23MAC260 Problem Sheet 2

Week 2

1. In lectures we looked at the elliptic curve defined by the equation

$$Y^2Z = X^3 + Z^3$$

or in affine form by

$$y^2 = x^3 + 1.$$

We saw that this curve contains the points $P = (2, 3)$ and $Q = (-1, 0)$, and we computed their sum: $P \oplus Q = (0, -1)$.

   (a) Calculate the point $P \oplus (P \oplus Q)$.

   (b) Write down the equation of the tangent line to the curve at the point P.

   (c) Use the previous part to calculate the point

$$2P := P \oplus P.$$

   (The definition of $P * P$ was given in Week 2 Lecture 1 page 2 of this week's notes.)

   (d) Verify that $2P \oplus Q = P \oplus (P \oplus Q)$.

   (e) In general for positive integers a, we use the notation aP to mean the point P added to itself a times, and $(-a)P$ to mean $O * P$ (which as we saw is the inverse of P for the operation $\oplus$) added to itself a times.
   Now compute as many points of the form $a\,P \oplus b\,Q$ (for a, $b \in \mathbb{Z}$) as you want.

2. Let C be the curve defined in affine form by

$$y^2 = 8x^3 - 12x^2 + 6x.$$

   (a) Show that C is an elliptic curve.

   (b) Show that the points

$$R = (0, 0)\,, \quad S = \left(\frac{3}{2}, 3\right)$$

   lie on the curve C.

(c) Calculate $R \oplus S$ and as many other points of the form $aR \oplus bS$ (for a, $b \in \mathbb{Z}$) as you want.

3. Let C be the elliptic curve defined in affine form by

$$y^2 = x^3 - x + 1.$$

(a) Show that the point $P = (1, 1)$ lies on the curve C.

(b) Caclulate $6P$. (Hint: to do this you need to calculate $2P$ and $3P$ but not $4P$ or $5P$.)

4. Let C be the elliptic curve defined in affine form by

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

(a) Show there are exactly 3 points $\{R_1, R_2, R_3\}$ on C with y-coordinate equal to 0.

(b) For each of the points R_i found in the previous part, show that $2R_i = O$.

(c) Show that if R_i and R_j are two distinct points found in (a) then $R_i \oplus R_j = R_k$, the other one of the points.

(d) Conclude that the set $\{O, R_1, R_2, R_3\}$ is a **subgroup** of the set of points on C.

The following question is not examinable.

I. In this problem you will prove the Proposition from Week 2:

Proposition: Let C be an irreducible cubic curve in $\mathbb{P}^2$. Let C_1 be another cubic and suppose

$$C \cap C_1 = \{p_1, \ldots, p_9\}.$$

If C_2 is any other cubic which contains $p_1, \ldots, p_8$, then C_2 also contains p_9. You can prove this via the following steps:

(a) Let $p_1, \ldots, p_5$ be 5 distinct points in $\mathbb{P}^2$. If no 4 of the points lie on a line, show there is a unique curve of degree 2 passing through all 5 points.

(b) Let $p_1, \ldots, p_8$ be 8 distinct points in the plane such that no 4 of them lie on a line and no 7 lie on a curve of degree 2. Show that the vector space of cubic polynomials which are zero at all 8 points has dimension equal to 2.

(c) Deduce the Proposition above.

(In your proof you may want to use **Bezout's Theorem:** if C and D are distinct irreducible curves of degree c and d repectively, then $C \cap D$ consists of at most cd points.)