E. Dummit's Math 7359 ~ Elliptic Curves and Modular Forms, Fall 2023 ~ Homework 4, due Fri Nov 17th.

Problems are worth points as indicated. Solve whichever problems you haven't seen before that interest you the most (suggestion: between 15 and 25 points' worth). Starred problems are especially recommended. Submit your assignments via Gradescope.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Oct 26)

1. [1pt] Suppose that $\varphi : G \to H$ is a surjective group homomorphism. Show that for any $h \in H$ there is a bijection between $\varphi^{-1}(h)$ and $\ker \varphi$.
2. [2pts*] Use Riemann-Hurwitz to prove directly that if $\varphi : E_1 \to E_2$ is a nonconstant separable morphism of elliptic curves then φ is everywhere unramified.

0.1.2 Exercises from (Oct 30)

1. [1pt*] Show that for any integer m and any isogeny $\varphi : E_1 \to E_2$, we have $[m]_{E_2} \circ \varphi = \varphi \circ [m]_{E_1}$.
2. [0pts] Show that when $\text{char}(k) = 0$, the group E_{tor} of all torsion points on E is isomorphic to $(\mathbb{Q}/\mathbb{Z}) \times (\mathbb{Q}/\mathbb{Z})$. [Hint: Note that E_{tor} is the direct limit of $E[n!]$ as $n \to \infty$.]
3. [3pts*] On the elliptic curve $y^2 = x^3 - x$ with the isogeny $[i](x, y) = (-x, iy)$, calculate the dual $\hat{\varphi}$ for $\varphi = [a] + [b][i]$ with $a, b \in \mathbb{Z}$. Use the result to find $\deg \varphi$ and compute the associated quadratic form.
4. [1pt] Let φ be the Frobenius map. Show that $a + b\varphi$ is separable if and only if $\text{char}(k)$ does not divide a.

0.1.3 Exercises from (Nov 2)

1. [3pts*] Verify the Hasse bound for $E : y^2 = x^3 + 4x + 1$ over $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{11}$, and $\mathbb{F}_{13}$ (optionally, also over $\mathbb{F}_9$, $\mathbb{F}_{25}$, and $\mathbb{F}_{27}$).
2. [1pt] Suppose X is the sum of q independent random variables each of which takes the values 0 and 2 each with probability 1/2. Show that the standard deviation of X is $\sqrt{q}$.
3. [3pts*] Find $\zeta_V(T)$ for $V = \mathbb{P}^n$ and for $\mathbb{P}^1 \times \mathbb{P}^1$.
4. [2pts] Verify the Weil conjectures for $C = \mathbb{P}^1$.
5. [3pts*] Show that for elliptic curves, the Weil conjectures are equivalent to the statement that $\zeta_C(T) = \dfrac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$ where α and β are complex conjugates of absolute value $\sqrt{q}$.

0.1.4 Exercises from (Nov 6)

1. [1pt] Suppose $h \in k(E)$ is a rational function that takes only finitely many values on E. Show that h is constant. (Note as always that k is algebraically closed.)
2. [2pts*] Suppose E is defined over F and $E[m] \subseteq E(F)$. Show that F contains the mth roots of unity.
3. [2pts] Suppose E is defined over $\mathbb{Q}$ and $p > 2$ is a prime. Show that the p-torsion subgroup of $E(\mathbb{Q})$ is either cyclic or trivial.

0.2 Additional Exercises

1. [6pts] The goal of this problem is to describe how to evaluate a function on a divisor. Let C be a smooth projective curve. For a divisor $D = \sum_{P \in C} n_P P$, its <u>support</u> is the set of P for which $n_P \neq 0$. If $f \in k(C)$ is any rational function such that $\text{div}(f)$ and D have disjoint supports, we define $f(D) = \prod_{P \in C} f(P)^{n_P}$: then disjointness assures us that $f(D)$ is defined and nonzero.
   (a) Suppose $\varphi : C_1 \to C_2$ is nonconstant. Show that $f(\varphi^* D) = (\varphi_* f)(D)$ for all $f \in k(C_1)^*$and $D \in \text{div}(C_2)$.
   (b) Suppose $\varphi : C_1 \to C_2$ is nonconstant. Show that $f(\varphi_* D) = (\varphi^* f)(D)$ for all $f \in k(C_2)^*$and $D \in \text{div}(C_1)$.
   (c) Suppose $f, g \in k(x)$ have disjoint support on $\mathbb{P}^1$. Show that $f(\text{div}\, g) = g(\text{div}\, f)$.
   (d) Suppose $f, g \in k(C)$ have disjoint support on C. Prove <u>Weil reciprocity</u>: that $f(\text{div}\, g) = g(\text{div}\, f)$.

