The genus-2 isogeny setting

Sabrina Kunzweiler
Ruhr-Universität Bochum

November 22, 2022

Talk in the Isogeny Club 2022.

Genus-2 curves and their Jacobians

What's a genus-2 curve?

Elliptic Curve $\mathcal{E}$

- Smooth, projective curve of genus-1 over a field K[1] with a specified base point.
- If $\mathrm{char}(K) \neq 2$, an elliptic curve admits an equation of the form

$$\mathcal{E} : y^2 = f(x), \text{ with } \deg(f) = 3,$$

and $\mathrm{disc}(f) \neq 0$, the **Weierstrass equation**.

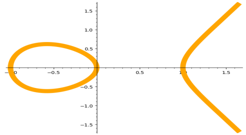


Figure 1: $y^2 = x(x^2 - 1)$

Today

- We consider smooth, projective curves of genus-2.
- If $\mathrm{char}(K) \neq 2$, a genus-2 curve admits an equation of the form

$$\mathcal{C} : y^2 = f(x), \text{ with } \deg(f) \in \{5, 6\},$$

and $\mathrm{disc}(f) \neq 0$, the **Weierstrass equation**.

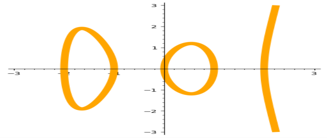


Figure 2: $y^2 = x(x^2 - 1)(x^2 - 4)$

[1] Throughout the presentation, all fields are perfect.

Points of genus-2 curves

The **set of points** of a genus-2 curve $\mathcal{C} : y^2 = f(x)$ is given by

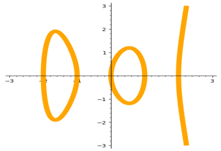
$$\mathcal{C}(\bar{K}) = \underbrace{\{(u,v) \in \bar{K}^2 \mid v^2 = f(u)\}}_{\text{affine points}} \cup \underbrace{\begin{cases} \{\infty\} & \text{if } \deg(f) = 5 \\ \{\infty_+, \infty_-\} & \text{if } \deg(f) = 6 \end{cases}}_{\text{point(s) at infinity}}.$$

A point $P \in \mathcal{C}(\bar{K})$ is K-rational if its coordinates are in K. The set of K-rational points is denoted $\mathcal{C}(K)$.

Example

$\mathcal{C} : y^2 = x(x^2-1)(x^2-4)$ over $\mathbb{F}_7$. The curve $\mathcal{C}$ has precisely 8 $\mathbb{F}_7$-rational points. More precisely,

$$\begin{aligned}\mathcal{C}(\mathbb{F}_7) = \{&\infty, (0,0), (1,0), (2,0),\\ &(5,0), (6,0), (3,1), (3,6)\}.\end{aligned}$$



❗ In contrast to elliptic curves, the set $\mathcal{C}(\bar{K})$ is **not** a group.

Weierstrass points

Let $\mathcal{C} : y^2 = f(x)$ be a genus-2 curve.

The **hyperelliptic involution** $\tau : \mathcal{C} \to \mathcal{C}$ is defined as $\tau(u, v) = (u, -v)$ on affine points and $\tau(\infty_\pm) = \infty_\mp$ if $\deg(f) = 6$, and $\tau(\infty) = \infty$ if $\deg(f) = 5$.

The **Weierstrass points** of $\mathcal{C}$ are the points fixed by τ.

- Every genus-2 curve has precisely 6 Weierstrass points in $\mathcal{C}(\bar{K})$.
- For example

$$\{\infty, (0,0), (1,0), (-1,0), (2,0), (-2,0)\}$$

  are the Weierstrass points of the curve $y^2 = x(x^2 - 1)(x^2 - 4)$.

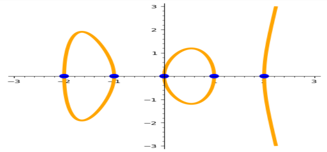


Figure 3: $\deg(f) = 5$

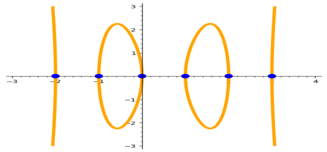


Figure 4: $\deg(f) = 6$

The divisor group

A **divisor** on a curve $\mathcal{C}/K$ is a formal sum of points:

$$D = \sum_{P \in \mathcal{C}(\bar{K})} n_P \cdot P, \text{ with } n_P \in \mathbb{Z}$$

and $n_P = 0$ for all but finitely many points P.

