23MAC260 Problem Sheet 3: Solutions

Week 3

Last updated March 4, 2024

1. Put each of the following curves in Weierstrass form:

   (a) $y^2 = -x^3 + 2x^2 + 3x - 1$

   Solution: The coefficient of x^3 is $A = -1$. So we put

   $$x = \frac{x'}{A} = -x'$$
   $$y = \frac{y'}{A} = -y'$$

   in our original equation to get

   $$(-y')^2 = -(-x')^3 + 2(-x')^2 + 3(-x') - 1$$

   which simplifies to

   $$(y')^2 = (x')^3 + 2(x')^2 - 3x' - 1.$$

   We rename our variables back to x and y to write this as

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

   The next step is to put $x' = x + \frac{\beta}{3} = x + \frac{2}{3}$. Replacing x by $x' - \frac{2}{3}$ in the above equation and simplifying we get

   $$y^2 = (x')^3 - \frac{13}{3}x' + \frac{43}{27}.$$

   Finally we write our variables as x and y again to get

   $$y^2 = x^3 - \frac{13}{3}x + \frac{43}{27}.$$

(b) $y^2 = 8x^3 - 4x^2 - 2x + 1$

Solution: In this case we have $A = 8$ so we put

$$x = \frac{x'}{8}$$
$$y = \frac{y'}{8}$$

to get

$$\left(\frac{y'}{8}\right)^2 = 8\left(\frac{x'}{8}\right)^3 - 4\left(\frac{x'}{8}\right)^2 - 2\left(\frac{x'}{8}\right) + 1$$

which simplifies to

$$(y')^2 = (x')^3 - 4(x')^2 - 16x' + 64$$

which we rewrite as

$$y^2 = x^3 - 4x^2 - 16x + 64.$$

Next we put $x = x' - \frac{\beta}{3} = x' + \frac{4}{3}$ and simplify to get

$$y^2 = (x')^3 - \frac{64}{3}x' + \frac{1024}{27}$$

or renaming the variables again

$$y^2 = x^3 - \frac{64}{3}x + \frac{1024}{27}.$$

(c) $y^2 = \omega x^3 + \omega^2 x^2 + x$ (where $\omega = \exp(2\pi i/3)$).

Solution: Here $A = \omega$ so we set

$$x = \frac{x'}{\omega}$$
$$y = \frac{y'}{\omega}$$

to get (after multiplying across by ω^2)

$$(y')^2 = (x')^3 + \omega^2(x')^2 + \omega x'.$$

Rename variables to write this as

$$y^2 = x^3 + \omega^2 x^2 + \omega x.$$

Next we put $x = x' - \frac{\beta}{3} = x' - \frac{\omega^2}{3}$ to get

$$y^2 = \left(x' - \frac{\omega^2}{3}\right)^3 + \omega^2\left(x' - \frac{\omega^2}{3}\right)^2 + \omega\left(x' - \frac{\omega^2}{3}\right).$$

Expanding out all terms on the right hand side, the coefficient of x' becomes

$$\begin{aligned} & 3\left(-\frac{\omega^2}{3}\right)^2 + 2\omega^2\left(-\frac{\omega^2}{3}\right) + \omega \\ =& \frac{\omega^4}{3} - 2\frac{\omega^4}{3} + \omega \\ =& \omega - \frac{\omega}{3} \quad (\text{ using } \omega^3 = 1) \\ =& \frac{2\omega}{3} \end{aligned}$$

and the constant term is

$$\begin{aligned} & \left(-\frac{\omega^2}{3}\right)^3 + \omega^2\left(-\frac{\omega^2}{3}\right)^2 + \omega\left(-\frac{\omega^2}{3}\right) \\ =& -\frac{1}{27} + \frac{1}{9} - \frac{1}{3} \\ =& -\frac{7}{27} \end{aligned}$$

so finally the Weierstrass form is

$$y^2 = x^3 + \frac{2\omega}{3} - \frac{7}{27}.$$

Which of these equations define elliptic curves?

