PAWS: Elliptic Curves and Abelian Varieties

Nir Elber

Fall 2023

Contents

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Theme 1
Homeworks

1.1 Homework 1

Problem 1.1.1. Go to https://www.lmfdb.org/Variety/Abelian/Fq/ and familiarize yourself with the database. Most of the words are probably unfamiliar right now, but by the end of PAWS you should have a pretty good idea of what most of them mean. Here are some questions to make this interesting:

(a) How many isogeny classes of elliptic curves defined over finite fields does the LMFDB currently contain?

(b) What percentage of these classes of curves are supersingular?[a]

(c) How many isogeny classes of elliptic curves defined over finite fields in the LMFDB have exactly 1 rational point?

(d) Write down all elliptic curves defined over $\mathbb{F}_2$.

  (i) How many of these are supersingular?

  (ii) How many rational points do they have?

  (iii) One of these curves should have exactly one rational point. What is the characteristic polynomial of its Frobenius endomorphism?

  (iv) Compare it to the L-polynomial of the isogeny class found in item (c).

[a] See [Sil09, Chapter 5] for the definition of ordinary/supersingular elliptic curves.

Problem 1.1.2. Let E be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $y^2z = x^3 + 17z^3$. Note that the following points are on $E(\mathbb{Q})$:

$$P = [-2 : 3 : 1], \quad Q = [4 : 9 : 1].$$

(a) Find at least five points on $E(\mathbb{Q})$ that are integer linear combinations[a] of P and Q.

(b) If you did item (a) by hand, check your calculations using your favorite computer algebra system.[b]

(c) Look up this curve in the LMFDB.

[a] In fact, we can obtain every point in $E(\mathbb{Q})$ in this way!
[b] For the relevant commands in SAGE, see this link.

Problem 1.1.3. Let E be the elliptic curve over $\mathbb{Q}$ defined by

$$y^2z = x^3 - xz^2.$$

(a) Using the group law defined in the lecture notes, compute the set of 2-torsion points $E[2](\overline{\mathbb{Q}})$.

(b) Compute the 3-torsion points $E[3](\overline{\mathbb{Q}})$.[a]

(c) Verify that this is a minimal Weierstrass equation over $\mathbb{Q}$, in the sense of [Sil09, Chapter VII]. Show that in characteristic 2, the same equation above defines a singular curve. In particular, conclude that E has bad reduction at 2.

(d) Verify that the same equation defines an elliptic curve $\bar{E}$ over $\mathbb{F}_3$. Compute the set of 3-torsion points $\bar{E}[3](\overline{\mathbb{F}}_3)$, and determine whether $\bar{E}$ is ordinary or supersingular.

(e) ($\star\star\star$) Show that $(x, y) \mapsto (-x, iy)$ defines an endomorphism of $\bar{E}_{\mathbb{F}_{3^2}}$. Here i is a root of $x^2 + 1 \in \mathbb{F}_3[x]$. Can you use this to determine the endomorphism ring of $\bar{E}_{\mathbb{F}_{3^2}}$?[b]

[a] Hint: $3P = 0$ implies that $2P = -P$.
[b] Hint: consider the p-Frobenius, c.f. below.

Problem 1.1.4. Let $q = p^r$ be a power of p, and assume $p > 3$. Let $E/\mathbb{F}_q$ be an elliptic curve with Weierstrass equation $E : y^2z = x^3 + Axz^2 + Bz^3$, with $A, B \in \mathbb{F}_q$. Define the *p-Frobenius twist* $E^{(p)}$ of E to be the curve defined by the Weierstrass equation $E^{(p)} : y^2z = x^3 + A^p x^2 z + B^p xz^2$. We define the *$p$-Frobenius morphism* $\phi_p : E \to E^{(p)}$ to be the morphism given by $\phi_p : [x_0 : y_0 : z_0] \mapsto [x_0^p : y_0^p : z_0^p]$ on $\overline{\mathbb{F}_q}$-points.

(a) Show that $\Delta(E^{(p)}) = \Delta(E)^p$ and $j(E^{(p)}) = j(E)^p$. Conclude that $E^{(p)}$ is an elliptic curve.[a]

(b) Verify that ϕ_p is an isogeny. That is, verify that it is a morphism of abelian varieties which is surjective on $\bar{\mathbb{F}}_q$-points and has finite kernel.

