E. Dummit's Math 7359 ~ Elliptic Curves and Modular Forms, Fall 2023 ~ Homework 5, due Wed Dec 13th.

Problems are worth points as indicated. Solve whichever problems you haven't seen before that interest you the most (suggestion: between 30 and 45 points' worth). Starred problems are especially recommended. Submit your assignments via Gradescope.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Nov 9)

1. [2pts] Show that when $E_1 = E = E_2$, the action $\Psi : \mathrm{End}(E) \to \mathrm{End}(T_l(E))$ with $\Psi(\varphi)$ mapping $(P_1, P_2, P_3, \dots) \in T_l(E)$ to $(\varphi(P_1), \varphi(P_2), \varphi(P_3), \dots) \in T_l(E)$ is a ring homomorphism.
2. [3pts] If $K = \mathbb{Q}(\sqrt{-D})$ is an imaginary quadratic field, its ring of integers $\mathcal{O}_K$ is $\mathbb{Z}[\alpha]$ where $\alpha = \begin{cases} \sqrt{-D} & \text{when } -D \equiv 2, 3 \pmod 4 \\ (1+\sqrt{-D})/2 & \text{when } -D \equiv 1 \pmod 4 \end{cases}$. Show that the orders of K are the rings of the form $R = \mathbb{Z} + f\mathcal{O}_K$ for a positive integer f, the conductor of R. [Hint: Show $[\mathcal{O}_K : R] = f$ is finite.]
3. [2pts*] Show that both the ring of naive integral quaternions $R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ and the ring of Hurwitz quarternions $H = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\dfrac{1+i+j+k}{2}$ are orders in the algebra $A = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ of rational quaternions, where $i^2 = j^2 = k^2 = ijk = -1$ as usual.
4. [2pts] Show that if S is a Noetherian integrally closed domain with fraction field F, then $R = M_{n\times n}(S)$ is an order in $A = M_{n\times n}(F)$.

0.1.2 Exercises from (Nov 13)

1. [2pts] If k is a field and D is a division ring with center k, show that the matrix algebra $M_{n\times n}(D)$ is a central simple k-algebra.
2. [2pts*] Show that the endomorphism ring of $y^2 = x^3 - x$ with the isogeny $[i](x, y) = (-x, iy)$ discussed previously, is isomorphic to $\mathbb{Z}[i]$.
3. [2pts] Show that if E and E' are isogenous then $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathrm{End}(E') \otimes \mathbb{Q}$. [Hint: Let $\varphi : E \to E'$ be an isogeny. Show that the map sending $f \in \mathrm{End}(E)$ to $\frac{1}{\deg \varphi}\varphi \circ f \circ \hat{\varphi} \in \mathrm{End}(E') \otimes \mathbb{Q}$ is an injective ring homomorphism.]
4. [2pts] When q is odd, for any $a \in \mathbb{F}_q$ show that $\chi(a) = a^{(q-1)/2}$. [Hint: $\mathbb{F}_q^\times$ is cyclic.]
5. [2pts] For a positive integer k, show that $\sum_{x\in\mathbb{F}_q} x^k$ is 1 when $(q-1)|k$ and is 0 when $(q-1) \nmid k$.

0.1.3 Exercises from (Nov 16)

1. [2pts*] Show that $y^2 = x^3 + x + 1$ is supersingular over $\mathbb{F}_{17}$ by computing both $\#E(\mathbb{F}_{17})$ and the coefficient of x^{16} in $(x^3 + x + 1)^8$ mod 17.
2. [2pts] Show that for an odd prime p, $y^2 = x^3 + x$ is supersingular over $\mathbb{F}_p$ if and only if $p \equiv 3 \pmod 4$.
3. [3pts*] Show for a prime $p > 3$, an elliptic curve $E/\mathbb{F}_p$ is supersingular if and only if $\#E(\mathbb{F}_p) = p+1$. Deduce that the pth-power Frobenius map φ has $\varphi^2 = [-p]$ and that $\hat{\varphi} = -\varphi$.
4. [2pts] Show that the elliptic curve $y^2 = x(x-1)(x-\lambda)$ in Legendre form is supersingular over $\mathbb{F}_q$ if and only if λ is a root of the polynomial $H_p(t) = \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 t^k$. [Remark: One may show that H_p is separable. By using some basic facts about equivalences of Legendre forms, one may give a precise count of the number of supersingular curves over $\mathbb{F}_p$.]
5. [2pts] Show that the surface obtained by gluing together two spheres along two branch cuts is topologically a torus.

0.1.4 Exercises from (Nov 20)

1. [1pt] Let $\omega = a\omega_1 + b\omega_2$. Show that $|\omega|^2 = xa^2 + yab + zb^2$ is a positive-definite quadratic form in (a, b), where $x = |\omega_1|^2$, $y = 2\mathrm{Re}(\omega_1\overline{\omega_2})$, $z = |\omega_2|^2$.

2. [2pts] Show that if $Q(a, b)$ is a positive-definite real quadratic form, then $\sum_{(0,0)\neq(a,b)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{Q(a,b)^k}$ diverges for $k \leq 1$ and converges absolutely for $k > 1$. [Hint: Compare to the corresponding integral, diagonalize the quadratic form, and use polar coordinates.]

3. [2pts] Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice. Show that $\sum_{0\neq\omega\in\Lambda} |\omega|^{-k}$ diverges for $k \leq 2$ and converges absolutely for $k > 2$.

0.1.5 Exercises from (Nov 27)

- [2pts] If the associated Weierstrass equation for Λ is $E : y^2 = 4x^3 + Ax + B$ for $A = -60G_4(\Lambda)$ and $B = -140G_6(\Lambda)$ and $\alpha \neq 0$, calculate the associated Weierstrass equation for $\alpha\Lambda$ and verify directly that the resulting elliptic curve is isomorphic to E.

