SOLUTIONS TO THE ELLIPTIC CURVES QUESTIONS ON THE 2006 EXAMINATION.

Question 1.

(i) [*Proof from lectures*]. Define $f_j(x)$ by:

$f(x+y) = f_0(x) + f_1(x)y + f_2(x)y^2 + \dots,$

so that $f_0(x) = f(x), f_1(x) = f'(x)$. Define $b_0 = -f(a_0)/f'(a_0)$. By $(*)$, $|b_0| < 1$.

Define $a_1 = a_0 + b_0 = a_0 - f(a_0)/f'(a_0)$. Then:

$|f'(a_1) - f'(a_0)| = |f'(a_0 + b_0) - f'(a_0)| = |(\text{poly in } a_0)b_0 + (\text{poly in } a_0)b_0^2 + \dots|$

$\leqslant |b_0| < |f'(a_0)|$ (by $(*)$),

so that $|f'(a_1)| = |f'(a_0)|$.

Also, $|f(a_1)| = |f(a_0 + b_0)| = |f_0(a_0) + f_1(a_0)b_0 + f_2(a_0)b_0^2 + \dots|$

$= |f_2(a_0)b_0^2 + \dots|$ [since $f_0(a_0) + f_1(a_0)b_0 = 0$]

$\leqslant \max_{j\geqslant 2}|f_j(a_0)||b_0|^j \leqslant |b_0|^2 = \frac{|f(a_0)|^2}{|f'(a_0)|^2} = \rho|f(a_0)| < |f(a_0)|$, where $\rho = \frac{|f(a_0)|}{|f'(a_0)|^2} < 1$.

Summarising: $|f'(a_1)| = |f'(a_0)|$ and $|f(a_1)| \leqslant \rho|f(a_0)| < |f(a_0)|$, where $\rho = \frac{|f(a_0)|}{|f'(a_0)|^2} < 1$.

For all n, given $a_n \in R$, define $b_n = -f(a_n)/f'(a_n)$ and $a_{n+1} = a_n + b_n = a_n - f(a_n)/f'(a_n)$.

Assume, as induction hypothesis, that:

$|f'(a_n)| = \dots = |f'(a_1)| = |f'(a_0)|$ and $|f(a_n)| \leqslant \rho|f(a_{n-1})| \leqslant \dots \leqslant \rho^n|f(a_0)|$. (1)

Then, as above: $|f'(a_{n+1})| = \dots = |f'(a_1)| = |f'(a_0)|$.

Then $|f(a_{n+1})| \leqslant |b_n|^2$ [justified as for the case $n = 0$ above]

$= \frac{|f(a_n)|^2}{|f'(a_n)|^2} = \frac{|f(a_n)|^2}{|f'(a_0)|^2}$ [by (1), the induction hypothesis]

$\leqslant \frac{|f(a_0)|}{|f'(a_0)|^2}|f(a_n)|$ [since $|f(a_n)| \leqslant |f(a_0)|$ by (1), the induction hypothesis]

$= \rho|f(a_n)| \leqslant \rho^{n+1}|f(a_0)|$ [by (1), the induction hypothesis].

By induction, $\forall n$, $|f'(a_n)| = |f'(a_0)|$ and $|f(a_n)| \leqslant \rho^n|f(a_0)|$ which $\to 0$ as $n \to \infty$. (2)

Now, $|b_n| = |f(a_n)|/|f'(a_n)| = |f(a_n)|/|f'(a_0)| \to 0$, so [by the theorem from lectures that a series converges in a non-Archimedean field iff its terms converge to 0]:

$a_n = a_0 + b_0 + b_1 + \dots + b_n$ converges to a, say.

By continuity of polynomials, $f(a) = \lim f(a_n) = 0$ [by (2)]. Furthermore:

$|a - a_0| = |\sum b_n| \leqslant \max |b_n| = \max \frac{|f(a_n)|}{|f'(a_n)|} = \max \frac{|f(a_n)|}{|f'(a_0)|} = \frac{|f(a_0)|}{|f'(a_0)|}$ [by (2)], as required.

For uniqueness, imagine that $\hat{a} \neq a$ also satisfied $f(\hat{a}) = 0$ and $|\hat{a} - a_0| \leqslant |f(a_0)|/|f'(a_0)|$.

