E. Dummit's Math 7359 ~ Elliptic Curves and Modular Forms, Fall 2026 ~ Homework 2, due Mon Nov 9th.

Solve whichever problems you haven't seen before that interest you the most (suggestion: between 20 and 35 points' worth). Starred problems are especially recommended. Prepare 2-3 problems to present on the assignment due date. **Use of generative AI to solve any of the problems is expressly forbidden**; however, if after solving a problem you discover that generative AI gives an entertainingly wrong solution, you are welcome to mention that!

0.1 In-Lecture Exercises

0.1.1 Exercises from (Oct 5)

1. [2pts] Show that we have an exact sequence $1 \to k^* \to k(E)^* \stackrel{\text{div}}{\to} \text{Div}^0(E) \stackrel{(6)}{\to} E \to 0$ where div represents the divisor map $f \mapsto \text{div}(f)$ and (6) represents the map discussed in (6) that takes a divisor $\sum_P n_P[P]$ and evaluates it as a sum of points on E.

0.1.2 Exercises from (Oct 8)

1. [2pts*] Show that the additivity relation $d(x+y) = dx + dy$, the Leibniz rule $d(xy) = x\,dy + y\,dx$, and $da = 0$ for all $a \in k$ also imply the power rule $d(x^n) = nx^{n-1}dx$ and the quotient rule $d(\frac{x}{y}) = \frac{y\,dx - x\,dy}{y^2}$ in $\Omega^1(C)$.

2. [2pts] Suppose C/k is a curve and $x_1, x_2, \ldots, x_n \in k(C)$. For any rational function $f \in k(x_1, \ldots, x_n)$, show the "chain rule": that $df = f_{x_1}\,dx_1 + \cdots + f_{x_n}\,dx_n$, where f_{x_i} denotes the usual partial derivative. [Hint: First show the result for polynomials f, then use the quotient rule.]

3. [2pts] Let $\text{char}(k) \neq 3$. On the elliptic curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, let t be a uniformizer at ∞. Show that the ratio $\frac{\omega}{dt} = -\frac{dy/dt}{3x^2 + 2a_2x + a_4}$ evaluates to a quantity that is defined and nonzero at ∞.

4. [2pts] Show that the power series expansion method yields an injective ring homomorphism of the metric space $\mathcal{O}_P(C)$ (under the metric induced by the discrete valuation v_P) into the formal power series ring $k[[t]]$ (under the metric induced by the order valuation v_t, giving the lowest-degree term with a nonzero coefficient).

5. [1pt] When the characteristic of k is not equal to 3, show that the formula $\omega = -\frac{dy}{f_x(x,y)}$ evaluates to a quantity that is defined and nonzero at ∞.

0.1.3 Exercises from (Oct 15)

1. [2pts*] For a divisor D on C, let $\Omega(D)$ to be the space of differentials ζ such that $\text{div}(\zeta) \geq D$. Show $\Omega(D)$ is a vector space and that $\Omega(D)$ is isomorphic to $L(\mathcal{C} - D)$ where $\mathcal{C}$ is any element of the canonical class of C. [Hint: Fix a differential ω, let $f \in L(\mathcal{C} - D)$, and consider $f \mapsto f\omega$, remembering the minus sign in the definition of the Riemann-Roch space $L(\mathcal{C} - D)$!]

2. [2pts] If $D \geq 0$, show that Riemann-Roch is equivalent to the statement that $\dim_k[L(D)/L(0)] + \dim_k[\Omega(D)/\Omega(0)] = \deg(D)$.

0.1.4 Exercises from (Oct 19)

1. [1pt] Compute the ramification index $e_\varphi(P)$ at all $P \in \mathbb{P}^1$ for $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $\varphi(x) = x^3$.

2. [2pts] Let $f \in k(x)$ be a nonconstant rational function. Show that a finite point $P \in k$ is ramified for the map $f : \mathbb{P}^1(k) \to \mathbb{P}^1(k)$ if and only if $f'(P) = 0$. Deduce that f has only finitely many ramified points. Under what conditions on f will ∞ be ramified?

