Solution to Question 1.

(a) [*Proof from lectures*]. We are given: $|f(a_0)| < |f'(a_0)|^2$ $(*)$. Define $f_j(x)$ by: $f(x+y) = f_0(x) + f_1(x)y + f_2(x)y^2 + \ldots$, 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:

$|f'(a_1) - f'(a_0)| = |f'(a_0 + b_0) - f'(a_0)| = |(\text{poly in } a_0)b_0 + (\text{poly in } a_0)b_0^2 + \ldots|$
$\leqslant |b_0| < |f'(a_0)|$ (by $(*)$), so that $|f'(a_1)| = |f'(a_0)|$.

Also, $|f(a_1)| = |f(a_0 + b_0)| = |f_0(a_0) + f_1(a_0)b_0 + f_2(a_0)b_0^2 + \ldots|$
$= |f_2(a_0)b_0^2 + \ldots|$ [since $f_0(a_0) + f_1(a_0)b_0 = 0$] $\leqslant |b_0|^2 = \frac{|f(a_0)|^2}{|f'(a_0)|^2}$
$= \rho|f(a_0)| < |f(a_0)|$, 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:

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

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

Then $|f(a_{n+1})| \leqslant |b_n|^2$ [justified as for $n = 0$ above] $= \frac{|f(a_n)|^2}{|f'(a_n)|^2}$
$= \frac{|f(a_n)|^2}{|f'(a_0)|^2}$ [by (1)] $\leqslant \frac{|f(a_0)|}{|f'(a_0)|^2}|f(a_n)|$ [by (1)] $= \rho|f(a_n)| \leqslant \rho^{n+1}|f(a_0)|$ [by (1)].

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 thm from lectures that a series converges in a non-Archimedean field iff its terms converge to 0]:

$a_n = a_0 + b_0 + b_1 + \ldots + b_n$ 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)].

For uniqueness, imagine that $\hat{a} \neq a$ also satisfied $f(\hat{a}) = 0$ and that:

$|\hat{a} - a_0| \leqslant |f(a_0)|/|f'(a_0)|$. Let $\hat{b} = \hat{a} - a \neq 0$.

Then $0 = f(\hat{a}) - f(a) = f(a + \hat{b}) - f(a) = \hat{b}f_1(a) + \hat{b}^2 f_2(a) + \ldots$ (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]**

(b) For any $x \in \mathbb{Z}$, if $11|x$ then $x^{10} \equiv 0 \pmod{11}$, and if $11 \nmid x$ then $x^{10} \equiv 1 \pmod{11}$ by Fermat's Little Theorem. So always $x^{10} \not\equiv 2 \pmod{11}$. Hence $|x^{10} - 2|_{11} = 1$ and so $|x^{10} - 2|_{11} \not\leqslant 11^{-3}$.

For any $x \in \mathbb{Z}$, $|x|_p = p^{-n}$, some $n \in \mathbb{Z}$, $n \geqslant 0$. Hence $|x^p|_p = p^{pn}$. Also $|p|_p = p^{-1}$, so $|x^p|_p \neq |p|_p$ and $|x^p - p|_p = \max(|x^p|_p, |p|_p) \geqslant |p|_p = p^{-1}$, using the theorem: $|\alpha|_p \neq |\beta|_p \implies |\alpha \pm \beta|_p = \max(|\alpha|_p, |\beta|_p)$. Hence $|x^p - p|_p \not\leqslant p^{-2}$.

Let $f(x) = x^2 + 2$, and take $x_0 = a_0 = 1$. Then $|x_0^2 + 2|_3 = 3^{-1}$. We want $x_1 = a_0 + a_1 3^1$ such that $|x_1^2 + 2|_3 \leqslant 3^{-2}$, that is: $(a_0 + a_1 3^1)^2 \equiv -2 \pmod{3^2}$ $\iff$ $1 + 2a_1 3^1 \equiv -2 \pmod{3^2}$ $\iff$ $2a_1 3^1 \equiv -3 \pmod{3^2}$ $\iff$ $2a_1 \equiv -1 \pmod{3}$. So take $a_1 = 1$ and $x_1 = a_0 + a_1 3^1 = 1 + 1 \cdot 3^1 = 4$.