Let $\hat{b} = \hat{a} - a \neq 0$.

Then $0 = f(\hat{a}) - f(a) = f(a + \hat{b}) - f(a) = \hat{b}f_1(a) + \hat{b}^2 f_2(a) + \dots$ (3)

But $|\hat{b}| = |\hat{a} - a_0 + a_0 - a| \leqslant \max(|\hat{a} - a_0|, |a - a_0|) \leqslant |f(a_0)|/|f'(a_0)|$

$< |f'(a_0)$ [by $(*)$] $| = |f_1(a_0)| = |f_1(a)|$ [by (1) and continuity of $|f'(x)|$].

This gives $|\hat{b}^j f_j(a)| \leqslant |\hat{b}^j| \leqslant |\hat{b}^2| < |\hat{b} f_1(a)|$ (since $|\hat{b}| \neq 0$ & $|\hat{b}| < |f_1(a)|$) for $j \geqslant 2$, so that the leading term of the sum in (3) has valuation strictly greater than the valuations of the other terms, which is inconsistent with the sum being 0. Hence a is unique. **[10 marks]**

(ii) [*They have seen a variation on an exercise sheet, although this one is substantially harder*]. For $p = 2$, can see the equation becomes $-y^2 \equiv 2 \pmod 4$, which is impossible, since $y \equiv 0, 1, 2, 3$ give $y^2 \equiv 0, 1, 0, 1$, respectively. Hence, there are no such $x, y \in \mathbb{Z}_2$. For $p = 3$, take $x = 1$, in which case we want $y \in \mathbb{Z}_3$ such that $3y^2 = -6$, that is: $f(y) = y^2 + 2 = 0$. But $a_0 = 1$ gives $|f(a_0)|_3 = 3^{-1}$ and $|f'(a_0)| = 1$, so by Hensel's Lemma, there exists $y \in \mathbb{Z}_3$ which is a root of f. For $p = 5$, take $x = 2$, in which case we want $y \in \mathbb{Z}_5$ such that $g(y) = 3y^2 - 22 = 0$. But $a_0 = 2$ gives $|g(a_0)|_5 = 5^{-1}$ and $|g'(a_0)| = 1$, so by Hensel's Lemma, there exists $y \in \mathbb{Z}_5$ which is a root of g. For $p = 7$, take $y = 0$, in which case we want $x \in \mathbb{Z}_7$ such that $h(x) = (4x^3 - 10)/3 = 0$. But $a_0 = -1$ gives $|h(a_0)|_7 = 7^{-1}$ and $|h'(a_0)| = 1$, so by Hensel's Lemma, there exists $x \in \mathbb{Z}_7$ which is a root of h. For $p \geqslant 11$, the curve is an elliptic curve mod p [since the only bad primes are $2, 3, 5$] and $\#\widetilde{\mathcal{E}}(\mathbb{F}_p) \geqslant p+1-2\sqrt{p} > 5$. At most 4 of these are 2-torsion, so there exists x_0 such that $h(x_0)$ is a nonzero residue mod p; applying Hensel's Lemma to $y^2 - h(x_0)$ gives the existence of a corresponding $y \in \mathbb{Z}_p$. In summary, there exist such $x, y \in \mathbb{Z}_p$ for all p except 2.

