Course MA342P — Sample Paper 2

Timothy Murphy

May 2, 2016

Attempt 4 questions. All carry the same mark.

1. Explain informally how two points on an elliptic curve are added. Find the sum P + Q of the points P = (-1, 0), Q = (2, 3) on the curve

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

over the rationals \mathbb{Q} . What are 2P and 2Q?

2. For which of the primes p = 2, 3, 5 does the elliptic curve

$$\mathcal{E}(\mathbb{Q}): y^2 = x^3 + x + 1$$

have good reduction modulo *p*?

Determine the group $\mathcal{E}(\mathbb{F}_p)$ in these cases.

3. Express the 5-adic integer $2/3 \in \mathbb{Z}_5$ in standard form

 $2/3 = a_0 + a_1 5 + a_2 5^2 + \dots \qquad (0 \le a_i < 5).$

Does there exist a 5-adic integer x such that $x^2 = 6$?

 Define the *rank* of a finitely-generated abelian group A (showing that it depends only on A).

How many abelian groups are there of orders 18, 27, 42?

Show that the multiplicative group F[×] of a finite field F is cyclic.
Find all the primitive roots in F₁₉.

6. Either show that the equation

$$x^4 + y^4 = z^4$$

has no solutions in non-zero integers x, y, z; or show that the equation

$$x^3 + y^3 = z^3$$

has no solutions in non-zero integers x, y, z.

7. Define the Weierstrass elliptic function $\varphi(z)$ associated to the lattice $\Lambda \subset \mathbb{C}$, and show that it satisfies a differential equation of the form

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