- The set of divisors on $\mathcal{C}$ forms a group, denoted $\mathrm{Div}_{\mathcal{C}}$.
- The degree of D is $\deg(D) = \sum_{P \in \mathcal{C}(\bar{K})} n_P$.
- The subgroup of divisors of degree-0 is denoted $\mathrm{Div}^0_{\mathcal{C}}$.
- A divisor D is K-rational, if it is fixed by the action of $\mathrm{Gal}(\bar{K}/K)$. Notation: $\mathrm{Div}_{\mathcal{C}}(K)$ and $\mathrm{Div}^0_{\mathcal{C}}(K)$.

Example $y^2 = x(x^2-1)(x^2-4)$ over $\mathbb{F}_7$

- $D_1 = 3 \cdot (0,0) - 2 \cdot (3,1) \in Div_{\mathcal{C}}$.
- Set $D_2 = (1,0) - (0,0)$, then $D_1 + D_2 = (1,0) + 2 \cdot (0,0) - 2 \cdot (3,1)$.
- $\deg(D_1) = 3 + (-2) = 1$.
- We have $D_3 = (4,i) + (4,-i) \in \mathrm{Div}_{\mathcal{C}}(\mathbb{F}_7)$, but $D_4 = (4,i) \notin \mathrm{Div}_{\mathcal{C}}(\mathbb{F}_7)$.

Equivalence of divisors

To a rational function $\phi \in \bar{K}(\mathcal{C})^*$, we associate the divisor

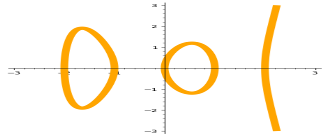
$$\operatorname{div}(\phi) = \sum_{P \in \mathcal{C}(\bar{K})} \operatorname{ord}_P(\phi) P \in \operatorname{Div}_{\mathcal{C}}^0,$$

where $\operatorname{ord}_P(\phi)$ is the order of vanishing of ϕ at P. A divisor of this form is called **principal**.

- Broadly: $\operatorname{div}(\phi)$ is the formal sum of the zeros and poles of ϕ, counted with multiplicity.
- $D, D' \in \operatorname{Div}_{\mathcal{C}}$ are called **equivalent** ($D \sim D'$) if $D - D'$ is a principal divisor.
- The equivalence classes of divisors form a group, the **Picard group** $\operatorname{Pic}_{\mathcal{C}}$.
- Similar to before, one defines $\operatorname{Pic}_{\mathcal{C}}^0, \operatorname{Pic}_{\mathcal{C}}(K)$ and $\operatorname{Pic}_{\mathcal{C}}^0(K)$.

Example $y^2 = x(x^2-1)(x^2-4)$ over $\mathbb{F}_7$

- $D_1 = \operatorname{div}(x-3) = (3,1) + (3,6) - 2 \cdot \infty$.
- $D_2 = (3,1) + (2,0) - (3,1) - (3,6) \sim D_3 = (3,1) + (2,0) - 2 \cdot \infty$, because $D_3 - D_2 = D_1$.



The Jacobian of a genus-2 curve

The **Jacobian** $\mathcal{J}(\mathcal{C})$ of a (genus-2) curve $\mathcal{C}$ over K is the 2-dimensional abelian variety such that over each field $K \subset L \subset \bar{K}$, we have $\mathcal{J}(\mathcal{C})(L) = \mathrm{Pic}^0_{\mathcal{C}}(L)$.