Alternative method: Note that for $p \nmid 2 \cdot 3\Delta$ (that is: $p \neq 2, 3, 5$, so that $\widetilde{\mathcal{E}}$ is still an elliptic curve mod p) and $p \geqslant 5$, we have $\#\widetilde{\mathcal{E}}(\mathbb{F}_p) \geqslant p + 1 - 2\sqrt{p} > 1$, and so the number of affine points is > 0; these are non-singular, since $\widetilde{\mathcal{E}}$ is still an elliptic curve mod p. Also, by a theorem from lectures, any non-singular point on $\widetilde{\mathcal{E}}(\mathbb{F}_p)$ lifts to a point on $\mathcal{E}(\mathbb{Q}_p)$; also, any affine non-singular point on $\widetilde{\mathcal{E}}(\mathbb{F}_p)$ lifts to a point on $\mathcal{E}(\mathbb{Q}_p)$ with $x, y \in \mathbb{Z}_p$ (since otherwise (x, y) maps to the point at infinity under the reduction map mod p). This shows the existence of such $x, y \in \mathbb{Z}_p$ for all p except $p = 2, 3$ and bad primes, so only still need to consider $p = 2, 3, 5$. Also, note that for $p = 3$ there is the non-singular affine point $(1, 1)$ on $\widetilde{\mathcal{E}}(\mathbb{F}_3)$, and for $p = 5$ there is the non-singular affine point $(2, 2)$ on $\widetilde{\mathcal{E}}(\mathbb{F}_5)$, and as before these must lift to points $(x, y) \in \mathcal{E}(\mathbb{Q}_p)$, with $x, y \in \mathbb{Z}_p$. This only leaves $p = 2$; when the equation becomes $-y^2 \equiv 2 \pmod 4$, which is impossible, since $y \equiv 0, 1, 2, 3$ give $y^2 \equiv 0, 1, 0, 1$, respectively. Hence, there are no such $x, y \in \mathbb{Z}_2$ (but there are such $x, y \in \mathbb{Z}_p$ for all $p \neq 2$). **[7 marks]**

(iii) [*Unseen*]. We may apply the general rule from lectures (which follows easily from Hensel's Lemma) that, if $p \neq 2$ and $|\alpha|_p = 1$, then α is a square in $\mathbb{Q}_p^*$ iff α is a quadratic residue in $\mathcal{F}_p$. An element $\alpha \in (\mathbb{Q}_p^*)^2$ iff (both $|\alpha|_p = p^r$ for r even and the leading digit a_r of α is a quadratic residue mod p) [N.B. if $|\alpha|_p = p^r$ for r odd, then $\alpha \neq \beta^2$ for any β, since $|\beta|_p = p^s$ for some integer s]. Let $H_1 = (\mathbb{Q}_p^*)^2$, and fix a quadratic nonresidue mod 5, say γ. Let $H_2 = \gamma H_1$, $H_3 = pH_1$, $H_4 = \gamma p H_1$. Since any nonresidue $= \gamma$(residue) and vice versa, these give all the cases when (a_r is a residue and r is even) [H1], (a_r is a nonresidue and r is

even) [H2], (a_r is a residue and r is odd) [H3], (a_r is a nonresidue and r is odd) [H4], which partition $\mathbb{Q}_p^*$. Hence there are precisely 4 distinct elements in $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, when $p \neq 2$.

Similarly, 1,3,5,7 are all distinct in $(\mathbb{Q}_2{}^*)^2$, since for $|\alpha|_2 = 1$, Hensel's Lemma gives that $\alpha \in (\mathbb{Q}_2{}^*)^2$ iff $\alpha \equiv 1 \pmod 8$. Furthermore, any $\alpha \equiv 1$ is equal to prrecisely one of $1, 3, 5, 7$ in $\mathbb{Q}_2{}^*/(\mathbb{Q}_2{}^*)^2$. For any α, if $|\alpha|_2 = 2^r$ with r even, then $\alpha = \alpha \cdot 2^r = 1, 3, 5$ or 7 in $\mathbb{Q}_2{}^*/(\mathbb{Q}_2{}^*)^2$, since $|\alpha \cdot 2^r|_2 = 1$. If r is odd, then $\alpha/2 = 2^r\alpha = 1, 3, 5$ or 7 in $\mathbb{Q}_2{}^*/(\mathbb{Q}_2{}^*)^2$, and so $\alpha = 2, 6, 10$ or 14 in $\mathbb{Q}_2{}^*/(\mathbb{Q}_2{}^*)^2$. So, there are 8 elements when $p = 2$, represented, say, by $1, 3, 5, 7, 2, 6, 10, 14$ (generated by $3, 5, 2$). **[8 marks]**

Question 2. Let R be any ring, and let F, G be formal groups over R.
(i) [*Proof from lectures*]. Let $P(T) = F_X(0, T)^{-1}$, so that $\omega(T) = P(T)\mathrm{d}T$. Note that $F_X(0, T) = 1 + \ldots$ is invertible, so that $P(T)$ is indeed a member of $R[[T]]$. Furthermore, $P(0) = 1$, so that it is normalised.

