Computing Functions on Jacobians and their quotients

Tony EZOME

Université des Sciences et Techniques de Masuku (USTM)
Franceville - Gabon

Bordeaux on October 6, 2015

Motivation

Jacobian Varieties are used for cryptologic applications :

Discrete Logarith Problem (DLP), Pairings, ...

Isogenies between Jacobians varieties can be used to move DLP from a group where it is easy to a group where it is more difficult, and conversely.

Besides (Mathematics are speaking for themselves) it is interesting to exhibit non-trivial elements in $\mathbf{K}(J)$, the functions field of a given Jacobian variety J, or to describe explicitly a given isogeny.

Background on schemes

1. A sheaf $\mathcal{F}$ of rings on a topological space X consists of:
   (a) Rings $\mathcal{F}(U)$, $\forall U$ open subset of X,
   (b) Restriction morphisms $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$, for all pair of open subsets such that $U \supset V$

   These 2 items $+$ 3 conditions about $\{0\}$, ρ_{UU}, and compositions.

2. An affine **K**-scheme consists of:
   (a) $\mathrm{Spec}(A)$ with Zariski topology, where A is a **K**-algebra,
   (b) Structure sheaf $\mathcal{O}_{\mathrm{Spec}(A)}$:
   $\mathcal{O}_{\mathrm{Spec}(A),\mathfrak{p}} = A_{\mathfrak{p}}, \mathcal{O}_{\mathrm{Spec}(A)}(A) = A, \ldots$

   Dimension of $\mathrm{Spec}(A)$ equals dimension of A.

3. $(X, \mathcal{O}_X)$ is a scheme if $X = \cup_{i \in I, \text{open}} X_i$ and $(X_i, \mathcal{O}_X|_{X_i})$ is affine: we have $\dim(X) = Sup(\dim(X_i))$

Background on schemes

A morphism of schemes $(f, f^{\#}) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ consists of a continuous map $f : X \to Y$ and a morphism of sheaves of rings $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$ such that for every $x \in X$, the stalk $f_x^{\#} : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is a local homomorphism

$$i.e \quad f_x^{\#-1}(m_x) = m_{f(x)}$$

An affine variety over $\mathbf{K}$ is the affine scheme associated to a finitely generated algebra over $\mathbf{K}$:
Affine space $\mathbb{A}^n_{\mathbf{K}} = Spec(\mathbf{K}[X_1, \dots, X_n])$ of dimension n is the simplest example.

An algebraic variety over $\mathbf{K}$ is a $\mathbf{K}$-scheme X such that $X = \cup_{0 \leq i \leq n, \text{open}} X_i$ and X_i an affine scheme:
Projective space $\mathbb{P}^n_{\mathbf{K}}$ of dimension n is a $\mathbf{K}$-algebraic variety.

Background on schemes

If $X = \mathrm{Spec}(\mathbf{K}[T_1, \ldots, T_n]/\mathrm{I}$ is an affine variety over $\mathbf{K}$, then the ring of regular functions on X is $\mathcal{O}_X(X) = \mathbf{K}[T_1, \ldots, T_n]/\mathrm{I}$. The field of rational functions on X is $\mathbf{K}(X) = \mathrm{Frac}(\mathcal{O}_X(X))$.

These definitions can be generalized in the general context of an arbitrary scheme. So we can talk about functions on an arbitrary scheme.

$(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)})$ is Noetherian (resp integral) if A is Noetherian ring (resp integral domain) .

A scheme X is Noetherian if it is a finite union of affine open X_i such that each $\mathcal{O}_X(X_i)$ is a Noetherian ring. X is integral iff for every open subset U, the ring $\mathcal{O}_X(U)$ is an integral domain .

Background on schemes

Let X be an scheme over a field $\mathbf{K}$. The set $X(\mathbf{K})$ of $\mathbf{K}$-rational points is defined by $X(\mathbf{K}) = \{x \in X; \mathbf{K}(x) = \mathbf{K}\}$ where $\mathbf{K}(x) = \mathcal{O}_{X,x}/m_x$ is the residue field of X at x.

