Math 203, Problem Set 8. Due Friday, December 5.

You may assume that the ground field is $k = \mathbb{C}$.

1. (*Pappus's theorem.*) Let l and m be two projective lines in $\mathbb{P}^2$, and let p_1, p_2, p_3 be points on $l \setminus l \cap m$ and q_1, q_2, q_3 be points on $m \setminus l \cap m$. Let L_{ij} be the line joining p_i and q_j. Show that the three points of intersection of the pairs of lines L_{ij} and L_{ji} are collinear. You may wish to find two cubics intersecting in 9 points.

2. (*The group law on elliptic curves.*)

(i) Consider two points $P([x_1 : y : 1])$ and $Q([x_2 : y_2 : 1])$ on the elliptic curve $\overline{E}_\lambda$:

$$y^2 z = x(x - z)(x - \lambda z),$$

where $P_0 = [0 : 1 : 0]$ is the origin. Prove that the sum

$$P \oplus Q = \begin{cases} [0 : 1 : 0] \text{ if } x_1 = x_2 \text{ but } y_1 \neq y_2 \\ [x_3 : y_3 : 1] \text{ if } x_1 \neq x_2 \end{cases},$$

where

$$x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 + 1 + \lambda - x_1 - x_2$$

$$y_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right) x_3 + \left(\frac{x_1 y_2 - y_1 x_2}{x_1 - x_2}\right).$$

What are the corresponding formulas if $P = Q$?

Hint: First let $y = mx + b$ be the line passing through P and Q. Find m and b in terms of x_1, y_1, x_2, y_2. Then substitute into the equation of the elliptic curve. Note if you know two of the roots of a cubic polynomial, the third one can be determined from one of the coefficients.

(ii) Show that if $\lambda \in \mathbb{Q}$, then the set of points on the elliptic curve with rational coordinates form an abelian group. You only need to check that if P, Q have rational coordinates, so do $-P$ and $P \oplus Q$. More generally, note that the group law on the elliptic curve $\overline{E}_\lambda$ can be defined even if the ground field is not algebraically closed.

3. (*Rational points on elliptic curves.*) Consider the point $P(0, 0)$ on cubic curve C with equation

$$y^2 + y = x^3 - x.$$

(i) Let $Q(a, b)$ be a point on the cubic. Show that the inverse $-Q$ has coordinates $(a, -1 - b)$ for the group law with zero element the point at infinity $[0 : 1 : 0]$. Find the coordinates of the point $P + Q$.

(ii) Find the coordinates of the point nP, for $n \leq 6$, and note that nP is a rational point on C. In fact, the group of rational points $C(\mathbb{Q})$ is generated by $P(0, 0)$.

4. (*Torsion points on cubics.*) Let C be a nonsingular cubic curve and $p_0 \in C$ an inflection point. Consider the group law on C with p_0 the zero element.

(i) Explain briefly that p is an inflection point on C if and only if p is a point of order 3 in the group law of (C, p_0). Derive that the line though any 2 inflection points intersects C in a third inflection point.

(ii) We proved in class that after a change of coordinates we may assume C can be written as

$$y^2z = x(x-z)(x-\lambda z) \text{ and } p_0 = [0:1:0].$$

Show that a further change of coordinates $\tilde{x} = x - z \cdot \frac{\lambda+1}{3}$ brings C into the form

$$y^2z = \tilde{x}^3 + a\tilde{x}z^2 + bz^3 \text{ and } p_0 = [0:1:0].$$

(iii) Possibly using (ii), show that C has *exactly* 9 distinct points of order 3, hence 9 inflection points.

Hint: Show that if $z = 0$, the only inflection point is $p_0 = [0:1:0]$. Next, assume $p = [\tilde{x} : y : 1]$ is a point of order 3 on the affine curve $y^2 = \tilde{x}^3 + a\tilde{x} + b$. Therefore, $2p = -p$. Find the coordinates of $2p$ and $-p$. Derive that $\tilde{x}$ satisfies a degree 4 equation, for instance

$$12\tilde{x}(\tilde{x}^3 + a\tilde{x} + b) = (3\tilde{x}^2 + a)^2.$$

Prove that there are *exactly* 4 values of $\tilde{x}$, and each value gives *exactly* 2 values of y. (You will need to show that there are no repeated roots of the quartic equation, for instance by computing the first derivative.) Count the inflection points $1 + 4 \times 2 = 9$.

(iv) From (i) and (iii), conclude that the inflection points form a subgroup of C isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(v) Possibly using (ii), show that there are exactly 4 tangent lines to C which pass though the inflection point p_0 (the same is therefore true for any inflection point). Conclude that C has exactly 4 points of order 2, and the subgroup of points of order 2 is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Remark: It can be shown that the n-torsion points form a group isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.