PAWS - Abelian Varieties over Finite Fields **Name:** Abhay Goel
Problem Set 1 **Date:** December 5, 2023

Exercise (Problem 1).

(a) When I last checked, LMFDB has 6184 elliptic curves defined over finite fields.

(b) Of these, 184 (i.e. 2.98

(c) There are 3, over $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_4$.

(d) Up to isomorphism, there are 5 elliptic curves over $\mathbb{F}_2$. One set of representative equations is:

$$y^2 + y = x^3 + x + 1$$
$$y^2 + xy + y = x^3 + 1$$
$$y^2 + y = x^3$$
$$y^2 + xy = x^3 + 1$$
$$y^2 + y = x^3 + x$$

  (a) The first, third, and fifth are supersingular, while the others are not.
  (b) They have 1 through 5 $\mathbb{F}_2$ points, respectively.
  (c) The first (with 1 rational point) has Frobenius endomorphism with characteristic polynomial $x^2 - 2x + 2$.
  (d) The isogeny class of the elliptic curve with 1 rational point over $\mathbb{F}_2$ has L-polynomial $1 - 2x + 2x^2$, which is the reciprocal polynomial of the characteristic above.

Exercise (Problem 2).

(a) We recall some basics. In the chart $z \neq 0$, we get E in the form $y^2 = x^3 + 17$. So, given points (a, b) and (c, d) on this curve, we can explicitly write the line between them as solutions of $y = b + \lambda(x - a)$ for

$$\lambda = \frac{d - b}{c - a}$$

If the third point of intersection with E is (u, v), then

$$x^3 + 17 = (b + \lambda(x - a))^2$$

The coefficient of x^2 is clearly $-\lambda^2$, so by the factorization $(x - a)(x - c)(x - u)$, we get

$$a + c + u = \lambda^2$$

i.e. $u = \lambda^2 - a - c$. Then v is immediate and the point $(u, -v)$ is the sum of these points on E.

For the case of $(a, b) = (-2, 3)$ and $(c, d) = (4, 9)$, we have that $\lambda = 1$, so $u = -1$ and $v = 4$. Hence $P + Q = [-1 : -4 : 1]$. Repeating this with $(a, b) = (-2, 3)$ and $(c, d) = (-1, -4)$, we have $\lambda = -7$, so $u = 52$ and $v = -375$. So, $2P + Q = [52 : 375 : 1]$.

We can also consider multiples of an individual point, e.g. $2P$. For this, $\lambda = \frac{3a^2}{2b} = 2$ is the slope of the tangent line, so $u = 8$ and $v = 23$. So $2P = [8 : -23 : 1]$.

Finally, most easily, we can compute $-P = [-2 : -3 : 1]$ and $-Q = [4 : -9 : 1]$ since these points form lines with P, Q, respectively, that pass through $O = [0 : 1 : 0]$.

(b) Done.

(c) Done.

Exercise (Problem 3).

(a) Note that clearly $[0 : 1 : 0]$ is 2-torsion (as the identity). The only other points of E that are 2-torsion are points in the chart $z \neq 0$ with $y = 0$. I.e. they are of the form $[x : 0 : 1]$, so they are solutions to $x^3 - x = 0$. These are $-1, 0, 1$ in $\overline{\mathbb{Q}}$. So, the 2-torsion points are $[0 : 1 : 0], [-1 : 0 : 1], [0 : 0 : 1], [1 : 0 : 1]$.

(b) Again, the identity is 3-torsion. Otherwise, let $P = [x : y : 1]$, and note that $3P = 0$ iff $2P = -P$. We have $-P = [x : -y : 1]$, so it remains to compute $2P = [u : -v : 1]$. From the notes, we have $u = \lambda^2 - 2x$ and $v = y + \lambda(u - x)$ for

$$\lambda = \frac{3x^2 - 1}{2y}$$

So, when $2P = -P$, we get $u = x$, which immediately implies $y = v$ as desired, and also requires $\lambda^2 = 3x$. I.e.

$$9x^4 - 6x^2 + 1 = (3x^2 - 1)^2 = 12xy^2 = 12x(x^3 - x) = 12x^4 - 12x^2$$

and so

$$0 = x^4 - 2x^2 - 1/3 = (x^2 - 1)^2 - 4/3$$

i.e. $x^2 - 1 = \pm 2/\sqrt{3}$, and so $x = \pm\sqrt{1 \pm 2/\sqrt{3}}$ has four solutions over $\overline{\mathbb{Q}}$. Each of these gives two points on E, so we have a total of nine 3-torsion points on E (including the identity).

(c) I'm not sure what this means; $\mathbb{Q}$ is not a local field. Note that the discriminant is 64, which is zero in $\mathbb{F}_2$, so indeed this is singular over $\mathbb{F}_2$ and has bad reduction.

(d) As the discriminant is not zero in $\mathbb{F}_3$, it indeed defines an elliptic curve there. For the computation of 3-torsion, much of the above still works, except of course division by 3. So, we seek solutions to:

$$0 = 3x^4 - 6x^2 - 1 = -1$$

which has no solutions. So, there are no 3-torsion points over $\overline{\mathbb{F}_3}$. Hence, $\overline{E}$ must be supersingular.

(e) TBD

Exercise (Problem 4).

(a) Directly:

$$\Delta(E^{(p)}) = -(4B^p)^2(-B^{2p}) - 8(2B^p)^3 = 16B^{4p} - 16B^{3p} = (16B^4 - 16B^3)^p$$

since $16 \in \mathbb{F}_p$, and

$$\Delta(E) = 16(4A^3 + 27B^2)$$

So I don't think the claim is true. If the p-Frobenius twist of E was defined by the Weierstrass equation

$$y^2z = x^3 + A^p xz^2 + B^p z^3$$

then we would have

$$\Delta(E^{(p)}) = 16(4(A^p)^3 + 27(B^p)^2) = \Delta(E)^p$$

as claimed. In this case, we would also have:

$$j(E^{(p)}) = -1728\frac{(4A^p)^3}{\Delta(E^{(p)})} = -1728\left(\frac{(4A)^3}{\Delta(E)}\right)^p = j(E)^p$$

again using that $4, 1728 \in \mathbb{F}_p$. Hence $E^{(p)}$ is defined by a nonsingular Weierstrass equation and so is an elliptic curve.

(b) To see that ϕ_p is a map of abelian varieties, it suffices to note that it is clearly a map of varieties, given by polynomial equations and mapping solutions of the first equation into solutions of the second, and it preserves the identity, since $\phi_p[0 : 1 : 0] = [0^p : 1^p : 0^p] = [0 : 1 : 0]$. To see that it is an isogeny, we wish to show that it surjects with finite kernel.

The surjectivity is clear, since $\overline{\mathbb{F}_q}$ is perfect, so every element is a p^{th} power. Further, if a point $[a : b : c]$ is in the kernel, then $[a^p : b^p : c^p] = [0 : 1 : 0]$, so $a = c = 0$ and $[a : b : c] = [0 : b : 0] = [0 : 1 : 0]$. So, the kernel is in fact trivial.