When $Y = \mathrm{Spec}(\mathbf{K}[T_1, \dots, T_n]/\mathrm{I})$ is an affine scheme over $\mathbf{K}$, the set $Y(\mathbf{K})$ of $\mathbf{K}$-rational points is equal to the algebraic set

$$\{(\alpha_1, \dots, \alpha_n) \in \mathbf{K}^n; \forall P(T) \in \mathrm{I}, P(\alpha) = 0\}.$$

A weak Hilbert's Nullstellensatz says that closed points of Y over $\overline{\mathbf{K}}$ can be identified with maximal ideals containing I: $\overline{\mathbf{K}}$-rational points of Y are closed points.

Cycles on schemes

Let X be a noehterian scheme. A cycle is a finite formal sum

$$Z = \sum_{x \in X} n_x [\ \overline{\{x\}}\ ]$$

Sum of two cycles is done component-wise, and $Z = 0$ iff $n_x = 0$ for every $x \in X$
Supp(Z) = finite union of $\overline{\{x\}}$ such that $n_x \neq 0$.
We say that $\overline{\{x\}}$ is of codimension 1 iff $\dim(O_{X,x}) = 1$.
A (Weil) divisor D on X is a cycle

$$D = \textstyle\sum_{x \in X} n_x [\ \overline{\{x\}}\ ]$$

such that each $x \in$ **Supp**(D) is of codimension 1. The degree of D is $\deg(D) = \sum_{x \in X} n_x$. Divisors form a subsgroup $\mathrm{Div}(X)$ of the group of cycles on X.

Divisors on schemes

Let X be a Noetherian scheme. For all $x \in X$ of codimension 1, the stalk $\mathcal{O}_{X,x}$ is a valuation ring. Let $\mathrm{ord}_x : \mathbf{K}(X) \to \mathbb{Z} \cup \{\infty\}$ be the normalized valuation of $\mathbf{K}(X)$ associated to $\mathcal{O}_{X,x}$. Then for all $f \in \mathbf{K}(X)$

$$(f) = \sum_{x \in X, \dim(\mathcal{O}_{X,x})=1} \mathrm{ord}_x(f)[\ \overline{\{x\}}\ ]$$

is a divisor on X. Such a divisor is called a principal divisor. We have

$$(fg) = (f) + (g).$$

Therefore principal divisors is a subgroup of $\mathrm{Div}(X)$.

$\mathrm{Cl}(X)$ is the quotient of $\mathrm{Div}(X)$ by the subgroup of principal divisors.

The Picard group of a scheme

1. A sheaf of $\mathcal{O}_X$-modules is an $\mathcal{F}$ such that for all open set $U \subset X$ the group $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$-module.
2. $\mathcal{F}$ is an invertible sheaf if it is an sheaf of $\mathcal{O}_X$-modules and if X can be recovered by open sets U for which $\mathcal{F}|_U$ is a free $\mathcal{O}_X|_U$-module of rank 1.
3. The Picard group $\mathrm{Pic}(X)$ of X is the group of isomorphisms classes of invertible sheaves under $\otimes$, identity element is $\mathcal{O}_X$.
4. If X is a regular Noetherian integral scheme (that is the case for smooth projective absolutely integral curves), then
$$\mathrm{Cl}(X) \cong Pic(X), \text{ the map } D \mapsto \mathcal{O}_X(D)$$
induces an isomorphism and we have
$$\mathcal{O}_X(D_1 + D_2) = \mathcal{O}_X(D_1) \otimes \mathcal{O}_X(D_2).$$

Background on curves

A curve over **K** is a an algebraic variety (i.e projective) over **K** whose irreducible components are of dimension 1.