3. [2pts*] Suppose k is a(n algebraically closed) field of characteristic p and let the Frobenius morphism Frob : $\mathbb{P}^1(k) \to \mathbb{P}^1(k)$ be given by $\text{Frob}(x) = x^p$. Verify that $\#\text{Frob}^{-1}(Q) = 1$ for all $Q \in \mathbb{P}^1$, and show that Frob is ramified at every point. Deduce that the requirement that a morphism φ be separable is necessary to ensure there are only finitely many ramified points.

4. [2pts] For a morphism $\varphi : C_1 \to C_2$, with any nonzero $f \in k(C_2)$ and any $P \in C_1$, show that $\text{ord}_P(\varphi^* f) = e_\varphi(P)\text{ord}_{\varphi(P)}(f)$.

0.1.5 Exercises from (Oct 22)

1. [1pt] Show that the degree map is multiplicative on isogenies: $\deg(\varphi \circ \psi) = (\deg \varphi)(\deg \psi)$.

2. [2pts] Let E_1 and E_2 be elliptic curves and define $\text{Hom}(E_1, E_2)$ to be the collection of all isogenies from E_1 to E_2. Show that $\text{Hom}(E_1, E_2)$ is an abelian group under the addition operation $(\varphi + \psi)P = \varphi(P) + \psi(P)$ for all $P \in E_1$ (where the addition on the right is the sum under the group law on E_2) for $\varphi, \psi \in \text{Hom}(E_1, E_2)$.

3. [1pt] Let E be an elliptic curve and define $\text{End}(E) = \text{Hom}(E, E)$ to be the collection of all isogenies from E to itself. Show that E is a ring with 1 having no zero divisors, with addition given as in the exercise above and multiplication given by composition. [Hint: For the lack of zero divisors, consider degrees.]

4. [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 $\ker \varphi$.

5. [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.

6. [2pts*] Let $E : y^2 = x^3 + ax^2 + bx$ be an elliptic curve over a field of characteristic not 2, with $b \neq 0$ and $a^2 - 4b \neq 0$ and let $E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Show that the map $\varphi : E \to E'$ with $\varphi(x, y) = (y^2/x^2, y(x^2 - b)/x^2))$ is an isogeny with kernel $\Phi = \{(0, 0), \infty\}$. [Hint: Show φ is a morphism, that it maps ∞ to ∞, and note $y^2/x^2 = (x^2 + ax + b)/x$.]

0.1.6 Exercises from (Oct 26)

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. [2pts] 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. [2pts*] On the elliptic curve $y^2 = x^3 - x$ with the isogeny $[i](x, y) = (-x, iy)$ discussed previously, for $\varphi = [a] + [b][i]$ with $a, b \in \mathbb{Z}$, calculate $\hat{\varphi}$. Use the result to find $\deg \varphi$ and compute the associated quadratic form.

4. [1pt] Let φ be the p-power Frobenius map in characteristic p. Show that $a + b\varphi$ is separable if and only if the characteristic p does not divide a.

5. [2pts*] 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 $\mathbb{F}_{27}$).

6. [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 $\sqrt{q}$.

0.1.7 Exercises from (Oct 29)

1. [2pts] Find $\zeta_V(T)$ for $V = \mathbb{P}^n$ and for $V = \mathbb{P}^1 \times \mathbb{P}^1$.

2. [1pt] Verify the Weil conjectures for $C = \mathbb{P}^1$.

3. [2pts*] 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 $\sqrt{q}$.

