Torsion of Hyperelliptic curves (of genus 2)

Naina Praveen

14 Nov 2025

Set-Up

Let K be our base field (e.g., $\mathbb{Q}_p$ or a number field). Let C be a genus 2 curve defined over K. Over the algebraic closure $\bar{K}$, the points of the Jacobian correspond to the group of degree 0 divisor classes, i.e.,

$$J(\bar{K}) \cong \mathrm{Pic}^0(C_{\bar{K}}).$$

The absolute Galois group $G_K := \mathrm{Gal}(\bar{K}/K)$ acts on the curve C, and therefore acts on the divisor classes in $J(\bar{K})$.
The Jacobian is an abelian variety and we would like to understand its torsion.

What is $J[2]$?

Let $f(x)$ have six distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_6$. Denote

$$P_i := (\alpha_i, 0)$$

and let

$$\mathcal{W} := \{P_1, P_2, P_3, P_4, P_5, P_6\}$$

be the set of Weierstrass points.

Lore tells us that

$$J[2] \cong (\mathbb{Z}/2\mathbb{Z})^4 ,$$

so there are 16 elements.
Turns out, we can build $J[2]$ using our set of 6 Weierstrass points!

What is $J[2]$?

Proposition

Let $\mathcal{U} \subseteq \mathcal{W}$ be any subset of *even* cardinality. The elements of $J[2]$ are given by divisor classes of the form

$$D_{\mathcal{U}} := \sum_{P \in \mathcal{U}} P - \frac{|\,\mathcal{U}\,|}{2} \left(\infty_1 + \infty_2 \right).$$

How many such subsets are there?

$$\binom{6}{0} + \binom{6}{2} + \binom{6}{4} + \binom{6}{6} = 1 + 15 + 15 + 1 = 32.$$

That's double the number we need! :(

What is $J[2]$?

Fact: $[D_{\mathcal{U}}] = [D_{\mathcal{W}\setminus\mathcal{U}}]$.
(For example, $D_{\{P_1,P_2\}} = D_{\{P_3,P_4,P_5,P_6\}}$)

So, the number of distinct classes is $32/2 = 16$. Yay! :)

But why is this 2-torsion?

What is $J[2]$?

We would like to show that $2 \cdot [D_{\mathcal{U}}] = 0$, i.e., $2 \cdot D_{\mathcal{U}}$ is a principal divisor.

First, we consider $g_i = (X - \alpha_i)$. We want to understand $\mathrm{div}(g_i)$, so we need to find out the orders of its zeroes and poles. It clearly has a zero at α_i of order 2 and ∞_1, ∞_2 are simple poles. So,

$$\mathrm{div}(g_i) = 2P_i - (\infty_1 + \infty_2).$$

In particular, we have $2P_i \sim \infty_1 + \infty_2$ for every $i = 1, \ldots, 6$.

What is $J[2]$?

We now use this to understand $2 \cdot D_{\mathcal{U}}$ for an eveen subset $\mathcal{U} \subseteq \mathcal{W}$. We have

$$2 \cdot D_{\mathcal{U}} = 2\left(\sum_{P_i \in U} P_i - \frac{|\,\mathcal{U}\,|}{2}(\infty_1 + \infty_2)\right) = \sum_{P_i \in U} 2P_i - |\,\mathcal{U}\,|\,(\infty_1 + \infty_2).$$

Set $g_{\mathcal{U}} = \prod_{P_i \in \mathcal{U}}(x - \alpha_i)$. Then,

$$\begin{aligned}\operatorname{div}(g_{\mathcal{U}}) &= \sum_{P_i \in \mathcal{U}} \operatorname{div}(x - \alpha_i) = \sum_{P_i \in \mathcal{U}} (2P_i - (\infty_1 + \infty_2)) \\ &= \left(\sum_{P_i \in \mathcal{U}} 2P_i\right) - |\,\mathcal{U}\,|\,(\infty_1 + \infty_2) = 2 \cdot D_{\mathcal{U}}.\end{aligned}$$

So, $[D_{\mathcal{U}}] \in J[2]$.