Solution:

For the first curve, the discriminant is

$$\begin{aligned} \Delta &= -4\left(-\frac{13}{3}\right)^2 - 27\left(\frac{43}{27}\right)^2 \\ &\neq 0 \end{aligned}$$

so this is an elliptic curve.

For the second curve, the discriminant is

$$\begin{aligned} \Delta &= -4\left(-\frac{4}{3}\right)^3 - 27\left(\frac{16}{27}\right)^2 \\ &= 0 \end{aligned}$$

so this equation **does not** define an elliptic curve.

For the last curve, the discriminant is

$$\begin{aligned}\Delta &= -4\left(\frac{2\omega}{3}\right)^3 - 27\left(-\frac{7}{27}\right)^2 \\ &= -\frac{32}{27} - \frac{7^2}{27} \\ &\neq 0\end{aligned}$$

so again it is an elliptic curve.

2. We defined the discriminant Δ of a cubic polynomial

$$f(x) = x^3 + ax + b$$

in Weierstrass form to be

$$\Delta = -4a^3 - 27b^2.$$

Now suppose that f has roots x_0, x_1, x_2.

(a) Write a and b in terms of x_0, x_1, and x_2. What is $x_0 + x_1 + x_2$?
Solution: If

$$x^3 + ax + b = (x - x_0)(x - x_1)(x - x_2)$$

then by multiplying out the right-hand side we find

$$\begin{aligned}a &= x_0x_1 + x_0x_2 + x_1x_2 \\ b &= -x_0x_1x_2.\end{aligned}$$

Since there is no x^2 term on the left-hand side, the x^2 term on the right-hand side must vanish also, hence

$$x_0 + x_1 + x_2 = 0.$$

(b) Prove that

$$\Delta = (x_0 - x_1)^2(x_0 - x_2)^2(x_1 - x_2)^2.$$

(Note: This gives a different proof that $\Delta = 0$ if and only if f has a multiple root.)
Solution: Using the identity $x_2 = -x_0 - x_1$ from the previous part, we get that

$$\begin{aligned}a &= x_0x_1 + x_0(-x_0 - x_1) + x_1(-x_0 - x_1) \\ &= -x_0^2 - x_1^2 - x_0x_1; \\ b &= -x_0x_1(-x_0 - x_1) \\ &= x_0^2x_1 + x_0x_1^2.\end{aligned}$$

So Δ can be written as

$$\begin{aligned}\Delta &= -4a^3 - 27b^2 \\ &= -4(-x_0^2 - x_1^2 - x_0x_1)^3 - 27(-x_0^2x_1 - x_0x_1^2)^2 \qquad (*)\end{aligned}$$

On the other hand, setting $x_2 = -x_0 - x_1$ in the right-hand side of the equation we're trying to prove, we get

$$\begin{aligned}&(x_0 - x_1)^2(2x_0 + x_1)^2(x_0 + 2x_1)^2 \\ &= 4x_0^6 + 12x_0^5x_1 - 3x_0^4y^2 - 26x_0^3x_1^3 - 3x_0^2x_1^4 + 12x_0x_1^5 + 4x_1^6 \qquad (**)\end{aligned}$$

Each of the expressions $(*)$ and $(**)$ is a homogeneous polynomial of degree 6 in x_0 and x_1. Comparing the coefficients of the 7 monomials $x_0^ix_1^{6-i}$ for $i = 0, \ldots, 6$, we verify that the two expressions are indeed equal. (In fact, since both $(*)$ and $(**)$ are symmetric in x_0 and x_1 we only need to compare these coefficients as far as the $x_0^3x_1^3$ term; if these are equal, then by symmetry the others must be too.)

3. (Week 3 notes, Section 3) For the elliptic curve

$$y^2 = x^3 + 73$$

and the point $P = (2, 9)$, use the formula from lectures to compute the points

$$2P,\ 3P,\ 4P.$$

(A calculator will be useful here.)

