Course 428a

Elliptic Curves II

Dr Timothy Murphy

Seminar Room Friday, 14 April 2000 16:15–17:45

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.

   Determine the good primes for the elliptic curve

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

2. Determine the group $\mathcal{E}(\mathbb{F}_p)$ for the curve

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

   and the primes $p = 3, 5, 7$. Hence or otherwise determine the torsion group of $\mathcal{E}(\mathbb{Q})$.

3. Prove that a finitely-generated abelian group A can be expressed as a direct sum

   $$A = F \oplus \mathbb{Z}^r,$$

   where F is finite; and show that r 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? Explain what you mean by a *fundamental parallelogram* Π for Λ?

   Show that the numbers of poles and zeros of $f(z)$ in Π are equal.

   Show also that if the zeros are $a_1, \ldots, a_r$ and the poles are $b_1, \ldots, b_r$ then

$$a_1 + \cdots + a_r \equiv b_1 + \cdots + b_r \bmod \Lambda.$$

5. Let s, u be the elements of the modular group Γ corresponding to the matrices

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

   Show that

$$s^2 = u^3 = 1;$$

   and prove that Γ is generated by s and u.

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 in the case $n = 4$.