SOLUTIONS TO THE ELLIPTIC CURVES QUESTIONS ON THE 2008 EXAMINATION.

Question 1.

(i) [*Seen similar on problem sheet*]. Suppose $x^3 = 5$ for some $x \in \mathbb{Q}_3$. Then $|x|_3^3 = |x^3|_3 = |5|_3 = 1$, so that $|x|_3 = 1$, and so x must have 3-adic expansion of the form $x = a_0, a_1a_2 \ldots = a_0 + a_1 3^1 + \ldots$, which means that $(a_0 + a_1 3^1 + \ldots)^3 = 5$ would give a solution $a_0 + a_1 3^1$ to the congruence $x^3 \equiv 5 \pmod{3^2}$. However, $0^3, 1^3, 2^3, 3^3, 4^3, 5^3, 6^3, 7^3, 8^3 \equiv 0, 1, 8, 0, 1, 8, 0, 1, 8 \pmod{3^2}$, respectively, so that there does not exist x with $x^3 \equiv 5 \pmod{3^2}$. Hence, there does not exist $x \in \mathbb{Q}_3$ such that $x^3 = 5$.

Suppose $x^3 = 5$ for some $x \in \mathbb{Q}_5$. Then $|x|_5^3 = |x^3|_5 = |5|_5 = 5^{-1}$, so that $|x|_5 = 5^{-1/3}$, which is impossible, since any $x \in \mathbb{Q}_5$ has $|x|_5 = 5^r$ for some $r \in \mathbb{Z}$. Hence, there does not exist $x \in \mathbb{Q}_5$ such that $x^3 = 5$.

Let $t_0 = -2$ and let $f(x) = x^3 - 5$. Then $|f(t_0)|_{13} = |(-2)^3 - 5|_{13} = |-13|_{13} = 13^{-1}$ and $|f'(t_0)|_{13} = |2t_0|_{13} = |4|_{13} = 1$, so that $|f(t_0)|_{13} < |f(t_0)|_{13}^2$. By Hensel's Lemma, there exists $a \in \mathbb{Z}_p \subset \mathbb{Q}_p$ such that $f(a) = 0$. Hence, there does exist $x \in \mathbb{Q}_{13}$ (namely: $x = a$) such that $x^3 = 5$. **[7 marks]**

(ii) [*Unseen*]. First note that $|-\frac{13}{8}|_3 = 1$, so that $-\frac{13}{8} = a_0, a_1a_2 \ldots = a_0 + a_1 3^1 + a_2 3^2 + \ldots$ and so: $-13 = 8(a_0 + a_1 3^1 + a_2 3^2 + \ldots)$. Then: $-13 \equiv 8a_0 \pmod 3$, so that $a_0 = 1$. It follows that: $-13 \equiv 8(1 + a_1 3^1) \pmod{3^2}$ and so: $-7 \equiv 8a_1 \pmod 3$, giving $a_1 = 1$. Then: $-13 \equiv 8(1 + 1 \cdot 3^1 + a_2 3^2) \pmod{3^3}$, and so: $-5 \equiv 8a_2 \pmod 3$, giving $a_2 = 2$. Similarly, $a_3 = 1, a_4 = 2$. One suspects that $-\frac{13}{8} = 1, \overline{12}$, so let $\alpha = 1, \overline{12}$ and let $\beta = \alpha - 1 = 0, \overline{12} = 3^1 + 2 \cdot 3^2 + 3^3 + 2 \cdot 3^4 + \ldots$. Then $(\beta - 3^1 - 2 \cdot 3^2)/3^2 = \beta$, giving: $\beta = -\frac{21}{8}$ and so $\alpha = \beta + 1 = -\frac{13}{8}$, as required.

