Topics: Elliptic curves.

7.1. Consider the curves given by the equations

$$C_1 : \; y^2 = x^3 \qquad \text{and} \qquad C_2 : \; y^2 = x^3 - 2x^2 + x.$$

Using calculus methods, find all the singular points of C_1 and C_2.

7.2. In this question we work out how to turn a more general type of Weierstrass equation into one of the type we have been working with: $y^2 = x^3 + ax + b$.

(a) Consider the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbf{F}. \tag{1}$$

Apply the change of variables

$$y = u - \frac{a_1x}{2} - \frac{a_3}{2}$$

and simplify to an equation of the form

$$u^2 = x^3 + b_2x^2 + b_4x + b_6 \tag{2}$$

for appropriate $b_i \in \mathbf{F}$.

(Here is where we have to assume that $2 \neq 0$ in $\mathbf{F}$.)

(b) In (2), apply the change of variables

$$x = v - \frac{b_2}{3}$$

and simplify to a short Weierstrass equation of the form

$$u^2 = v^3 + c_4v + c_6$$

for appropriate $c_i \in \mathbf{F}$.

(Here is where we have to assume that $3 \neq 0$ in $\mathbf{F}$.)

7.3. Fix a parameter c and let $P = (x_0, y_0)$ be a point on the elliptic curve

$$E_c : \; y^2 = x^3 + c.$$

Use the duplication formula to compute the coordinates of $[2]P$.

Compare your answer to Bachet's recipe for producing a new point (x_1, y_1) from an existing point (x_0, y_0) on E_c.

7.4. Consider an elliptic curve

$$E : \; y^2 = f(x) = x^3 + ax + b \qquad \text{with } a, b \in \mathbf{Z}$$

and a point $P = (x_1, y_1) \in E(\mathbf{Q})$ with $y_1 \neq 0$.

Recall that the x-coordinate of the point $[2]P$ is given by

$$x_2 = \frac{x_1^4 - 2ax_1^2 - 8bx_1 + a^2}{(2y_1)^2}.$$

Let $g(x) = x^4 - 2ax^2 - 8bx + a^2$ be the polynomial appearing in the numerator.

(a) Find polynomials of the form

$$r(x) = c_2x^2 + c_0, \qquad s(x) = d_3x^3 + d_1x + d_0$$

with integer coefficients depending on a and b, such that

$$r(x)g(x) - s(x)f(x) = 4a^3 + 27b^2.$$

[**Hint**: Start by figuring out how d_3 and c_2 are related, then by looking at the overall constant term and making an educated guess for what c_0 and d_0 should be.]

(b) Use part (a) and the approach in Proposition 3.14 to show that if P and $[2]P$ both have integer coordinates, then either $y_1 = 0$ or $y_1^2 \mid 4a^3 + 27b^2$.

7.5. Consider an elliptic curve given by a Weierstrass equation

$$E: \; y^2 = f(x) = x^3 + ax + b, \qquad a, b \in \mathbf{R}.$$

(a) Let $P = (x_1, y_1)$ be a point of order three. Use the formulas for $[2]P$ and $-P$ to find a polynomial ψ of degree 4 such that $\psi(x_1) = 0$.

(b) Show that $\psi(x) = 2f(x)f''(x) - f'(x)^2$ and $\psi'(x) = 12f(x)$.

(c) Use part (b) to show that ψ and ψ' have no common roots; conclude that ψ has simple roots.

(d) Show that

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} = \frac{\psi(x)}{4yf(x)}.$$

(e) Use part (d) to show that if P is a point of order three then it is an inflection point on the curve (a point where the second derivative changes sign).

(f) Prove that ψ has exactly two real roots, say $\alpha_1 < \alpha_2$. Prove that $f(\alpha_1) < 0$ and $f(\alpha_2) > 0$.

[**Hint**: Use the formulas in part (b) to think about the stationary points and the roots of ψ. Maybe draw some pictures of what the degree 4 polynomial ψ can look like.]

(g) How many points of order three are there in $E(\mathbf{R})$?