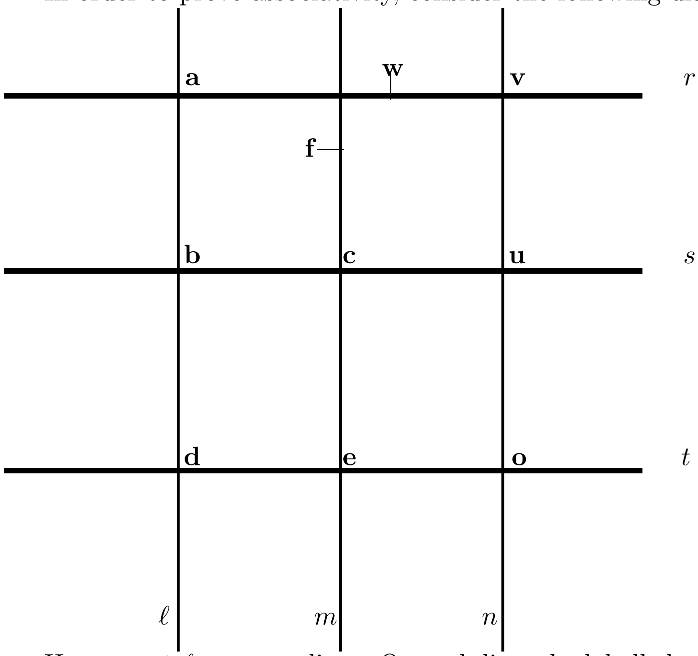
Solution to Question 1.
(a) [*Proof from lectures*]. For any two points $\mathbf{a}, \mathbf{b}$ on $\mathcal{C}$, let $\ell_{\mathbf{a},\mathbf{b}}$ denote the line which meets $\mathcal{C}$ at $\mathbf{a}, \mathbf{b}$ [if $\mathbf{a}, \mathbf{b}$ are distinct then $\ell_{\mathbf{a},\mathbf{b}}$ is the unique line through $\mathbf{a}, \mathbf{b}$; if $\mathbf{a} = \mathbf{b}$ then $\ell_{\mathbf{a},\mathbf{b}}$ is the line tangent to $\mathcal{C}$ at $\mathbf{a} = \mathbf{b}$]. Then $\ell_{\mathbf{a},\mathbf{b}}$ and $\mathcal{C}$ have 3 points of intersection (Bézout). Let $\mathbf{d}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\mathbf{a},\mathbf{b}}$. Let $\mathbf{c}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\mathbf{o},\mathbf{d}}$. We define $\mathbf{a} + \mathbf{b} = \mathbf{d}$.

We recall from lectures the following lemma.

Lemma. Let $P_1, \ldots, P_8$ be such that no 4 points lie on a line and no 7 points lie on a conic. Then there exists a unique point P_9 which is a 9th point of intersection of any two cubics passing through $P_1, \ldots, P_8$.

In order to prove associativity, consider the following diagram.



Here, r, s, t, ℓ, m, n are lines. On each line, the labelled points are the points of intersection between $\mathcal{C}$ and that line. From our construction of the law for adding points: $\mathbf{a} + \mathbf{b} = \mathbf{e}$, and so: $(\mathbf{a} + \mathbf{b}) + \mathbf{c}$ is the 3rd point of intersection on $\ell_{\mathbf{o},\mathbf{f}}$. Similarly, $\mathbf{b} + \mathbf{c} = \mathbf{v}$, and $\mathbf{a} + (\mathbf{b} + \mathbf{c}) =$ is the 3rd point of intersection on $\ell_{\mathbf{o},\mathbf{w}}$. To show $(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \mathbf{a} + (\mathbf{b} + \mathbf{c})$, it is sufficient to show that $\mathbf{f} = \mathbf{w}$. Let $F_1 = \ell mn$ and $F_2 = rst$, both of which are cubic curves.

$\mathcal{C}$ and F_1 have 8 common points: $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \mathbf{o}$.