Now, let $\alpha = a_0, \overline{a_1a_2} = a_0 + a_1p + a_2p^2 + a_1p^3 + a_2p^4 + \ldots$, and $\beta = \alpha - a_0 = 0, \overline{a_1a_2} = a_1p + a_2p^2 + a_1p^3 + a_2p^4 + \ldots$. Then $(\beta - a_1p - a_2p^2)/p^2 = \beta$, so that $\beta = (-a_1p - a_2p^2)/(p^2 - 1)$ and $\alpha = \beta + a_0 = (p^2a_0 - a_0 - a_1p - a_2p^2)/(p^2 - 1)$. **[6 marks]**

(iii) [*Unseen*]. First note that $x = 0, y = 0$ satisfies $f(x, y) = x^3 + y^3 = 0$, $(\partial f/\partial x)(x, y) = 3x^2 = 0$ and $(\partial f/\partial x)(x, y) = 3y^2 = 0$, so that $(0, 0)$ is a singular point on $\widetilde{\mathcal{E}}(\mathbb{F}_p)$. Suppose that (x, y) on $\mathcal{E}$ reduces mod p to $(0, 0)$ on $\widetilde{\mathcal{E}}(\mathbb{F}_p)$. Then $|x|_p, |y|_p < 1$, indeed $|x|_p, |y|_p \leqslant p^{-1}$ (since any p-adic value is one of: $\ldots ..., p^{-2}, p^{-1}, 1, p^1, p^2, \ldots$, so that if a p-adic value is < 1 then it must be $\leqslant p^{-1}$), so that $|x|_p^3 \leqslant p^{-3}$. But $|p|_p = p^{-1}$ and so $|x|_p^3 \neq |p|_p$ which means that $|p - x^3|_p = \max(|x|_p, |p|_p) = p^{-1}$. Since x, y satisfy $y^3 = p - x^3$, we must therefore have:

$|y|_p^3 = p^{-1}$, which contradicts the fact that $|y|_p^3 = p^{3r}$ for some integer r. Hence, $(0,0)$ does not lift to a point on $\mathcal{E}(\mathbb{Q}_p)$. Letting $\mathcal{D} : x^3 + y^3 = p^3$, we see that $\widetilde{\mathcal{D}} = \widetilde{\mathcal{E}}$ and $(0,0) \in \widetilde{\mathcal{D}}(\mathbb{F}_p)$ does lift to the point $(0,p)$ on $\mathcal{D}(\mathbb{Q}_p)$. **[6 marks]**

(iv) [*Unseen*]. Let $\alpha, \beta, \gamma \in \mathbb{F}_p \backslash \{0\}$ be the reductions mod p of a, b, c, respectively. The map $x \mapsto x^2$ on F_p takes $0 \mapsto 0$, and is a 2-to-1 map on $\mathcal{F}_p \backslash \{0\}$. It follows that the both of the sets $\{\alpha x^2 : x \in \mathbb{F}_p\}$ and $\{\gamma - \beta y^2 : y \in \mathbb{F}_p\}$ have size $(p-1)/2 + 1 = (p+1)/2$. Since $\mathcal{F}_p$ has only p elements, and the sum of the sizes of the given sets is $p+1$, there must be an element common to both sets. That is, there must exist $x_0, y_0 \in \mathcal{F}_p$ such that $\alpha x_0^2 = \gamma - \beta y_0^2$, and so $\alpha x_0^2 + \beta y_0^2 = \gamma$. Since $\alpha, \beta, \gamma \neq 0$, at least one of x_0, y_0 is nonzero; say that $x_0 \neq 0$. Let $y \in \mathbb{Z}$ be any choice of $y \equiv y_0$ modulo p. Then $c - by^2 \in \mathbb{Z}$, satisfies $|c - by^2|_p = 1$ and there exists an x_0 such that $|ax_0^2 - (c - by^2)|_p < 1$. Applying Hensel's Lemma to the polynomial $F(T) = aT^2 - (c - by^2)$ gives that there must exist an $x \in \mathbb{Z}_p$ such that $F(x) = 0$, that is: $ax^2 + by^2 = x$, as required. **[6 marks]**

Question 2.

(i) [*Proof from lectures*]. The Nagell-Lutz Theorem states that, if (x, y) is a $\mathbb{Q}$-rational torsion point on $\mathcal{E} : Y^2 = X^3 + AX + B$, where $A, B \in \mathbb{Z}$, then $x, y \in \mathbb{Z}$ and $y = 0$ or $y^2 | \Delta$, where $\Delta = 4A^3 + 27B^2$.

Proof. We are given the result that $x, y \in \mathbb{Z}$. If $y = 0$ then the result is satisfied; otherwise, (x, y) is not 2-torsion and we consider $(x_2, y_2) = 2(x, y)$, with $(x_2, y_2) \neq \mathbf{o}$, and so $x_2, y_2 \in \mathbb{Q}$. But (x_2, y_2) is also a torsion point, so $x_2, y_2 \in \mathbb{Z}$. Now, the line tangent to $\mathcal{E}$ at (x, y) has slope $(3x^2 + A)/(2y)$, from which we immediately get: $x_2 = \big((3x^2 + A)/(2y)\big)^2 - 2x$. Now, we know $x_2, x \in \mathbb{Z}$ and so $\big((3x^2 + A)/(2y)\big)^2 \in \mathbb{Z}$. It follows that $4y^2 | (3x^2 + A)^2$ and so $y^2 | (3x^2 + A)^2 = \psi_1(x)$. Also, $y^2 = x^3 + Ax + B = \psi_2(x)$. Using the identity given on the exam paper, $y^2 | (\phi_1(x)\psi_1(x) + \phi_2(x)\psi_2(x)) = \Delta$, as required. **[9 marks]**

(ii) [*Seen similar on a problem sheet*]. Let $\mathcal{E} : y^2 = x^3 + x + 1$. Here, $A = B = 1$, so that $2\Delta = 2(4A^3 + 27B^2) = 2 \cdot 31$, and so $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$ for any $p \neq 2, 31$. Letting $p = 3$, we have: $\widetilde{\mathcal{E}}(\mathbb{F}_3) = \{\mathbf{o}, (0,1), (0,2), (1,0)\}$, so that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) | \#\widetilde{\mathcal{E}}(\mathbb{F}_3) = 4$. Letting $p = 5$, we have: $\widetilde{\mathcal{E}}(\mathbb{F}_5) = \{\mathbf{o}, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}$, so that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) | \#\widetilde{\mathcal{E}}(\mathbb{F}_5) = 9$. Since $\gcd(9,5) = 1$, it follows that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) = 1$ with $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\mathbf{o}\}$ [Alternatively, can apply Nagell-Lutz]. Hence the point $(0,1) \in \mathcal{E}(\mathbb{Q})$ is non-torsion, so that $\mathcal{E}(\mathbb{Q})$ is infinite. **[5 marks]**

(iii) [*Unseen*]. Let $\mathcal{E} : y^2 = x^3 + D$. Here $2\Delta = 2 \cdot 27 \cdot D^2$, and we are given that $D \not\equiv 0$ modulo each of $5, 7, p$, and so $\#\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is a factor of $\#\widetilde{\mathcal{E}}(\mathbb{F}_5), \#\widetilde{\mathcal{E}}(\mathbb{F}_7), \#\widetilde{\mathcal{E}}(\mathbb{F}_p)$ where the prime $p \equiv 1 \pmod{p}$. First note the map $x \mapsto x^3$ is an injection on $\mathbb{F}_5$ [since $0^3, 1^3, 2^3, 3^3, 4^3 \equiv 0, 1, 3, 2, 4 \pmod 5$]. Letting $y = 0, \ldots, 4$, for each such y there is then a unique $x \in \mathbb{F}_5$ such that $x^3 = y^2 - D$. It follows that there are 5 affine points in $\widetilde{\mathcal{E}}(\mathbb{F}_5)$ which, together with $\mathbf{o}$, gives $\#\widetilde{\mathcal{E}}(\mathbb{F}_5) = 6$. Hence $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) | 6$. Also mod 7, we see that $\widetilde{\mathcal{E}} : y^2 = x^3 + 2$, since we are given