0.1.8 Exercises from (Nov 2)

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*] With $E : y^2 = x^3 - 7x + 6$ over $\mathbb{F}_{13}$, compute $e_2((1,0),\infty)$, $e_2((1,0),(10,0))$, and $e_2(\infty,(1,0))$.
3. [3pts] With $E : y^2 = x^3 + 5$ over $\mathbb{F}_{13}$, compute $e_2((2,0),(5,0))$, $e_2((2,0),(6,0))$, and $e_2((5,0),(2,0))$.
4. [1pt*] Suppose E is defined over F and $E[m] \subseteq E(F)$. Show that F contains the mth roots of unity.
5. [1pt*] 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. [4pts] Our construction of the group law on an elliptic curve E relies on describing the points (P, Q, R) with $P + Q + R$ equal to the identity. The goal of this problem is to examine how much of the structure of a group is determined by this information. Let G be a multiplicative group with identity e and define $S = \{(g, h, k) \in G \times G \times G : ghk = e\}$ to be the set of ordered triples whose product is the identity.
   (a) Show that the set S along with the knowledge of which element of G is the identity fully determines the "multiplication-table function" $\cdot : G \times G \to G$ with $(g, h) \mapsto gh$.
   (b) Show that if G contains no elements of order 3, then S alone determines the group operation in G.
   (c) Find an example of a set S that does not uniquely determine the group structure of G.
2. [7pts*] The goal of this problem is to study curves of genus 2. So let C be a smooth projective curve of genus 2 and let $\mathcal{C}$ be the canonical class.
   (a) Show that $l(\mathcal{C}) = 2$ and deduce that $\mathcal{C}$ contains an effective divisor $D = P + Q$ for some points $P, Q \in C$ (which may be equal).
   (b) Continuing (a), let $x \in L(D)$ be nonconstant: then x has at most two poles, (potentially) located at P and Q. Show that x cannot have only one pole of order 1. [Hint: If so, then $x \in L(P)$; show this would imply C is isomorphic to $\mathbb{P}^1$.]
   (c) Continuing (b), deduce that $\deg(\mathrm{div}_x) = 2$ and thus that the extension degree $[k(C) : k(x)] = 2$ has degree 2. Conclude (when $\mathrm{char}(k) \neq 2$) that C is a hyperelliptic curve: a curve with an affine equation of the form $y^2 = p(x)$ for some (squarefree) polynomial $p(x)$.
   (d) Continuing (c), show that $p(x)$ has degree 5 or 6. [Hint: Apply Riemann-Hurwitz to $\varphi : C \to \mathbb{P}^1$ with $\varphi(x, y) = [1 : x]$. Note ∞ is ramified only when $\deg p$ is odd.]
3. [6pts*] The goal of this problem is to study the structure of a singular elliptic curve E. By an appropriate translation we may assume that the singular point is at $(0, 0)$.
   (a) Show that the resulting affine Weierstrass equation of E is of the form $y^2 + a_1xy = x^3 + a_2x^2$. (Remember that for $E = V(f)$, both partial derivatives of f vanish at the singular point.)
   (b) Show that the rational map $\varphi : E \to \mathbb{P}^1$ with $\varphi(x, y) = [X : Y]$ is defined at all points of E other than the singular point.
   (c) Construct an inverse map $\psi : \mathbb{P}^1 \to E \backslash \{(0, 0)\}$ for the map φ in part (b). [Hint: Let $t = y/x$ and use the Weierstrass equation to write x and y in terms of t.]
   (d) Deduce that E is birational to $\mathbb{P}^1$. Why is E not isomorphic to $\mathbb{P}^1$?

4. [5pts*] The goal of this problem is to prove a result known as the Weierstrass gap theorem. Let C be a smooth projective curve of genus g, and suppose $P \in C$. The main task is to investigate the spaces $L(nP)$ for various n: we say that an integer n is a pole number for P if there exists $\alpha \in k(C)$ such that $\mathrm{div}_-(\alpha) = -nP$, and otherwise (if there is no such α) we say n is a gap number for P.

   (a) Show that the set of pole numbers for P is an additive semigroup.

   (b) Show that if $n \geq 2g$, then $l((n-1)P) < l(nP)$. Deduce that there exists an element $\alpha \in k(C)$ such that $\mathrm{div}_-(\alpha) = -nP$ and conclude that each $n \geq 2g$ is a pole number.