$\mathcal{C}$ and F_2 also have these 8 common points: $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \mathbf{o}$. From the above lemma, the 9th point of intersection of $\mathcal{C}$ and F_1 must be the same as the 9th point of intersection of $\mathcal{C}$ and F_2; that is, $\mathbf{f} = \mathbf{w}$, as required. **[10 marks]**

(b) Statement of Hensel's Lemma: Let K be a field, complete with respect to a non-Archimedean valuation $|\ |$, with valuation ring $R = \{x \in K : |x| \leq 1\}$.

Let $f(x) \in R[x]$ and let $a_0 \in R$ satisfy: $|f(a_0)| < |f'(a_0)|^2$. Then there exists a unique $a \in R$ such that $f(a) = 0$ and $|a - a_0| \leq |f(a_0)|/|f'(a_0)|$.

Imagine $x, y \in \mathbb{Z}_2$ satisfy $x^2 - 2y^2 = 3$. Then $x^2 - 2y^2 \equiv 3 \pmod 8$. This gives $|x|_2 = 1$ (otherwise $1 = |3|_2 = |x^2 - 2y^2|_2 < 1$), and so $x^2 = (1 + 2k)^2 \equiv 1 \pmod 8$, and $y^2 \equiv 0, 1$ or $4 \pmod 8$, so that $x^2 - 2y^2 \equiv 1$ or $7 \not\equiv 3 \pmod 8$, a contradiction. Hence: no solutions $x, y \in \mathbb{Z}_2$.

Imagine $x, y \in \mathbb{Z}_3$ satisfy $x^2 - 2y^2 = 3$. Then $|y|_3 = 1$ (otherwise $|2y^2|_3 \leqslant 3^{-2}$ and $3^{\text{even}} = |x^2|_3 = |3 + 2y^2|_3 = \max(|3|_3, |2y^2|_3) = 3^{-1}$, using the theorem: $|\alpha|_p \neq |\beta|_p \implies |\alpha \pm \beta|_p = \max(|\alpha|_p, |\beta|_p)$. Then: $x^2 \equiv 2y^2$ and and so $(x/y)^2 \equiv 2 \pmod 3$, impossible, since $\left(\frac{2}{3}\right) = -1$. Hence: no solutions $x, y \in \mathbb{Z}_3$.

For $p \neq 2, 3$, the set $\{x^2 : x \in \mathbb{F}_p\}$ has size $(p+1)/2$, since $x \mapsto x^2$ is 2-to-1 on $\mathbb{F}_p^*$ and maps $0 \mapsto 0$. Similarly the set $\{3 + 2y^2 : y \in \mathbb{F}_p\}$ has size $(p+1)/2$. These cannot be disjoint, since $(p+1)/2 + (p+1)/2 > p = \#\mathbb{F}_p$, so there exist $x_0, y_0 \in \mathbb{Z}$ such that $x_0^2 \equiv 3 + 2y_0^2 \pmod p$, and cannot have both $|x_0|_p < 1$ and $|y_0|_p < 1$ (since $|3|_p = 1$), so $|x_0|_p = 1$ or $|y_0|_p = 1$, wlog $|x_0|_p = 1$. For $f(x) = x^2 - (3 + 2y_0^2)$, we have $|f(x_0)|_p < 1$ and $|f'(x_0)|_p = |3x_0^2|_p = 1$, so by Hensel's lemma, there exists $x_1 \in \mathbb{Z}_p$ such that $f(x_1) = 0$, that is: $x_1, y_0 \in \mathbb{Z}_p$ such that $x_1^2 - 2y_0^2 = 3$. [**7 marks**; Unseen]

(c) For $p = 3$, set $z = 1$; then $y^3 - z^3 + b - a \equiv y^3 - 1 \pmod{27}$. Let $f(y) = y^3 - 1^3 + b - a$. Let $y_0 = 1$. Then $|f(y_0)|_3 = |b - a|_3 \leqslant 3^{-3}$ and $|f'(y_0)|_3 = |3|_3 = 3^{-1}$, so that $|f(y_0)|_3 < |f'(y_0)|_3^2$. By Hensel's lemma, there exists $y_1 \in \mathbb{Z}_3$ such that $f(y_1) = 0$. Then: $y = y_1, z = 1$ and x arbitrary gives a solution in $\mathbb{Z}_3$ to $y^3 - z^3 + b - a = 0$ and so to the given equation.