All the curves in this talk will be projective, smooth and absolutely integral: $\mathrm{Proj}(k[x,y,z]/(zy^2-(x-a_1z)(x-a_2z)(x-a_3z))$, where a_1,a_2,a_3 are distinct, is a good example.

For all divisor $D \in \mathrm{Div}(C)$, the invertible sheaf $\mathcal{O}_C(D)$ is the space $H^0(C,\mathcal{O}(D)) = \{f \in \overline{\mathbf{K}}(C); (f) \geq -D\} \cup \{0\}$

It is a finite-dimensional $\overline{\mathbf{K}}$-vector space. We denote $\ell(D) = \dim_{\overline{\mathbf{K}}}(H^0(C,\mathcal{O}_C(D))$

Background on curves

Theorem (Riemann-Roch)

Let C a smooth curve and K_C a canonical divisor on C. Then there is an integer $g \geq 0$, called the genus of C, such that for every divisor $D \in \mathrm{Div}(C)$,

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1.$$

Genus 1 smooth curves $C/\mathbf{K}$ which are absolutely irreducible with at least one $\mathbf{K}$-rational point are called elliptic curves.

Hyperelliptic curves over $\mathbf{K}$ are smooth curves $C/\mathbf{K}$ of genus $g \geq 2$ whose functions field $\mathbf{K}(C)$ is a separable extension of degree 2 of the rational function field $\mathbf{K}(x)$ for some function x.

Background on curves

Let C a genus $g \geq 2$ smooth absolutely integral curve over $\mathbf{K}$.

$$\mathrm{Pic}(C) = \sqcup_{d\in\mathbb{Z}} Pic^{d}(C)$$

Where $\mathrm{Pic}^{d}(C)$ represents classes of divisors of degree d.

In particular $J_C = \mathrm{Pic}^{0}(C)$ is the jacobian variety of C.

J is an abelian variety of dimension g, that is:

1. J is a algebraic variety over $\mathbf{K}$
2. $J_C(\overline{\mathbf{K}})$ has a group structure (identity element $e \in J_C(\mathbf{K})$) such that the multiplication and inversion operations are given by regular functions on J_C

Background on abelian varieties

A morphism $f : A_1 \to A_2$ between 2 abelian varieties is an isogeny if f is surjective, and f has finite kernel (in fact f is also a group morphism).

Let A an abelian varietiy. For any $n \in \mathbb{Z}$, exponentiations $[n] : A \to A$ defined by $[n](x) = \underbrace{x \oplus \ldots \oplus x}_{n-\text{times}}$ are isogenies.

Let u a point of an abelian variety A, we call

$$\begin{tikzcd} t_u : & \mathrm{Pic}(A) \arrow[r] & \mathrm{Pic}(A) \\ & D \arrow[r, mapsto] & D + u := D_u \end{tikzcd}$$

the translation by u.

Background on Jacobian varieties

Let C a genus $g \geq 2$ smooth absolutely integral curve over $\mathbf{K}$.

Let $W \subset \mathrm{Pic}^{g-1}(C)$ be the algebraic set representing classes of effective divisors of degree $g-1$.

Let $\iota : C \to J_C$ be the map such that for all $P \in C$, $\iota(P)$ is equal to the classe of $[P]$ in $\mathrm{Pic}^1(C)$,

$$\text{then } W_{-(g-1)\iota(P)} \in J_C.$$

Recall that a zero-cycle on J_C is a cycle $Z = \sum_{i=1}^n e_i[u_i\ ]$ such that $u_i \in J_C(\overline{\mathbf{K}})$ is closed point for all i

Then for all divisor $D \in Div(J_C)$, the translate $D_{\sum_i e_i u_i}$ and the sum $\sum_i e_i D_{u_i}$ are also divisors on J_C.

Computing functions in the case of elliptic curves

Note that any elliptic curve is an abelian variety, in fact they are equal to their Jacobians.