Do you think there is an integer n such that $nP = O$? (We will provide a definite answer later in the module.)

Solution: The given curve is in Weierstrass form, so we can use the formulas from lectures (Week 3 Theorem 3.1) to calculate

$$\begin{aligned}2P &= P \oplus P \\ 3P &= 2P \oplus P \\ 4P &= 2P \oplus 2P\end{aligned}$$

We find

$$\begin{aligned}2P &= \left(-\frac{32}{9}, -\frac{143}{27}\right) \\ 3P &= \left(\frac{5111}{625}, -\frac{389016}{15625}\right) \\ 4P &= \left(\frac{3668032}{184041}, \frac{7057368001}{78953589}\right).\end{aligned}$$

If there was a multiple n such that $nP = 0$, this would mean that $(n-1)P \oplus P = O$. From our definition of addition this would mean that $(n-1)P$ and P would have the same x-coordinate. On the other hand, it seems from the calculations above that as we increase the multiple n, the coordinates of the point nP are becoming more and more complicated. So it doesn't seem as if this is going to happen. We'll see in the next part of the module that for an elliptic curve equation with integer coefficients like the one abve, any point of finite order must in fact have integer coefficients.

4. Consider the family of curves C_t given by the equation

$$Y^2Z = tX^3 - XZ^2 - Z^3$$

where $t \in \mathbf{C}$ is a parameter. As we vary the parameter t, we get a family of cubic curves in $\mathbf{P}^2$.

(a) Find all values of t such that C_t is not an elliptic curve. (Hint: use the discriminant Δ.)

Solution: First, setting $t = 0$ in the above equation we get

$$Y^2Z = -XZ^2 - Z^3.$$

The dehomogenisation of the cubic on the right-hand side is $-x - 1$, which is not a cubic in x and therefore does not have 3 distinct roots. So for $t = 0$ the curve is not an elliptic curve.

Let us now assume that $t \neq 0$. To compute the discriminant we have to put the curve

$$C_t: \quad Y^2Z = tX^3 - XZ^2 - Z^3$$

into Weierstrass form. First dehomogenise to get the affine equation:

$$C_t: \quad y^2 = tx^3 - x - 1$$

This has $A = t$, so we put $x = x'/t$ and $y = y'/t$ and clear denominators to get

$$(y')^2 = (x')^3 - tx' - t^2$$

or renaming variables as usual

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

This is in Weierstrass form, with discriminant

$$\begin{aligned}\Delta &= -4a^3 - 27b^2 \\ &= 4t^3 - 27t^4.\end{aligned}$$

We are assuming that $t \neq 0$, so we can divide by t^3 to see that $\Delta = 0$ if and only if $4 - 27t = 0$, that is, $t = \frac{4}{27}$.

So C_t is not an elliptic curve if and only if $t = 0$ or $t = \frac{4}{27}$.

(b) What does the curve C_0 (obtained by setting $t = 0$ in the equation above) look like?

Solution: Setting $t = 0$ in the above equation we get

$$Y^2Z = -XZ^2 - Z^3.$$

To see what this curve looks like, we can write the equation as

$$Z\left(Y^2 + XZ + Z^2\right) = 0.$$

So the curve C_0 is a union $C_0 = L \cup Q$, where L is the line at infinity $\{Z = 0\}$ and Q is the conic curve $\{Y^2 + XZ + Z^2 = 0\}$. One can check that the homogeneous quadratic $Y^2 + XZ + Z^2$ is irreducible, and so Q is an irreducible conic. To see how the line L and the conic Q intersect, we set $Z = 0$ in this quadratic. This gives $Y^2 = 0$, so L and Q meet only at the point $[1, 0, 0]$. Bezout's theorem says that a line and a conic in $\mathbf{P}^2$ should meet in two points, counted with multiplicity, so the intersection at $[1, 0, 0]$ must be tangential.

Here is a sketch of C_0: