Elliptic Curves. Sheet 8.
(Some exam-style questions and the 2006,2007,2008 Exams).

The following exam-style questions and the 2006,2007,2008 Exams need not be handed in for classes; they are intended primarily to help you with your revision in Trinity Term (when I shall have consultation sessions, in case you have any questions during your Trinity Term revision). Of course, there are no guarantees about whether specific topics in the exam-style questions and the 2006,2007,2008 Exams will be asked in this year's exam. Note that the parts (i),(ii),... of a question may or may not be related to each other. Note that, in the 2006,2007,2008 Exams, two of the questions have portions that are 'bookwork' (reproducing proofs from lectures). It will also be true of this year's exam that two of the questions will include some bookwork. I bring to your attention the new 2008/09 Part C Examination Conventions (which have been posted at: www.maths.ox.ac.uk/notices/undergrad), in particular note the change this year to the number of questions available (described in 3.1 *Structure of Papers*). You will probably also find it helpful to have a calculator in the exam; please see the examination regulations for a description of the types of calculators allowed.

Elliptic Curves. Some Exam-style Questions.

Question 1.

(i) Find an $x \in \mathbb{Z}$ such that $|x^2+3|_7 < 7^{-1}$.

(ii) For what prime p does $-\frac{9}{8}$ have p-adic expansion $1, \overline{2} = 1 + 2p + 2p^2 + 2p^3 + \ldots$?

(iii) Let $p \equiv 1 \pmod 3$ be prime. Show that -3 is a quadratic residue mod p [*Hint: consider separately the cases* $p \equiv 1$ (*mod* 4) *and* $p \equiv 3$ (*mod* 4)]. Use Hensel's Lemma to deduce that -3 is a square in $\mathbb{Q}_p^*$.

(iv) Let $q \equiv 1 \pmod{27}$ be prime. Show that $(X^2+3)(X^3-q) = 0$ has solutions in $\mathbb{R}$ and every $\mathbb{Q}_p$.

Question 2.

(i) Find the torsion group over $\mathbb{Q}$ of the elliptic curve $Y^2 = X^3 + 3$.

(ii) Find the torsion group over $\mathbb{Q}$ of the elliptic curve $Y^2 = X^3 + 4X$.

(iii) Let $n \in \mathbb{Z}$ satisfy $n \neq 0, \pm 1$. Show that $\big(n, \pm n(n+1)\big)$, $\big(-n, \pm n(n-1)\big)$ are points of order 4 on the elliptic curve $Y^2 = X(X+1)(X+n^2)$. Find the torsion group over $\mathbb{Q}$ when $n \equiv 2$ (modulo 5).

(iv) Let $k \in \mathbb{Z}$, $k \neq 0$, let $\mathcal{E}$ be the elliptic curve $Y^2 = X^3 - k^2X + k^3$, and let (x, y) be a point of finite order in $\mathcal{E}(\mathbb{Q})$. Show that $|y| \leqslant 5|k|^3$ and $|x| \leqslant 3|k|^2$.

Question 3. Let $\mathcal{C} : Y^2 = X(X^2 + aX + b)$ and $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1)$, where $a, b \in \mathbb{Z}$ with $b(a^2 - 4b) \neq 0$ and $a_1 = -2a$, $b_1 = a^2 - 4b$. Let the map ϕ [which you may assume to be a homomorphism] be defined as usual by

$$\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto (\frac{y^2}{x^2}, y - \frac{by}{x^2}).$$

Let q be defined as usual by

$$q : \mathcal{D}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u \text{ when } u \neq 0,$$

$$q : (0, 0) \mapsto b_1, \quad q : \underline{\mathbf{o}} \mapsto 1,$$

where $\underline{\mathbf{o}}$ denotes the point at infinity on $\mathcal{D}$.

(i) Show that the image of q is a subset of the finite set

$$\{r : r \text{ is a square free integer and } r|b_1\}.$$

(ii) Find the rank of the elliptic curve $Y^2 = X(X^2 + 2X + 3)$.

Question 4. A four-letter word $L_1L_2L_3L_4$ has been divided into two pairs: L_1L_2 and L_3L_4. Each of these pairs has been converted into an integer (of at most 4 digits) via the standard map: $A \mapsto 01, B \mapsto 02, \ldots, Z \mapsto 26$. These integers have been encoded by taking each to the power of $d = 4451$, modulo $N = 10001$. The encoded message reads:

6847, 2577.