that $D \equiv 2 \pmod 7$, and so: $\widetilde{\mathcal{E}}(\mathbb{F}_7) = \{\mathbf{o}, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$, giving: $\#\widetilde{\mathcal{E}}(\mathbb{F}_7) = 9$. Hence: $\#\mathcal{E}_{\text{tors}}(\mathbb{Q})|9$, which we can combine with $\#\mathcal{E}_{\text{tors}}(\mathbb{Q})|6$ to obtain $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) = 1$ or 3. Finally, mod p, note that $x \to x^3$ is a 3-to-1 map on $\mathbb{F}_p^*$ (since $p \equiv 1 \pmod p$) and there is no point on $\widetilde{\mathcal{E}} \pmod p$ with $x = 0$ (since D is not a quadratic residue mod p), so that the number of affine points on $\widetilde{\mathcal{E}}(\mathbb{F}_p)$ is divisible by 3. After including $\mathbf{o}$, we see that $\#\widetilde{\mathcal{E}}(\mathbb{F}_p)$ is not divisible by 3; since also $\#\mathcal{E}_{\text{tors}}(\mathbb{Q})|\#\widetilde{\mathcal{E}}(\mathbb{F}_p)$, we now know that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) = 1$, with $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\mathbf{o}\}$. **[5 marks]**

(iv) [*Unseen*]. The line tangent to $\mathcal{E}$ at $(x,y) = (2,2i)$ has slope $\lambda = (3x^2 - 10x + 4)/(2y) = i$, so the x-coordinate of the third point of intersection is $\lambda^2 + 5 - 2x = 0$, so that $2(2,2i) = (0,0)$, which has order 2, so that $(2,2i)$ has order 4. Similarly, $2(1 - i\sqrt{3}, 3 + i\sqrt{3}) = (1,0)$ and $2(4 + 2\sqrt{3}, 6 + 4\sqrt{3}) = (4,0)$ also have order 4 (or can use 2-isogenies between $\mathcal{E}$ and $y^2 = x(x^2 + 10x + 9)$. Note that the roots of the cubic $x(x-1)(x-4)$ are distinct mod 5, so that 5 is a prime of good reduction. Now, $\widetilde{\mathcal{E}}(\mathbb{F}_5) = \{\mathbf{o}, (1,0), (2,1), (2,4), (3,2), (3,3), (4,0)\}$, so that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q})|8$. But $\{\mathbf{o}, (0,0), (1,0), (4,0)\} \leq \mathcal{E}_{\text{tors}}(\mathbb{Q})$ so that $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = 4$ or 8. There cannot be any further points of order 2 in $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ since these are of the form $(x,0)$. If $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = 8$ there would have to exist a point $(x_0, y_0) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$ of order 4. But then (x_0, y_0), $(x_0, y_0) + (0,0)$, $(x_0, y_0) + (1,0)$ and $(x_0, y_0) + (4,0)$ would give 4 distinct points of order 4 in $\mathcal{E}_{\text{tors}}(\mathbb{Q})$, and the given $(2,2i), (1 - i\sqrt{3}, 3 + i\sqrt{3}), (4 + 2\sqrt{3}, 6 + 4\sqrt{3})$, with their conjugates and negatives, would give a further 10 points of order 4 in $\mathcal{E}_{\text{tors}}(\mathbb{C})$, giving a total of at least 14 distint points of order 4 in $\mathcal{E}_{\text{tors}}(\mathbb{C})$. However, this is impossible, since multiplication-by-2 is a 4-to-1 map and so there can be at most 12 points of order 4 (the preimages of the 3 points of order 2). Hence there are no points of order 4 in $\mathcal{E}_{\text{tors}}(\mathbb{Q})$, so that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) = 4$ [alternatively, can use Nagell-Lutz to show that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) = 4$]. Finally, note for any prime $p \neq 2, 3$, $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$, so that at least one of $-3, -1, 3$ is a quadratic residue mod p. So, at least one of the points $(2,2i), (1 - i\sqrt{3}, 3 + i\sqrt{3}), (4 + 2\sqrt{3}, 6 + 4\sqrt{3})$ of order 4 is in $\widetilde{\mathcal{E}}(\mathbb{F}_p)$, as well as $\mathbf{o}, (0,0), (1,0), (4,0)$, so that $\widetilde{\mathcal{E}}(\mathbb{F}_p) \geq 8$, as required. **[6 marks]**

