E. Dummit's Math 7359 ∼ Elliptic Curves and Modular Forms, Fall 2023 ∼ Homework 3, due Fri Nov 3rd.

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 12)

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 property (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 16)

- Recall that the space $\Omega(C)$ of <u>meromorphic differential 1-forms</u> on C is the k-vector space consisting of symbols of the form dx for $x \in k(C)$, subject to the following three relations:

  1. The additivity relation $d(x+y) = dx + dy$ for all $x, y \in k(C)$
  2. The Leibniz rule $d(xy) = x\,dy + y\,dx$ for all $x, y \in k(V)$
  3. Derivatives of constants are zero: $da = 0$ for all $a \in k$.

1. [2pts*] Show that the relations (1)-(3) also imply the power rule $d(x^n) = nx^{n-1}dx$ and the quotient rule $d(\frac{x}{y}) = \dfrac{x\,dy - y\,dx}{y^2}$.
2. [2pts] Suppose C/k is a curve and $x_1, x_2, \dots, x_n \in k(C)$. For any rational function $f \in k(x_1, \dots, x_n)$, 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 $\dfrac{\omega}{dt} = -\dfrac{dy/dt}{3x^2 + 2a_2x + a_4}$ evaluates to a quantity that is defined and nonzero at ∞.

0.1.3 Exercises from (Oct 19)

1. [2pts] 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 and let $f \in L(\mathcal{C} - D)$ and consider $f \mapsto f\omega$. The proof of property (7) of differentials on Oct 16 is the special case $D = 0$.]
2. [2pts] If $D \geq 0$, show that Riemann-Roch is equivalent to the statement that $\dim_k(L(D)/L(0)) + \dim_k(\Omega(D)/\Omega(0)) = \deg(D)$.
3. [2pts*] Compute the ramification index $e_\varphi(P)$ for all points $P \in \mathbb{P}^1$ for the map $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $\varphi(x) = x^3$.
4. [3pts*] 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?
5. [2pts*] Suppose k is a(n algebraically closed) field of characteristic p and let the Frobenius morphism $\text{Frob} : \mathbb{P}^1(k) \to \mathbb{P}^1(k)$ 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 hypothesis that φ be separable is necessary to ensure there are only finitely many ramified points.

0.1.4 Exercises from (Oct 23)

1. [2pts] Let $\varphi : C_1 \to C_2$ be a nonconstant map of (smooth projective) curves. For any nonzero $f \in k(C_2)$ and any $P \in C_1$, show that $\text{ord}_P(\varphi^* f) = e_\varphi(P)\text{ord}_{\varphi(P)}(f)$.
2. [2pts*] Show that the degree map is multiplicative on isogenies: $\deg(\varphi \circ \psi) = (\deg \varphi)(\deg \psi)$.
3. [1pt] 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 $\varphi, \psi \in \text{Hom}(E_1, E_2)$.
4. [2pts] 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.]
5. [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 $\ker \varphi$.
6. [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.

0.2 Additional Exercises

1. [5pts] The goal of this problem is to study the group structure on 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 $\mathbb{P}^1$?
2. [5pts] 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 $L(\mathcal{C})$ contains an effective divisor $D = P + Q$ for some points $P, Q \in C$ (which may be equal).
   (b) Continuing (a), let $x \in l(\mathcal{C})$ 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 $\deg(\text{div}_{-}x) = 2$ and thus that the extension degree $[k(C) : k(x)] = 2$ has degree 2. Conclude 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. [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 $\text{div}_{-}(\alpha) = -nP$, 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 (i.e., it is closed under addition and contains 0).
   (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 $\text{div}_{-}(\alpha) = -nP$ 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 $i_g \leq 2g - 1$.