2. [7pts] The goal of this problem is to give another construction for the Weil pairing using Weil reciprocity (see the exercise above for relevant definitions). Let E be an elliptic curve and $P, Q \in E[m]$ for some positive integer m. Also let D_P and D_Q be any degree-0 divisors such that the point sum of D_P resolves to P, the point sum of D_Q resolves to Q, and the supports of these divisors are disjoint.

   (a) Show that mD_P and mD_Q are principal, say with $\text{div}(f_P) = mD_P$ and $\text{div}(f_Q) = mD_Q$.

   Now define the pairing $\langle P, Q\rangle = \dfrac{f_P(D_Q)}{f_Q(D_P)}$.

   (b) Show that once we select D_P and D_Q, $\langle P, Q\rangle$ is independent of the specific choices of f_P and f_Q. [Hint: Show that for $D \in \text{Div}^0(E)$, the value of $f(D)$ depends only on $\text{div}(f)$ and D.]

   (c) Show that $\langle P, Q\rangle$ is independent of the choices for D_P and for D_Q. [Hint: If $D_{P'}$ is another choice for D_P show that $D_P - D_{P'} = \text{div}(v)$ is principal and then use Weil reciprocity.]

   (d) Show that $\langle P, Q\rangle$ is an mth root of unity. [Hint: Use Weil reciprocity.]

   (e) Show that $\langle P, Q\rangle$ is the Weil pairing $e_m(P, Q)$.

3. [6pts*] The goal of this problem is to show that the Hasse bound also holds for singular elliptic curves. Suppose $q > 3$ is a prime power and E is a singular elliptic curve over $\mathbb{F}_q$.

   (a) Show that the singular point has coordinates in $\mathbb{F}_q$. [Hint: It is unique and thus fixed by the Galois group of $\overline{\mathbb{F}_q}/\mathbb{F}_q$.]

   By (a) we may apply an appropriate translation to move the singular point to $(0, 0)$ and thus assume that E has a Weierstrass equation of the form $y^2 = x^2(x + c)$ for some $c \in \mathbb{F}_q$.

   (b) When $c = 0$, so that the singularity of E is a cusp, show that the group E_{ns} of nonsingular points on E is isomorphic to the additive group $\mathbb{F}_q$. Deduce that $\#E(\mathbb{F}_q) = q + 1$. [Hint: Show that the map $\varphi : E_{ns} \to \mathbb{F}_q$ with $\varphi(X : Y : Z) = X/Y$ is a group isomorphism.]

   (c) When c is a nonzero square, so that the singularity of E is a node, show that the group of nonsingular points on E is isomorphic to the multiplicative group $\mathbb{F}_q^\times$. Deduce that $\#E(\mathbb{F}_q) = q$. [Hint: Show that the map $\varphi : E_{ns} \to \mathbb{F}_q^\times$ with $\varphi(X : Y : Z) = \frac{Y-\alpha X}{Y+\alpha X}$ is a group isomorphism, where $\alpha^2 = c$ in $\mathbb{F}_q$.]

   (d) When c is a nonsquare, so that the singularity of E is a node, show that the group of nonsingular points on E is isomorphic to the group $\mu_{q+1} = \{z \in \mathbb{F}_{q^2} : z^{q+1} = 1\}$ of $(q + 1)$st roots of unity in $\mathbb{F}_{q^2}$. Deduce that $\#E(\mathbb{F}_q) = q + 2$. [Hint: Show that the map $\varphi : E_{ns} \to \mu_{q+1}$ with $\varphi(x, y) = \frac{y-\alpha x}{y+\alpha x}$ is a group isomorphism, where $\alpha^2 = c$ in $\mathbb{F}_{q^2}$.]

   Remark: The three different cases in (b), (c), and (d) are respectively known as additive reduction, split multiplicative reduction, and nonsplit multiplicative reduction.

4. [6pts] The goal of this problem is to find some elliptic curves over finite fields having exactly 2023 points. You may find useful the observation that the number of points on $y^2 = x^3 + Ax + B$ modulo p is $p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3+Ax+B}{p}\right)$ where the symbol represents the Jacobi symbol modulo p.

   (a) Use the Hasse bound to find the range of possible primes p such that there could exist an elliptic curve $E/\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = 2023$.

   (b) Choose three primes p in the middle of the range for (a) and find an elliptic curve $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = 2023$. (You will want to use a computer for this.)

   (c) Find an elliptic curve $E/\mathbb{F}_p$ for the smallest and largest primes in the range for (a). (You will quickly see that this is much harder to do than for primes closer to 2023!)

5. [3pts] Choose a four-digit prime p. Plot a histogram for the number of points of at least 5000 randomly-chosen elliptic curves $y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$. What does the distribution look like? Can you identify any general or specific features?

   - Remark: The Sato-Tate conjecture, now proven, asks the same question but the other way around, namely: for a specific elliptic curve over different fields $\mathbb{F}_p$, what does the distribution of values of the quantity $\frac{1}{2\sqrt{p}}[\#E(\mathbb{F}_p) - p - 1] \in [-1, 1]$ look like?