Question 3.

(i) [*Proof from lectures*]. Let $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2, r \in \operatorname{im} q, r \in \mathbb{Z}, r$ square free. We want to prove that $r|b_1$. Suppose $r = q(u,v)$, where $(u,v) \in \mathcal{D}(\mathbb{Q})$, which must exist since $r \in \operatorname{im} q$. Then: $r = q(u,v) = u = u^2 + a_1u + b_1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ [since $u(u^2 + a_1u + b_1) = v^2$]. So, $r, u, u^2 + a_1u + b_1$ are all the same modulo squares, which means we can write:

$$u^2 + a_1u + b_1 = rs^2, \quad u = rt^2, \quad \text{for some } s, t \in \mathbb{Q}.$$

Hence: $(rt^2)^2 + a_1(rt^2) + b_1 = rs^2$. Let $t = \ell/m$, where $\ell, m \in \mathbb{Z}$ and $\gcd(\ell, m) = 1$. Then: $r^2\ell^4/m^4 + a_1r\ell^2/m^2 + b_1 = rs^2$, and so: $r^2\ell^4 + a_1r\ell^2m^2 + b_1m^4 = r(m^2s)^2$. Now, $a_1, b_1, r, \ell, m \in \mathbb{Z}$, so the LHS of this last equation is in $\mathbb{Z}$, and so the RHS is also in $\mathbb{Z}$; that is: $r(m^2s)^2 \in \mathbb{Z}$. Since r is square free, we must therefore have $m^2s \in \mathbb{Z}$. Define:

$n = m^2 s \in \mathbb{Z}$. Then our equation becomes:

$$r^2\ell^4 + a_1 r\ell^2 m^2 + b_1 m^4 = rn^2, \quad \text{for some } \ell, m, n \in \mathbb{Z},\ \gcd(\ell, m) = 1. \qquad (\dagger)$$

We want to show that $r|b_1$, and we know that r is square free. It is sufficient to show, for any prime p, that $p|r \Rightarrow p|b_1$.

> Imagine $p|r$ and $p \not| \ b_1$, for some prime p. Then $p|r^2\ell^4, a_1 r\ell^2 m^2, rn^2$ and so by $(\dagger)$, $p|b_1 m^4$, which in turn gives: $p|m$ [since $p \not| \ b_1$]. Hence, since now $p|r$ and $p|m$, we have: $p^2|r^2\ell^4, a_1 r\ell^2 m^2, b_1 m^4$, and so by $(\dagger)$, $p^2|rn^2$, which in turn gives: $p|n$ [since r is square free]. Hence, since now $p|r, m, n$, we have: $p^3|a_1 r\ell^2 m^2, b_1 m^4, rn^2$, and so by $(\dagger)$, $p^3|r^2\ell^4$, which in turn gives: $p|\ell$ [since r is square free]. This is a contradiction, since $p|\ell$ and $p|m$ but $\gcd(\ell, m) = 1$.