An elliptic curve $E/\mathbf{K}$ can be seen as the locus in $\mathbb{P}^2_{\mathbf{K}}$ of a cubic equation with only one point (the base point $O = [0 : 1 : 0]$) on the line at ∞.
Thus E/bK is the union of O and the locus in $\mathbb{A}^2_{\mathbf{K}}$ of

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

The function field is $\mathbf{K}(E) = \mathbf{K}(x, y)$.

So a point P of E is completely determined by $x(P)$ and $y(P)$ of the generators of its functions fields $\mathbf{K}(E)$.

Computing functions in the case of elliptic curves

Vélu's Formulae (1971):

Let $d \geq 3$ an odd integer, and $\mathbf{K}$ a field of characteristic p. Let E an elliptic curve over $\mathbf{K}$, and $T \in E(\mathbf{K})$ a point of order d. We denote $V = \langle T \rangle$ the subgroup generated by T. For all $k \in \mathbb{Z}$, we denote $x_k = x \circ t_{kT}$ and $y_k = y \circ t_{kT}$. Vélu defined

$$x' = x + \sum_{1 \leq k \leq d-1} (x_k - x(kT)) \text{ et } y' = y + \sum_{1 \leq k \leq d-1} (y_k - y(kT))$$

Theses functions are invariant on V, that is $\forall (e, v) \in E \times V$, we have

$$x'(e+v) = x'(e) \qquad \text{and } y'(e+v) = y'(e).$$

So $x', y' \in \mathbf{K}(E/V)$.

In fact, $\mathbf{K}(E/V) = \mathbf{K}(x', y')$.

Computing functions in the case of elliptic curves

By setting

$$\begin{aligned}
&\textstyle\sum_{1\leq k\leq d-1}\left(y_k - y(kt)\right),\\
&w_4 = \textstyle\sum_{1\leq k\leq (d-1)/2} 6x(kT)^2 + b_2x(kT) + b_4,\\
&w_6 = \textstyle\sum_{1\leq k\leq (d-1)/2} 10x(kT)^3 + 2b_2x(kT)^2 + 3x(kT) + b_6,\\
&a^{'}4 = a_1 - 5w_4, \quad a_6^{'} = a_6 - b_2w_4 - 7w_6,\\
&a_1^{'} = a_1, \quad a_2^{'} = a_2, a_3{}' = a_3,
\end{aligned}$$

Vélu chowed that

$$(y')^2 + a_1^{'}x'y' + a_3^{'} = (x')^3 + a_2^{'}(x')^2 + a_4^{'}x' + a_6^{'}.$$

So the quotient $E' = E/V$ is an elliptic curve and $\mathbf{K}(E') = \mathbf{K}(x', y')$.
The isogeny $f : E \to E'$ is completely defined by the functions x' and y':

$$\forall P \in E,\ f(P) = (x'(P), y'(P)).$$

Related works

Robert and Lubicz (2012) have provided general methods, extensions of Vélu's formulae, for quotienting abelian varieties (not necessarily Jacobians varieties)

Jacobians of genus 2 curves was studied by Dolgachev et Lehavi (2008), and Smith (2012).

The methods we describe here are different from those of these authors. These constructions, used since Weil (1948), use zéros-cycles and divisors.

It is a joint work with J.-M. Couveignes.

Computing functions on Jacobians

Theorem (of the square)

Let A be an abelian variety over $\mathbf{K}$, and let $\mathcal{L}$ be an invertible sheaf on A. Then for all $x, y \in A(\mathbf{K})$, we have $t_{x+y}^{*}\mathcal{L} \otimes \mathcal{L} \cong t_x^{*}\mathcal{L} \otimes t_y^{*}\mathcal{L}$.

