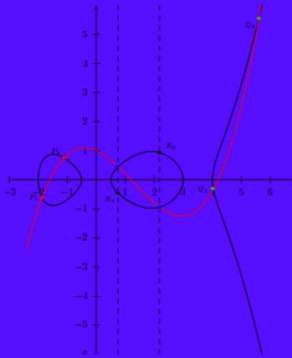
ALVARO GONZALEZ HERNANDEZ

Study group on isogeny-based cryptography

Hyperelliptic curves and their jacobians



Outline of the talk

1. Why to do cryptography in curves with genus greater than 1?
2. Constructing the jacobian.
3. Principally polarised supersingular abelian varieties.

Carl Gustav Jacob Jacobi

Why to do cryptography in curves with genus greater than 1?

Why to do cryptography in genus $g > 1$ curves?

- Elliptic curves allow us to develop a Diffie-Hellman key exchange based on the group law on an elliptic curve.
- Given a genus $g > 1$ curve $\mathcal{C}$, we can also define a group law on an associate algebraic abelian variety known as the **jacobian variety** $J_{\mathcal{C}}$.
- The practical incentive for using these curves is that

$$\#J_{\mathcal{C}}(\mathbb{F}_q) = O(q^g)$$

Therefore, we can get similar complexity, using q of much smaller size!

Why genus 2? 🤔

1. 2 comes just after 1!
2. Every genus 2 curve is hyperelliptic.
3. The jacobian of a genus 2 curves have some properties that makes arithmetic even faster than in the elliptic curve case.

Despite some few technical difficulties, there is nothing stopping us from considering curves with genus $g > 2$ (anyone interested?).

Constructing the jacobian

Set-up 🔧 ⚙️

We will denote by $\mathcal{C}$ a projective irreducible **curve** of genus g over a perfect field k.

For the sake of convenience, we will work in affine coordinates x, y, and we will consider the point of infinity ∞ to have projective coordinates $[0 : 1 : 0]$ (the reasons why I say ”the” point of infinity will become evident later when I specify which kinds of curves we will be studying in this talk).

$k(\mathcal{C})$ will denote the **function field** of $\mathcal{C}$, $\mathcal{C}(k)$ will denote the k-rational points.

Divisors of a curve

A **divisor** is a formal sum of points of $\mathcal{C}(\overline{k})$ with coefficients in $\mathbb{Z}$.
The divisors of a curve form a group

$$\mathrm{Div}(\mathcal{C}) = \Big\{ \sum_{P \in \mathcal{C}(\overline{K})} n_P P \mid n_P \in \mathbb{Z} \Big\}$$

We can associate to each function $f \in k(\mathcal{C})^\times$ a **principal divisor**

$$\mathrm{div}(f) = \sum_{P \in \mathcal{C}(\overline{K})} \mathrm{ord}_P(f) P$$

The principal divisors form a subgroup $\mathrm{Prin}(\mathcal{C}) \subset \mathrm{Div}(\mathcal{C})$.

Picard group and the connected component of the identity

Picard group

We can define the group $\mathrm{Pic}(\mathcal{C}) = \mathrm{Div}(\mathcal{C}) / \mathrm{Prin}(\mathcal{C})$.

There is a natural **degree** homomorphism

$$\begin{aligned} \mathrm{Div}(\mathcal{C}) &\longrightarrow \mathbb{Z} \\ \sum_{P \in \mathcal{C}(\overline{K})} n_P P &\longmapsto \sum_{P \in \mathcal{C}(\overline{K})} n_P \end{aligned}$$

which extends to $\mathrm{Pic}(\mathcal{C})$ and whose kernel is

$$\mathrm{Pic}^0(\mathcal{C}) = \{[D] = D + \mathrm{div}(f) \mid \deg(D) = 0, f \in k(\mathcal{C})\}$$

An example in the case of elliptic curves

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_5$ defined by $y^2 = x^3 + 1$

$$\begin{aligned} \operatorname{div}(x-2) &= (2,-2) + (2,2) - 2\infty \\ \operatorname{div}(y-x-1) &= (1,0) + (0,1) + (2,-2) - 3\infty \end{aligned}$$

Reorganising, we get that

$$\begin{aligned} (1,0) + (0,1) - 2\infty &= \operatorname{div}(y-x-1) - (2,-2) + \infty \\ &= \operatorname{div}(y-x-1) - \operatorname{div}(x-2) + (2,2) - \infty \\ &= \operatorname{div}\left(\frac{y-x-1}{x-2}\right) + (2,2) - \infty \end{aligned}$$