The above assumption that $p|r$ and $p \not| \ b_1$ let to a contradiction, and so it is impossible for any prime p to satisfy $p|r$ and $p \not| \ b_1$. This is the same as saying that $p|r \Rightarrow p|b_1$ for any prime p. Since r is square free, we conclude that $r|b_1$, as required **[12 marks]**

(ii) [*Seen similar on a problem sheet*].
Let $\mathcal{C} : Y^2 = X(X^2 + aX + b) = X(X^2 + 3X - 3)$, where $a = 3, b = -3$, and isogenous curve $\mathcal{D} : Y^2 = X(X^2 + a_1 X + b_1) = X(X^2 - 6X + 21)$, where $a_1 = -6, b_1 = 21$, with the usual isogeny $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto (y^2/x^2, y + 3y/x^2)$, and dual isogeny $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) : (u, v) \mapsto (\frac{1}{4}v^2/u^2, \frac{1}{8}(v - 21v/u^2))$.

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u$, 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 $\{d : d \text{ is square free and } d|b_1\} = \{\pm 1, \pm 3, \pm 7, \pm 21\}$. Also, $\mathbf{o} \mapsto 1$, $(0, 0) \mapsto 21$, so that $\{1, 21\} \subset \text{im}q \subset \{\pm 1, \pm 3, \pm 7, \pm 21\}$.

We know that $3 \in \text{im}q$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $3 \cdot \ell^4 + a_1\ell^2 m^2 + (b_1/3) \cdot m^4 = n^2$ that is: $3\ell^4 - 6\ell^2 m^2 + 7m^4 = n^2$, which is satsfied by $\ell = m = 1, n = 2$, giving that there exists $(u, v) \in \mathcal{D}(\mathbb{Q})$ with $u = r(\ell/m)^2 = 3(1/1)^2 = 3$. Indeed $(3, 6) \in \mathcal{D}(\mathbb{Q})$ with $q : (3, 6) \mapsto 3$. [Alternatively, could have just searched on $\mathcal{D}$ to find the point $(3, 6) \in \mathcal{D}(\mathbb{Q})$ and $q : (3, 6) \mapsto 3$.] Similarly $(7, -14) \in \mathcal{D}(\mathbb{Q})$ [which is $(0, 0) + (3, 6)$] and $q : (7, -14) \mapsto 7$. In summary, $q : \mathbf{o} \mapsto 1$, $(0, 0) \mapsto 21$, $(3, 6) \mapsto 3$, $(7, -14) \mapsto 7$, so that $\{1, 3, 7, 21\} \subset \text{im}q \subset \{\pm 1, \pm 3, \pm 7, \pm 21\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in \text{im}q$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a_1\ell^2 m^2 + (b_1/(-1)) \cdot m^4 = n^2$ that is: $-\ell^4 - 6\ell^2 m^2 - 21m^4 = n^2$. This is impossible in $\mathbb{R}$ (the left hand side is $\leqslant 0$ and the right hand side is $\geqslant 0$, and equality only occurs when $\ell^4 = 21m^4 = n^2 = 0$, implying $\ell = m = n = 0$, which is not allowed). Hence $-1 \notin \text{im}q$.

We conclude that im$q = \{1, 3, 7, 21\}$, and so $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\mathbf{o}, (0, 0), (3, 6), (7, -14)\}$ is generated by $(0, 0)$ and $(3, 6)$.

The map $\hat{q} : \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x,y) \mapsto x$, for $(x,y) \neq (0,0)$, with $\hat{q} : (0,0) \mapsto b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with $\mathrm{im}\hat{q}$ contained in $\{d : d \text{ is square free and } d|b\} = \{\pm 1, \pm 3\}$. Also, $\mathbf{o} \mapsto 1$ and $(0,0) \mapsto -3$, so that $\{1,-3\} \subset \mathrm{im}\hat{q} \subset \{\pm 1, \pm 3\}$.