We need to show that ω is an invariant differential; that is, $\omega \circ F(T, S) = \omega(T)$, which is equivalent to: $P\big(F(T, S)\big)F_X(T, S) = P(T)$ so, in our case, it is sufficient to show:

$$F_X\big(0, F(T, S)\big)^{-1} F_X(T, S) = F_X(0, T)^{-1},$$

which is true iff:

$$F_X\big(0, F(T, S)\big) = F_X(T, S)F_X(0, T).$$

But this last statement is immediate from differentiating $F\big(U, F(T, S)\big) = F\big(F(U, T), S\big)$ [associativity] with respect to U to get: $F_X\big(U, F(T, S)\big) = F_X\big(F(U, T), S\big)F_X(U, T)$ and setting $U = 0$. Hence ω is an invariant differential.

Suppose that $\hat{\omega} = Q(T)\mathrm{d}T \in R[[T]]\mathrm{d}T$ is also an invariant differential, so that $Q(T)$ satisfies $Q\big(F(T, S)\big)F_X(T, S) = Q(T)$. Substituting $T = 0$ gives $Q(S)F_X(0, S) = Q(0)$, so that $Q(S) = Q(0)F_X(0, S)^{-1}$. It follows that $\hat{\omega} = a\omega$, where $a = Q(0)$. **[9 marks]**
(ii) [*Proof from lectures*]. First, note that $\omega_G \circ f\big(F(T, S)\big) = \omega_G\big(G(f(T), f(S)\big) = \omega_G \circ f(T)$, so that $\omega_G \circ f$ is an inviariant differential on G. From part (a), it follows that $\omega_G \circ f = a\ \omega_F$, for some $a \in R$. Since ω_F, ω_G are normalised, $(1 + \ldots)\mathrm{d}f(T) = a(1 + \ldots)\mathrm{d}T$, and so $(1 + \ldots)f'(T)\mathrm{d}T = a(1 + \ldots)\mathrm{d}T$; equating constant terms gives $a = f'(0)$, as required.

Let ω be the normalised invariant differential on F. Since $[p](T) = pT + \ldots$, it satisfies $[p]'(0) = p$. Applying the previous result to $[p]$, a homomorphism from F to itself, gives: $\omega \circ [p] = [p]'(0)\omega = p\omega$, and so

$$p\omega(T) = \omega \circ [p](T) = (1 + \ldots)\mathrm{d}([p](T)) = (1 + \ldots)[p]'(T)\mathrm{d}T.$$

Hence $[p]'(T) \in p\, R_T$. Each term a_nT^n in $[p](T)$ must then satisfy $p|na_n$ and so $p|n$ or $p|a_n$, as required. **[8 marks]**
(iii) [*Unseen*]. Let $\mathcal{E}$ be the given curve, which is of the form $Y^2 = X^3 - M^2X + N^2$, where $M = m^2+1$ and $N = 3n$. First note that for $m \equiv 0, 1, 2 \pmod 3$, $M \equiv 1, 2, 2 \pmod 3$, so that M is never divisible by 3. Hence $\Delta = 4(-M^2)^3+27(N^2)^2 = -4M^6+27N^4$ is never 0,

and so the curve is non-singular and is an elliptic curve. It has the obvious point $(0, N)$. Let $P = 2(0, N) \in \mathcal{E}(\mathbb{Q})$. The tangent to $\mathcal{E}$ at $(0, N)$ has slope $(3 \cdot 0^2 - M^2)/(2 \cdot N) = -M^2/2N$, and so the x-coordinate of $P = 2(0, N)$ is $\left(-M^2/2N\right)^2 - 2 \cdot 0$, which is not an integer, since the numerator is not divisible by 3, but the denominator $N = 3n$ is divisible by 3. Therefore P is not a torsion point (using the result from lectures that any torsion point in $\mathcal{E}(\mathbb{Q})$ must have both coordinates in $\mathbb{Z}$), and so must be of infinite order, giving that $\mathcal{E}(\mathbb{Q})$ is infinite, as required. **[8 marks]**

Question 3.