You may assume that N is the product of two primes.

(i) Factorise N by applying Pollard's "$p - 1$" method, using base 2 and exponent 68.

(ii) Use the factorisation of N to decode the message (which is the name of the animal used as the mascot for the sports teams at the University of California at Santa Cruz).

(iii) Let A be an Abelian group with group operation $+$, and let $h : A \longrightarrow \mathbb{R}$ satisfy:

(1) For any $Q \in A$, there exists $C_1 = C_1(Q)$ such that $h(P + Q) \leqslant 2h(P) + C_1$ for all $P \in A$.

(2) There exists C_2, independent of P, such that $h(2P) \geqslant 4h(P) - C_2$ for all $P \in A$.

(3) For any C_3, the set $\{P \in A : h(P) \leqslant C_3\}$ is finite.

Suppose also that $A/2A$ is finite. Prove that A is finitely generated.

(iv) Let A and h be as in (c). Suppose that P is a torsion element of A [that is: there exists an integer $N > 0$ such that NP is the identity element of A]. Show that $h(P) \leqslant \frac{1}{3}C_2$.

Elliptic Curves Questions from the 2006 Examination.

Question 1.

(i) Let K be a field, complete with respect to a non-Archimedean valuation $|\ |$, with valuation ring $R = \{x \in K : |x| \leqslant 1\}$. Prove Hensel's Lemma, that if $f(x) \in R[x]$ and $a_0 \in R$ satisfies $|f(a_0)| < |f'(a_0)|^2$, then there exists a unique $a \in R$ such that $f(a) = 0$ and $|a - a_0| \leqslant |f(a_0)|/|f'(a_0)|$.

(ii) For which primes p do there exist $x, y \in \mathbb{Z}_p$ such that $3y^2 = 4x^3 - 10$?

(iii) For prime $p \neq 2$, determine how many elements there are in the set $\mathbb{Q}_p^*/\left(\mathbb{Q}_p^*\right)^2$. Determine how many elements there are in the set $\mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2$.

Question 2. Let R be any ring (commutative, with 1), and let F, G be formal groups over R.

(i) Show that there exists a unique normalised invariant differential for F, which is given by $\omega = F_X(0,T)^{-1}\mathrm{d}T \in R[[T]]\mathrm{d}T$, and that every invariant differential for F is of the form $a\omega$ for some $a \in R$.

(ii) Let f be a homomorphism over R from F to G. Let ω_F, ω_G be the normalised invariant differentials on F, G, respectively. Show that $\omega_G \circ f = f'(0)\ \omega_F$. Deduce that, for any prime p, there exist $f, g \in R[[T]]$ such that $[p](T) = pf(T) + g(T^p)$ [where $[p]$ represents the multiplication-by-p map on F].

(iii) Let $m, n \in \mathbb{Z}$, with $n \neq 0$. Show that the curve $Y^2 = X^3 - (m^2+1)^2X + 9n^2$ has infinitely many $\mathbb{Q}$-rational points.

Question 3.

(i) Find a proper factor of $N = 1517$ by applying the Elliptic Curve Method, using the curve $Y^2 = X^3 + 7X - 7$ and $4P$, where $P = (1, 1)$.

(ii) Find the torsion group over $\mathbb{Q}$ of the elliptic curve $Y^2 = X^3 - 2X$.

(iii) Let $\mathcal{E}_k$ be the elliptic curve $Y^2 = X^3 + k$, where $k \in \mathbb{Q}$ and $k \neq 0$. Show that there is always a point of order 3 in $\mathcal{E}_k(\mathbb{C})$ which is not in $\mathcal{E}_k(\mathbb{Q})$.

Question 4.

(i) Find the rank of the elliptic curve $Y^2 = X(X^2 + 3X + 5)$.

(ii) For any prime $p \equiv 5 \pmod 8$, show that the elliptic curve $Y^2 = X^3 + p^2X$ has rank 0.

Elliptic Curves Questions from the 2007 Examination.

Question 1.

(i) Find an $x \in \mathbb{Z}$ such that $|x^2+2|_3 < 3^{-2}$. Show that there does not exist $x \in \mathbb{Z}$ such that $|x^2+3|_3 < 3^{-2}$.

(ii) Let $p \neq 2$ be prime. Find the p-adic expansion of $\frac{1+2p}{p-p^3}$.

(iii) Does there exist a prime p such that $p = p^p$ in $\mathbb{Q}_p^*/\big(\mathbb{Q}_p^*\big)^p$?

(iv) Let q, r be distinct primes, and let $\alpha, \beta \in \mathbb{Q}$. Show that there exists a sequence $x_n \in \mathbb{Q}$ such that $x_n \to \alpha$ with respect to $|\ \ |_q$, and $x_n \to \beta$ with respect to $|\ \ |_r$, as $n \to \infty$. Does there exist a sequence $y_n \in \mathbb{Q}^*$ such that $y_n \to 0$ with respect to $|\ \ |_p$ for all primes p, and $y_n \to 0$ with respect to $|\ \ |_\infty$, as $n \to \infty$?

Question 2.

(i) Let K be field, complete with respect to a discrete non-Archimedean valuation, $R = \{x \in K : |x| \leqslant 1\}$, $\mathcal{M} = \{x \in K : |x| < 1\}$, and assume that $R/\mathcal{M}$ is of characteristic p, for some prime p. Let $F(X,Y)$ be a formal group defined over R and suppose that $z \in \mathcal{M}$ has exact order p^n, for some $n \geqslant 1$, with respect to the group operation $x \oplus y = F(x,y)$ on $\mathcal{M}$. Show that:

$$|z| \geqslant |p|^{\frac{1}{p^n - p^{n-1}}}.$$

[You may assume the result that, for any prime p, the multiplication by p map $[p](T)$ can be written as $[p](T) = pf(T) + g(T^p)$, for some $f(T) = T + \ldots \in R[[T]]$ and $g(T) \in R[[T]]$.]

(ii) Let $\mathcal{E} : y^2 = x^3 + Ax + B$, be an elliptic curve, where $A, B \in \mathbb{Z}_p$, and let $\widetilde{\mathcal{E}}$ denote the reduction of $\mathcal{E}$ modulo p. Show that any $(x,y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ satisfies $|x|_p \leqslant 1, |y|_p \leqslant 1$.
When $\widetilde{\mathcal{E}}$ is non-singular, show that $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$.

(iii) Let $D \in \mathbb{Z}$, $D > 0$, $D \equiv 2 \pmod 3$. Describe the torsion group over $\mathbb{Q}$ of the elliptic curve $Y^2 = X^3 + DX$.

Question 3. Let $\mathcal{C} : Y^2 = X(X^2 + aX + b)$ and $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1)$, where $a, b \in \mathbb{Z}$ with $b(a^2 - 4b) \neq 0$ and $a_1 = -2a$, $b_1 = a^2 - 4b$. Let the map ϕ [which you may assume to be a homomorphism] be defined as usual by

$$\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x,y) \mapsto \Big(\frac{y^2}{x^2},\ y - \frac{by}{x^2}\Big) = \Big(\frac{x^2 + ax + b}{x},\ y - \frac{by}{x^2}\Big).$$

Let q be defined as usual by

$$q : \mathcal{D}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u,v) \mapsto u \text{ when } u \neq 0,$$

$$q : (0,0) \mapsto b_1,\ \ q : \underline{\mathbf{o}} \mapsto 1.$$

(i) Show that q is a homomorphism.
[You are only required to show that $q(P+Q) = q(P)q(Q)$ in the typical case when none of $P, Q, P+Q$ are $(0,0)$ or $\underline{\mathbf{o}}$.]

(ii) Show that q has kernel $\phi(\mathcal{C}(\mathbb{Q}))$.

(iii) Find the rank of the elliptic curve $Y^2 = X(X^2 + X - 2)$.

Question 4.

(i) Find a proper factor of $N = 10573$ by applying the Elliptic Curve Method, using the curve $Y^2 = X^3 - X - 5$ and $3P$, where $P = (2, 1)$.