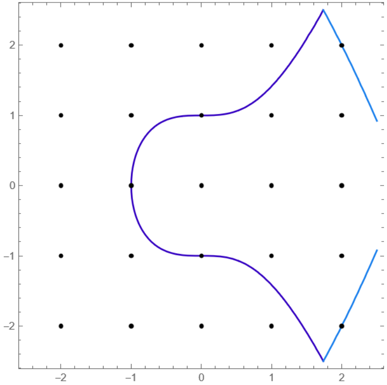
An example in the case of elliptic curves

Therefore, as

$$(1,0)+(0,1)-2\infty=\operatorname{div}(\tfrac{y-x-1}{x-2})+(2,2)-\infty,$$

over $\mathrm{Pic}^0(\mathcal{E})$ we get that

$$[(1,0)-\infty]+[(0,1)-\infty]=[(2,2)-\infty]$$



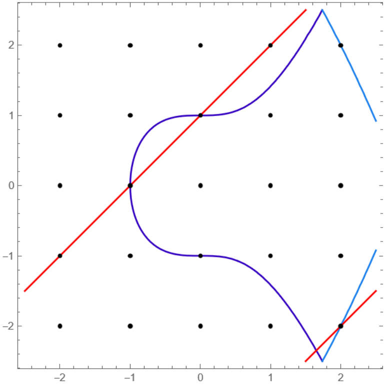
An example in the case of elliptic curves

Therefore, as

$$(1,0)+(0,1)-2\infty=\operatorname{div}(\tfrac{y-x-1}{x-2})+(2,2)-\infty,$$

over $\operatorname{Pic}^0(\mathcal{E})$ we get that

$$[(1,0)-\infty]+[(0,1)-\infty]=[(2,2)-\infty]$$



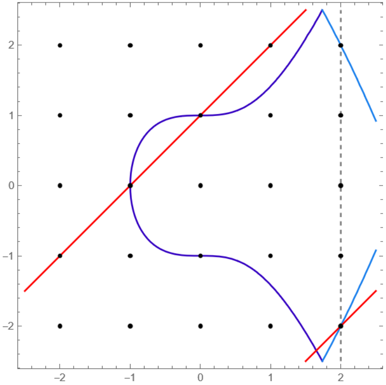
An example in the case of elliptic curves

Therefore, as

$$(1,0) + (0,1) - 2\infty = \mathrm{div}(\tfrac{y-x-1}{x-2}) + (2,2) - \infty,$$

over $\mathrm{Pic}^0(\mathcal{E})$ we get that

$$[(1,0) - \infty] + [(0,1) - \infty] = [(2,2) - \infty]$$



An example in the case of elliptic curves

Therefore, as

$$(1,0)+(0,1)-2\infty=\operatorname{div}\left(\tfrac{y-x-1}{x-2}\right)+(2,2)-\infty,$$

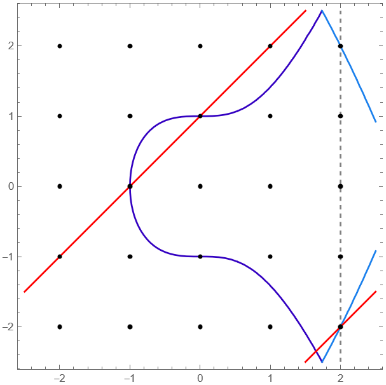
over $\mathrm{Pic}^0(\mathcal{E})$ we get that

$$[(1,0)-\infty]+[(0,1)-\infty]=[(2,2)-\infty]$$

This suggest that there is an isomorphism

$$\begin{aligned}\mathcal{E}(\overline{\mathbb{F}_5}) &\longrightarrow \mathrm{Pic}^0(\mathcal{E})\\ P &\longmapsto [P-\infty]\end{aligned}$$

Observation: the point ∞ is **special**.



Jacobian of a curve

Under the assumption that we choose a suitable point of $\mathcal{E}$, we can explicitly identify the elements of $\mathrm{Pic}^0(\mathcal{E})$ with the points of a projective variety $\mathcal{X}$ (in this case $\mathcal{E}$) in such a way that the operation in $\mathrm{Pic}^0(\mathcal{E})$ can be described nicely in terms of rational functions of $k(\mathcal{X})$.

