. 27).

S. Ionica, C. Martindale, D. Robert, and M. Streng. “Isogeny graphs of ordinary abelian surfaces over a finite field”. Mar. 2013. In preparation.

S. Ionica and E. Thomé. “Isogeny graphs with maximal real multiplication.” In: *IACR Cryptology ePrint Archive* 2014 (2014), p. 230 (cit. on pp. 40, 41).

D. Kohel. “Endomorphism rings of elliptic curves over finite fields”. PhD thesis. University of California, 1996 (cit. on pp. 5, 11, 15).

D. Lubicz and D. Robert. “Computing isogenies between abelian varieties”. In: *Compositio Mathematica* 148.5 (Sept. 2012), pp. 1483–1515. DOI: 10.1112/S0010437X12000243. arXiv: 1001.2016 [math.AG]. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf. HAL: hal-00446062.

D. Lubicz and D. Robert. “Computing separable isogenies in quasi-optimal time”. Feb. 2015. URL: http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf. HAL: hal-00954895. (Cit. on p. 25).

E. Milio. “A quasi-linear algorithm for computing modular polynomials in dimension 2”. In: *arXiv preprint arXiv:1411.0409* (2014) (cit. on pp. 27, 28).

E. Milio and D. Robert. “Cyclic modular polynomials for Hilbert surface”. July 2015. In preparation.

F. Morain. “Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques”. In: *J. Théor. Nombres Bordeaux* 7 (1995), pp. 255–282 (cit. on p. 7).

F. Richelot. “Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes”. In: *C. R. Acad. Sci. Paris* 2 (1836), pp. 622–627 (cit. on p. 24).

F. Richelot. “De transformatione Integralium Abelianorum primiordinis commentation”. In: *J. reine angew. Math.* 16 (1837), pp. 221–341 (cit. on p. 24).

A. Rostovtsev and A. Stolbunov. “Public-key cryptosystem based on isogenies”. In: *International Association for Cryptologic Research. Cryptology ePrint Archive* (2006). eprint: http://eprint.iacr.org/2006/145 (cit. on p. 8).

R. Schoof. “Counting points on elliptic curves over finite fields”. In: *J. Théor. Nombres Bordeaux* 7.1 (1995), pp. 219–254 (cit. on p. 7).

N. Smart. “An analysis of Goubin’s refined power analysis attack”. In: *Cryptographic Hardware and Embedded Systems-CHES 2003* (2003), pp. 281–290 (cit. on p. 8).

B. Smith. *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*. Feb. 2009. arXiv: 0806.2995 (cit. on p. 6).

B. Smith. “Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method”. In: *Arithmetic, geometry, cryptography and coding theory* 574 (2012), pp. 159–170 (cit. on p. 24).

A. Sutherland. "Computing Hilbert class polynomials with the Chinese remainder theorem". In: *Mathematics of Computation* 80.273 (2011), pp. 501–538 (cit. on pp. 7, 14).

E. Teske. "An elliptic curve trapdoor system". In: *Journal of cryptology* 19.1 (2006), pp. 115–133 (cit. on p. 8).

J. Vélu. "Isogénies entre courbes elliptiques". In: *Compte Rendu Académie Sciences Paris Série A-B* 273 (1971), A238–A241 (cit. on pp. 5, 9).