Now, define the *q-Frobenius endomorphism* by $\phi_q := \phi_p^r$. Note that $\phi_q([x_0 : y_0 : z_0]) = [x_0^q : y_0^q : z_0^q]$.

(a) Show that ϕ_q is an endomorphism of E that commutes with any other endomorphism of E.

(b) Show that the $\mathbb{F}_q$-rational points of E are exactly the $\overline{\mathbb{F}_q}$-points of E fixed by ϕ_q. More generally, we have $E(\mathbb{F}_q n)$ is the set of fixed points of $\phi_{q^n} : E(\mathbb{F}_q b) \to E(\mathbb{F}_q b)$.

[a] This is to show that $E^{(p)}$ is a nonsingular plane cubic with a rational point O. You can use the fact that a plane cubic is nonsingular if and only if its discriminant is non-zero. For formulas of $\Delta(E)$ and $j(E)$, see [Sil09, Section III.1].

Problem 1.1.5. Let n be a square-free positive integer and let E be the elliptic curve $y^2 = x^3 - n^2x$. Let q be a power of a prime p, such that p does not divide $2n$, and $q \equiv 3 \pmod 4$. Show that

$$\#E(\mathbb{F}_q) = q + 1.$$

Problem 1.1.6. Let X_1 and X_2 be varieties over a field k.

(a) If X_1 and X_2 are given the structure of a group variety, show that their product $X_1 \times X_2$ naturally inherits the structure of a group variety.

(b) Suppose $Y := X_1 \times X_2$ carries the structure of an abelian variety. Show that X_1 and X_2 each have a unique structure of an abelian variety such that $Y = X_1 \times X_2$ as abelian varieties.

Proof. Here we go. Let (X_1, e_1, i_1, μ_1) and (X_2, e_2, μ_2) be our needed abelian varieties throughout.

(a) This is direct. Note that the object $X_1 \times X_2$ continues to be a geometrically integral projective variety because all these adjectives are preserved by base change and composition, allowing us to run around the following square.

$$\begin{tikzcd} X_1 \times X_2 \arrow[r] \arrow[d] & X_1 \arrow[d] \\ X_2 \arrow[r] & \operatorname{Spec} k \end{tikzcd}$$

Now, we define $e\colon \operatorname{Spec} k \to X_1 \times X_2$ as $e := (e_1, e_2)$. We define $\mu\colon (X_1 \times X_2)^2 \to (X_1 \times X_2)$ via the composite

$$(X_1 \times X_2)^2 \cong X_1^2 \times X_2^2 \xrightarrow{(\mu_1,\mu_2)} X_1 \times X_2.$$

Lastly, we define $i := (i_1, i_2)$ to be the inversion map $X_1 \times X_2 \to X_2 \times X_2$.

We would like to check that all of our diagrams commute. This is essentially immediate. For example, to check that

$$\begin{tikzcd} (X_1 \times X_2)^3 \arrow[r, "(\mu,1)"] \arrow[d, "(1,\mu)"'] & (X_1 \times X_2)^2 \arrow[d, "\mu"] \\ (X_1 \times X_2)^2 \arrow[r, "\mu"] & X_1 \times X_2 \end{tikzcd}$$

commutes, it is enough to check that it commutes on S-points for any scheme S (in particular, one can take $S = (X_1 \times X_2)^3$ and then plug in the point id_S), but then this will directly follow from the construction and some group theory. I won't write this out.

(b) Note that there is an inclusion map $\iota_\bullet\colon X_\bullet \to Y$ by $\iota_\bullet(x) := (x, e_2)$; rigorously, this is the map $(\mathrm{id}_{X_\bullet}, e_2)$; similarly, there are projection maps $\pi_\bullet\colon Y \to X_\bullet$ given by $\pi_\bullet(x_1, x_2) := x_\bullet$.

Now, for uniqueness, note that having $Y = X_1 \times X_2$ implies that $\mu_Y = (\mu_1, \mu_2)$ and $i_Y = (i_1, i_2)$ and $e_Y = (e_1, e_2)$. Thus, we can recover $e_\circ$ as $\pi_\bullet \circ e_Y$, we can recover $i_\bullet$ as $\pi_\bullet \circ i_Y \circ \iota_\bullet$, and we can recover $\mu_\bullet$ as $\pi_\bullet \circ \mu_Y \circ (\iota_\bullet, \iota_\bullet)$.