We next want $x_2 = a_0 + a_1 3^1 + a_2 3^2$ such that $|x_2^2 + 2|_3 \leqslant 3^{-3}$, that is: $(a_0 + a_1 3^1 + a_2 3^2)^2 \equiv -2 \pmod{3^3} \iff 4^2 + 2 \cdot 4 a_2 3^2 \equiv -2 \pmod{3^3} \iff 8 a_2 3^2 \equiv -18 \pmod{3^3} \iff 8 a_2 \equiv -2 \pmod 3$. So take $a_2 = 2$ and $x_2 = a_0 + a_1 3^1 + a_2 3^2 = 22$. Note that already $|x_2^2 + 2|_3 = |484 + 2|_3 = |486|_3 = |2 \cdot 3^5|_3 = 3^{-5}$, so we can take $x = 22$ as our solution.

Let $f(x) = x^2 + 7$, and take $x_0 = 1$, so that $|f(x_0)|_2 = |1^2 + 7|_2 = 2^{-3}$ and $f'(x) = 2x$, so that $|f'(x_0)|_2 = 2^{-1}$. We use the method in the proof of Hensel's lemma. Let $x_1 = x_0 - f(x_0)/f'(x_0) = 1 - (1^2 + 7)/(2 \cdot 1) = 1 - 4 = -3$. Then $|f(x_1)|_2 = |(-3)^2 + 7|_2 = |16|_2 = 2^{-4}$. Let $x_2 = x_1 - f(x_1)/f'(x_1) = -3 - \big((-3)^3 + 7\big)/\big(2 \cdot (-3)\big) = -3 - 16/(-6) = -1/3$. Then $|f(x_2)|_2 = |(-1/3)^2 + 7|_2 = |64/9|_2 = 2^{-6}$. Let $x_3 = x_2 - f(x_2)/f'(x_2) = -1/3 - \big((-1/3)^2 + 7\big)/\big(2 \cdot (-1/3)\big) = -1/3 + (64/9)/(2/3) = 31/3$. Then $|f(x_3)|_2 = |(31/3)^2 + 7|_2 = |(31 + 96)/9|_2 = |1024/9|_2 = 2^{-10}$. So, we can take $x = 31/3$ as a solution (there are also integer solutions: $\pm 181, \pm 331, \pm 693, \pm 843$). [**8 marks**; Seen similar types of examples]

(c) Let $\mathcal{C} : Y^2 = f(X) = p_1 X^4 - p_1 p_2^2 p_3^2 = p_1 (X^2 + p_2 p_3)(X^2 - p_2 p_3)$, so $f'(X) = 4 p_1 X^3$. Any repeated root x_0 of $f(X)$ must satisfy $f(x_0) = f'(x_0) = 0$, and so $0 = 4(p_1 x_0^4 - p_1 p_2^2 p_3^2) - x_0 (4 p_1 x_0^3) = -4 p_1 p_2^2 p_3^2$. So $\widetilde{\mathcal{C}}$ over $\mathbb{F}_p$ (for $p \neq 2, p_1, p_2, p_3$) has $\tilde{f}(x)$ with no repeated roots, so by a theorem from lectures, $\widetilde{\mathcal{C}}(\mathbb{F}_p)$ has at least $p - 1 - 2\sqrt{p}$ affine points; if also $p \geqslant 7$ this is positive, so there is an affine point $(x_1, y_1) \in \widetilde{\mathcal{C}}(\mathbb{F}_p)$, which is nonsingular (since $\tilde{f}(x)$ has no repeated roots), and so lifts to a point $(x_2, y_2) \in \mathcal{C}(\mathbb{Q}_p)$ (by the theorem that any nonsingular point on $\widetilde{\mathcal{C}}(\mathbb{F}_p)$ lifts to a point on $\mathcal{C}(\mathbb{Q}_p)$). This shows the result for all $p \notin \{2, 3, 5, p_1, p_2, p_3\}$.

For $p = 2$, note that $p_2 p_3 \equiv 1 \pmod 8$, so $p_2 p_3 \in (\mathbb{Q}_2^*)^2$ [by Cor to HL], so there exists $x_3 \in \mathbb{Q}_2$ such that $x_3^2 = p_2 p_3$, and we can take $x = x_3, y = 0$ as a solution. For $p = 3$, note that $p_2 p_3$ or $-p_2 p_3 \equiv 1 \in (\mathbb{F}_3^*)^2$, so by Cor to HL, $-p_2 p_3$ or $p_2 p_3 \in (\mathbb{Q}_3^*)^2$, so there exists $x_4 \in \mathbb{Q}_3$ such that $x_4^2 = -p_2 p_3$ or $p_2 p_3$, and we can take $x = x_4, y = 0$ as a solution.

For $p = p_1$, we are given $p_2, p_3 \in (\mathbb{F}_{p_1}^*)^2$ and so $p_2 p_3 \in (\mathbb{F}_{p_1}^*)^2$, so by Cor to HL, $p_2 p_3 \in (\mathbb{Q}_{p_1}^*)^2$. Then there exists $x_5 \in \mathbb{Q}_{p_1}^*$ such that $x_5^2 = p_2 p_3$ and we can take $x = x_5, y = 0$ as a solution.

For $p = p_2$, let $x_6 = 1 \in \mathbb{Q}_{p_2}^*$. Then $f(x_6) = p_1 (1 + p_2 p_3)(1 - p_2 p_3) \equiv p_1 \in (\mathbb{F}_{p_2}^*)^2$, so by Cor to HL, $p_1 (1 + p_2 p_3)(1 - p_2 p_3) \in (\mathbb{Q}_{p_2}^*)^2$. Then there exists $\beta \in \mathbb{Q}_{p_2}^*$ such that $\beta^2 = p_1 (1 + p_2 p_3)(1 - p_2 p_3)$, and $x = x_6 = 1, y = \beta$ is a solution. The argument for $p = p_3$ is the same.

For $p = 5$, if some $p_i = 5$ then we are already covered by the above cases $p = p_1, p_2$ or p_3, so assume $p_1 \neq 5$, $p_2 \neq 5$, $p_3 \neq 5$. Then $p_2 p_3 \not\equiv 0 \pmod 5$. If $p_2 p_3 \equiv 1$ or $4 \pmod 5 \in (\mathbb{F}_5^*)^2$ then (by Cor to HL) there exists $x_7 \in \mathbb{Q}_5^*$ such that $x_7^2 = p_2 p_3$ and $x = x_7, y = 0$ is a solution. So assume $p_2 p_3 \equiv 2$ or 3, so that $p_2^2 p_3^2 \equiv 4 \pmod 5$ and $f(x) \equiv p_1 (x^4 + 1) \pmod 5$. If $p_1 \in (\mathbb{F}_5^*)^2$ then (by Cor to HL) there exists $\gamma \in \mathbb{Q}_5^*$ such that $\gamma^2 = p_1$ so that $x = 0, y = \gamma$ is a solution; if $p_1 \notin (\mathbb{F}_5^*)^2$ then $2 p_1 \in (\mathbb{F}_5^*)^2$ (since $2 \notin (\mathbb{F}_5^*)^2$) so by Cor to HL, there exists $\delta \in \mathbb{Q}_5^*$ such that $\delta^2 = 2 p_1$, so $x = 1, y = \delta$ is a solution. [**7 marks**; Unseen]

Solution to Question 2

(a) [*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. **[8 marks]**

(b) For $\mathcal{E} : Y^2 = X^3 - 3$, we have $\Delta = 4 \cdot 0^3 + 27 \cdot (-3)^2 = 3^5$. Let $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$. By Nagell-Lutz, $x, y \in \mathbb{Z}$ and $y = 0$ or $y^2|\Delta$, so $y \in \{0, \pm 1, \pm 3, \pm 9\}$. Hence $x^3 = y^2 + 3 \in \{3, 4, 12, 84\}$, a contradiction, since these are not cubes. Hence $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is the trivial group $\{\mathbf{o}\}$.

Let $p > 3$. Then $p \equiv 1$ or $2 \pmod 3$.

When $p \equiv 1 \pmod 3$, then:

$p \equiv 1 \pmod 4 \implies \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ [by QR] $= \left(\frac{1}{3}\right) = 1.$

$p \equiv 3 \pmod 4 \implies \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = -\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ [by QR] $= \left(\frac{1}{3}\right) = 1.$

In all cases $\left(\frac{-3}{p}\right) = 1$, so there exists $\alpha \in \mathbb{F}_p$ such that $\alpha^2 = -3$. Then $(0, \alpha) \in \widetilde{\mathcal{E}}(\mathbb{F}_p)$ and the line $Y = \alpha$ substituted into $\widetilde{\mathcal{E}}$ gives: $\alpha^2 = X^3 - 3$, so $X^3 = 0$, so that $Y = \alpha$ intersects $\widetilde{\mathcal{E}}$ three times at $(0, \alpha)$. Hence $3(\alpha, 0) = \mathbf{o}$ (and $(\alpha, 0) \neq \mathbf{o}$), so $(\alpha, 0)$ has order 3, giving: $3|\#\widetilde{\mathcal{E}}(\mathbb{F}_p)$.

When $p \equiv 2 \pmod 3$, then: $\gcd(3, p - 1) = 1$, so there exist $\lambda, \mu \in \mathbb{Z}$ such that $3\lambda + (p - 1)\mu = 1$. For any $x_1, x_2 \in \mathbb{F}_p^*$ we have:

$x_1^3 = x_2^3 \implies x_1^3 = x_2^3$ and $x_1^{p-1} = x_2^{p-1}$ (by FLT)

$\implies x_1^{3\lambda} x_1^{(p-1)\mu} = x_1^{3\lambda} x_1^{(p-1)\mu} \implies x_1^{3\lambda+(p-1)\mu} = x_1^{3\lambda+(p-1)\mu} \implies x_1 = x_2.$

Hence the map $x \mapsto x^3$ is injective and so surjective : $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$. Also: $0 \mapsto 0$, so that $x \mapsto x^3$ is a bijection : $\mathbb{F}_p \longrightarrow \mathbb{F}_p$. Then, for all $y = 0, 1, \ldots, p-1 \in \mathbb{F}_p$ there exists a unique $x \in \mathbb{F}_p$ such that $x^3 = y^2 + 3$. Hence there are precisely p affine points, and so $\widetilde{\mathcal{E}}(\mathbb{F}_p)$ (including $\mathbf{o}$, the point at infinity) satisfies $\widetilde{\mathcal{E}}(\mathbb{F}_p) = p+1 \equiv 0 \pmod 3$, so that again: $3|\#\widetilde{\mathcal{E}}(\mathbb{F}_p)$. [**7 marks**; Unseen]

(c) Let $\mathcal{E} : Y^2 = X^3 + X^2 - X$. Then $(0, 0) \in \mathcal{E}(\mathbb{Q})$ has order 2, so $(0, 0) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$. Calculate $2(1, 1)$, as follows. $2YY' = 3X^3+2X-1$, so that $Y' = 4/2 = 2$ at $(1, 1)$, and so $Y = 2X - 1$ is the line tangent to $\mathcal{E}$ at $(1, 1)$. Substituting $Y = 2X-1$ into $\mathcal{E}$ gives: $(2X-1)^2 = X^3+X^2-X$, and so: $X^3-3X^2+\ldots = 0$. Hence the x-coordinate of $2(1, 1)$ is: $3 - 1 - 1 = 1$. So, the third point of intersection is $(1, 1)$, giving $2(1, 1) = (1, -1)$ and $3(1, 1) = \mathbf{o}$. So $(1, 1)$ is of order 3 and $(1, 1) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$.

Hence:
$\{\mathbf{o}, (1,1), (1,-1), (0,0), (0,0)+(1,1) = (-1,1), (0,0)+(1,-1) = (-1,-1)\}$
$\leqslant \mathcal{E}_{\text{tors}}(\mathbb{Q})$.
Also, $\mathcal{E} : Y^2 = X(X^2+X-1)$ and the discriminant of X^2+X-1 is 5, so there are no repeated roots of $\tilde{f}(x)$ when $p \neq 5$ and $\widetilde{\mathcal{E}}$ is nonsingular when $p \neq 2, 5$. Hence 3 is a prime of good reduction, and we find that:
$\widetilde{\mathcal{E}}(\mathbb{F}_3) = \{\mathbf{o}, (1,1), (1,2), (0,0), (2,1), (2,2)\}$,
so that $\#\widetilde{\mathcal{E}}(\mathbb{F}_p) = 6$. By a theorem from lectures, $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) | \#\widetilde{\mathcal{E}}(\mathbb{F}_p) = 6$. Hence:
$\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\mathbf{o}, (1,1), (1,-1), (0,0), (-1,1), (-1,-1)\}$. [**6 marks**; Seen similar]

(d) Imagine $|x| > \max(2|A|, |\Delta| + |B|)$. Then:
$|y^2| = |x^3 + Ax + B| \geqslant |x|^3 - |A||x| - |B| = |x|^2|x| - |A||x| - |B|$
$> 4|A|^2|x| - |A||x| - |B| \geqslant 4|A||x| - |A||x| - |B|$ [since $A \in \mathbb{Z}$]
$= 3|A||x| - |B| \geqslant |x| - |B| \geqslant (|\Delta| + |B|) - |B| = |\Delta|$,
a contradiction with Nagell-Lutz. [**4 marks**; Unseen]

Solution to Question 3

(a) [*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: $u^2 + a_1u + b_1 = rs^2, u = rt^2$, for some $s, t \in \mathbb{Q}$. Hence: $(rt^2)^2 + a_1(rt^2) + b_1 = rs^2$. Let $t = \ell/m$, where $\ell, m \in \mathbb{Z}$, $\gcd(\ell, m) = 1$. 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: $n = m^2s \in \mathbb{Z}$. Then our equation becomes:

$$r^2\ell^4 + a_1r\ell^2m^2 + b_1m^4 = rn^2, \quad \text{for some } \ell, m, n \in \mathbb{Z},\ \gcd(\ell, m) = 1. \quad (\dagger).$$

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 $p \nmid b_1$, for some prime p. Then $p|r^2\ell^4, a_1r\ell^2m^2, rn^2$ and so by $(\dagger)$, $p|b_1m^4$, which in turn gives: $p|m$ [since $p \nmid b_1$]. Hence, since now $p|r$ and $p|m$, we have: $p^2|r^2\ell^4, a_1r\ell^2m^2, b_1m^4$, 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: $p^3|a_1r\ell^2m^2, b_1m^4, rn^2$, 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 $p \nmid b_1$ let to a contradiction, and so it is impossible for any prime p to satisfy $p|r$ and $p \nmid b_1$. 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 **[9 marks]**

(b) Let $\mathcal{C} : Y^2 = X(X^2 - X - 1)$. Here, $a = -1, b = -1$ and so $a_1 = -2a = 2, b_1 = a^2 - 4b = 5$, giving $\mathcal{D} : V^2 = U(U^2 + 2U + 5)$.

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 $r|b_1 = 5, r \in \mathbb{Z}$, r square free, that is, $\operatorname{im} q \leqslant \{\pm 1, \pm 5\}$. But $q(\mathbf{o}) = 1$, $q(0, 0) = b_1 = 5$, so that $\{1, 5\} \leqslant \operatorname{im} q$. There is one nontrivial coset: -1. Then $W_r : r\ell^4 + a_1\ell^2m^2 + (b_1/r)m^4 = n^2$, for some $\ell, m, n \in \mathbb{Z}$, not all 0, with $\gcd(\ell, m) = 1$ becomes: $W_{-1} : -\ell^4 + 2\ell^2m^2 - 5m^4 = n^2$. On completing the square: $-(\ell^2 - m^2)^2 - 4m^4 = n^2$. Then LHS $\leqslant 0$ and RHS $\geqslant 0$ and both sides are equal only when $\ell = m = n = 0$, impossible. Hence $-1 \notin \operatorname{im} q$, giving $\operatorname{im} q = \{1, 5\}$ and $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \langle(0, 0)\rangle \cong C_2$.

Step 2. Find $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$. Here $\hat{q} : \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Consider $r|b = -1, r \in \mathbb{Z}$, r square free, that is, $\operatorname{im} \hat{q} \leqslant \{\pm 1\}$. But $\hat{q}(\mathbf{o}) = 1$, $\hat{q}(0, 0) = b = -1$, Hence $\operatorname{im} \hat{q} = \{\pm 1\}$ and $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \langle(0, 0)\rangle \cong C_2$.

Step 3. Find $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}))$, which is generated by $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \{\mathbf{o}, (0, 0)\}$ 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 $((1 \pm \sqrt{5})/2, 0) \notin \mathcal{C}(\mathbb{Q})$. Hence the rank is 0. [**7 marks**; Seen similar.]

(c) Let $\mathcal{C} : Y^2 = X(X^2 + p)$. Here, $a = 0, b = p$ and so $a_1 = -2a = 0, b_1 = a^2 - 4b = -4p$, giving $\mathcal{D} : V^2 = U(U^2 - 4p)$.

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 $r|b_1 = -4p, r \in \mathbb{Z}$, r square free, that is, im $q \leqslant \{\pm 1, \pm 2, \pm p, \pm 2p\}$. But $q(\mathbf{o}) = 1$, $q(0,0) = b_1 = -4p = -p$, so that $\{1, -p\} \leqslant$ im q. There are three nontrivial coset: $-1, 2, -2$. Then $W_r : r\ell^4 + a_1\ell^2m^2 + (b_1/r)m^4 = n^2$, for some $\ell, m, n \in \mathbb{Z}$, not all 0, with $\gcd(\ell, m) = 1$ becomes: $W_{-1} : -\ell^4 + 4pm^4 = n^2$. Imagine $p \nmid \ell$. Then $-1 \equiv (n/\ell)^2 \pmod p$, and so $\left(\frac{-1}{p}\right) = 1$, impossible since we are given $p \equiv 3 \pmod 4$, and so $p|\ell$. Hence $p|n$ and so, $p^2|\ell^4$, $p^2|n^2$, giving $p^2|4pm^4$ and so $p|m$, a contradiction. Hence $-1 \notin$ im q.

Now consider $W_2 : 2\ell^2 - 2pm^4 = n^2$ and $W_{-2} : -2\ell^4 + 2pm^4 = n^2$.

