22MAC260 Problem Sheet 2: Solutions

Week 2

Last updated February 19, 2024

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 $Q = (-1, 0)$.

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

Solution: In the Week 2 lectures we showed that $P \oplus Q = (0, -1)$. For brevity let's call this point R; we want to find $P \oplus R$.

The line $\overline{PR}$ has slope $\frac{-1-3}{0-2} = 2$ so its equation has the form

$$y = 2x + c;$$

plugging in the coordinates of P we find that $c = -1$. So the equation is

$$\overline{PR}: \; y = 2x - 1.$$

Substituting into the equation of our curve $y^2 = x^3 + 1$ we get

$$\begin{aligned} (2x-1)^2 &= x^3 + 1 \\ \Leftrightarrow x^3 - 4x^2 + 4x &= 0. \end{aligned}$$

This cubic has a root $x = 0$ corresponding to R and a **double** root at $x = 2$ corresponding to P. This means that the line $\overline{PR}$ is tangent to the curve at P. So $P * R = P = (2, 3)$ and hence $P \oplus R = (2, -3)$.

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

Solution: We just saw that the line $\overline{PR}$ is tangent to the curve at P. The equation of this line is

$$y = 2x - 1.$$

(c) Use the previous part to calculate the point

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

(The definition of $P * P$ was given in the Week 2 lectures.)
Solution: From the previous part we know that

$$P * P = R = (0, -1)$$

and hence

$$2P = (0, 1).$$

(d) Verify that $2P \oplus Q = P \oplus (P \oplus Q)$.
Solution: From the previous part we have

$$2P = (0, 1) = P * Q$$

hence

$$\begin{aligned} 2P * Q &= (P * Q) * Q \\ &= P \\ &= (2, 3). \end{aligned}$$

So

$$\begin{aligned} 2P \oplus Q &= (2, -3) \\ &= P \oplus (P \oplus Q). \end{aligned}$$

(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 $-P$ added to itself a times. Now compute as many points of the form $a\,P \oplus b\,Q$ (for a, $b \in \mathbf{Z}$) as you feel like.
Solution: Since $Q = (-1, 0)$ has y-coordinate equal to zero, we know that $-Q = O * Q = Q$, hence $2Q = 0$.
Our calculations above show that

$$\begin{aligned} 2P \oplus Q &= (2, -3) \\ &= -P. \end{aligned}$$

Hence

$$\begin{aligned} 3P \oplus Q &= O\,; \quad \text{that is,} \\ 3P &= -Q \\ &= Q. \end{aligned}$$

In particular this shows that $6P = 2Q = O$.
Hence can write down all the multiples of P:

$$\begin{aligned}
P &= (2,3) \\
2P &= (0,1) \\
3P = Q &= (-1,0) \\
4P = -2P &= (0,-1) \\
5P = -P &= (2,-3) \\
6P &= O
\end{aligned}$$

$$\text{and in general } \forall n \in \mathbf{Z},\ nP = \overline{n}P$$

where $\overline{n} = n \bmod 6$. So for any a, $b \in \mathbf{Z}$, we have

$$\begin{aligned}
aP \oplus bQ &= (a+3b)P \\
&= kP
\end{aligned}$$

where $k = (a+3b) \bmod 6$.

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.
   Solution: We need to show that the cubic $8x^3 - 12x^2 + 6x$ has 3 distinct roots. We can factorise it as

$$\begin{aligned}
8x^3 - 12x^2 + 6x &= 8x(x^2 - \frac{3}{2}x + \frac{3}{4}) \\
&= 8x\left(x - \frac{3}{2} - \sqrt{-\frac{3}{4}}\right)\left(x - \frac{3}{2} + \sqrt{-\frac{3}{4}}\right)
\end{aligned}$$

   So the cubic has 3 distinct roots (one real root at $x = 0$ and two complex conjugate roots), therefore it defines an elliptic curve.

   (b) Show that the points

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

   lie on the curve C.
   Solution: We simply substitute the coordinates of R and S into the equation of C and see that it is satisfied. For R this is very easy; for S we find

$$\begin{aligned}
8\left(\frac{3}{2}\right)^3 - 12\left(\frac{3}{2}\right)^2 + 6\left(\frac{3}{2}\right) &= 8 \cdot \frac{27}{8} - 12 \cdot \frac{9}{4} + 9 \\
&= 27 - 27 + 9 \\
&= 3^2
\end{aligned}$$

   so the coordinates of S do satisfy the equation of C.