(ii) For any elliptic curve $\mathcal{E}$ and
$(s,t) \in \mathcal{E}(\mathbb{Q})$ with $s, t \in \mathbb{Q}$ and $s = \frac{c}{d}$, $c, d \in \mathbb{Z}$, $\gcd(c,d) = 1$,
let the height function $h_x(s,t)$ be defined, as usual, by:

$$h_x\big((s,t)\big) = \log \max\big(|c|, |d|\big),$$

and define $h_x(\underline{\mathbf{o}}) = 0$.

Let $\mathcal{C}$, $\mathcal{D}, \phi$ be as defined in the previous question. Find a constant k, which depends only on a, b, such that $h_x\big(\phi(P)\big) \leqslant 2\big(h_x(P)\big) + k$, for all $P \in \mathcal{C}(\mathbb{Q})$. Find a constant ℓ, which depends only on a, b, such that $h_x\big(2P\big) \leqslant 4\big(h_x(P)\big) + \ell$, for all $P \in \mathcal{C}(\mathbb{Q})$.

(iii) Let $p \neq 2$ be prime, let $m \in \mathbb{F}_p^*$ and let $\mathcal{E}$ be the elliptic curve $Y^2 = X(X^2 + m^2)$, defined over $\mathbb{F}_p$. Show that $\#\mathcal{E}(\mathbb{F}_p)$ is always divisible by 4.
[You may wish to consider separately the cases $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.]

Elliptic Curves Questions from the 2008 Examination.

Question 1.

(i) Decide whether there exists $x \in \mathbb{Q}_p$ such that $x^3 = 5$ for each of: $p = 3, 5, 13$.

(ii) Find the 3-adic expansion of $-\frac{13}{8}$. For any prime p, and $a_0, a_1, a_2 \in \{0, \ldots, p-1\}$, express $a_0, \overline{a_1 a_2} = a_0 + a_1 p + a_2 p^2 + a_1 p^3 + a_2 p^4 + \ldots$ in the form m/n, where $m, n \in \mathbb{Z}$.

(iii) Let $\mathcal{E} : x^3 + y^3 = p$, defined over $\mathbb{Q}_p$, and let $\widetilde{\mathcal{E}} : x^3 + y^3 = 0$, defined over $\mathbb{F}_p$, be the reduction of $\mathcal{E}$ modulo p. Show that $(0,0)$ is a singular point on $\widetilde{\mathcal{E}}(\mathbb{F}_p)$ and that it does not lift to a point on $\mathcal{E}(\mathbb{Q}_p)$. Find a curve $\mathcal{D}$, nonsingular and defined over $\mathbb{Q}_p$, such that $\widetilde{\mathcal{D}} = \widetilde{\mathcal{E}}$ and such that $(0,0) \in \widetilde{\mathcal{D}}(\mathbb{F}_p)$ does lift to a point on $\mathcal{D}(\mathbb{Q}_p)$.

(iv) Let $p \neq 2$ be prime and let $a, b, c \in \mathbb{Z}_p$ satisfy $|a|_p = |b|_p = |c|_p = 1$. Show that there exist $x, y \in \mathbb{Z}_p$ such that $ax^2 + by^2 = c$.

[You might first wish to consider, for any $\alpha, \beta, \gamma \in \mathbb{F}_p \backslash \{0\}$, the sizes of the sets $\{\alpha x^2 : x \in \mathbb{F}_p\}$ and $\{\gamma - \beta y^2 : y \in \mathbb{F}_p\}$.]

Question 2.

(i) State and prove the Nagell-Lutz Theorem for $\mathbb{Q}$-rational torsion points on the elliptic curve $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. [You may assume the result that any $\mathbb{Q}$-rational torsion point (x, y) on such a curve satisfies $x, y \in \mathbb{Z}$. You may also use the polynomial identity: $\phi_1(X)\psi_1(X) + \phi_2(X)\psi_2(X) = 4A^3 + 27B^2$, where $\phi_1(X) = 3X^2 + 4A$, $\psi_1(X) = (3X^2 + A)^2$, $\phi_2(X) = -27(X^3 + AX - B)$ and $\psi_2(X) = X^3 + AX + B$.]

(ii) Find the torsion group over $\mathbb{Q}$ for the elliptic curve $y^2 = x^3 + x + 1$, and deduce that this curve has infinitely many rational points.