Now let $p \neq 3$. If $a \equiv 0 \pmod p$ then take $y = 1$ and $f(x) = x^3 - 1^3 + a$ and $x_0 = 1$. Then $|f(x_0)|_p < 1$ and $|f'(x_0)|_p = |3|_p = 1$, so by HL there exists $x_1 \in \mathbb{Z}_p$ such that $f(x_1) = 0$. Then $x_1 = x_1, y = 1$ and z arbitrary gives a solution in $\mathbb{Z}_p$ to $x^3 - y^3 + a = 0$ and so to the given equation. Similarly if $b \equiv 0 \pmod p$ then there is a solution in $\mathbb{Z}_p$ to $x^3 - z^3 + b$; similary if $b - a \equiv 0 \pmod p$ then there is a solution in $\mathbb{Z}_p$ to $y^3 - z^3 + b - a = 0$. So, now assume that $a \not\equiv 0$, $b \not\equiv 0$, $b - a \not\equiv 0 \pmod p$. The map $x \mapsto x^3$ is at most 3-to-1 on $\mathbb{F}_p^*$ (since $x^3 - \alpha$ has at most 3 solutions) and $0 \mapsto 0$. So, $\#\{x^3 : x \in \mathbb{F}_p\} \geqslant (p-1)/3 + 1 = (p+2)/3$, and similarly $\{y^3 - a : y \in \mathbb{F}_p\}$ and $\{z^3 - b : z \in \mathbb{F}_p\}$. Hence these sets cannot all be disjoint, since $(p+2)/3 + (p+2)/3 + (p+2)/3 > \#\mathbb{F}_p$. So, there exist $x_0, y_0, z_0 \in \mathbb{Z}$ such that $x_0^3 - y_0^3 + a \equiv 0$ or $x_0^3 - z_0^3 + b \equiv 0$ or $y_0^3 - z_0^3 + b - a \equiv 0 \pmod p$, wlog say that $x_0^3 - y_0^3 + a \equiv 0 \pmod p$. Since $a \not\equiv 0 \pmod p$, $x_0 \not\equiv 0$ or $y_0 \not\equiv 0$, wlog $x_0 \not\equiv 0 \pmod p$. Let $f(x) = x^3 - y_0^3 + a$. Then $|f(x_0)|_p < 1$ and $|f'(x_0)|_p = |3x_0^2|_p = 1$, so by HL there exists $x_1 \in \mathbb{Z}_p$ such that $f(x) = 0$. Then $x = x_1, y = y_0$ and z arbitrary is a solution in $\mathbb{Z}_p$ to $x^3 - y^3 + a = 0$ and so to the given equation. Hence, there are solutions in $\mathbb{Z}_p$ for all p.

Imagine there were a solution $x, y, z \in \mathbb{Z}$. Then $x^3 - y^3 + a = 0$ or $x^3 - z^3 + b = 0$ or $y^3 - z^3 + b - a = 0$. But $x^3 - y^3 + a \equiv (0 \text{ or } \pm 1) - (0 \text{ or } \pm 1) + 4 \not\equiv 0 \pmod 9$, so $x^3 - y^3 + a \neq 0$. Similarly $x^3 - z^3 + b \not\equiv 0 \pmod 9$ so $x^3 - z^3 + b \neq 0$. Also, $y^3 - z^3 + b - a \equiv (0 \text{ or } \pm 1) - (0 \text{ or } \pm 1) + 3 \not\equiv 0 \pmod 7$, so $y^3 - z^3 + b - a \neq 0$. Hence there are no solutions in $\mathbb{Z}$. [**8 marks**; Unseen]

Solution to Question 2

(a)(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 the associativity axiom $F\big(U, F(T,S)\big) = F\big(F(U,T),S\big)$ 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 $a = Q(0)$. **[7 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 $a_n T^n$ in $[p](T)$ must then satisfy $p|na_n$ and so $p|n$ or $p|a_n$, as required. **[6 marks]**

(b)(i) Differentiating: $2YY' = 3X^2 + 2(\alpha+\beta)X + \alpha\beta$, so the tangent to $\mathcal{C}$ at (x,y) is $Y = \lambda X + \mu$, where $\lambda = \big(3x^2 + 2(\alpha+\beta)x + \alpha\beta\big)/(2y)$. This meets $\mathcal{C}$ at points whose x-coordinates satisfy $(\lambda X + \mu)^2 = X(X+\alpha)(X+\beta)$, so that $0 = X^3 - (\lambda^2 - \alpha - \beta)X^2 + \ldots$. Hence the x-coordinate of $2(x,y)$ equals $-(\text{coeff of } X^2) - 2x = \lambda^2 - \alpha - \beta - 2x$, which equals

$$\frac{\big(3x^2 + 2(\alpha+\beta)x + \alpha\beta\big)^2}{4x(x+\alpha)(x+\beta)} - \alpha - \beta - 2x = \frac{(x^2 - \alpha\beta)^2}{4x(x+\alpha)(x+\beta)}.$$

The points of order 2 in $\mathcal{C}(\mathbb{Q})$ are $(0,0), (\alpha,0), (\beta,0)$, and so:

$$\mathcal{C}(\mathbb{Q}) \text{ has a point of order 4} \iff (0,0) \text{ or } (-\alpha,0) \text{ or } (-\beta,0) \in 2\mathcal{C}(\mathbb{Q}). \quad (*)$$

If $(0,0) \in 2\mathcal{C}(\mathbb{Q})$ then $(0,0) = 2(x,y)$ for some $(x,y) \in \mathcal{C}(\mathbb{Q})$, and so using the above duplication formula on the x-coordinate, we have: $(x^2-\alpha\beta)^2 = 0$, so that $\alpha\beta \in (\mathbb{Q}^*)^2$ and $x^2 = \alpha\beta$. Then $y^2 = x(x+\alpha)(x+\beta) = x(x+\alpha)(x+x^2/\alpha) = x^2(x+\alpha)^2/\alpha$. Hence $\alpha = \big(x(x+\alpha)/y\big)^2 \in (\mathbb{Q}^*)^2$, and so also $\beta = x^2/\alpha \in (\mathbb{Q}^*)^2$.

Conversely, if $\alpha, \beta \in (\mathbb{Q}^*)^2$, say $\alpha = a^2$ and $\beta = b^2$ for some $a, b \in \mathbb{Q}^*$. Then $(ab, ab(a+b)) \in \mathcal{C}(\mathbb{Q})$ [since $ab(ab+a^2)(ab+b^2) = a^2b^2(a+b)^2$], and from the above duplication formula, the x-coordinate of $2(ab, ab(a+b))$ is 0, so that $2(ab, ab(a+b)) = (0,0)$. Hence $(0,0) \in 2\mathcal{C}(\mathbb{Q})$. In summary:

$$(0,0) \in 2\mathcal{C}(\mathbb{Q}) \iff \alpha \in (\mathbb{Q}^*)^2 \text{ and } \beta \in (\mathbb{Q}^*)^2. \qquad (1)$$

The map $(x,y) \mapsto (x+\alpha, y)$ is a birational transformation from $\mathcal{C}$ to the curve $\mathcal{C}' : Y^2 = X(X-\alpha)(X+\beta-\alpha)$, so that:

$$(-\alpha,0) \in 2\mathcal{C}(\mathbb{Q}) \iff (0,0) \in 2\mathcal{C}'(\mathbb{Q}) \iff -\alpha \in (\mathbb{Q}^*)^2 \text{ and } \beta-\alpha \in (\mathbb{Q}^*)^2. \quad (2)$$

The map $(x,y) \mapsto (x+\beta, y)$ is a birational transformation from $\mathcal{C}$ to the curve $\mathcal{C}'' : Y^2 = X(X-\beta)(X+\alpha-\beta)$, so that:

$$(-\beta,0) \in 2\mathcal{C}(\mathbb{Q}) \iff (0,0) \in 2\mathcal{C}''(\mathbb{Q}) \iff -\beta \in (\mathbb{Q}^*)^2 \text{ and } \alpha-\beta \in (\mathbb{Q}^*)^2. \quad (3)$$

Substituting $(1), (2), (3)$ into $(*)$ gives the required result. [**6 marks**; Unseen]

(ii) Here $\mathcal{C} : Y^2 = X(X+c^4)(X+d^4) = X(X^2+(c^4+d^4)X+c^4d^4)$ and the 2-isogenous curve is $\mathcal{D} : V^2 = U\big(U^2 - 2(c^4+d^4)U + (c^4-d^4)^2\big)$ where, from lectures, the 2-isogenies are $\phi : \mathcal{C} \mapsto \mathcal{D} : (x,y) \mapsto \big((y/x)^2, y - c^4d^4y/x^2\big)$ and $\hat{\phi} : \mathcal{D} \mapsto \mathcal{C} : (u,v) \mapsto \big((1/4)(v/u)^2, (1/8)(v-(c^4-d^4)^2v/u^2)\big)$, satisfying $\hat{\phi} \circ \phi = [2]$. By the previous part, we have that $P = (c^2d^2, c^2d^2(c^2+d^2)) \in \mathcal{C}(\mathbb{Q})$ is a point of order 4. The x-coordinate of P is $c^2d^2 \in (\mathbb{Q}^*)^2$ so by a theorem from lectures, $P \in \hat{\phi}(\mathcal{D}(\mathbb{Q}))$, so that $P = \hat{\phi}((u,v))$, for some $(u,v) \in \mathcal{D}(\mathbb{Q})$. Then $(1/4)(v/u)^2 = c^2d^2$ and so $v = \pm 2cdu$. Substituting this into $\mathcal{D}$ gives $(\pm 2cdu)^2 = u(u^2 - 2(c^4+d^4)u + (c^4-d^4)^2)$, so that

$$\begin{aligned} 0 &= u\big(u^2 - 2(c^2+d^2)^2u + (c+d)^2(c^2+d^2)(c-d)^2(c^2+d^2)\big) \\ &= u\big(u-(c+d)^2(c^2+d^2)\big)\big(u-(c-d)^2(c^2+d^2)\big). \end{aligned}$$

But $\hat{\phi} : (0,0) \mapsto \mathbf{o}$, so that $u = (c \pm d)^2(c^2+d^2) \in (\mathbb{Q}^*)^2$, since we are given that $c^2+d^2 \in (\mathbb{Q}^*)^2$. So, by the same theorem from lectures, $(u,v) \in \phi(\mathcal{C}(\mathbb{Q}))$, so that $(u,v) = 2(x,y)$, for some $(x,y) \in \mathcal{C}(\mathbb{Q})$). Then $P = \hat{\phi} \circ \phi((x,y)) = 2(x,y)$; already know that P is a point of order 4 so that (x,y) is a point of order 8 in $\mathcal{C}(\mathbb{Q})$), as required.

As an example, take $c = 3, d = 4$, so that $c^2 + d^2 = 25 \in (\mathbb{Q}^*)^2$, and then $\mathcal{C} : Y^2 = X(X+3^4)(X+4^4)$ has a point of order 8 in $\mathcal{C}(\mathbb{Q})$. [**6 marks**; Unseen]

Solution to Question 3

(a) [*Proof from lectures*]. Let $(u_1, v_1), (u_2, v_2), (u_3, v_3)$ be 3 points on $\mathcal{D}(\mathbb{Q})$ which sum to $\mathbf{o}$, so that $(u_1, v_1) + (u_2, v_2) = (u_3, -v_3)$. Then these are the 3 points of intersection between $\mathcal{D}$ and some line defined over $\mathbb{Q}$: $Y = \ell X + m$, say. Substituting $Y = \ell X + m$ into $\mathcal{D}$ gives: $X(X^2 + a_1 X + b_1) - (\ell X + m)^2$, whose 3 roots must be u_1, u_2, u_3. That is: $X(X^2 + a_1 X + b_1) - (\ell X + m)^2 = (X - u_1)(X - u_2)(X - u_3)$. Equating constant terms gives: $u_1 u_2 u_3 = m^2 = 1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, and so $u_1 u_2 = 1/u_3 = u_3$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Therefore, by the definition of q we have: $q\big((u_1, v_1)\big)q\big((u_2, v_2)\big) = q\big((u_3, v_3)\big)$, as required. **[5 marks]**

(b) Let $\mathcal{C} : Y^2 = X(X^2 - pX + p^2)$. Here, $a = -p, b = p^2$ and so $a_1 = -2a = 2p, b_1 = a^2 - 4b = -3p^2$, giving $\mathcal{D} : V^2 = U(U^2 + 2pU - 3p^2) = U(U - p)(U + 3p)$.

Step 1. Find $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$. Here $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$. We need to consider $r | b_1 = -3p^2, r \in \mathbb{Z}$, r square free, that is, im $q \leqslant \{\pm 1, \pm 3, \pm p, \pm 3p\}$. But $q(\mathbf{o}) = 1$, $q(0, 0) = b_1 = -3$, $q(p, 0) = p$, $q(-3p, 0) = -3p$, so that $\{1, -3, p, -3p\} \leqslant$ im q. There is just one nontrivial coset: take -1 as the representative. Then $W_r : r\ell^4 + a_1 \ell^2 m^2 + (b_1/r)m^4 = n^2$, for some $\ell, m, n \in \mathbb{Z}$, not all 0, with $\gcd(\ell, m) = 1$ becomes: $W_{-1} : -\ell^4 + 2p\ell^2 m^2 + 3p^2 m^4 = n^2$. On completing the square: $-(\ell^2 - pm^2)^2 + 4p^2 m^4 = n^2$. Imagine $2|\ell$. Then $3p^2 m^4 \equiv n^2 \pmod 4$ and so $2|m$ (ow LHS $\equiv 3$ and RHS $\equiv 1$ mod 4), a contradiction. Hence $2 \nmid \ell$. Imagine $2|m$. Then $-\ell^4 \equiv n^2 \pmod 4$ and so $2|\ell$ (ow LHS $\equiv 3$ and RHS $\equiv 1$ mod 4), a contradiction. Hence $2 \nmid m$.

Hence $\ell^2 \equiv 1$ and $m^2 \equiv 1 \pmod 8$, so $\ell^2 - pm^2 \equiv 1 - 5 \equiv 4 \pmod 8$ (since $p \equiv 5$ mod 8), so that $2|n$, so write $n = 2n'$ for some $n' \in \mathbb{Z}$. Then $-\big((\ell^2 - pm^2)/2\big)^2 + p^2 m^2 = n'^2$. But $(\ell^2 - pm^2)/2 \equiv 2 \pmod 4$ and so is $\equiv 2$ or $6 \pmod 8$, so that $\big((\ell^2 - pm^2)/2\big)^2 \equiv 4 \pmod 8$. Then LHS $= -\big((\ell^2 - pm^2)/2\big)^2 + p^2 m^2 \equiv 4 + 1 \equiv 5 \pmod 8$, whereas RHS $= n'^2 \equiv 0, 1$ or $4 \pmod 8$, a contradiction. Hence $-1 \notin$ im q, giving im $q = \{1, -3, p, -3p\}$ and $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\mathbf{o}, (0, 0), (p, 0), (-3p, 0)\} = \langle (0, 0), (p, 0) \rangle \cong C_2 \times C_2$.

Step 2. Find $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$. Here $\hat{q} : \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$. We need to consider $r | b = p^2, r \in \mathbb{Z}$, r square free, that is, im $\hat{q} \leqslant \{\pm 1, \pm p\}$. But $\hat{q}(\mathbf{o}) = 1$, $\hat{q}(0, 0) = b = 1$, so that $\{1\} \leqslant$ im $\hat{q}$. There are three nontrivial cosets: $-1, -p, p$. Then $\widehat{W_r} : r\ell^4 + a\ell^2 m^2 + (b/r)m^4 = n^2$ for some $\ell, m, n \in \mathbb{Z}$, not all 0, with $\gcd(\ell, m) = 1$. For $r < 0$, we see that LHS $\leqslant 0$ and RHS $\geqslant 0$, and both sides are equal only when $\ell = m = n = 0$, a contradiction. Hence $-1, -p \notin$ im $\hat{q}$. For $r = p$, we have: $\widehat{W_p} : p\ell^4 - p\ell^2 m^2 + pm^4 = n^2$, giving $p|n$ so write $n = pn'$. Then $\ell^4 - \ell^2 m^2 + m^4 = pn'^2$. Multiplying by 4 and completing the square gives: $(2\ell^2 - m^2)^2 + 3m^4 = 4pn'^2$. Hence $(2\ell^2 - m^2)^2 \equiv -3m^4 \pmod p$. Imagine $p \nmid m$. Then $\big((2\ell^2 - m^2)/m^2\big)^2 \equiv -3 \pmod p$, giving $\left(\frac{-3}{p}\right) = 1$. but in fact $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ [by QR, since $p \equiv 1 \pmod 4$] $= \left(\frac{2}{3}\right)$ [since $p \equiv 2 \pmod 3$] $= -1$, a contradiction. Hence $p|m$; but then from $\ell^4 - \ell^2 m^2 + m^4 = pn'^2$ we see also that $p|\ell$, impossible. So $p \notin$ im $\hat{q}$. Hence im $\hat{q} = \{1\}$ and $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \{\mathbf{o}\}$, the trivial group.

Step 3. Find $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}))$, which is generated by $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \{\mathbf{o}\}$ and $\hat{\phi}\big(\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))\big) = \hat{\phi}\big(\langle(0,0),(p,0)\rangle\big) = \langle(0,0)\rangle$, since $\hat{\phi}:(0,0)\mapsto\mathbf{o}$, $(p,0)\mapsto(0,0)$. Hence $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})) = \langle(0,0)\rangle \cong C_2$. From lectures, $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})) \cong \mathcal{C}(\mathbb{Q})[2]\times C_2^r$. Here $\mathcal{C}(\mathbb{Q})[2] = \{\mathbf{o},(0,0)\}\cong C_2$, since $((p\pm p\sqrt{-3})/2,0)\notin\mathcal{C}(\mathbb{Q})$. Hence the rank is 0. [**10 marks**; Seen similar.]

(c) Let $\mathcal{C}: Y^2 = X(X^2-p_1p_2)$. Here, $a=0, b=-p_1p_2$ so $a_1=0, b_1=4p_1p_2$, giving $\mathcal{D}: V^2 = U(U^2+4p_1p_2)$.
Step 1. Find $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$. Here $q:\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))\longrightarrow\mathbb{Q}^*/(\mathbb{Q}^*)^2$. We need to consider square free $r|b_1=4p_1p_2$, that is, im $q\leqslant\langle-1,2,p_1,p_2\rangle$. But $q(\mathbf{o})=1$, $q(0,0)=b_1=p_1p_2$. Also, for any $r<0$, $W_r: r\ell^4+a_1\ell^2m^2+(b_1/r)m^4=n^2$ (for some $\ell,m,n\in\mathbb{Z}$, not all 0, with $\gcd(\ell,m)=1$) has LHS $\leqslant 0$ and RHS $\geqslant 0$, with both sides equal only when $\ell=m=n=0$, so that $r\notin$ im q. Hence $\{1,p_1p_2\}\leqslant$ im $q\leqslant\{1,2,p_1,2p_1,p_2,2p_2,p_1p_2,2p_1p_2\}$. There are three nontrivial cosets: take $2,p_1,2p_1$ as representatives.
Lemma $(*)$. $W_r: r\ell^4+(4p_1p_2/r)m^4=n^2$, $i\in\{1,2\}$; if $p_i\nmid r$ then $p_i\nmid\ell$. Proof: $p_i|\ell$ gives $p_i|n$, so: $p_i^2|\ell^4$, $p_i^2|n^2$, so that $p_i^2|(4p_1p_2/r)m^4$ and $p_i|m$, contradiction.

$W_2: 2\ell^4+2p_1p_2m^4=n^2$, so $2\ell^4\equiv n^2 \pmod{p_1}$. By $(*)$: $p_1\nmid\ell$. $2\equiv(n/\ell^2)^2$, so $\left(\frac{2}{p_1}\right)=1$, impossible since $p_1\equiv 3 \pmod 8$. Hence $2\notin$ im q.

$W_{p_1}: p_1\ell^4+4p_2m^4=n^2$. $p_1\ell^4\equiv n^2 \pmod{p_2}$. By $(*)$: $p_2\nmid\ell$. $p_1\equiv(n/\ell^2)^2$, so $\left(\frac{p_1}{p_2}\right)=1$, impossible since given $\left(\frac{p_1}{p_2}\right)=-1$. Hence $p_1\notin$ im q.