There is only one coset to check, represented by -1, say. 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: $-\ell^4 + 3\ell^2 m^2 + 3m^4 = n^2$. Multiply both sides by 4 and rewrite as: $-(2\ell^2 - 3m^2)^2 + 21m^4 = 4n^2$. Reducing modulo 3 gives $-(2\ell^2 - 3m^2)^2 \equiv n^2$ (modulo 3). If n were coprime to 3, then this would give: $((2\ell^2 - 3m^2)/n)^2 = -1$ in $\mathcal{F}_3$, contradicting the fact that -1 is not a quadratic residue modulo 3. So, $3|n$ and so $3|(2\ell^2 - 3m^2)$ also. This means that $3^2|(2\ell^2 - 3m^2)^2$ and $3^2|n^2$, which can be combined with $-(2\ell^2 - 3m^2)^2 + 21m^4 = 4n^2$ to give: $3^2|21m^4$ and so $3|7m^4$, giving $3|m$. Also, from $3|(2\ell^2 - 3m^2)$ we deduce $3|2\ell^2$ and so $3|\ell$. This contradicts the fact that $\gcd(\ell, m) = 1$. Hence our equation is impossible in $\mathbb{Q}_3$, and so impossible in $\mathbb{Q}$. Hence $-1 \notin \mathrm{im}\hat{q}$.

We conclude that $\mathrm{im}\hat{q} = \{1, -3\}$, 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 $\hat{\phi}\big((3,6)\big) = (\frac{1}{4}\frac{6^2}{3^2}, \frac{1}{8}(6 - \frac{21 \cdot 6}{3^2})) = (1,-1)$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0,0), (1,-1)$, and is isomorphic to $C_2 \times C_2$. We also know that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})/2\mathcal{C}_{\mathrm{tors}}(\mathbb{Q}) \times C_2^r$, which is isomorphic to $\mathcal{C}(\mathbb{Q})[2] \times C_2^r$, where $\mathcal{C}(\mathbb{Q})[2]$ is the 2-torsion group and r is the rank. The 2-torsion points on $\mathcal{C} : Y^2 = X(X^2 + 3X - 3)$ are $\mathbf{o}$ together with the points of the form $(x, 0)$, where x is a root of $X(X^2 + 3X - 3)$, that is: $(0,0)$, $(-\frac{3}{2} + \frac{\sqrt{21}}{2}, 0)$ and $(-\frac{3}{2} - \frac{\sqrt{21}}{2}, 0)$, of which only $\mathbf{o}$ and $(0,0)$ are in $\mathcal{C}(\mathbb{Q})[2]$, giving that $\mathcal{C}(\mathbb{Q})[2]$ is isomorphic to C_2. Combining this with the facts (already found) that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic both to $C_2 \times C_2$ and to $\mathcal{C}(\mathbb{Q})[2] \times C_2^r$, give that $\mathcal{C}(\mathbb{Q})$ has rank 1. **[13 marks]**

Question 4.

(a) (i) [*Unseen*]. Using the given: $|h_x(P+Q) + h_x(P-Q) - 2h_x(P) - 2h_x(Q)| \leq C \quad (*)$, with $Q = P$, we get: $|h_x(2P) - 4h_x(P)| \leq C \quad (**)$,
so the result is true for $m = 2$, taking $C_2 = C$. Now, suppose the that result is true for all $k \leq m$, that is, there exists C_k such that:

$|h_x(kP) - k^2 h_x(P)| \leq C_k \quad (***)$,

for all $P, Q \in \mathcal{E}(\mathbb{Q})$. Using $(*)$ with mP, P as P, Q, respectively, gives:
$|h_x((m+1)P) + h_x((m-1)P) - 2h_x(mP) - 2h_x(P)| \leq C$, so that
$|h_x((m+1)P) - (m+1)^2 h_x(P) + h_x((m-1)P) - (m-1)^2 h_x(P) - 2(h_x(mP) - m^2 h_x(P))| \leq C$.
Hence, $|h_x((m+1)P) - (m+1)^2 h_x(P)| \leq$