WHAT IS $J[2]$?

So really, all this boils down to just taking $\mathcal{U} = \{P_i, P_j\}$, as

$$\begin{aligned} D_{\mathcal{U}} &= [P_i + P_j - (2/2)(\infty_1 + \infty_2)] \\ &= [P_i + P_j - (\infty_1 + \infty_2)] \\ &= [P_i + P_j - 2P_j] && (\text{as } 2P_j \sim \infty_1 + \infty_2) \\ &= [P_i - P_j] \end{aligned}$$

And $\binom{6}{2} = 15$ and $\mathcal{O}_J = D_\varnothing$.

What happens if you add two points in $J[2]$?

What is $J[2]$?

Claim: Let $\mathcal{U}, \mathcal{V} \subset \mathcal{W}$ be even cardinality subsets. Then,

$$D_{\mathcal{U}} + D_{\mathcal{V}} = D_{\mathcal{U}\Delta\mathcal{V}}.$$

Proof:

$$\begin{aligned}
D_{\mathcal{U}} + D_{\mathcal{V}} &= \left(\sum_{P\in\mathcal{U}} P - \frac{|\,\mathcal{U}\,|}{2}(\infty_1 + \infty_2)\right) + \left(\sum_{P\in\mathcal{U}} P - \frac{|\,\mathcal{V}\,|}{2}(\infty_1 + \infty_2)\right) \\
&= \left(\sum_{P\in\mathcal{U}} P + \sum_{P\in\mathcal{U}} P\right) - \left(\frac{|\,\mathcal{U}\,| + |\,\mathcal{V}\,|}{2}(\infty_1 + \infty_2)\right) \\
&= \left(\sum_{P\in\mathcal{U}\Delta\mathcal{V}} P + \sum_{P\in\mathcal{U}\cap\mathcal{V}} 2P\right) - \left(\frac{|\,\mathcal{U}\,| + |\,\mathcal{V}\,|}{2}(\infty_1 + \infty_2)\right) \\
&= \left(\sum_{P\in\mathcal{U}\Delta\mathcal{V}} P\right) + |\,\mathcal{U}\cap\mathcal{V}\,| \cdot (\infty_1 + \infty_2) - \left(\frac{|\,\mathcal{U}\,| + |\,\mathcal{V}\,|}{2}(\infty_1 + \infty_2)\right) \\
&= \sum_{P\in\mathcal{U}\Delta\mathcal{V}} P - \frac{|\,\mathcal{U}\Delta\mathcal{V}\,|}{2}(\infty_1 + \infty_2) \qquad \square
\end{aligned}$$

What is $J[2]$?

- Similarly(ish) one can show that $D_{\mathcal{U}} = D_{\mathcal{W} \setminus \mathcal{U}}$.
- What if $\deg(f(x)) = 5$? Can define $D_{\mathcal{U}} = \sum_{P \in U} P - \mid U \mid \cdot \infty$.

What is $J[3]$?

What about $J[3]$?
Not as nice, sadly :(

But, thanks to Tim Dokchitser, Christopher Doris and Harry Spencer, we have the following:

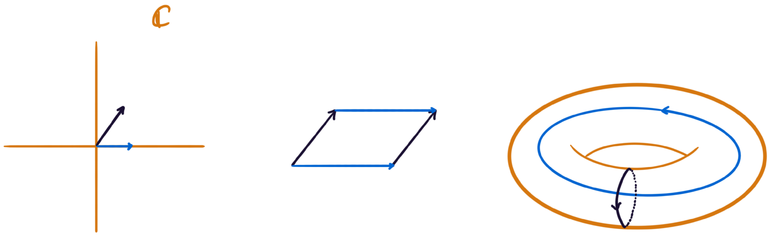
Proposition

Let C/K be a genus 2 curve over a field of characteristic different from 2 and 3 with model $y^2 = f(x)$. There is a one-to-one correspondence between the non-zero 3-torsion points of $J(C)$ and the union of the three sets of tuples $(u_1, \ldots, u_7), (v_1, \ldots, v_6)$ and $(w_1, \ldots, w_5)$ respectively satisfying the equalities