(i) [*Seen similar on an exercise sheet*]. The line tangent to $\mathcal{E}$ at $P = (1, 1)$ has slope y' given by $2yy' = 3x^2 + 7$, with $x = 1, y = 1$; that is, the slope is $10/2 = 5$. This tangent line also goes through $(1, 1)$ and so has equation: $Y = 5X - 4$. The x-coordinate of $2P$ is therefore $5^2 - (1 + 1) = 23$, and the y-coordinate is: $-(5 \cdot 23 - 4) = -111 \equiv 1406$, so that $Q = 2P \equiv (23, 1406)$ (modulo $N = 1517$). We now wish to compute $4P = 2Q = 2(23, 1406)$, and so the first step is to find the line tangent to $\mathcal{E}$ at Q. This has slope y' given by $2yy' = 3x^2 + 7$, with $x = 23, y = 1406$, that is, $y' = 1594/2812$. In order to compute this modulo $N = 1517$, we must first find the inverse of 2812 modulo 1517. Using Euclid's Algirithm: $2812 = 1 \cdot 1517 + 1295$, $1517 = 1 \cdot 1295 + 222$, $1295 = 5 \cdot 222 + 185$, $222 = 1 \cdot 185 + 37$, $185 = 5 \cdot 37 + 0$. So, we cannot find the inverse of 2812 (modulo $N = 1517$), and this step has given us a proper factor 37 of N. **[8 marks]**

(ii) [*Seen similar on an exercise sheet*]. The elliptic curve has $\Delta = 4A^3 + 27B^2 = 4 \cdot (-2)^3 + 27 \cdot 0^2 = -32$, and so has good reduction at all primes p except $p = 2$. Taking $p = 3$, we find that $\mathcal{E}(\mathbb{F}_3) = \{\underline{\mathbf{o}}, (0, 0), (2, 1), (2, 2)\}$, and since $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{E}(\mathbb{F}_3)$, this gives that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid 4$. Taking $p = 5$, we find that $\mathcal{E}(\mathbb{F}_5) = \{\underline{\mathbf{o}}, (0, 0), (1, 2), (1, 3), (2, 2), (2, 3), (3, 1), (3, 4), (4, 1), (4, 4)\}$, and since $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{E}(\mathbb{F}_5)$, this gives that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid 10$. Hence, $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \gcd(4, 10) = 2$. However, there are the obvious torsion points: $\underline{\mathbf{o}}$ and $(0, 0)$ and so $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\underline{\mathbf{o}}, (0, 0)\}$. **[7 marks]**

(iii) [*Unseen*]. Using $2YY' = 3X^2$, we see that the slope of the curve at any (x, y) is $3x^2/(2y)$, and so the tangent to the curve at (x, y) is the line: $Y = \left(\frac{3x^2}{2y}\right)X + c$, for some c. The x-coordinate of the third point of intersection is then: $\left(\frac{3x^2}{2y}\right)^2 - x - x = \frac{9x^4 - 8xy^2}{4y^2} = \frac{9x^4 - 8x(x^3+k)}{4(x^3+k)} = \frac{x(x^3-8k)}{4(x^3+k)}$. Furthermore $3(x, y) = \mathbf{o} \iff 2(x, y) = -(x, y) = (x, -y) \iff \left(\frac{x(x^3-8k)}{4(x^3+k)}, ?\right) = (x, -y) \iff \frac{x(x^3-8k)}{4(x^3+k)} = x$ [the $\Rightarrow$ of the last step is trivial; for $\Leftarrow$, note that if $2(x, y)$ has that same x-coordinate as (x, y) then $2(x, y) = (x, -y)$ or (x, y); but the latter would imply $(x, y) = \mathbf{o}$, which we have excluded]. Note further that this last condition on x is satisfied when $x(x^3 - 8k) = 4x(x^3 + k)$, that is: $x(x^3 + 4k) = 0$. This gives on $\mathcal{E}_k(\mathbb{C})$ the points $(0, \sqrt{k})$ and $(-\sqrt[3]{4k}, i\sqrt{3k})$. But it is impossible for both $\sqrt{k}$ and $i\sqrt{3k}$ to be in $\mathbb{Q}$

(indeed they cannot both be in $\mathbb{R}$), so that at least one of these points of order 3 is not in $\mathcal{E}_k(\mathbb{Q})$. **[10 marks]**

Question 4.