Such a variety $\mathcal{X}$ is what is known as an **abelian variety**.

Jacobian of a curve

In general, it can be proven that, given a curve $\mathcal{C}$ of genus $g > 1$, the group $\mathrm{Pic}^0(\mathcal{C})$ can be identified with an abelian variety known as the **jacobian variety** $\mathcal{J}_{\mathcal{C}}$ of $\mathcal{C}$.

Furthermore, it can be seen that the dimension of $\mathcal{J}_{\mathcal{C}}$ is equal to the genus of $\mathcal{C}$.

Abel-Jacobi map

Considering a special point (for instance, ∞), there is a natural way of embedding $\mathcal{C}$ in its jacobian through the known as the **Abel-Jacobi map**:

$$\begin{aligned} \mathcal{C} &\longrightarrow \mathrm{Pic}^0(\mathcal{C}) \\ P &\longmapsto [P - \infty] \end{aligned}$$

In the complex case, this map can be computed explicitly by integrating differential forms of $\Omega^1(\mathbb{C}(\mathcal{C}))$.

Understanding the jacobian

Let us now assume that $\mathcal{C}$ is a hyperelliptic curve $y^2 = f(x)$ of genus $g > 1$ with f a polynomial with odd degree, and let

$$\begin{aligned} \iota : \mathcal{C} &\longrightarrow \mathcal{C} \\ (x, y) &\longmapsto (x, -y) \end{aligned}$$

Reduce representative for classes

As a consequence of Riemann-Roch, we have the following convenient result:

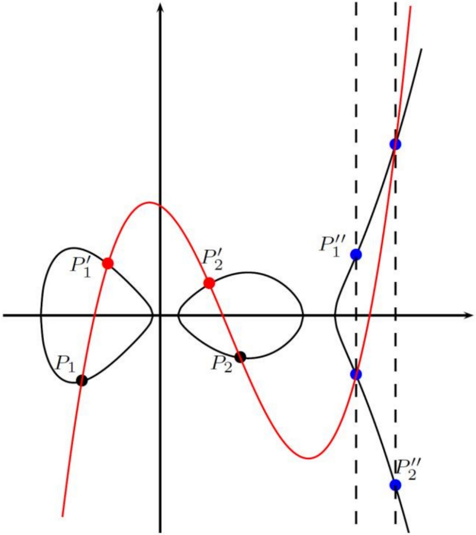
Every element $[D] \in \mathrm{Pic}^0(\mathcal{C})$ can be expressed in a unique way as

$$[D] = [P_1 + \cdots + P_r - r\infty]$$

for some $P_1, \ldots, P_r \in \mathcal{C}$ depending on $[D]$ such that

- $P_i \neq \infty$
- $P_i \neq \iota(P_j)$ for $i \neq j$
- $r \leq g$

Adding elements in the jacobian



Let $[D_1] = [P_1 + \cdots + P_r - r\infty]$ and $[D_2] = [P_1' + \cdots + P_s' - s\infty]$.

Consider the interpolation polynomial $g(x)$ that goes through all the P_i and P_j'.

Then, if the $g(x)$ intersects $\mathcal{C}$ in $\iota(P_1''), \ldots, \iota(P_t'')$,

$$[D_1] + [D_2] = [P_1'' + \cdots + P_t'' - t\infty]$$

Principally polarised supersingular abelian varieties

Projective models of the jacobian

We saw that an abelian variety is an algebraic group that can be embedded in some projective space.

For cryptographic applications, we are interested in finding an embedding of the jacobian in an actual projective space. When we fix such embedding (that is we find equations and set coordinates on our abelian variety), we say that it is a **principally polarised abelian variety** (PPAV).

Handwavy polarisations

A **polarisation** on an abelian variety is analogous to choosing a distinguished point ∞ on an elliptic curve: this choice of a divisor gives us embeddings in projective spaces via Riemann-Roch spaces.

This is not pretty, for instance, in the case of genus 2, we have that the jacobian can be embedded as 72 quadratic equations in $\mathbb{P}^{15}$ (Flynn) or, at best, as 10 quadratic and 3 cubic equations in $\mathbb{P}^8$ (Grant).

Why then?

Because we need to polarise abelian varieties to compute with them, from the cryptographic point of view, principally polarised abelian varieties are the “correct” higher-dimensional generalizations of elliptic curves.

