


ABELIAN VARIETIES OVER FINITE FIELDS: PROBLEM SET 1

SANTIAGO ARANGO-PÍÑEROS, SEOKHYUN CHOI, ALICE LIN, YUXIN LIN, AND MINGJIA ZHANG

Instructions: The goal of this problem set is to get some experience working with abelian varieties, with an emphasis on elliptic curves over finite fields. Problems marked (\star) , $(\star\star)$, and $(\star\star\star)$ denote beginner, intermediate, and advanced problems, respectively. For the computational problems () you may use [CoCalc](#) or [MAGMA](#)'s online calculators.

Elliptic curves. In the lecture notes, we discussed Weierstrass models for elliptic curves defined over a field k of characteristic different from 2. When $\text{char}(k) = 2$, elliptic curves still admit a long Weierstrass model

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$


To recall the invariants of an elliptic curve given in this form, you can fire up **SageMath** and type:

```
1 var("a1,a2,a3,a4,a6")
2 E = EllipticCurve([a1,a2,a3,a4,a6])
3 E.discriminant()
4 E.j_invariant()
```

Other useful commands for elliptic curves can be found [here](#).

Problem 1 (\star)

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:

- (1) How many isogeny classes of elliptic curves defined over finite fields does the LMFDB currently contain?
- (2) What percentage of these classes of curves are [supersingular](#)?^a
- (3) How many isogeny classes of elliptic curves defined over finite fields in the LMFDB have exactly 1 rational point?
- (4) ()^b Write down all elliptic curves defined over \mathbb{F}_2 .
 - (a) How many of these are supersingular?
 - (b) How many rational points do they have?
 - (c) One of these curves should have exactly one rational point. What is the characteristic polynomial of its Frobenius endomorphism?
 - (d) Compare it to the L -polynomial of the isogeny class found in [item 3](#).

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

^bYou can do this problem by hand, but you might want to use your favorite computer algebra system.

The [Mordell-Weil theorem](#) states that if A is an abelian variety defined over a number field K , then $A(K)$ is a finitely generated abelian group.

Problem 2 (\star)

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 $E(\mathbb{Q})$:

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

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

- (2) (≡) If you did [item 1](#) by hand, check your calculations using your favorite computer algebra system.^b
(3) Look up this curve in the LMFDB.

^aIn fact, we can obtain every point in $E(\mathbb{Q})$ in this way!

^bFor the relevant commands in SageMath, see [this link](#).

Abelian varieties over finite fields often arise as the “reduction modulo primes” of abelian varieties defined over a number field. For elliptic curves, this process is very concrete.

Problem 3 (★)

Let E be the elliptic curve over \mathbb{Q} defined by

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

- (1) Using the group law defined in the lecture notes, compute the set of 2-torsion points $E[2](\overline{\mathbb{Q}})$.
- (2) Compute the 3-torsion points $E[3](\mathbb{Q})$.^a
- (3) 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.
- (4) 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.
- (5) (★★) 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

^aHint: $3P = 0$ implies that $2P = -P$.

^bHint: consider the p -Frobenius, c.f. below.

In this question, we are going to study a distinguished element in the endomorphism ring of an elliptic curve over finite field: the famous Frobenius endomorphism.

Problem 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 $E^{(p)}: y^2z = x^3 + A^p xz^2 + B^p z^3$. We define the p -Frobenius morphism $\phi_p: E \rightarrow E^{(p)}$ 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.

- (1) Show that $\Delta(E^{(p)}) = \Delta(E)^p$ and $j(E^{(p)}) = j(E)^p$. Conclude that $E^{(p)}$ is an elliptic curve.^a
- (2) Verify that ϕ_p is an isogeny. That is, verify that it is a morphism of abelian varieties which is surjective on $\overline{\mathbb{F}}_q$ -points and has finite kernel.

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

- (1) Show that ϕ_q is an endomorphism of E that commutes with any other endomorphism of E .
- (2) 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 $\phi_{q^n}: E(\overline{\mathbb{F}}_q) \rightarrow E(\overline{\mathbb{F}}_q)$.

^aThis 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 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

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

Generalities on abelian varieties. As a first (underwhelming) example of a higher-dimensional abelian variety, you can take the product of two elliptic curves!

Problem 6 (★ [EVdGM12, Exercise 1.1 in pg. 15])

Let X_1 and X_2 be varieties over a field k .

- (1) 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.
- (2) 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.

Morphisms between products of abelian varieties decompose.

Problem 7 (★★ [EVdGM12, Exercise 1.4 in pg. 15])

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

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

In the lecture notes, we defined group varieties as group objects in the category of k -varieties. What about ring varieties?

Problem 8 (★★ [EVdGM12, Exercise 1.3 in pg. 15])

A ring variety over a field k is a commutative group variety $(X, +, 0)$ over k , together with a ring multiplication morphism $X \times X \rightarrow X$ 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.

The following problems require some background in Algebraic Geometry. By definition, irreducible topological spaces are connected. The converse is true for group varieties.

Problem 9 (★★★)

Let G be a group variety over a field k .

- (1) Show that there exists a unique irreducible component N containing the identity element e .
- (2) Show that N is a normal subgroup of finite index in G .
- (3) Show that irreducible components of G are exactly connected components of G . Conclude that if G is connected, then G is irreducible.
- (4) Show that each open subgroup of G contains N .
- (5) Show that each closed subgroup of finite index in G contains N .
- (6) Conclude that if G is connected, then G is the only open subgroup and is the only closed subgroup of finite index.

Problem 10 (★★★ [EVdGM12, Exercise 1.2 in pg. 15])

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 $X \hookrightarrow X_S$.

- (1) 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].)
- (2) Suppose $X = \mathrm{Spec}(A)$ is affine. Then we have:

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

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

- (3) Suppose X is a group variety over k . Let $\tau : S \rightarrow X$ 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 $\text{Aut}^1(X_S/S)$. 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

^aYou can check [EVdGM12][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?

The previous problem might be useful to solve the next two.

Problem 11 (***)

Show that every morphism from the projective line to an abelian variety is constant. ^a

^aHint: The canonical bundle of an abelian variety is trivial.

Problem 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.

REFERENCES

- [EVdGM12] Bas Edixhoven, Gerard Van der Geer, and Ben Moonen, *Abelian varieties*, 2012, Available at <http://van-der-geer.nl/~gerard/AV.pdf>, p. 331.
- [Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. No. 52, Springer-Verlag, New York-Heidelberg, 1977. MR 463157
- [Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

DEPARTMENT OF MATHEMATICS, EMORY UNIVERSITY, ATLANTA, GA 30322, USA

Email address: santiago.arango@emory.edu

URL: <https://sarangop1728.github.io/>