(i) [*Seen similar on an Exercise Sheet*]. Let $\mathcal{C} : Y^2 = X(X^2+aX+b) = X(X^2+3X+5)$, where $a = 3, b = 5$, and isogenous curve $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1) = X(X^2 - 6X - 11)$, where $a_1 = -2a = -6, b_1 = a^2 - 4b = -11$, with the usual isogeny $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto (y^2/x^2, y - 5y/x^2)$, and dual isogeny $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) : (u, v) \mapsto (\frac{1}{4}v^2/u^2, \frac{1}{8}(v + 11v/u^2))$.

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u$, for $(u, v) \neq (0, 0)$, with $q : (0, 0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, is an injection with im$q$ contained in $\{d : d \text{ is square free and } d|b_1\} = \{\pm1, \pm11\}$. Also, $\mathbf{o} \mapsto 1$, $(0, 0) \mapsto -11$ and the obvious point $(-1, 2) \mapsto -1$, so that $1, -11, -1 \in$ im$q$; but im$q$ is a group, so $11 \in$ im$q$ also, and indeed we can just take: $(0, 0)+(-1, 2) = (11, 22)$, which maps to 11 under q. Hence, $\{\pm1, \pm11\} \subset$ im$q \subset \{\pm1, \pm11\}$, that is im$q = \{\pm1, \pm11\}$, and so $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\mathbf{o}, (0, 0), (-1, 2), (11, 22)\}$, that is, $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ is generated by $(0, 0), (-1, 2)$.

The map $\hat{q} : \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u$, for $(u, v) \neq (0, 0)$, with $\hat{q} : (0, 0) \mapsto a_1^2 - 4b_1 = b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with im$\hat{q}$ contained in $\{d : d \text{ is square free and } d|b\} = \{\pm1, \pm5\}$. Also, $\mathbf{o} \mapsto 1$ and $(0, 0) \mapsto 5$, so that $\{1, 5\} \subset$ im$\hat{q} \subset \{\pm1, \pm5\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in$ im$\hat{q}$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a\ell^2m^2 + (b/(-1)) \cdot m^4 = n^2$; that is: $-\ell^4 + 3\ell^2m^2 - 5m^4 = n^2$. Multiply both sides by 4 and rewrite as: $-(2\ell^2 - 3m^2)^2 - 11m^4 = 4n^2$. We can see that the LHS is $\leqslant 0$ and the RHS is $\geqslant 0$, and the equation is satisfied iff $(2\ell^2 - 3m^2) = 11m^4 = 4n^2 = 0$. From this we see that $m = n = 0$, which when combined with $2\ell^2 - 3m^2 = 0$ gives that $\ell = 0$, also, which is a contradiction. Hence $-1 \notin$ im$\hat{q}$.

We conclude that im$\hat{q} = \{1, 5\}$, and so $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ is generated by $(0, 0)$.

Finally, since multiplication by 2 in $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi}\circ\phi$, we have that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $(0, 0)$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0, 0)\big) = \mathbf{o}$ and $\hat{\phi}\big((-1, 2)\big) = (1, 3)$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0, 0)$ and $(1, 3)$ and so is the group $C_2 \times C_2$. Now $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q}) \times C_2^{rank}$, and $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q})$ is isomorphic to the 2-torsion group of $\mathcal{C}_{\text{tors}}(\mathbb{Q})$ which is C_2 (consisting only of $\mathbf{o}$ and $(0, 0)$), so that $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q})$ is isomorphic to C_2. Conclusion: rank = 1. **[13 marks]**

(ii) [*Unseen*]. Let $\mathcal{C} : Y^2 = X(X^2+aX+b) = X(X^2+p^2)$, where $a = 0, b = p^2$, and isogenous curve $\mathcal{D} : Y^2 = X(X^2+a_1X+b_1) = X(X^2-4p^2)$, where $a_1 = -2a = 0, b_1 = a^2-4b = -4p^2$, with the usual isogeny $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto (y^2/x^2, y - p^2y/x^2)$, and dual isogeny $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) : (u, v) \mapsto (\frac{1}{4}v^2/u^2, \frac{1}{8}(v + 4p^2v/u^2))$.