We will make frequent use of the following

Corollary (very useful)

Let C a genus $g \geq 2$ smooth absolutely integral curve over $\mathbf{K}$. Let $\mathfrak{u} = \sum_{i=1}^{\mathrm{I}} e_i[u_i]$ be a zero-cycle on $J_{\overline{\mathbf{K}}}$ where $(e_1, \dots, e_{\mathrm{I}}) \in \mathbb{Z}^{\mathrm{I}}$ and $(u_1, \dots, u_{\mathrm{I}}) \in J(\overline{\mathbf{K}})^{\mathrm{I}}$. We set

$$s(\mathfrak{u}) = \sum_{i=1}^{\mathrm{I}} e_i u_i \in J(\overline{\mathbf{K}}) \quad \text{and} \quad deg(\mathfrak{u}) = \sum_{i=1}^{\mathrm{I}} e_i \in \mathbb{Z}.$$

Then $\sum_{i=1}^{\mathrm{I}} e_i W_{u_i} - W_{s(\mathfrak{u})} - (deg(\mathfrak{u}) - 1)W$ is a principal divisor.

Eta Function

Let $\mathrm{I} \geq 1$ an integer $\mathfrak{u} = \sum_{i=1}^{\mathrm{I}} e_i[u_i]$ a zero-cycle on $J_{\overline{\mathbf{K}}}$ where $(e_1, \ldots, e_{\mathrm{I}}) \in \mathbb{Z}^{\mathrm{I}}$ and $(u_1, \ldots, u_{\mathrm{I}}) \in J(\overline{\mathbf{K}})^{\mathrm{I}}$. We set

$$s(\mathfrak{u}) = \sum_{i=1}^{\mathrm{I}} e_i u_i \in J(\overline{\mathbf{K}}) \text{ and } deg(\mathfrak{u}) = \sum_{i=1}^{\mathrm{I}} e_i \in \mathbb{Z}.$$

From our very useful corollary,
$\sum_{i=1}^{\mathrm{I}} e_i W_{u_i} - W_{s(\mathfrak{u})} - (deg(\mathfrak{u}) - 1)W$ is a principal divisor.

Let $y \in J(\overline{\mathbf{K}})$ not in the support of this diviseur. Call $\eta_W[\mathfrak{u}, y]$ the unique function on $J_J(\overline{\mathbf{K}})$ having divisor

$$(\eta_W[\mathfrak{u}, y]) = \sum_{i=1}^{\mathrm{I}} e_i W_{u_i} - W_{s(\mathfrak{u})} - (deg(\mathfrak{u}) - 1)W$$

and such that $\eta_W[\mathfrak{u}, y](y) = 1$

Eta Function

Eta Functions are at the heart of this work.

For an odd prime ℓ different from the characteristic of $\mathbf{K}$, when u runs over $J[\ell](\overline{\mathbf{K}})$ the functions $\eta_W[u]$ generate the space $H^0(J_{\overline{\mathbf{K}}}, \mathcal{O}_{J_{\overline{\mathbf{K}}}}(\ell W_{-(g-1)\iota(O)}))$, where O is a $\mathbf{K}$-rational point on $J_{\overline{\mathbf{K}}}$.

To find a basis of this space, we selected $u_i \in J[\ell](\overline{\mathbf{K}})$, and w_i for $1 \leq i, j \leq \mathrm{I}$ If the rank of the matrix $(\eta_W[\mathfrak{u}_\mathrm{i}](w_i))_{1 \leq i,j \leq \mathrm{I}}$ is ℓ^g, we deduce a basis.

We will see that if a subgroup V in the ℓ-torsion is well chosen, then Eta functions are invariant on V and we get functions on the quotient J/V.

Now we are going to explain how to evaluate them.

Alpha Function

Let f be a degree d function on J_C such that

$$(f) = \sum_{i=1}^{d} Z_i - \sum_{i=1}^{d} P_i,$$

If x is a class in J there exists a unique degree d divisor D_x such that $x \sim D_x - go$. Writing $D_x = D_1 + \cdots + D_g$ we can associate to f the function $\alpha[f] \in \mathbf{K}(J)$ defined by

$$\alpha[f](x) = f(D_1) \times \cdots \times f(D_g).$$

Its divisor is

$$(\alpha[f]) = \sum_{i=1}^{d} W_{Z_i} - \sum_{i=1}^{d} W_{P_i}.$$

That corresponds to the first part of the divisor of the previous Eta Function.