   (c) Show that there are exactly g gap numbers $i_1 < i_2 < \cdots < i_g$ for P, and that $i_1 = 1$ and $i_g \leq 2g-1$.

5. [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 $\mathbb{F}_q$, and let E_{ns} denote the group of nonsingular points on E (under the usual group law definition).

   (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 E_{ns} is isomorphic to the multiplicative group $\mathbb{F}_q^\times$. Deduce that $\#E(\mathbb{F}_q) = q$. [Hint: Show that $\varphi : E_{ns} \to \mathbb{F}_q^\times$ 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 E_{ns} 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 $\varphi(X:Y:Z) = \frac{Y-\alpha X}{Y+\alpha X}$ 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.

6. [9pts] The goal of this problem is to collect some standard facts about the l-adic numbers. Let l be a prime.

   (a) Show that the function $\left|l^n \frac{x}{y}\right|_l = l^{-n}$ when $l \nmid x, y$ (and with $|0|_l = 0$) is a non-Archimedean norm on $\mathbb{Q}$: that $|x|_l = 0$ if and only if $x = 0$, that $|xy|_l = |x|_l |y|_l$, and that $|x+y|_l \leq \max(|x|_l, |y|_l)$. Deduce that $|\cdot|_l$ makes $\mathbb{Q}$ into a metric space.

   (b) For any Cauchy sequence $\{a_n\}_{n\geq 1}$ in $\mathbb{Q}$ under $|\cdot|_l$, show that $\lim_{n\to\infty} |a_n|_l$ exists and in fact, is eventually constant. Show also that two equivalent Cauchy sequences have the same limit value (we say two sequences $\{a_n\}$, $\{b_n\}$ are equivalent when $\lim_{n\to\infty} |a_n - b_n|_l = 0$).

   Now define $\mathbb{Q}_l$ to be the topological completion of $\mathbb{Q}$ under $|\cdot|_l$: that is, the set of equivalence classes of Cauchy sequences of rational numbers under $|\cdot|_l$. By (b) we may extend the metric $|\cdot|_l$ to $\mathbb{Q}_l$ by setting $|\{a_n\}|_l = \lim_{n\to\infty} |a_n|_l$. Observe that $\mathbb{Q}$ injects into $\mathbb{Q}_l$ as the constant sequences.

   (c) Show that $\mathbb{Q}_l$ is a field of characteristic zero under termwise addition and multiplication.

   (c) Let $\mathbb{Z}_l = \{x \in \mathbb{Q}_l : |x|_l \leq 1\}$. Show that each equivalence class in $\mathbb{Z}_l$ has a unique representative of the form $\{b_n\}_{n\geq 0}$ where $b_n = a_0 + a_1 l + \cdots + a_d l^d$ for some base-l digits $a_i \in \{0, 1, 2, \ldots, l-1\}$ for each i. (In other words, $\mathbb{Z}_l$ looks like "base-l power series".)

   (d) Show that $\mathbb{Z}_l$ is a local ring with unique maximal ideal $M = (l)$.

   (e) Show that $\mathbb{Q}_l = \mathbb{Z}_l[1/l]$. Deduce that every element of $\mathbb{Q}_l$ can be written in the form $\sum_{n=-k}^{\infty} a_n l^n$ for some $a_i \in \{0, 1, 2, \ldots, l-1\}$. (In other words, $\mathbb{Q}_l$ looks like "base-l Laurent series".)

   (f) Define $\overline{D}(a,r) = \{x \in \mathbb{Q}_l : |x-a| \leq r\}$ to be the closed disc of radius $r \geq 0$ centered at $a \in \mathbb{Q}_l$ and likewise set $D(a,r) = \{x \in \mathbb{Q}_l : |x-a| < r\}$. Show that $\overline{D}(a,r) = \overline{D}(b,r)$ and $D(a,r) = D(b,r)$ for any $b \in D(a,r)$ (i.e., every point in a disc is a center), and that every closed set is open.