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

Solution: To calculate $R \oplus S$ we first find the line $\overline{RS}$. This line has slope

$$m = \frac{3-0}{\frac{3}{2}-0} = 2$$

and since it passes through $R = (0,0)$ its equation must be $y = 2x$. Substituting this into the equation of C we get

$$\begin{aligned} (2x)^2 &= 8x^3 - 12x^2 + 6x \\ \Leftrightarrow 8x^3 - 16x^2 + 6x &= 0 \\ \Leftrightarrow x^3 - 2x^2 + \frac{3}{4}x &= 0 \end{aligned}$$

We know this cubic has roots at $x = 0$ corresponding to R and $x = \frac{3}{2}$ correspnding to S, and the x-coordinate of $R * S$ is the 3rd root. For a monic cubic, the sum of the roots is minus the coefficient of x^2, so the 3rd root is $x = 2 - 0 - \frac{3}{2} = \frac{1}{2}$. Since the point $R * S$ lies on the line $y = 2x$, its y-coordinate must therefore be $y = 1$. So we find

$$R * S = \left(\frac{1}{2}, 1\right)$$

and finally

$$R \oplus S = \left(\frac{1}{2}, -1\right).$$

To find further points of the form $aR \oplus bS$, we first compute $R \oplus 2S = S \oplus (R \oplus S)$. The line joining S to $R \oplus S$ has slope

$$\begin{aligned} m &= \frac{3-(-1)}{\frac{3}{2}-\frac{1}{2}} \\ &= 4 \end{aligned}$$

while the tangent line to the curve at S has slope

$$\begin{aligned} \frac{dy}{dx}(S) &= \frac{24x^2 - 24x + 6}{2y}(S) \\ &= \frac{24 \cdot \frac{9}{4} - 24 \cdot \frac{3}{2} + 6}{2 \cdot 3} \\ &= \frac{54 - 36 + 6}{6} \\ &= 4 \end{aligned}$$

So both lines pass through S and have the same slope, hence they must be equal. This implies

$$\begin{aligned} S * (R \oplus S) &= S \quad \text{so} \\ S \oplus (R \oplus S) &= -S \quad \text{in other words} \\ R \oplus 2S &= -S \end{aligned}$$

This gives

$$3S = -R.$$

As before, since the y-coordinate of R equals zero, we have $2R = O$, therefore $R = -R$ and $3S = R$.

The final result is therefore exactly analagous to Question 1: we have

$$S = \left(\frac{3}{2}, 3\right), \; 2S = R * S = \left(\frac{1}{2}, 1\right), \; 3S = R,$$
$$4S = -2S = \left(\frac{1}{2}, -1\right), \; 5S = -S = \left(\frac{3}{2}. -3\right), \; 6S = O$$

and

$$aR \oplus bS = kS$$

where $k = 3a + b \mod 6$.

Remark: It is not an accident that the results of Questions 1 and 2 correspond so closely. In fact, there is an affine linear change of coordinates that transforms the curve in Question 2 to the curve in Question 1, and maps the points R and S to the points Q and P respectively. So one could say that Question 2 does the calculations of Question 1 again, in different coordinates.

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 point P.

Solution: This is a simple substitution.

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

Solution: We start by computing $2P$. Remember that $2P$ is defined to be $O*(P * P)$ where $P * P$ means the third point of C that lies on the tangent line at P.

Let $f = y^2 - x^3 + x - 1$. Then the tangent line to C at P has slope

$$\begin{aligned} \frac{\partial y}{\partial x}(P) &= \frac{\partial f/\partial x}{\partial f/\partial y}(P) \\ &= \left(\frac{3x^2-1}{2y}\right)_{|P} \\ &= 1 \end{aligned}$$

so its equation is

$$\begin{aligned} y - 1 &= 1 \cdot (x-1) \quad \text{i.e.} \\ y &= x. \end{aligned}$$

Substituting this into the equation of C we get

$$\begin{aligned} x^2 &= x^3 - x + 1 \quad \text{i.e.} \\ x^3 - x^2 - x + 1 &= 0 \end{aligned}$$

We know this has a double root at $x = 1$ corresponding to P. This means that $(x-1)^2$ divides the above cubic; loooking at the constant term we see that the third root must then be $x = -1$. Substituting this into the equation of the tangent line we get $y = -1$ also, and so we have $P * P = (-1, -1)$. As before, this gives $2P = (-1, 1)$.