Beta function

Let D a divisor on C with degree $2g-1$. Set $g = \ell(D)$. Let $f = (f_k)_{1 \leq k \leq g}$ be a basis of $\mathcal{L}(D)$.

For $P = (P_l)_{1 \leq l \leq n} \in C^g$ we set

$$\beta_1[f](P) = \det(f_k(P_l))_{k,l}$$

This $\beta[f]$ is a function on C^g.

We define a functions $\beta_2[f]$ on $\mathrm{Pic}^g(C)$, and $\beta[f]$ on $\mathbf{K}(J_C)$ such that $\beta_1[f] = \beta_2[f] \circ j^g$ and $\beta_2[f] = \beta[f] \circ t_{-go} \circ j^g$ where $j^g : C^g \to \mathrm{Pic}^g(C)$ is the integration Jacoby map

One shows that $(\eta) = (\alpha[f]\beta[f])$.
Since $\alpha[f]$ and $\beta[f]$ are evaluated efficiently, so η is.

Theta functions

A principal polarization on the jacobian J_C is the algebraic equivalence class of an invertible sheaf of the form $\mathcal{L} = \mathcal{O}_{J_C}(D)$, where D is an effective divisor on J_C.

Theorem

Let ℓ be an odd prime such that $(\ell, \mathrm{Char}(\mathbf{K})) = 1$. Let $\mathcal{L}$ a principal polarization on the jacobian J_C. Let V be a maximal isotropic subgroup of $J_C[\ell]$ and $\lambda : J_C :\rightarrow J_C/V$ the quotient map. Then J_C/V admits a principal polarisation $\mathcal{O}_{J_C/V}(D)$ such that $\lambda^*\mathcal{O}_{J_C/V}(D) \cong \mathcal{L}^\ell$.

In fact global sections space $H^0(J_C, \mathcal{O}_{J_C/V}(D))$ is isomorphic to global section space $H^0(J_C, \mathcal{L})$ which are invariant on V : these are the Theta functions associated to $\mathcal{O}_{J_C/V}(D)$ and they generate $H^0(J_C, \mathcal{L})$

Computing functions on quotients of Jacobians

Let $\ell \geq 3$ an odd prime such that $\ell \neq \mathrm{Char}(\mathbf{K})$. Let $V \subset J[\ell]$ be a maximal isotropic subgroup in the ℓ-torsion, and $f : J \to J/V$ be the quotient map.

From the previous theorem, we know that if $\mathcal{O}_{J_c}(D)$ is a principal polarization then there is an principal polarization D on J/V such that $X = f^*D$ (we denote $\mathcal{O}_{J_c}(X) = \mathcal{O}_{J_c}(\ell D)$)

Recall that η_X is the unique function having divisor

$$(\eta_X[\mathfrak{u}, y]) = \sum_{i=1}^{\mathrm{I}} e_i X_{u_i} - X_{s(\mathfrak{u})} - (deg(\mathfrak{u}) - 1)X$$

and such that $\eta_W[\mathfrak{u}, y](y) = 1$, where $\mathfrak{u} = \sum_{i=1}^{\mathrm{I}} e_i[u_i]$ a zero-cycle on J.

Computing functions on quotients of Jacobians

Set $v_i = f(u_i) \in J/V$ for $1 \leq i \leq \mathrm{I}$ and let $\mathfrak{b} = f(\mathfrak{u}) = \sum_{i=1}^{\mathrm{I}} e_i[v_i]$ the image of $\mathfrak{u}$ in the group of zero-cyles on J/V.