$W_{2p_1}: 2p_1\ell^4+2p_2m^4=n^2$, so $2p_1\ell^4\equiv n^2 \pmod{p_2}$. By $(*)$: $p_2\nmid\ell$. $2p_1\equiv(n/\ell^2)^2$, so $\left(\frac{2p_1}{p_2}\right)=1$, impossible since $\left(\frac{2p_1}{p_2}\right)=\left(\frac{2}{p_2}\right)\left(\frac{p_1}{p_2}\right)=1\cdot(-1)=-1$. Hence $2p_1\notin$ im q.

So: im $q=\{1,p_1p_2\}$ and $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))=\{\mathbf{o},(0,0)\}=\langle(0,0)\rangle\cong C_2$.
Step 2. Find $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$. Here $\hat{q}:\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))\longrightarrow\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Note $\hat{q}:(0,0)\mapsto b=-p_1p_2$ and $r|b$, so that $\{1,-p_1p_2\}\leqslant\{\pm1,\pm p_1,\pm p_2\pm p_1p_2\}$. There are three nontrivial cosets; take $-1,p_1,-p_1$ as representatives. Here $\widehat{W}_r: r\ell^4+a\ell^2m^2+(b/r)m^4=n^2$, some $\ell,m,n\in\mathbb{Z}$, not all 0, with $\gcd(\ell,m)=1$.
Lemma $(**)$. $\widehat{W}_r: r\ell^4-(p_1p_2/r)m^4=n^2$, $i\in\{1,2\}$; if $p_i\nmid r$ then $p_i\nmid\ell$. Proof: $p_i|\ell$ gives $p_i|n$, so: $p_i^2|\ell^4$, $p_i^2|n^2$, so that $p_i^2|(p_1p_2/r)m^4$ and $p_i|m$, contradiction.

$\widehat{W}_{-1}: -\ell^4+p_1p_2m^4=n^2$. $-\ell^4\equiv n^2 \pmod{p_1}$. By $(**)$: $p_1\nmid\ell$. $-1\equiv(n/\ell^2)^2$ so $\left(\frac{-1}{p_1}\right)=1$, impossible since $p_1\equiv 3\pmod 4$. Hence $-1\notin$ im $\hat{q}$.

$\widehat{W}_{p_1}: p_1\ell^4-p_2m^4=n^2$. $p_1\ell^4\equiv n^2\pmod{p_2}$. By $(**)$: $p_2\nmid\ell$. $p_1\equiv(n/\ell^2)^2$ so $\left(\frac{p_1}{p_2}\right)=1$, impossible since given $\left(\frac{p_1}{p_2}\right)=-1$. Hence $p_1\notin$ im $\hat{q}$.

$\widehat{W}_{-p_1}: -p_1\ell^4+p_2m^4=n^2$. $-p_1\ell^4\equiv n^2\pmod{p_2}$. By $(**)$: $p_2\nmid\ell$. $-p_1\equiv(n/\ell^2)^2$ so $\left(\frac{-p_1}{p_2}\right)=1$, impossible since $\left(\frac{-p_1}{p_2}\right)=\left(\frac{-1}{p_2}\right)\left(\frac{p_1}{p_2}\right)=1\cdot(-1)=-1$. Hence $-p_1\notin$ im $\hat{q}$.

So: im $\hat{q}=\{1,-p_1p_2\}$ and $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))=\{\mathbf{o},(0,0)\}=\langle(0,0)\rangle\cong C_2$.
Step 3. Find $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}))$, which is generated by $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))=\langle(0,0)\rangle$ and $\hat{\phi}\big(\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))\big)=\hat{\phi}\big(\langle(0,0)\rangle\big)=\{\mathbf{o}\}$, since $\hat{\phi}:(0,0)\mapsto\mathbf{o}$. Hence $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}))=\langle(0,0)\rangle\cong C_2$. From lectures, $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}))\cong\mathcal{C}(\mathbb{Q})[2]\times C_2^r$. Here $\mathcal{C}(\mathbb{Q})[2]=\{\mathbf{o},(0,0)\}\cong C_2$, since $(\pm\sqrt{p_1p_2},0)\notin\mathcal{C}(\mathbb{Q})$. Hence the rank is 0. [**10 marks**; Unseen.]