Course 428

Elliptic Curves II

Dr Timothy Murphy

Exam Hall Friday, 7 April 2000 9:00–11:00

Attempt 5 questions. (If you attempt more, only the best 5 will be counted.) All questions carry the same number of marks.

1. What is meant by saying that an elliptic curve has *good reduction* at the prime p?

   Sketch the proof that if p is a good prime then the map

   $$\mathcal{E}(\mathbb{Q}) \to \mathcal{E}(\mathbb{F}_p)$$

   is a homomorphism.

   What happens if p is bad?

   Determine the good primes for the elliptic curve

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

2. If the elliptic curve

   $$y^2 = x^3 + ax^2 + bx + c$$

   has good reduction at p, show that the torsion subgroup of $\mathcal{E}(\mathbb{Q})$ is mapped injectively into $\mathcal{E}(\mathbb{F}_p)$.

   Let $\mathcal{E}(\mathbb{Q})$ be the curve

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

   Determine the group $\mathcal{E}(\mathbb{F}_p)$ for two good primes p, and hence or otherwise determine the torsion group of $\mathcal{E}$.

3. Prove that a finite abelian group A is a direct sum of cyclic subgroups of prime-power order; and show that the set of prime-powers depends only on A.

4. What is a *lattice* $\Lambda \subset \mathbb{C}$; and what is meant by saying that $f(z)$ is *elliptic* with respect to Λ?

   Define the Weierstrass elliptic function $\wp(z)$ associated to Λ, and show that $\wp(z)$ is indeed elliptic with respect to Λ.

   Show that every even elliptic function $f(z)$ with respect to Λ is a rational function of $\wp(z)$, ie

$$f(z) = \frac{P(\wp(z))}{Q(\wp(z))}$$

   where $P(w), Q(w)$ are polynomials.

5. Show that the group $\mathrm{SL}(2, \mathbb{Z})$ is generated by

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

6. Explain how a lattice $\Lambda \subset \mathbb{C}$ gives rise to an elliptic curve

$$\mathcal{E}(\mathbb{C}) : y^2 = x^3 + bx + c;$$

   and sketch the proof that every elliptic curve of this form arises in this way from a unique lattice Λ.

7. Prove Fermat's Last Theorem *either* for the case $n = 3$ *or* for the case $n = 4$.