From our very useful corollary, there is a function on J/V with divisor $\mathcal{Z} = \sum_{i=1}^{\mathrm{I}} e_i D_{v_i} - D_{s(\mathfrak{b})} - (deg(\mathfrak{b}) - 1)D$. Composing this function with f we obtain a function on J having the same divisor as $\eta_X[\mathfrak{u}, y]$

So $\eta_X[\mathfrak{u}, y]$ is invariant by V and can be identified with the unique function $\tilde{f}$ such that $(\tilde{f}) = \mathcal{Z}$ and $\tilde{f}(f(y)) = 1$:

$$\forall z \in J, \tilde{f}(\overline{z}) = \eta_X[\mathfrak{u}, y](z).$$

Computing functions on Jacobians of genus 2 curves

Let $C : v^2 = h_C(u)$ be the affine equation of a genus 2 smooth absolutely integral curve. Let O_C be the unique place at infinity. Let J_C be the Jacobian of C. Set

$$\begin{tikzcd} j_C : & C \arrow[r] & J_C \\ & P \arrow[r, mapsto] & {[P] - [O_C]} \end{tikzcd}$$

Let $V \subset J[\ell]$ be a maximal isotropic subgroup in the ℓ-torsion. Let D the polarization on J_C/V introduced previously.

If D is a smooth curve and absolutely integral curve of genus 2, then the quotient J_C/V is equal to Jacobian J_D.

We set $D : y^2 = h_D(x)$ the affine equation of D.

Computing functions on Jacobians of genus 2 curves

1. Let K_D be a canonical divisor on D. Call $D^{(2)}$ the symmetric square of D and let $j_D^{(2)} : D^{(2)} \to J_D$ be the map defined by $z = j_D^{(2)}(\{Q_1, Q_2\}) \sim Q_1 + Q_2 - 2K_D$.
This is a birational morphism: $\mathbf{K}(D^{(2)}) = \mathbf{K}(J_D)$

2. Set $f : J_C \to J_D$ the quotient isogeny.

$$\begin{tikzcd}
 & D^{(2)} \arrow[dd, "j_D^{(2)}"] \\
C \arrow[ur, "G"] \arrow[d, "j_C"] \arrow[dr, "F"] & \\
J_C \arrow[r, "f"] & J_D
\end{tikzcd}$$

We define a function$F$ such that $F = f \circ j_C ,$ then $\exists ! G$ such that this diagram commute

Computing functions on Jacobians of genus 2 curves

For all $z \in J_D$ such that $z \sim Q_1 + Q_2 - 2K_D$,

We define the Mumford coordinates

$$\begin{aligned}
\mathbf{s}(z) &= x(Q_1) + x(Q_2), \\
\mathbf{p}(z) &= x(Q_1).x(Q_2), \\
\mathbf{q}(z) &= y(Q_1).y(Q_2), \\
\mathbf{r}(z) &= (y(Q_2) - y(Q_1))/(x(Q_2) - x(Q_1)).
\end{aligned}$$

The function field of J_D is $\mathbf{K}(\mathbf{s}, \mathbf{p}, \mathbf{q}, \mathbf{r})$.

Computing functions on Jacobians of genus 2 curves

$\forall P = (u, v)$ on C, we have $F(w_C(P)) = F((u, -v)) = -F(P)$ where w_C is the hyperelliptic involution on C. Hence

$$\begin{array}{rcl} \mathbf{s}(F(P)) & = & \mathbf{S}(u), \\ \mathbf{p}(F(P)) & = & \mathbf{P}(u), \\ \mathbf{q}(F(P)) & = & \mathbf{Q}(u), \\ \mathbf{r}(F(P)) & = & v\mathbf{R}(u), \end{array}$$

where **S**, **P**, **Q**, **R** are rational fractions in one variable.

They provide a compact description of the isogeny f.