Two ways of viewing elements in $\mathcal{J}(\mathcal{C})(K)$:

1. $\mathcal{J}(\mathcal{C})(K) = \mathrm{Pic}^0_{\mathcal{C}}(K)$, and for any $R \in \mathcal{J}(\mathcal{C})(K) \setminus \{0\}$, there exist unique points $P_1, P_2 \in \mathcal{C}(\bar{K})$ with $\tau(P_1) \neq P_2$, so that

$$R = [P_1 + P_2 - D_\infty], \text{ with } D_\infty = \begin{cases} 2 \cdot \infty & \text{if } \deg(f) = 5, \\ \infty_+ + \infty_- & \text{if } \deg(f) = 6. \end{cases}$$

2. $\mathcal{J}(\mathcal{C})$ is a variety, i.e. the zero locus of a set of polynomials.
   - For example $\mathcal{J}(\mathcal{C})$ can be written as the zero locus of 72 polynomials in $\mathbb{P}^{15}$, so a point $R \in J(\mathcal{C})$ is of the form

$$R = (r_0 : r_1 : \cdots : r_{15}).$$

   - Comparison: Abelian varieties of dimension 1 are elliptic curves, and can be written as the zero locus of one polynomial in $\mathbb{P}^2$:

$$\mathcal{E} : Y^2 Z = X^3 + aXZ^2 + bZ^3.$$

Mumford presentation

Let $R \in \mathcal{J}(\mathcal{C})(K)$ and consider the unique presentation from the previous slide, i.e. $R = [P_1 + P_2 - D_\infty]$ and for simplicity assume that $P_1 = (u_1, v_1)$, $P_2 = (u_2, v_2)$ are affine points. We define

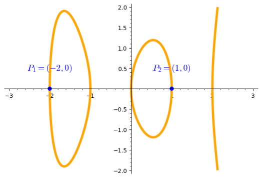
- $a = (x - u_1)(x - u_2) \in K[x]$,
- $b = b_1 x + b_0$, so that $b(u_1) = v_1$ and $b(u_2) = v_2$.

Then (a, b) is called the **Mumford presentation** of R and we denote $R = J(a, b)$.

Example: $y^2 = x(x^2 - 1)(x^2 - 4)$ over $\mathbb{F}_7$

Consider $(a, b) = (x^2 + x - 2, 0)$.
We have $a = (x - 1)(x + 2)$, hence

- $u_1 = 1, u_2 = -2$ and
- $v_1 = b(1) = 0$,
  $v_2 = b(-2) = 0$.



This means $R = J(a, b) = [(1, 0) + (-2, 0) - 2 \cdot \infty]$.

Isogenies of Jacobians of genus-2 curves

Torsion elements over a finite field (char$(K) = p$)

Elliptic Curve $\mathcal{E} : y^2 = f(x)$

- $\mathcal{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ for $m \in \mathbb{N}$ with $p \nmid m$.
- The **Weil pairing**

  $$e_m : \mathcal{E}[m] \times \mathcal{E}[m] \to \boldsymbol{\mu}_m$$

  is a bilinear, alternating pairing.

Example: $m = 2$, $f = \prod_{i=1}^{3}(x - r_i)$

- $\mathcal{E}[2] \setminus \{0\} = \{P_i = (r_i, 0) \mid i \in \{1, 2, 3\}\}$.
  $\Rightarrow$ Correspondence between Weierstrass points of $\mathcal{E}$ and 2-torsion elements of $\mathcal{E}$.

$$e_2(P_i, P_j) = \begin{cases} -1 & \text{if } i \neq j, \\ 1 & \text{otherwise.} \end{cases}$$

Genus-2 curve $\mathcal{C} : y^2 = f(x)$

- $\mathcal{J}(\mathcal{C})[m] \cong (\mathbb{Z}/m\mathbb{Z})^4$ for $m \in \mathbb{N}$ with $p \nmid m$.
- The **Weil pairing**

  $$e_m : \mathcal{J}(\mathcal{C})[m] \times \mathcal{J}(\mathcal{C})[m] \to \boldsymbol{\mu}_m$$

  is a bilinear, alternating pairing.

Example: $m = 2$, $f = \prod_{i=1}^{6}(x - r_i)$

- $\mathcal{J}(\mathcal{C})[2] \setminus \{0\} = \{R_{ij} = J\left((x - r_i)(x - r_j), 0\right) \mid i \neq j\}$.
  $\Rightarrow$ Correspondence between pairs of Weierstrass points of $\mathcal{C}$ and 2-torsion elements of $\mathcal{J}(\mathcal{C})$.

$$e_2(R_{ij}, R_{kl}) = \begin{cases} -1 & \text{if } \mid \{i, j\} \cap \{k, l\} \mid = 1, \\ 1 & \text{otherwise.} \end{cases}$$

(ℓ,ℓ)-isogenies with $\ell \neq p$

Elliptic Curves

- An **ℓ-isogeny** is an isogeny $\phi : \mathcal{E} \to \mathcal{E}' = \mathcal{E}/G$, where $G \cong \mathbb{Z}/\ell\mathbb{Z}$ (and $e_{\ell|_G} \equiv id$).
- Let (P, Q) be a (symplectic) basis for $\mathcal{E}[\ell]$. Then for any $a \in \mathbb{Z}/\ell\mathbb{Z}$, the group

$$G = \langle P + aQ \rangle$$

  defines an ℓ-isogeny.
- In total: $\ell + 1$ different ℓ-isogenies at $\mathcal{E}$ (we are missing the isogeny with kernel $G = \langle Q \rangle$ in the description above).

Jacobians of genus-2 curves

- An **(ℓ,ℓ)-isogeny** is an isogeny $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{A} = \mathcal{J}(\mathcal{C})/G$,[2] where $G \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ and $e_{\ell|_G} \equiv id$.
  $\Rightarrow G$ is called **maximal ℓ-isotropic**.
- Let (R_1, R_2, S_1, S_2) be a *symplectic* basis for $\mathcal{J}(\mathcal{C})[\ell]$, then for any $a, b, c \in \mathbb{Z}/\ell\mathbb{Z}$, the group

$$G = \langle R_1 + aS_1 + bS_2,\ R_2 + bS_1 + cS_2 \rangle$$

  defines an (ℓ,ℓ)-isogeny.
- In total: $\ell^3 + \ell^2 + \ell + 1$ different ℓ-isogenies at $\mathcal{J}(\mathcal{C})$ (we are missing $\ell^2 + \ell + 1$ isogenies in the description above).

[2] In general, $\mathcal{A}$ is a principally polarized abelian surface. In most cases this is again the Jacobian of a genus-2 curve $\mathcal{C}'$.

$(2,2)$-Isogenies

Let $\mathcal{C} : y^2 = g_1(x)g_2(x)g_3(x)$ with $g_i = g_{2,i}x^2 + g_{1,i}x + g_{0,i}$ and write

$$\delta = \det \begin{pmatrix} g_{1,0} & g_{1,1} & g_{1,2} \\ g_{2,0} & g_{2,1} & g_{2,2} \\ g_{3,0} & g_{3,1} & g_{3,2} \end{pmatrix}.$$

- The group $G = \langle J(g_1, 0), J(g_2, 0)\rangle = \{0, J(g_1, 0), J(g_2, 0), J(g_3, 0)\}$ is maximal 2-isotropic.
- If $\delta \neq 0$, then $\mathcal{J}(\mathcal{C})/G = \mathcal{J}(\mathcal{C}')$, where

  $$\mathcal{C}' : y^2 = h_1(x)h_2(x)h_3(x) \quad \text{with } h_i = \delta^{-1}(g'_{i+1}g_{i+2} - g_{i+1}g'_{i+2}).$$

  The isogeny $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ is called **Richelot isogeny**

Example $\mathcal{C} : y^2 = x(x^2 - 1)(x^2 - 4)$ over $\mathbb{F}_{11}$

Set $G = \langle J(x^2 - x, 0), J(x^2 + 3x + 2, 0)\rangle$. This means

$$\left.\begin{array}{lcrcrcr} g_1 & = & 0 & - & 1x & + & 1x^2, \\ g_2 & = & 2 & + & 3x & + & 1x^2, \\ g_3 & = & -2 & + & 1x & + & 0x^2. \end{array}\right\} \delta = -1 \text{ and } \begin{array}{ll} h_1 & = -x^2 + 4x - 3, \\ h_2 & = x^2 - 4x + 2, \\ h_3 & = -4x^2 - 4x + 2. \end{array}$$

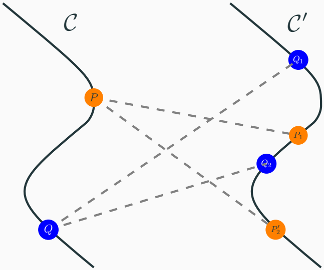
Hence $\mathcal{C}' : y^2 = 4x^6 + 5x^5 - 5x^4 - 2x^3 + x^2 - 2x - 1$

Richelot correspondence

To compute the images of points under the Richelot isogeny $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$, one can use the **Richelot correspondence**:

$$\mathcal{R}: \quad 0 = g_1(u)h_1(u') + g_2(u)h_2(u')$$
$$vv' = g_1(u)h_1(u')(u - u')$$

for points $(P, P') = ((u, v), (u', v')) \in \mathcal{C} \times \mathcal{C}'$.



The correspondence induces a map $\mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$:

$$[P + Q - D_\infty] \mapsto \underbrace{[P_1 + P_2 + Q_1 + Q_2 - 2D'_\infty]}_{\text{unreduced representation}} = [P' + Q' - D'_\infty].$$

Example $\mathcal{C} : y^2 = x(x^2-1)(x^2-4)$

With $G = \langle J(x^2-x,0), J(x^2+3x+2,0)\rangle$, we obtain the correspondence

$$\mathcal{R}: \quad 0 = 4uu'^2 - u^2 - 5uu' + 2u'^2 - 2u + 3u' + 4,$$
$$vv' = (u^2-u)(-u'^2+4u'-3)(u-u').$$

Let's compute the image of the element $R = J(x^2-x-1, 2x-4)$.

- $R = [(4,4)+(8,1)-2\cdot\infty]$.
- Set $P = (4,4)$ and $Q = (8,1)$.

$$\mathcal{R}_{(u,v)=P}: \quad 0 = -4(u'^2-4u'+5) = -4(u'-2-i)(u'-2+i)$$
$$4v' = -2u'-3.$$

  So $P_1 = (2+i, 1-5i)$, $P_2 = (2-i, 1+5i)$.
  Similarly: $Q_1 = (-3,0), Q_2 = (-4,-2)$.
- $\phi(R) = [P_1+P_2+Q_1+Q_2-2D_\infty] \in \mathcal{J}(\mathcal{C}')$ and it remains to compute the reduced form $[P'+Q'-D_\infty]$ using Cantor's algorithm.

Different methods for the evaluation of Richelot isogenies

Methods I

Goal: Given an element $J(a,b) \in \mathcal{J}(\mathcal{C})(K)$, compute $\phi(J(a,b)) \in \mathcal{J}(\mathcal{C})(K)$.

0. **Standard Algorithm** (from the last slide):
   - Requires factorization of the polynomial a.
   - Divisors $[P_1 + P_2 - D'_\infty]$ and $[Q_1 + Q_2 - D'_\infty]$ are possibly not K-rational.
1. **Gröbner basis approach** [Castryck-Decru '22]:
   Define

$$I = \big(a, y-b, y^2 - f(x), g_1(x)h_1(x') + g_2(x)h_2(x'),$$
$$yy' - g_1(x)h_1(x')(x-x')\big) \subset K[x,y,x',y']$$

   and compute the elimination ideal J with respect to x, y, i.e.

$$J = I \cap K[x', y'].$$

   In the general case: $J = (a_{new}(x'), y' - b_{new}(x'))$, where $\deg(a_{new}) = 4$ and $\deg(b_{new}) = 3$. The pair (a_{new}, b_{new}) is the (unreduced) Mumford presentation of $[P_1 + P_2 + Q_1 + Q_2 - 2D_\infty]$.
   - No factorizations or field extensions required.
   - Gröbner basis computation is "short" and can also be made explicit (see e.g. the Sagemath implementation of the attack [Oudompheng, Pope '22]).

Methods II

2. **Explicit Formulae** [K. '22]

   General idea: Perform computations symbolically with coefficients in $\mathbb{Z}[g_{00}, \ldots, g_{23}, a_1, a_0, b_1, b_0]$.