- [3pts*] Under the correspondence of $E(\mathbb{C})$ with C/Λ, show that the m-torsion points on $E(\mathbb{C})$ correspond to the m-division points $\frac{1}{m}\Lambda = \{z : mz \in \Lambda\}$ in $\mathbb{C}/\Lambda$. Deduce that $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.

- [2pts] Continuing the exercise above, let e_m be the Weil pairing on $E[m]$ with $E[m]$ viewed as $\frac{1}{m}\Lambda/\Lambda$. For $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, show that $e_m(\frac{a\omega_1+b\omega_2}{m}, \frac{c\omega_1+d\omega_2}{m}) = e^{2\pi i(ad-bc)/m}$.

- [2pts] Let φ be an endomorphism of an elliptic curve $E/\mathbb{C}$ corresponding to a scaling α on the associated lattice Λ. Show that $\deg\varphi = \#\ker\varphi = \#(\Lambda/\alpha\Lambda) = \alpha\overline{\alpha} = V$, where V is the ratio of the area of a fundamental parallelogram for $\alpha\Lambda$ to the area of a fundamental parallelogram for Λ.

0.1.6 Exercises from (Nov 30)

- [2pts] For the lattices $\Lambda = \mathbb{Z} + \mathbb{Z}\rho$ where $\rho = e^{2\pi i/3}$ is a nonreal cube root of unity, and $\Lambda = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$, find the endomorphism rings of the associated elliptic curves.

- [1pt] Let G be a group acting simply transitively on a set S, meaning that for any $a, b \in S$ there exists a unique $g \in G$ with $g \cdot a = b$. Prove that $\#G = \#S$.

- [2pts] Compute the endomorphism rings of $y^2 = x^3 + x$, $y^2 = x^3 - 35x + 98$, and $y^2 = x^3 + 4x^2 + 2x$.

- [2pts*] Find an elliptic curve having complex multiplication by $\mathcal{O}_{\sqrt{-11}} = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$.

- [2pts] For the lattice $\Lambda = \mathbb{Z} + \mathbb{Z}i$ show that $G_6(\Lambda) = 0$. Deduce that the associated elliptic curve is of the form $y^2 = x^3 + Ax$. What is the j-invariant of this curve? What is its endomorphism ring?

- [2pts] For the lattice $\Lambda = \mathbb{Z} + \mathbb{Z}e^{2\pi i/3}$ show that $G_4(\Lambda) = 0$. Deduce that the associated elliptic curve is of the form $y^2 = x^3 + B$. What is the j-invariant of this curve? What is its endomorphism ring?

- [1pt] For $a, b, c, d \in \mathbb{R}$ with $ad - bc > 0$ and $\tau \in \mathbb{H}$ show $\mathrm{im}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{(ad-bc)\mathrm{im}(\tau)}{|c\tau+d|^2} > 0$.

- [1pt] Show that the action of the modular group on $\mathbb{H}$ is faithful (i.e., that the identity is the only element acting trivially on all of $\mathbb{H}$).

- [1pt] For $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $\Gamma(1)$, show that S has order 2 and ST has order 3.

- [1pt] Show that the stabilizer in $\Gamma(1)$ of ∞ is the subgroup $\langle T \rangle$.

0.1.7 Exercises from (Dec 4)

- [2pts*] Show that the space of weakly modular functions of weight $2k$ is a $\mathbb{C}$-vector space, and that the product of weakly modular functions of weights $2k$ and $2l$ yields a weakly modular function of weight $2k+2l$.
- [2pts] For $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ show that $d(\gamma z) = (cz+d)^{-2}dz$. Deduce that f is weakly modular of weight $2k$ if and only if the differential k-form $f(z)\,dz^k$ is invariant under the action of $\Gamma(1)$.
- [2pts] If $f \in \mathcal{M}_6$, $\mathcal{M}_8$, or $\mathcal{M}_{10}$, show that f/G_6, f/G_4^2, or $f/(G_4G_6)$ is constant, respectively.
- [1pt] Show that the number of nonnegative integer solutions (a,b) to $2a+3b=k$ is equal to $\lfloor k/6 \rfloor + 1$ except when $k \equiv 1 \pmod 6$ in which case it is instead $\lfloor k/6 \rfloor$.
- [2pts] Using $\zeta(10) = \pi^{10}/93555$, prove that $G_{10} = 5G_4G_6/11$.

0.2 Additional Exercises

1. [4pts] If E is an elliptic curve over a finite field then the group of points of E is the direct product of two cyclic groups, which raises the question: does every product of two cyclic groups occur as the group of some elliptic curve over a finite field? The goal of this problem is to construct a counterexample, so suppose E is an elliptic curve over a field $\mathbb{F}_q$ whose group of $\mathbb{F}_q$-points is isomorphic to $(\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$.
   (a) Show that 11 does not divide q.
   (b) Show that $E[11] \subseteq E(\mathbb{F}_q)$. Deduce that $\mathbb{F}_q$ contains the 11th roots of unity and thus that $q \equiv 1 \pmod{11}$. [Hint: Weil pairing.]
   (c) Show that there are no possible prime powers q satisfying (b) and the Hasse bound. Conclude that there is no elliptic curve $E/\mathbb{F}_q$ whose group of $\mathbb{F}_q$-points is isomorphic to $(\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$.
2. [20pts*] Discuss something interesting you learned in this course. Which topic(s) did you like the most? Which topic(s) did you like least? Which topic(s) would you have liked to see more of? Do you have any other feedback about the course format or structure?