Now, for existence

■

Problem 1.1.7. Let A_1, A_2, B_1, B_2 be abelian varieties over a field k. Show that

$$\operatorname{Hom}(A_1 \times A_2, B_1 \times B_2) \cong \operatorname{Hom}(A_1, B_1) \times \operatorname{Hom}(A_1, B_2) \times \operatorname{Hom}(A_2, B_1) \times \operatorname{Hom}(A_2, B_2).$$

Proof. We will actually show that $A \times B$ is a biproduct in the category of abelian varieties, using the maps i_A, i_B, π_A, and π_B all defined in the previous problem. The result will then follow from general category theory. ■

Problem 1.1.8. A *ring variety* over a field k is a commutative group variety $(X, +, 0)$ over k, together with a ring multiplication morphism $X \times X \to X$ written as $(x, y) \mapsto x \cdot y$, and a k-rational point $1 \in X(k)$, such that the ring multiplication is associative, distributive with respect to addition, and 1 is a 2-sided identity element. Show that the only connected complete ring variety is a point.

Problem 1.1.9. Let G be a group variety over a field k.

(a) Show that there exists a unique irreducible component N containing the identity element e.

(b) Show that N is a normal subgroup of finite index in G.

(c) Show that irreducible components of G are exactly connected components of G. Conclude that if G is connected, then G is irreducible.

(d) Show that each open subgroup of G contains N.

(e) Show that each closed subgroup of finite index in G contains N.

(f) Conclude that if G is connected, then G is the only open subgroup and is the only closed subgroup of finite index.

Problem 1.1.10. Let X be a variety over a field k. Write $k[\epsilon] := k[t]/(t^2)$ for the ring of dual numbers over k, and let $S := \mathrm{Spec}(k[\epsilon])$. Write $\mathrm{Aut}^1(X_S/S)$ for the group of automorphisms of X_S over S which reduce to the identity on the special fiber $X \hookrightarrow X_S$.

(a) Let x be a k-valued point of X. Show that the tangent space $(T_X)_x := (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$ is in natural bijection with the space of $k[\epsilon]$-valued points of X which reduce to x modulo ϵ. (cf. [Har77, Chapter II, Exercise 2.8].)

(b) Suppose $X = \mathrm{Spec}(A)$ is affine. Then we have:

$$H^0(X, \mathcal{T}_{X/k}) \cong \mathrm{Hom}(\Omega^1_{A/k}, A) \cong \mathrm{Der}_k(A, A)$$

Show that $H^0(X, \mathcal{T}_{X/k}) \cong \mathrm{Aut}^1(X_S/S)$. We denote this isomorphism as $h : H^0(X, \mathcal{T}_{X/k}) \to \mathrm{Aut}^1(X_S/S)$. Then for a group variety X that is not affine, we can take an affine cover of X and get the isomorphism $h : H^0(X, \mathcal{T}_{X/k}) \to \mathrm{Aut}^1(X_S/S)$.

(c) Suppose X is a group variety over k. Let $\tau : S \to X$ be a tangent vector at e, the identity section. Let t_τ be the right translation by τ morphism, so it is an element in $\mathrm{Aut}^1(X_S/S)$. Show that the associated global vector field $\zeta := h^{-1}(t_\tau)$ is invariant under the right-translation map. That is, $t_y^*\zeta = \zeta$ for all $y \in X(k)$. Here, $t_y(x) = m(x, y)$ is the right translation by y morphism. [a]

[a] You can check [EVM12][Proposition 15, pg. 8] for a more explicit description of the associated vector field ζ. It turns out that the vector field is not preserved under the left translation. Can you see why?

Problem 1.1.11. Show that every morphism from the projective line to an abelian variety is constant.[a]

[a] Hint: The canonical bundle of an abelian variety is trivial.

Problem 1.1.12. Show that 1-dimensional abelian varieties have genus one. In particular, we can define an elliptic curve to be a 1-dimensional abelian variety.

Bibliography

[Har77] Robin Hartshorne. *Algebraic geometry*. Vol. No. 52. Graduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496. ISBN: 0-387-90244-9.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

[EVM12] Bas Edixhoven, Gerard Van der Geer, and Ben Moonen. *Abelian varieties*. Available at http://van-der-geer.nl/~gerard/AV.pdf. 2012.

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.