$$\begin{aligned} f(x) &= (u_4x^3 + u_3x^2 + u_2x + u_1)^2 - u_7(x^2 + u_6x + u_5)^3 \\ &= (v_4x^3 + v_3x^2 + v_2x + v_1)^2 - v_6(x + v_5)^3 \\ &= (w_4x^3 + w_3x^2 + w_2x + w_1)^2 - w_5. \end{aligned}$$

What is $J[n]$?

Now, let us try to understand n-torsion for any n. First, let's go back to an elliptic curve. We know that $E \cong \mathbb{C}/\Lambda$, for some lattice $\Lambda \subset \mathbb{C}$.



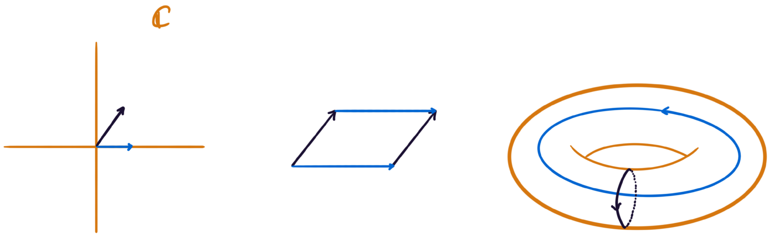
We're going to look at "periods" to determine how we get to the torus from a lattice.

What is $J[n]$?

(Black box) Fact:

The dimension of the space of holomorphic differentials on a compact Riemann surface is equal to its genus g.

In our case, the genus is 1 and you may have encountered the invariant differential $\omega = dx/y$.



Our torus has two fundamental loops, call them γ and δ.

What is $J[n]$?

So, we let

$$\int_\gamma \omega = \tau_1 \quad \text{and} \quad \int_\delta \omega = \tau_2,$$

and then our lattice is given by

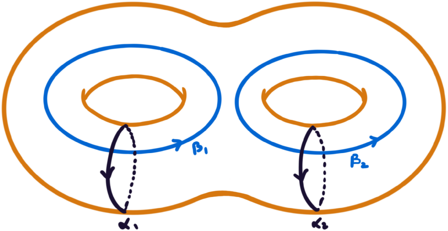
$$\Lambda = \mathbb{Z}\tau_1 + \mathbb{Z}\tau_2.$$

So, finding $P \in E$ such that $n \cdot P = \mathcal{O}_E$, is the same as finding $z \in \mathbb{C}$ such that $n \cdot z \in \Lambda$. These are generated by $(k_1\tau_1)/n$ and $(k_2\tau_2)/n$, for $k_i \in \{0, \ldots, n-1\}$. There are n^2 and $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

What is $J[n]$?

An analogous process works for genus 2 curves, instead we go from $\mathbb{C}^2$ to a two-holed torus.

$\mathbb{C}^2$



What is $J[n]$?

Fact:

For a hyperelliptic curve, a basis for the space of holomorphic differentials is given by $x^i dx/y$, where $i = 0, \ldots, g-1$.

