Modular forms: problem set 5

Due August 3

***Exercise 1.** Let E be given by the equation $y^2 = x^3 + ax + b$, let P be the poitn (x, y).

(1) Show that the x-coordinate of $2P$ is given by
$$\frac{x^4 - 2ax^2 + 8bx + a^2}{4y^2}.$$

(2) Find a similar formula for the y-coordinate of $2P$.

(3) Find a polynomial in x whose roots are the x-coordinates of the 3-torsion points. Using this, deduce that $\#E[3] \leq 9$ (of course, we already know that $E[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$, but this is a *new* proof). [Hint: a point $P \in E$ is 3-torsion if and only if $2P = -P$.]

***Exercise 2.** Let E be an elliptic curve. The goal of this problem is to show that the map
$$E \longrightarrow \mathrm{Pic}^0(E)$$
$$P \mapsto (P) - (\infty)$$
is a group isomorphism. Note that this gives another natural interpretation of the group law on an elliptic curve (and proves that it is indeed a group law).

Note that, either by Alec's lecture or by exercise 3, we have $K_E = 0 \in \mathrm{Pic}^0(E)$. So the Riemann-Roch theorem for an elliptic curve says that $\ell(D) - \ell(-D) = \deg D$.

(1) Show that $(P) = (Q)$ as elements of $\mathrm{Pic}(E)$ if and only if $P = Q$ as points on E. Conclude that the map above is injective. [Hint: Riemann-Roch.]

(2) Show that the map above is surjective. [Hint: Riemann-Roch.]

(3) Show that if P, Q, R are colinear on E then $(P) + (Q) + (R) - 3(\infty) = 0$ in $\mathrm{Pic}^0(E)$. Deduce that the above map is a group isomorphism.

Exercise 3. This exercise fleshes out an example from Alec's lecture. Let E be the projective curve given in affine coordinates by $y^2 = (x - e_1)(x - e_2)(x - e_3)$ for e_1, e_2, e_3 distinct.

(1) Let $\mathfrak{m} = (x - e_i, y)$ be the maximal ideal at $P_i = (e_i, 0)$. Show that y is a uniformizer at P_i, i.e. show that $y \notin \mathfrak{m}^2$. Conclude that $\mathrm{ord}_{P_i}(x - e_i) = 2$. [Hint: let $\overline{K}[E]_{P_i}$ be the local ring at P_i and $\kappa = \overline{K}[E]_{P_i}/\mathfrak{m}$ be the residue field. Recall that since E is nonsingular, $\dim_\kappa \mathfrak{m}/\mathfrak{m}^2 = 1$. Conclude that to show y is a uniformizer, it suffices to show that $x - e_i \in \mathfrak{m}^2$.]

(2) Change to (x, z)-coordinates, and show that the function $x - e_i$ from part (1) becomes $\frac{x - e_i z}{z}$. Then show that $\mathrm{ord}_\infty(x - e_i) = -2$.

(3) Conclude that $\mathrm{div}(x - e_i) = 2(P_i) - 2(\infty)$ and $\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(\infty)$.

(4) Now compute that $\mathrm{div}(dx) = \mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(\infty)$. Conclude that $\frac{dx}{y}$ is a differential on E without poles or zeros.