(iii) Let $D \in \mathbb{Z}$ satisfy $D \not\equiv 0 \pmod 5$ and $D \equiv 2 \pmod 7$. Suppose also that there exists a prime $p \equiv 1 \pmod 3$ such that D is not a quadratic residue mod p. Find the torsion group over $\mathbb{Q}$ for the elliptic curve $y^2 = x^3 + D$.

(iv) Let $\mathcal{E} : y^2 = x(x-1)(x-4)$. Show that $(2, 2i), (1 - i\sqrt{3}, 3 + i\sqrt{3}), (4 + 2\sqrt{3}, 6 + 4\sqrt{3})$ each have order 4 in $\mathcal{E}(\mathbb{C})$. Show that $\#\widetilde{\mathcal{E}}(\mathbb{F}_p)$ is divisible by 8, for all primes $p \neq 2, 3$. Show that the torsion group of $\mathcal{E}(\mathbb{Q})$ has order 4.

Question 3. Let $\mathcal{C} : Y^2 = X(X^2 + aX + b)$ and $\mathcal{D} : Y^2 = X(X^2 + a_1 X + b_1)$, where $a, b \in \mathbb{Z}$ with $b(a^2 - 4b) \neq 0$ and $a_1 = -2a$, $b_1 = a^2 - 4b$. Let the map ϕ [which you may assume to be a homomorphism] be defined as usual by

$$\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto \Big(\frac{y^2}{x^2},\ y - \frac{by}{x^2}\Big) = \Big(\frac{x^2 + ax + b}{x},\ y - \frac{by}{x^2}\Big).$$

Let q be defined as usual by

$$q : \mathcal{D}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u \text{ when } u \neq 0,$$

$$q : (0,0) \mapsto b_1, \quad q : \underline{\mathbf{o}} \mapsto 1.$$

(i) Show that the image of q is a subset of the finite set

$$\{r : r \text{ is a square free integer and } r | b_1\}.$$

(ii) Find the rank of the elliptic curve $Y^2 = X(X^2 + 3X - 3)$. [Standard results may be used without proof, provided they are accurately stated.]

Question 4.

(a) For any elliptic curve $\mathcal{E}$ and $(s,t) \in \mathcal{E}(\mathbb{Q})$ with $s, t \in \mathbb{Q}$ and $s = \frac{c}{d}$, $c, d \in \mathbb{Z}$, $\gcd(c,d) = 1$, let the height function $h_x(s,t)$ be defined, as usual, by:

$$h_x\big((s,t)\big) = \log \max\big(|c|, |d|\big),$$

and define $h_x(\underline{\mathbf{o}}) = 0$.

(i) Show that, for any $m \geqslant 1$, there is a constant C_m, independent of P, such that $|h_x(mP) - m^2 h_x(P)| \leqslant C_m$, for all $P \in \mathcal{E}(\mathbb{Q})$.

(ii) Show that, for any $P \in \mathcal{E}(\mathbb{Q})$, the sequence $4^{-n} h_x(2^n P)$ is Cauchy and therefore convergent in $\mathbb{R}$ as $n \to \infty$.

[You may use the result that there exists a constant C, independent of P, Q, such that $|h_x(P+Q) + h_x(P-Q) - 2h_x(P) - 2h_x(Q)| \leqslant C$, for all $P, Q \in \mathcal{E}(\mathbb{Q})$.]

(b) Let K be field, complete with respect to a discrete non-Archimedean valuation, $R = \{x \in K : |x| \leqslant 1\}$, $\mathcal{M} = \{x \in K : |x| < 1\}$, and assume that $R/\mathcal{M}$ is of characteristic p, for some prime p. Let $F(X,Y)$ be a formal group defined over R, and let $F(\mathcal{M})$ denote the set $\mathcal{M}$ together with the group operation: $x \oplus y = F(x,y)$. For any $m \geqslant 1$, let $[m](x)$ denote, as usual, $x \oplus \ldots \oplus x$ [m times]. Show that, for any $x \in \mathcal{M}$, the sequence $[p^n](x) \to 0$ as $n \to \infty$.

(c) Let $p \equiv 1 \pmod{12}$ and $q \equiv 5 \pmod{12}$ be primes. Show that there exists an elliptic curve of the form $y^2 = x^3 + ax - a$, with $a \in \mathbb{Z}$, for which the Elliptic Curve Method, using $3(1,1)$, successfully factorises $N = pq$.