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u$, for $(u, v) \neq (0, 0)$, with $q : (0, 0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, is an injection with im$q$ contained in $\{d : d \text{ is square free and } d|b_1\} =$

$\{\pm 1, \pm 2, \pm p, \pm 2p\}$. Also, $\mathbf{o} \mapsto 1$, $(0,0) \mapsto -1$, $(2p,0) \mapsto 2p$, $(-2p,0) \mapsto -2p$, so that $\{\pm 1, \pm 2p\} \subset \mathrm{im}q \subset \{\pm 1, \pm 2, \pm p, \pm 2p\}$. There is only one coset to check, represented by -2, say. We know that $-2 \in \mathrm{im}q$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-2) \cdot \ell^4 + a_1 \ell^2 m^2 + (b_1/(-2)) \cdot m^4 = n^2$; that is: $-2\ell^4 + 2p^2 m^4 = n^2$. Since $p \equiv 5 \pmod 8$, $\left(\frac{-2}{p}\right) = -1$, and so $p|\ell$, $p|n$. Let $\ell = p\ell'$, $n = pn'$. Then $-2p^2(\ell')^4 + 2m^4 = (n')^2$. Since also $\left(\frac{2}{p}\right) = -1$, this implies $p|m$, $p|n'$. This gives a contradiction, since $p|\ell, p|m$ and $\gcd(\ell, m) = 1$. Hence $-2 \notin \mathrm{im}q$, giving that $\mathrm{im}q = \{\pm 1, \pm 2p\}$, and $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\underline{\mathbf{o}}, (0,0), (2p,0), (-2p,0)\}$.

The map $\hat{q} : \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u,v) \mapsto u$, for $(u,v) \neq (0,0)$, with $\hat{q} : (0,0) \mapsto a_1^2 - 4b_1 = b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with $\mathrm{im}\hat{q}$ contained in $\{d : d \text{ is square free and } d|b\}$ $= \{\pm 1, \pm p\}$. Also, $\mathbf{o} \mapsto 1$ and $(0,0) \mapsto p^2 = 1$, so that $\{1\} \subset \mathrm{im}\hat{q} \subset \{\pm 1, \pm p\}$.

We know that $-1 \in \mathrm{im}\hat{q}$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a\ell^2 m^2 + (b/(-1)) \cdot m^4 = n^2$; that is: $-\ell^4 - p^2 m^4 = n^2$, clearly impossible in $\mathbb{R}$. Hence $-1 \notin \mathrm{im}\hat{q}$. Similarly, $-p \notin \mathrm{im}\hat{q}$. We know that $p \in \mathrm{im}\hat{q}$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $p \cdot \ell^4 + a\ell^2 m^2 + (b/p) \cdot m^4 = n^2$; that is: $p\ell^4 + pm^4 = n^2$, and so $p|n$. Letting $n = pn'$, the equation becomes $\ell^4 + m^4 = p^2(n')^2$, which in turn implies $p|\ell, p|m$, since $-1 \not\equiv a^4$ for any a [as can be seen by taking both sides of $-1 \equiv a^4$ to the power of $(p-1)/4$]. This again contradicts $\gcd(\ell, m) = 1$, and so $p \notin \hat{q}$.

We conclude that $\mathrm{im}\hat{q} = \{1\}$, and so $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \{\underline{\mathbf{o}}\}$.

Finally, since multiplication by 2 in $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi} \circ \phi$, we have that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $\underline{\mathbf{o}}$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0,0)\big) = \mathbf{o}$, and $\hat{\phi}\big((2p,0)\big) = (0,0)$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0,0)$, and so is the group C_2. Now $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})/2\mathcal{C}_{\mathrm{tors}}(\mathbb{Q}) \times C_2^{rank}$, and $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})/2\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})$ is isomorphic to the 2-torsion group of $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})$ which is C_2 (consisting only of $\mathbf{o}$ and $(0,0)$), so that $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})/2\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})$ is isomorphic to C_2. Conclusion: rank $= 0$. **[12 marks]**

General Comment: In the above solutions, I have given everything in full pedantic detail, in order to make every step as clear as possible to a non-specialist. Students could gain full marks from intelligently shortened versions of the above answers.