Next we compute $3P = 2P \oplus P$. The line joining $2P$ to P has slope 0 so its equation is $y = 1$. Substituting this into the equation of C gives

$$x^3 - x = 0$$

which has roots at $x = \pm 1$, corresponding to $2P$ and P respectively, and at $x = 0$, corresponding to $2P * P$. So we get $2P * P = (0, 1)$ and hence $3P = (0, -1)$.

Finally we can compute $6P$ as $3P * 3P$ (so no need to find $4P$ or $5P$). The tangent line to C at $3P$ has slope

$$\left(\frac{3x^2-1}{2y}\right)_{|3P} = \frac{1}{2}$$

so its equation is

$$\begin{aligned} y + 1 &= \frac{1}{2}x \quad \text{i.e.} \\ y &= \frac{1}{2}x - 1. \end{aligned}$$

Substituting this into the equation of C we get

$$\left(\frac{1}{2}x - 1\right)^2 = x^3 - x + 1 \quad \text{i.e.}$$
$$x^3 - \frac{1}{4}x^2 = 0$$

This has a double root at $x = 0$ corresponding to $3P$, and the third root is at $x = \frac{1}{4}$. Putting $x = \frac{1}{4}$ into the equation of the tangent line we get $y = -\frac{7}{8}$, so $3P * 3P = -\frac{7}{8}$ and hence finally

$$6P = \left(\frac{1}{4}, \frac{7}{8}\right).$$

Remark: This shows that even if we start with a curve like C whose equation has integer coefficients, and a point like P whose coordinates are integers, the addition process can give us points with non-integer coordinates. We will get a better understanding in Week 5 of what this tells us about P.

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.

Solution: The point $(x_0, 0)$ lies on C if and only if x_0 is a root of $x^3 - x$, hence we get three such points $R_1 = (-1, 0)$, $R_2 = (0, 0)$, $R_3 = (1, 0)$.

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

Solution: For any i we know that the tangent line to the curve is vertical, since if $f = y^2 - x^3 + x$ we get

$$\frac{\partial f}{\partial y}(R_i) = 2y(R_i) = 0.$$

Any vertical line intersects C again at O, hence $R_i * R_i = O$ and $R_i \oplus R_i = O * O = O$.

(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.

Solution: For any distinct i and j, the line joining R_i to R_j is just the x-axis. This intersects the curve at the third point R_k.

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

Solution: There are 3 conditions to check: (i) the set is closed under the operation; (ii) the set contains the identity element; (iii) the set contains the inverse of each of its elements.

(i) We showed that $R_i \oplus R_j = R_k$ for $i \neq j$ and $R_i \oplus R_i = O$ for each i. Finally $O \oplus O = O$ and $R_i \oplus O = R_i$ for each i. So the given set is closed under the operation $\oplus$.

(ii) By definition the set contains the idenity element O.

(iii) The identity element O is its own inverse. For each i we showed that $2R_i = O$, which is equivalent to $-R_i = R_i$. So every element in the set is its own inverse — in particular, the set contains the inverse of each of its elements.

Remark: For concreteness we proved the above fact for a specific curve. But we didn't really use any special properties of the curve. In fact the same argument shows the following: for any elliptic curve E, its **2-torsion subgroup**

$$E[2] := \{P \in E \mid 2P = O\}$$

is a group with 4 elements in which each element has order 1 or 2, hence $E[2]$ is isomorphic to the Klein 4-group V_4.

The following question is not examinable.

I. In this problem you will prove the Proposition on p.8 of the Week 2 notes:

Proposition: Let C be an irreducible cubic curve in $\mathbf{P}^2$. 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 $\mathbf{P}^2$. 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 space of cubic polynomial 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.)