We are given that $p \equiv 3 \pmod 4$, so either $p \equiv 3 \pmod 8$ or $p \equiv 7 \pmod 8$.
Case $p \equiv 3 \pmod 8$. Then $\left(\frac{2}{p}\right) = -1$. Consider W_2 above. Imagine $p \nmid \ell$. Then W_2 gives $2 \equiv (n/\ell^2)^2 \pmod p$, impossible, so that $p|\ell$. Hence $p|n$ and so, $p^2|\ell^4$, $p^2|n^2$, giving $p^2|2pm^4$ and so $p|m$, and contradiction. Hence $2 \notin$ im q. So $\langle -p\rangle \leqslant$ im $q \leqslant \langle -p, -2\rangle$.
Case $p \equiv 7 \pmod 8$. Then $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = -1 \cdot 1 = -1$. Consider W_{-2} above. Imagine $p \nmid \ell$. Then W_{-2} gives $-2 \equiv (n/\ell^2)^2 \pmod p$, impossible, so that $p|\ell$. Hence $p|n$ and so, $p^2|\ell^4$, $p^2|n^2$, giving $p^2|2pm^4$ and so $p|m$, and contradiction. Hence $-2 \notin$ im q. So $\langle -p\rangle \leqslant$ im $q \leqslant \langle -p, 2\rangle$.

In either case, $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \langle(0,0)\rangle$ or $\langle(0,0), R\rangle$, for some $R \in \mathcal{D}(\mathbb{Q})$.

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 $r|b = p, r \in \mathbb{Z}$, r square free, that is, im $\hat{q} \leqslant \{\pm 1, \pm p\}$. But $\hat{q}(\mathbf{o}) = 1$, $\hat{q}(0,0) = b = p$, so that $\{1, p\} \leqslant$ im $\hat{q}$. There is one nontrivial coset: -1. Then $\widehat{W}_r : r\ell^4 + a\ell^2m^2 + (b/r)m^4 = n^2$ for some $\ell, m, n \in \mathbb{Z}$, not all 0, $\gcd(\ell, m) = 1$. Then for $\widehat{W}_{-1} : -\ell^4 - pm^4 = n^2$ we see that LHS $\leqslant 0$ and RHS $\geqslant 0$, and both sides are equal only when $\ell = m = n = 0$, a contradiction. It follows that $-1 \notin$ im $\hat{q}$. Hence im $\hat{q} = \{1, p\}$ and $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \{\mathbf{o}, (0,0)\} = \langle(0,0)\rangle$.

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 $\hat{\phi}\big(\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))\big) = \hat{\phi}\big(\langle(0,0)\rangle\big) = \{\mathbf{o}\}$ or $\hat{\phi}\big(\langle(0,0), R\rangle\big) = \langle\hat{\phi}(R)\rangle$, since $\hat{\phi} : (0,0) \mapsto \mathbf{o}$. Hence $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})) \cong C_2$ or $C_2 \times C_2$. 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 $(\pm\sqrt{-p}, 0) \notin \mathcal{C}(\mathbb{Q})$. Hence the rank is 0 or 1.

Now assume that $p \equiv 7 \pmod{16}$. Then $p \equiv 7 \pmod 8$ and by the above argument (using the second case), im $q \leqslant \langle -p, 2\rangle$ and:

rank $= 0 \iff \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \langle(0,0)\rangle \iff$ im $q = \langle -p\rangle \iff 2 \notin$ im q. So, sufficient to show $2 \notin$ im q. Recall $W_2 : 2\ell^2 - 2pm^4 = n^2$. Then $2|n$, so write $n = 2n'$, some $n' \in \mathbb{Z}$, giving: $\ell^4 - pm^4 = 2n'^2$, so: $2|\ell \iff 2|m$; but $\gcd(\ell, m) = 1$, so $2 \nmid \ell$ and $2 \nmid m$. Hence $\ell^2 \equiv 1 \pmod 8$, so $\ell^2 \equiv 1$ or 9 and $\ell^4 \equiv 1 \pmod{16}$; similarly $m^4 \equiv 1 \pmod{16}$. Then LHS $= \ell^4 - pm^4 \equiv 1 - p \equiv 1 - 7 \equiv -6 \equiv 10 \pmod{16}$, giving: $10 \equiv 2n'^2 \pmod{16}$, so $5 \equiv n'^2 \pmod 8$. But $n'^2 \equiv 0, 1$ or $4 \pmod 8$, a contradiction. Hence $2 \notin$ im q and the rank is 0, as required. [**9 marks**; Unseen.]
