E. Dummit's Math 7359 ∼ Elliptic Curves and Modular Forms, Fall 2023 ∼ Homework 1, due Fri Sep 29th.

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. Submit your assignments via Gradescope.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Sep 7)

1. [3pts] Show that graph of $y^2 = x^3 + Ax + B$ over $\mathbb{R}$ will have two components when the polynomial $x^3 + Ax + B$ has three distinct real roots, and will have one component otherwise.

2. [1pt] (Tedious) Suppose E is an elliptic curve with a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on E. Show that the additive inverse is given by $-P_1 = (x_0, -y_0 - a_1x_0 - a_3)$, and the sum $P_1 + P_2$ is given by ∞ when $x_1 = x_2$ and $y_1 = -y_2 - a_1x_2 - a_3$ and by (x_3, y_3) where $x_3 = m^2 + a_1m - a_2 - x_1 - x_2$ and $y_3 = -(m + a_1)x_3 - b - a_3$ where $y = mx + b$ is the line joining P_1 and P_2 (or the tangent line when $P_1 = P_2$), which explicitly has $m = \dfrac{y_2 - y_1}{x_2 - x_1}$, $b = \dfrac{x_2y_1 - x_1y_2}{x_2 - x_1}$ when $P_1 \neq P_2$ and has $m = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$ and $b = \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$ when $P_1 = P_2$.

0.1.2 Exercises from (Sep 11)

1. [3pts*] Pick an elliptic curve in Weierstrass form (e.g., $y^2 = x^3 + 4x + 1$) and after checking whether it is nonsingular, find all of its points over $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{11}$, and $\mathbb{F}_{13}$, and identify the group structure explicitly in each case.

2. [2pts] Show that by making an appropriate change of variables, any rational Weierstrass form can be converted into one with A, B integers. Illustrate by finding a Weierstrass form with integer coefficients for $y^2 = x^3 + \frac{3}{2}x + \frac{2}{5}$.

3. [3pts] (Tedious) Let E be an elliptic curve and $P = (x, y)$ be a point on E. Define the polynomials $\varphi_0 = 0$, $\varphi_1 = 1$, $\varphi_2 = 2y$, $\varphi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$, $\varphi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$, and in general $\varphi_{2n+1} = \varphi_{n+2} \cdot \varphi_n^3 - \varphi_{n-1}\varphi_{n+1}$ and $\varphi_{2n} = \dfrac{\varphi_n}{2y} \cdot (\varphi_{n+2}\varphi_{n-1}^3 - \varphi_{n-2}\varphi_{n+1}^2)$ for $n \geq 2$.

   (a) With $y^2 = x^3 + Ax + B$, show that φ_n can be written as a polynomial in $\mathbb{Z}[x, A, B]$ when n is odd and can be written as y times a polynomial in $\mathbb{Z}[x, A, B]$ when n is even.

   (b) Show that φ_n^2 is a polynomial of degree $n^2 - 1$ in x with leading coefficient n^2 while $x\varphi_n^2 - \varphi_{n-1}\varphi_{n+1}$ is a polynomial of degree n^2 in x with leading coefficient 1.

   (c) Show that the coordinates of $[n]P$ are (x_n, y_n) where $x_n = \dfrac{x\varphi_n^2 - \varphi_{n-1}\varphi_{n+1}}{\varphi_n^2}$ and $y_n = \dfrac{\varphi_{n+2}\varphi_{n-1}^2 - \varphi_{n-2}\varphi_{n+1}^2}{4y\varphi_n^3}$.

0.1.3 Exercises from (Sep 18)

1. [2pts*] Draw $V(x)$, $V(x^2)$, $V(y - x)$, $V(y - x^2)$, $V(xy)$, $V(x, y)$, and $V(y^2 - x^3 - x)$ in $\mathbb{A}^2(\mathbb{R})$.

2. [3pts] Identify $I(S)$ in $\mathbb{R}[x, y]$ for $S = \{(t, 0) : t \in \mathbb{R}\}$, $\{(t^2, t) : t \in \mathbb{R}\}$, $\{(1, 1)\}$, $\{(0, 0), (1, 1)\}$, $\{(\cos t, \sin t) : t \in \mathbb{R}\}$, and $\{(t, \sin t) : t \in \mathbb{R}\}$.

