1. Consider the equation

\[ x^3 - y^2 = 7. \]

While studying the group law on a smooth cubic we noted that if the cubic has coefficients in \( \mathbb{Q} \), then any line through two rational points of the curve (or tangent to one rational point of the curve) would meet the curve in another rational point.

The point \((x, y) = (2, 1)\) is a solution to the equation. Let’s use the idea above to find another.

(a) Find the equation of the tangent line to \( x^3 - y^2 = 7 \) at the point \((2, 1)\). (The technique of implicit differentiation from first-year calculus is a good method to use.)

(b) Substitute the equation of the line into (1.1) to get a cubic equation in \( x \).

(c) Factor the equation in (b) and use the new root to find a new point on the curve. (Be sure to test the point you found to ensure that it satisfies (1.1).)

2. We can use a similar method of intersecting with lines to find an algebraic parameterization of points on the circle.

(a) Write down the equation of the line passing through the points \((-1, 0)\) and \((0, t)\).

(b) The line from (a) intersected with the conic \( x^2 + y^2 = 1 \) will have two points of intersection (since a conic has degree 2). One of them is \((-1, 0)\). Find the other one as a function of \( t \).

(c) Check that your solution from (b) satisfies \( x^2 + y^2 + 1 \).

Integer solutions to \( X^2 + Y^2 = Z^2 \) are called pythagorean triples. The equation \( X^2 + Y^2 = Z^2 \) is the homogenization of \( x^2 + y^2 = 1 \), and hence rational points on the circle give rise to pythagorean triples.

(d) Evaluate your solution in (b) at \( t = 4, 5, \) and \( 6 \). For each of your points write it as \([x : y : 1]\) in \( \mathbb{P}^2 \) and clear denominators to get a different representation of that point as \([X : Y : Z]\) with \( X, Y, \) and \( Z \) relatively prime integers.

(e) Which pythagorean triples did you find?
3. In this problem we will compute in the group law of the elliptic curve \( E \) given by \( ZY^2 - X^3 - 17Z^3 = 0 \) in \( \mathbb{P}^2 \) (or its dehomogenized form: \( y^2 = x^3 + 17 \)).

Before doing any specific computations, let us work out some general formulae for addition.

(a) First show that the additive inverse of a point \([a : b : c] \neq [0 : 1 : 0]\) on \( E \) is the point \([a : -b : c]\). (Suggestion: The line connecting \([a : b : c]\) and \([0 : 1 : 0]\) is \( cX - aZ = 0 \).)

It is a bit easier to work in affine coordinates in the chart \( U_2 \), with the point \((x, y)\) corresponding to the point \([x : y : 1] \in \mathbb{P}^2\).

(b) Deduce from (a) that the additive inverse of \((x, y) \in E\) is \((x, -y) \in E\).

(c) Suppose that \( y = mx + b \) is the equation of a line joining two points \((x_1, y_1)\) and \((x_2, y_2)\) of \( E \). Show that the \( x \)-coordinate of \((x_1, y_1) + (x_2, y_2)\) is \( m^2 - x_1 - x_2 \), and that the \( y \)-coordinate is \(-m(m^2 - x_1 - x_2) - b\). (Suggestion: For the \( x \)-coordinate, substitute \( y = mx + b \) into the equation of \( E \), and use the relationship between the coefficient of \( x^2 \) and the sum of the roots, see for example H5, Question 3(c).)

(d) Suppose that \( y = mx + b \) is the equation of the tangent line to the curve \( E \) at a point \( P = (x_1, y_1) \). Give formulae as in (c) for the \( x \) and \( y \) coordinates of \( P + P \).

(e) Let \((x_1, y_1)\) be a point of \( E \). Use implicit differentiation to compute the slope \( m \) of the tangent line to \( E \) at \((x_1, y_1)\).

Let \( P = (-2, 3) \) and \( Q = (2, 5) \). Both are points of \( E \).

(f) Compute \( 2Q - P \).

(g) Compute \( 3P - Q \).

The problems may be handed in to my office (or my mailbox) at 507 Jeff.