How do principally polarised abelian varieties look like? 👀

1. Every 1-dimensional PPAV is an **elliptic curve**.

2. Every 2-dimensional PPAV is isomorphic to the **jacobian of a genus 2 curve** (necessarily hyperelliptic).

   ➡️ They can sometimes be isomorphic to the **product of 2 elliptic curves**.

$$
\begin{aligned}
y^2 = Ax^6 + Bx^4 + Cx^2 + D &\longrightarrow y^2 = Ax^3 + Bx^2 + Cx + D \\
(x, y) &\longmapsto (x^2, y)
\end{aligned}
$$

$$
\begin{aligned}
y^2 = Ax^6 + Bx^4 + Cx^2 + D &\longrightarrow y^2 = Dx^3 + Cx^2 + Bx + A \\
(x, y) &\longmapsto (1/x^2, y/x^3)
\end{aligned}
$$

How do principally polarised abelian varieties look like? 👀

❸ Every 3-dimensional PPAV is isomorphic to the **jacobian of a genus 3 curve** (either hyperelliptic or non-hyperelliptic).

- ➡️ They can sometimes be isomorphic to the **product of an elliptic curve with a genus 2 jacobian**.
  - ➡️ They can sometimes be isomorphic to the **product of 3 elliptic curves**.

Not all g-dimensional PPAVs are isomorphic to the jacobian of a curve for $g > 3$.

Some random facts about abelian varieties over finite fields

Let $\mathcal{A}$ be a g-dimensional abelian variety over $\mathbb{F}_q$. Then,

- The cardinality of $\mathcal{A}(\mathbb{F}_q)$ is

$$(q^{1/2} - 1)^{2g} \leq \#\mathcal{A}(\mathbb{F}_q) \leq (q^{1/2} + 1)^{2g}$$

- $\mathcal{A}[\ell^k](\overline{\mathbb{F}_q}) \cong (\mathbb{Z}/\ell^k\mathbb{Z})^{2g}$ when $\ell \neq p$.
- $\mathcal{A}[p^k](\overline{\mathbb{F}_q}) \cong (\mathbb{Z}/p^k\mathbb{Z})^r$ for $0 \leq r \leq g$ (independent of k).

Isogenies of abelian varieties

An **isogeny of abelian varieties** is a finite, (geometrically) surjective morphism that maps 0 to 0.

Given a principally polarised abelian variety $\mathcal{A}$ (with special divisor $[D]$), there is always a degree 1 isogeny λ_D from $\mathcal{A}$ to a dual abelian variety $\hat{\mathcal{A}}$.

This isogeny allows us to define a Weil pairing on the n-torsion $\mathcal{A}[n]$ by

$$\langle \quad , \quad \rangle_{\lambda_D} : \quad \mathcal{A}[n] \times \mathcal{A}[n] \longrightarrow \mu_n$$

for $(n, p) = 1$.

Isogeny of principally polarised abelian varieties

A subgroup $G \subseteq A[n]$ is **isotropic** if the Weil pairing $\langle\quad,\quad\rangle_{\lambda_D}$ is trivial when restricted to G.

An isotropic subgroup G is **maximal isotropic** if there is no isotropic subgroup of $\mathcal{A}$ which properly contains G.

Then, an **isogeny of principally polarised abelian varieties** is an isogeny whose kernel maximal isotropic.

Just why?

Why do we need this definition?

We need to respect polarisations if we want to realise the isogeny as a projective map.

For elliptic curves, any cyclic subgroup $G \subseteq E(k)$ of order ℓ coprime to the characteristic of k is maximal isotropic inside $\ker[\ell] = E[\ell]$. Hence, $E \to E/G$ is an isogeny of principally polarised abelian varieties.

Types of isogenies

- $(\ell, \ldots, \ell)$-isogenies, which are the isogenies with kernel isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^g$.
- Cyclic isogenies, which are the isogenies with kernel isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$.

These are all very difficult to compute (theta functions and projective embeddings). But the first kind are the main object of our isogeny graph.

Supersingular vs superspecial

Supersingular: isogenous to a product of supersingular elliptic curves.

Superspecial: supersingular and isomorphic as an unpolarised PPAV to a product of supersingular elliptic curves.

The distinction is subtle, but if you start with a superspecial PPAV and use only separable isogenies (no p-isogenies), then you stay superspecial.

That's all I had to say!