C9.1b Elliptic Curves
Checked by: Victor Flynn

Roger Heath-Brown 24/02/2011

Do not turn this page until you are told that you may do so

1. Find an $m \in \mathbb{N}$ such that $|m^3 - 7|_5 < 5^{-1}$. Show that there is no $n \in \mathbb{N}$ such that $|n^3 - 7|_3 < 3^{-1}$.

Show that the equation $x^3 + 2y^3 + 4z^3 = 0$, with x, y and z all in $\mathbb{Q}_2$, has only the solution $x = y = z = 0$.

Determine necessary and sufficient conditions on $x \in \mathbb{Q}_2$ for the sum $\sum_{n=0}^{\infty} x^n/n!$ to be convergent in $\mathbb{Q}_2$

[*You may use without proof the facts that* $2^{n-1} \mid n!$ *whenever* n *is a power of* 2*, and that* 2^n *never divides* $n!$.]

State Hensel's Lemma.

Let a and b be integers. Show that the elliptic curve $y^2 = x^3 + ax + b$ has infinitely many points (x, y) in $\mathbb{Z}_p$, for any prime $p \geq 5$ of good reduction.

[*You may use any standard facts about elliptic curves that you require, providing that they are clearly stated.*]

Let a and b be integers as before. If the elliptic curve $y^2 = x^3 + ax + b$ has bad reduction at a prime $p \geq 5$, what can you say about the polynomial $x^3 + ax + b$, considered modulo p? Show that $y^2 = x^3 + ax + b$ has infinitely many points (x, y) in $\mathbb{Z}_p$, for any prime $p \geq 5$ of bad reduction.

[*You may wish to consider separately the two cases which arise.*]

2. Let R be a commutative ring with a 1. Define a *Formal Group* $F(X, Y)$ over R.

If $R[[T]]$ denotes the power series ring over R, show that there is a unique element $i(T) \in TR[[T]]$ such that $F(T, i(T)) = 0$. Show further that we have $F(T, 0) = T$.

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}_p$, with $A, B \in \mathbb{Z}_p$. Using any facts about formal groups that you require, show that if $E_1(\mathbb{Q}_p)$ is the kernel of the reduction map $E_0(\mathbb{Q}_p) \to E_{\mathrm{ns}}(\mathbb{F}_p)$ then $E_1(\mathbb{Q}_p)$ is torsion-free.

Deduce that if $y^2 = x^3 + ax + b$ is an elliptic curve over $\mathbb{Q}$, with $a, b \in \mathbb{Z}$, then any non-trivial torsion point $P = (x, y)$ has $x, y \in \mathbb{Z}$. Using reduction into $\mathbb{F}_3$, show that there are at most 6 non-trivial torsion points with $3 \nmid y$.

3. Let $D : V^2 = U(U^2 + a_1U + b_1)$ be an elliptic curve, with $a_1, b_1 \in \mathbb{Z}$ and $a_1(a_1^2 - 4b_1) \neq 0$. Define $q : D(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ by setting $q(u, v) = u$ for $u \neq 0$ and $q(u, v) = b_1$ for $u = 0$. Define also $q(\underline{0}) = 1$ for the point at infinity. Show that q is a homomorphism.

[*You need only verify the homomorphism condition for pairs of points P, Q for which none of P, Q or $P + Q$ is $(0, 0)$ or the point at infinity.*]

Show further that the image of q is finite.

Suppose $A, B, C, D \in \mathbb{N}$ are such that A^2, B^2, C^2, D^2 form a 4-term arithmetic progression. Show that the curve $E : y^2 = x(x^2 + 5x + 4)$ has a rational point (x, y) with $x = -2B^2C^{-2}$.

Use descent via 2-isogeny to show that $\#\left(E(\mathbb{Q})/2E(\mathbb{Q})\right) \leq 4$.

Find the rank of E.

[*You may use without proof the fact that if $\mathcal{E}$ is an elliptic curve, then*

$$\#\left(\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})\right) = \#\left(\mathcal{E}_{\text{tors}}(\mathbb{Q})/2\mathcal{E}_{\text{tors}}(\mathbb{Q})\right) \times 2^r,$$

where r is the rank of $\mathcal{E}$. You may also use without proof that $E_{\text{tors}}(\mathbb{Q}) \cong C_4 \times C_2$ and that the torsion points have $x = -4, -2, -1, 0$ or 2.]

Deduce that in fact A, B, C, D are all equal.