3. [2pts] Prove that for any subset S of $k[x_1, \ldots, x_n]$, $S \subseteq I(V(S))$ and $V(S) = V(I(V(S)))$.

4. [2pts] Prove that for any subset X of $\mathbb{A}^n(k)$, $X \subseteq V(I(X))$ and $I(X) = I(V(I(X)))$.

5. [1pt] If k is finite, show that the irreducible affine algebraic sets in $\mathbb{A}^n(k)$ are $\emptyset$ and single points.

6. [3pts*] If k is infinite, show that the irreducible affine algebraic sets in $\mathbb{A}^2(k)$ are $\emptyset$, $\mathbb{A}^2(k)$, single points, and curves of the form $V(f)$ for a monic irreducible polynomial $f \in k[x, y]$. [Hint: Show that if $f, g \in k[x, y]$ are relatively prime, then (f, g) contains a nonzero polynomial in $k[x]$ and a nonzero polynomial in $k[y]$.]

0.2 Additional Exercises

1. [4pts*] Find an elliptic curve in Weierstrass form that has a rational point of order 4. (You may construct this curve in any manner you like, other than looking one up.)

2. [5pts*] Find generators and the group structure for the group of rational torsion points on each curve. (You can check your answers with Sage, but you should use Nagell-Lutz to identify the candidate torsion points themselves first.)

   (a) $y^2 = x^3 + 1$.

   (b) $y^2 = x^3 - 48$.

   (c) $y^2 = x^3 - 7x + 6$.

   (d) $y^2 = x^3 - 4x^2 + 16$.

   (e) $y^2 = x^3 - 14x^2 + 81x$.

3. [5pts*] The L-Functions and Modular Forms Database (LMFDB, to its friends) contains data on many other algebraic objects of interest, including elliptic curves. Using the database, find an example of a Weierstrass form of an elliptic curve E with the given properties:

   (a) $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to $\mathbb{Z}/9\mathbb{Z}$.

   (b) $E(\mathbb{Q})$ contains a point of order 10.

   (c) $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

   (d) $E(\mathbb{Q}(i))$ is isomorphic to $\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

   (e) $E(\mathbb{Q}(\sqrt{2}))$ is isomorphic to $\mathbb{Z}/11\mathbb{Z}$.

4. [3pts] The algebra package Sage can, for reasonably nice elliptic curves E and number fields K, compute generators for the group $E(K)$. For each of the curves you found from the LMFDB in problem (3) above, use Sage to compute generators for the group of torsion points and the group of torsion-free points over the field requested (i.e., $\mathbb{Q}$ for (a)-(c), $\mathbb{Q}(i)$ for (d), $\mathbb{Q}(\sqrt{2})$ for (e)).

5. [6pts] Recall that a discrete valuation on a field F is a surjective function $v : F^\times \to \mathbb{Z}$ with $v(0) = \infty$, $v(ab) = v(a) + v(b)$ for all $a, b \in F$, and $v(a + b) \geq \min(v(a), v(b))$ for all $a, b \in F$. The valuation ring R is the set of elements $r \in F$ with $v(r) \geq 0$. Show the following, where $t \in R$ is a uniformizer (i.e., an element with $v(t) = 1$):

   (a) For any $r \in F^\times$, either r or $1/r$ is in R.

   (b) An element $u \in R$ is a unit of R if and only if $v(u) = 0$. In particular, if $\zeta \in F$ is any root of unity, then $v(\zeta) = 0$.

   (c) If $r \in R$ is nonzero and $v(r) = n$, then r can be written uniquely in the form $r = ut^n$ for some unit $u \in R$.

   (d) Every nonzero ideal of R is of the form (t^n) for some $n \geq 0$.

   (e) The ring R is a Euclidean domain (hence also a PID and a UFD) and also a local ring.

   (f) The ring S is a DVR if and only if it is a PID and a local ring but not a field.