Computing functions on Jacobians of genus 2 curves

The morphism $F : C \to J_D$ induces a map

$$F^* : H^0(J_C, \Omega^1_{J_D/\mathbf{K}}) \to H^0(C, \Omega^1_{C/\mathbf{K}}).$$

So the vector $(\mathbf{S}, \mathbf{P}, \mathbf{Q}, \mathbf{R})$ satisfies a first order differential system.

A basis for $H^0(\Omega^1_{C/\mathbf{K}}, C)$ is made of du/v and udu/v.

We identify $H^0(\Omega^1_{J_D/\mathbf{K}}, J_D)$ with the invariant subspace of $H^0(\Omega^1_{D\times D/\mathbf{K}}, D \times D)$ by the permutation of the two factors.

We deduce that a basis for this space is made of $dx_1/y_1 + dx_2/y_2$ and $x_1dx_1/y_1 + x_2dx_2/y_2$.

Computing functions on Jacobians of genus 2 curves

Let $M = (m_{i,j})_{1 \leq i,j \leq 2}$ be the matrix of F^* with respect to these two bases. So

$$\begin{array}{rcl} F^*(dx_1/y_1 + dx_2/y_2) & = & (m_{1,1} + m_{2,1} \times u) \times du/v, \\ F^*(x_1dx_1/y_1 + x_2dx_2/y_2) & = & (m_{1,2} + m_{2,2} \times u) \times du/v \end{array}$$

Set $\mathbf{L} = \mathbf{K}((t))$. We call

$$P(t) = (u(t), v(t))$$

the point on $C(\mathbf{L})$ corresponding to the value t of the local parameter $u - u_P$. The image of $P(t)$ by F is the class of $Q_1(t) + Q_2(t) - K_D$ where $Q_1(t)$ and $Q_2(t)$ are two $\mathbf{L}$-points on D.

Computing functions on Jacobians of genus 2 curves

$$\begin{tikzcd}
\operatorname{Spec}\mathbf{K}[[t]] \arrow[r, "t\mapsto(Q_1(t),Q_2(t))"] \arrow[d, "t\mapsto P(t)"] & D\times D \arrow[d] \\
C \arrow[r, "F"] & J_D.
\end{tikzcd}$$

Equations involving the matrix of F^* and commutativity of the previous diagram give us the following equation

$$\begin{cases}
\frac{\dot{x}_1(t)}{y_1(t)}+\frac{\dot{x}_2(t)}{y_2(t)} & = & \frac{(m_{1,1}+m_{2,1}\times u(t))\times\dot{u}(t)}{v(t)}, \\
\frac{x_1(t)\times\dot{x}_1(t)}{y_1(t)}+\frac{x_2(t)\times\dot{x}_2(t)}{y_2(t)} & = & \frac{(m_{1,2}+m_{2,2}\times u(t))\times\dot{u}(t)}{v(t)}, \\
y_1(t)^2 & = & h_D(x_1(t)), \\
y_2(t)^2 & = & h_D(x_2(t)).
\end{cases}$$

Computing functions on Jacobians of genus 2 curves

For $\mathbf{K} = \mathbf{F}_{1009}$,
$C : v^2 = u(u-1)(u-2)(u-3)(u-85)$ and
$D : y^2 = x(x-513)(x-51)(x-243)(x-987)$.

We compute
$P(t) = (832 + t, 361 + 10t + 14t^2 + O(t^3))$
$Q_1(t) = (973 + 889t + 57t^2 + O(t^3), 45 + 209t + 39t^2 + O(t^3)),$
$Q_2(t) = (946 + 897t + 252t^2 + O(t^3), 911 + 973t + 743t^2 + O(t^3$

Using the previous differential system, we deduce

$$m_{1,1} = 186, \; m_{1,2} = 864, \; m_{2,1} = 853, \; m_{2,2} = 640.$$

Using again this differential system, we deduce $\mathbf{S}, \mathbf{P}, \mathbf{Q}$ and $\mathbf{R}$.

Thank you!