Course MA342P — Sample Paper 1

Timothy Murphy

April 27, 2016

Attempt 4 questions. All carry the same mark. The word 'curve' always means projective curve.

1. Explain informally how two points on an elliptic curve are added.

   Find the sum $P+Q$ of the points $P=(0,1),\ Q=(1,2)$ on the curve
   $$y^2 = x^3 + 2x + 1$$
   over the rationals $\mathbb{Q}$. What is $2P$?

2. Show that all cubics through 8 given points in general position in the plane pass through a 9th point.

   Hence or otherwise show that addition on an elliptic curve is associative.

3. Define the discriminant of a polynomial, and find the discriminant of
   $$f(x) = x^3 + x^2 - x + 2.$$
   How many real roots does this polynomial have?

   Define the resultant of two polynomials, and find the resultant of
   $$f(x) = x^2 + 3,\ g(x) = x^3 + 2.$$

4. What is meant by saying that a point on the curve
   $$y^2 + Ax + B = x^3 + ax^2 + bx + c$$
   is *singular*? What are the points at infinity on this curve? Are any of them singular?

   Find a condition on A, B, a, b, c for the curve to contain a singular point.

5. Find the order of the point $P=(0,0)$ on the elliptic curve
   $$y^2 + y = x^3 - x.$$

6. Show that the elliptic curve

$$E : y^2 + xy = x^3 - x^2 - 2x - 1$$

has good reduction modulo 2 and 5; and determine the groups $\mathcal{E}(\mathbb{F}_2)$ and $\mathcal{E}(\mathbb{F}_5)$.

What can you deduce about the group of points of finite order on $\mathcal{E}(\mathbb{Q})$?

7. Define a *lattice* $L \subset \mathbb{C}$. Show that the series

$$\frac{1}{z^2} + \sum_{\omega \in L,\, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

defines a function $\wp(z)$ which is periodic with respect to L.

Show also that $\wp(z)$ satisfies the functional equation

$$\wp'(z)^2 = 4\wp(z)^3 + A\wp(z) + B$$

for certain constants A, B.