So, for our genus 2 curve, we have a basis given by $\omega_1 = dx/y$ and $\omega_2 = xdx/y$. Set

$$\omega = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} dx/y \\ xdx/y \end{pmatrix}.$$

Our double donut has four fundamental loops $\gamma_1, \gamma_2, \delta_1, \delta_2$, and so we obtain

$$\tau_1 = \int_{\gamma_1} \omega = \begin{pmatrix} \int_{\gamma_1} dx/y \\ \int_{\gamma_1} xdx/y \end{pmatrix}, \quad \tau_2 = \int_{\gamma_2} \omega = \begin{pmatrix} \int_{\gamma_2} dx/y \\ \int_{\gamma_2} xdx/y \end{pmatrix}$$

$$\tau_3 = \int_{\delta_1} \omega = \begin{pmatrix} \int_{\delta_1} dx/y \\ \int_{\delta_1} xdx/y \end{pmatrix} \quad \tau_4 = \int_{\delta_2} \omega = \begin{pmatrix} \int_{\delta_2} dx/y \\ \int_{\delta_2} xdx/y \end{pmatrix}$$

This $g \times 2g$ matrix is called the "period matrix".

WHAT IS $J[n]$?

Sidenote: The $g \times 2g$ period matrix can be written as

$$[A_{g\times g} \mid B_{g\times g}] \Rightarrow [A^{-1}A \mid A^{-1}B] = [I_{g\times g} \mid A^{-1}B_{g\times g}],$$

and sometimes people call $A^{-1}B$ the period matrix.

So, we have $\Lambda = \mathbb{Z}\tau_1 + \mathbb{Z}\tau_2 + \mathbb{Z}\tau_3 + \mathbb{Z}\tau_4$. Our n-torsion points are given by $k_i\tau_i/n$, and so $J[n] \cong (\mathbb{Z}/n\mathbb{Z})^4$.

What is $J[n]$?

To get the points back on the curve, we know that the isomorphism between E and $\mathbb{C}/\Lambda$ is given via the Weierstrass $\wp$ function, in particular $(x, y) = (\wp(z), \wp(z)')$. Using this isomorphism, we can write

$$\wp(nz) = \wp(z) - \text{ some recurrence}$$

to obtain things called **division polynomials**. The solutions to this n-divison polynomials give you the x-coordinates of the n-torsion. For example, for an elliptic curve $y^2 = x^3 + Ax + B$,,

$$\begin{aligned}
\psi_0 &= 0, \quad \psi_1 = 1, \quad \psi_2 = 2y, \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
&\vdots \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad \text{for } m \geq 2 \\
\psi_{2m} &= \left(\frac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \qquad \text{for } m \geq 3
\end{aligned}$$

What is $J[n]$?

TL,DR; they look ugly.

You can do the same for hyperelliptic curves of genus 2, but I am not going to write them down. See Kanayama (2005).

Computers work with points on Jacobians using a thing called Mumford representation, which essentially represents (almost) every divisor on J as two polynomials $(u(x), v(x))$. There is a way to compute division polynomials using these Mumford coordinates (they still ugly), see Bernatska (2025).

What about J_{tors}?

What about $J_{\mathrm{tors}} = \bigcup_n J[n]$?

Good news and bad news! There's no equivalent of Mazur's theorem, but some things follow analogously to elliptic curves.

Let K be a local field, and let $\varphi : E(K) \to \widetilde{E}(k)$ be the reduction map, and let $E_1(K) = \ker(\varphi)$. Then, $E_1(K) \cong \mathfrak{m}$, the maximal ideal in K. Using the theory of formal groups, one can show that $E_1(K)$ contains no n-torsion for $(n, p) = 1$.

Similarly, we have a reduction map $\varphi : J(K) \to \widetilde{J}(k)$ with kernel $J_1(K)$, and $J_1(K) \cong \mathfrak{m} \times \mathfrak{m}$. Using the theory of formal groups again, one can show that $J_1(K)$ contains no n-torsion if $(n, p) = 1$.

What about J_{tors}?

There exists a short exact sequence

$$0 \to J_1(K) \to J(K) \to \widetilde{J}(k) \to 0.$$

So, to compute $J(K)_{\text{tors}}$, we can compute $\#\widetilde{J}(k)$ for some nice p's, and we must have that $J(K)_{\text{tors}}$ is a subgroup of all of these $\widetilde{J}(k)$'s, so in particular $\#J(K)_{\text{tors}}$ must divide the gcd of $\#\widetilde{J}(k)$'s.

One can then use heights to narrow search space and actually compute these points.

Example

Consider

$$y^2 = x^8 + 2x^7 + 3x^6 + 4x^5 + 9x^4 + 8x^3 + 7x^2 + 2x + 1.$$

It's bad primes of reduction are $2, 3, 13177$.

One can compute $\#J(\mathbb{F}_p)$ using the formula

$$\#\widetilde{J}(\mathbb{F}_p) = \frac{1}{2}(\#C(\mathbb{F}_p)^2 + \#C(\mathbb{F}_{p^2})) - p.$$

We compute that $\#\widetilde{J}(\mathbb{F}_5) = 180$ and $\#\widetilde{J}(\mathbb{F}_7) = 666$, so $\#J(\mathbb{Q})_{\text{tors}} \mid 18$. A closer inspection shows that

$$\#\widetilde{J}(\mathbb{F}_5) \cong \mathbb{Z}/3Z \times \mathbb{Z}/60\mathbb{Z} \quad \text{and} \quad \#\widetilde{J}(\mathbb{F}_7) \cong \mathbb{Z}/666\mathbb{Z},$$

so we may conclude that $J(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/6\mathbb{Z}$.

One can show that $\#J(\mathbb{Q})[2] = 2$, and the point $[(0, -1) - \infty_1]$ is a rational point of order 3.

What do we do with torsion? Galois theory!

The coordinates of the n-torsion points are algebraic numbers, so we can adjoin these coordinates to K to obtain $K(J[n])$, called the **n-division field**.

How does $G_{\overline{K}/K}$ act on this field?

How does $G_{\overline{K}/K}$ act on $K(J[n])$?

$J[n]$ is a 4-dimensional vector space. By picking P_1, P_2, P_3, P_4 of $J[n]$ as a basis, we can represent any automorphism of this space as a 4×4 matrix. Because the Galois action respects linearity, we can actually get a representation

$$\rho_n : G_K \to \mathrm{GL}_4(\mathbb{Z}/n\mathbb{Z}).$$

Question: Is the image actually all of $\mathrm{GL}_4(\mathbb{Z}/n\mathbb{Z})$?
Answer: No, because I lied.

$\mathbb{C}^2/\Lambda$ is not automatically a Jacobian. It is an analytic description of the Jacobian, but we need an algebraic description as well.

A necessary and sufficient ingredient required for a complex torus $\mathbb{C}^g/\Lambda$ to be a projective variety is the existence of a positive definite Hermitian form H on $\mathbb{C}^g$ such that the imaginary part $E := im(H)$ on $\Lambda \times \Lambda$ is integral. This form H is called a **polarisation**.

For a Jacobian, there is a canonical choice of this pairing that we are going to call a **principal polarisation**. More precisely, our Jacobian comes with a map

$$J \times J \longrightarrow \mathbb{Z}.$$

What on earth does this mean for us?

Let K be a field containing the n^{th} roots of unity. We can define a Weil pairing

$$e_n : J[n] \times J[n] \longrightarrow \mu_n(K),$$

that is a bilinear, alternating, non-degenerate form, a.k.a a symplectic form. This means that $J[n]$ is actually a symplectic vector space over $\mathbb{Z}/n\mathbb{Z}$!

So, we actually get a map from

$$\rho_n : G_K \longrightarrow \mathrm{GSp}_4(\mathbb{Z}/n\mathbb{Z}).$$

Open image theorems

Serre in 1972 showed that for non-CM elliptic curves, the image of $\rho_n : G_K \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is surjective for all but finitely many primes. This is called the open-image theorem.

In 1986, in a letter to Vignèras, Serre showed that for a dimension 2 (or 6, or an odd dimension) abelian variety, if the endomorphism ring of the abelian variety is $\mathbb{Z}$, then image of ρ_ℓ is surjective on $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for all but finitely many primes.