$|h_x((m+1)P) - (m+1)^2 h_x(P) + h_x((m-1)P) - (m-1)^2 h_x(P) - 2(h_x(mP) - m^2 h_x(P))| +$
$|h_x((m-1)P) - (m-1)^2 h_x(P)| + 2|h_x(mP) - m^2 h_x(P)| \leq C + C_{m-1} + 2C_m$, where C_{m-1}, C_m exist by the induction hypothesis $(***)$. Hence the result by induction. **[6 marks]**

(ii) [*Unseen*]. For any m, n, wlog $n \geq m$ we have: $|4^{-n} h_x(2^n P) - 4^{-m} h_x(2^m P)|$
$= |4^{-n} h_x(2^n P) - 4^{-(n-1)} h_x(2^{n-1} P) + 4^{-(n-1)} h_x(2^{n-1} P) - \ldots - 4^{-m} h_x(2^m P)|$
$\leq |4^{-n} h_x(2^n P) - 4^{-(n-1)} h_x(2^{n-1} P)| + \ldots + |4^{-(m+1)} h_x(2^{m+1} P) - 4^{-m} h_x(2^m P)|$
$\leq C(4^{-n} + 4^{-(n-1)} + \ldots + 4^{-(m+1)}) \leq \frac{C}{3 \cdot 4^m} \to 0$ as $m, n \to \infty$, giving that the sequence is Cauchy and so convergent (since it is a sequence in $\mathbb{R}$). **[5 marks]**

(b) [*Unseen*]. From lectures, we know that 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 $g(T) \in R[[T]]$. Let $x \in \mathcal{M}$, and let x_n denote $[p^n](x)$. Let $\gamma = \min(|p|, |x|) < 1$. Trivially, $|x_1| \leqslant \gamma$. Furthermore, $|x_{n+1}| = |[p^{n+1}(x)| = |[p](x_n)| = |pf(x_n) + g(x_n^p)| \leq \gamma |x_n|$, so that, for all n we have: $|x_n| \leq \gamma^n \to 0$, giving $x_n \to 0$, as required. **[6 marks]**

(c) [*Unseen*]. The line tangent to $\mathcal{E}$ at $P = (1, 1)$ has slope y' given by $2yy' = 3x^2 + a$, with $x_1 = 1, y_1 = 1$; that is, the slope is $(a+3)/2$. This tangent line also goes through $(1, 1)$ and so has equation: $Y = ((a+3)/2)X - (a+1)/2$. Substituting this line into $\mathcal{E}$, we see that the x-coordinate of the third point of intersection is: $x_2 = (a+3)^2/4 - 1 - 1 = ((a+3)^2 - 8)/4$, with corresponding $y_2 = -(((a+3)/2)x_2 - (a+1)/2)$, so that $(x_2, y_2) = 2(x_1, y_1)$. We have so far only had divisions by 2, which are allowable since p, q are odd. In order to compute $3(1, 1)$, we first need the slope of the line through (x_1, y_1) and (x_2, y_2), namely $(y_1 - y_2)/(x_1 - x_2)$, which involves finding the inverse, modulo N, of $((a+3)^2 - 8)/4 - 1$ and so the inverse of: $(a+3)^2 - 12$ modulo N, for which the first step is to compute the gcd of $(a+3)^2 - 12$ and N. Since $p \equiv 1 \pmod{12}$, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ [by quadratic reciprocity, since $p \equiv 1 \pmod 4$] $= \left(\frac{1}{3}\right) = 1$, so that 3 is a quadratic residue modulo p. Similarly, 3 is not a quadratic residue modulo q. Hence there exists α such that $\alpha^2 \equiv 3$ (modulo p). Taking $a = 2\alpha - 3$ gives that $(a+3)^2 - 12$ is divisible by p, but is not divisible by q (since 3 is not a quadratic residue modulo q). Hence the gcd of $(a+3)^2 - 12$ and N gives the proper factor p of N. **[8 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.