   $\Rightarrow$ Explicit formulae for the coefficients of the polynomials $a_{new} = x^4 + a_3' x^3 + a_2' x^2 + a_1' x + a_0',\ b_{new} = b_3' x^3 + b_2' x^2 + b_1' x + b_0'$ with $a_i', b_i' \in \mathbb{Z}[g_{00}, \ldots, g_{23}, a_1, a_0, b_1, b_0]$.

   - Problem: These formulae are huge and less efficient then the Gröbner basis computation with explicit values.

   Solution: Introduce a new form of hyperelliptic equation (similar to Montgomery form for elliptic curves):

$$\mathcal{C} : y^2 = E \cdot x(x^2 - Ax + 1)(x^2 - Bx + C)$$

   $\Rightarrow$ Compact formulae for the polynomials $a_{new'}, b_{new'}$.

   - As in approach 2, the computation of factorizations and field extensions is avoided.

3. **Kummer surface approach**

   Recall: As a a variety, $\mathcal{J}(\mathcal{C})$ can be written as the zero-locus of 72 equations in $\mathbb{P}^{15}$. We consider the Kummer surface $\mathcal{K} = \mathcal{J}(\mathcal{C})/\langle \pm 1 \rangle$. Explicit representation in $\mathbb{P}^3$:

   $$\mathcal{K} : F(x_0, x_1, x_2, x_3) = 0 \quad \text{for a quartic } F \in K[x_0, x_1, x_2, x_3].$$

   We denote $K(\mathcal{C}) = \mathcal{K}$.

   - $\mathcal{K}$ is *not* an abelian variety. In particular, the points on $\mathcal{K}$ do not form a group.
   - Analogue to x-only arithmetic for elliptic curves.
   - There exists an explicit representation for $\phi : \mathcal{K}(\mathcal{C}) \to \mathcal{K}(\mathcal{C}')$ corresponding to a $(2, 2)$-isogeny $\phi : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C}')$ [Cassels-Flynn '96].
   - There also exist $(2, 2)$-isogeny formulas on *squared* Kummer surfaces [Gaudry '07, Costello '18].

Methods IIIb

Using the curve form $\mathcal{C} : y^2 = (x^2 - 1)(x^2 - A)(Ex^2 - Bx + C)$, the map

$$\phi : \mathcal{K}(\mathcal{C}) \to \mathcal{K}(\mathcal{C}')$$

has a very compact representation $\phi : (x_0, x_1, x_2, x_3) \mapsto M \cdot (x_0^2, x_0x_1, \ldots, x_3^2)$ with $M \in \mathbb{Z}[A, B, C, E]^{4\times 10}$, [K. (in preparation)].

```
def KummerRichelot(coefficients, point):
        [A,B,C,E] = coefficients
        [x0,x1,x2,x3] = point

        y0 = (A*(E-C) - C)*x0^2 + C*x1^2 - B*x1*x2 + E*x2^2 + x0*x3
        y1 = A*B*x0^2 -2 (A*(C + E) + C)*x0*x1 + 2(A*E + C)*(C + E)/B*x1^2
          + B*(A + 1)*x0*x2 - 2*(A*E + C - E)*x1*x2 + B*x2^2 + x1*x3
        y2 = A*C*x0^2 - A*B*x0*x1 + A*E*x1^2 - (A*E - C + E)*x2^2 + x2*x3
        y3 = (A^2*(4*E^2 - B^2) - A*B^2)*x0^2 + A*B^2*x1^2 + 4*A*(2*C*E - A*B)*x0*x2
         - ((A + 1)*B^2 - 4*C^2)*x2^2 + 4*A*E*x0*x3 + 4*C*x2*x3 + x3^2

        return [y0,y1,y2,y3]
```

John William Scott Cassels and E Victor Flynn.
***Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230.**
Cambridge University Press, 1996.

Michael Stoll.
Arithmetic of hyperelliptic curves.
Summer Semester, 2014.

Wouter Castryck and Thomas Decru.
An efficient key recovery attack on sidh (preliminary version).
Cryptology ePrint Archive, 2022.

Sabrina Kunzweiler.
Efficient computation of $(2^n, 2^n)$-isogenies.
Cryptology ePrint Archive, 2022.

Thank you!