**Final Honour School of Mathematics Part C**

---

# Course Title: C9.1b. Elliptic Curves
# Lecturer: Prof Roger Heath Brown

---

**16/2/12**

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

**1.** (a) Find an integer $m$ such that $|m^2 - 2|_7 \leq 7^{-3}$, and show that there is no integer $n$ with $|n^3 - 2|_7 \leq 7^{-3}$.

If $p$ is a prime and the integer $k$ is a multiple of $p$, show that the sum $1 + k + k^2 + \ldots$ converges in $\mathbb{Q}_p$, and find its limit.

Show that

$$3^{2^n} \to 1$$

in $\mathbb{Q}_2$. Deduce that for any integers $a, b \in \mathbb{Z}$ there is a sequence $c_n \in \mathbb{Z}$ such that $c_n \to a$ in $\mathbb{Q}_2$ and $c_n \to b$ in $\mathbb{Q}_3$.

(b) Let $N \in \mathbb{N}$ be a product of two primes $p$ and $q$, and let $P$ be a point modulo $N$ on an elliptic curve $\mathcal{E}$ defined over $\mathbb{Z}/N\mathbb{Z}$. If one calculates $kP$ modulo $N$, under what condition will the Elliptic Curve Method reveal the factors $p$ and $q$ of $N$?

Let $P$ be the point $(3, 4)$ on the elliptic curve $y^2 = x^3 - 11$. Using the Elliptic Curve Method, factorize 391 by calculating $3P$.

**2.** (a) Let $R$ be a commutative ring with a 1. What does it mean to say that $F(X, Y) \in R[[X, Y]]$ is a formal group defined over $R$? Show that there is a unique power series $i(T) \in R[[T]]$ such that $F(T, i(T)) = 0$.

Let $P(T)\,\mathrm{d}T$ be a differential form for the formal group. Write down the condition on $P$ which must be satisfied for $P(T)\,\mathrm{d}T$ to be an invariant differential. Given that $F(0, T) = T$, show that the choice $P(T) = F_X(0, T)^{-1}$ produces an invariant differential.

(b) Let $p$ be an odd prime. Suppose that $\mathcal{E} : y^2 = x^3 + Ax + B$ is an elliptic curve over $\mathbb{Q}_p$, with good reduction at $p$. What can you say about torsion elements in the kernel of the reduction map $\mathcal{E}(\mathbb{Q}_p) \to \tilde{\mathcal{E}}(\mathbb{F}_p)$ ? (Proof not required.) Deduce that $\mathcal{E}_{\mathrm{tors}}(\mathbb{Q}_p)$ is finite.

(c) Let $n$ be a positive integer. By considering primes $\equiv 5 \pmod 6$ show that the curve $y^2 = x^3 + n^2$ has at most 6 rational torsion points.

[*You may assume that for any integer $m$, the congruence $x^3 \equiv m \pmod p$ has exactly one solution $x$ modulo $p$, provided that $p$ is a prime $\equiv 5 \pmod 6$. You may also assume that for any positive integer $k$ there are infinitely many primes $p \equiv 5 \pmod 6$ for which $(p + 1)/6$ is coprime to $k$.*]

**3.** Let $a, b \in \mathbb{Z}$ with $b(a^2 - 4b) \neq 0$, and write $\mathcal{C} : y^2 = x(x^2 + ax + b)$ for the corresponding elliptic curve. Let $\mathcal{D} : v^2 = u(u^2 + a_1 u + b_1)$ be the dual curve, where $a_1 = -2a$ and $b_1 = a^2 - 4b$. Suppose that $\phi : \mathcal{C} \to \mathcal{D}$ and $\widehat{\phi} : \mathcal{D} \to \mathcal{C}$ are the associated isogenies, and let $\mathcal{G} = \mathcal{C}(\mathbb{Q})$ and $\mathcal{H} = \mathcal{D}(\mathbb{Q})$ be the associated Mordell–Weil groups.

Explain, without proofs, how one defines a non-trivial homomorphism $q$ from $\mathcal{H}$ to $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, with kernel $\phi(\mathcal{G})$. (Proof not required.)

Show that if $(u, v) \in \mathcal{H}$ with $u \neq 0$, then one may write $u = rw^2$ with $w \in \mathbb{Q}$ and with $r$ being a square-free integer dividing $b_1$.

Specifying any properties of $\phi$ and $\widehat{\phi}$ you may require, show that

$$\#\left(\frac{\mathcal{G}}{2\mathcal{G}}\right) \leq \#\left(\frac{\mathcal{G}}{\widehat{\phi}(\mathcal{H})}\right) \#\left(\frac{\mathcal{H}}{\phi(\mathcal{G})}\right).$$

Find a set of coset representatives for $\mathcal{G}/\widehat{\phi}(\mathcal{H})$ and for $\mathcal{H}/\phi(\mathcal{G})$ when $\mathcal{C}$ is the curve $y^2 = x(x^2 + 5x + 3)$, and hence find the order of $\mathcal{G}/2\mathcal{G}$.