1. (a) State and prove Hensel's Lemma.

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

Proof. [*From lectures*] 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 $f_0(a_0) + f_1(a_0)b_0 = 0$]
$\leqslant \max_{j \geqslant 2}|f_j(a_0)||b_0|^j \leqslant |b_0|^2 = \frac{|f(a_0)|^2}{|f'(a_0)|^2} = \rho|f(a_0)| < |f(a_0)|$, 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:
$|f'(a_n)| = \ldots = |f'(a_1)| = |f'(a_0)|$ 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 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]:
$a_n = a_0 + b_0 + b_1 + \ldots + b_n$ 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)], 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 $0 = f(\hat{a}) - f(a) = f(a + \hat{b}) - f(a) = \hat{b}f_1(a) + \hat{b}^2 f_2(a) + \ldots$ (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)
(i) Which numbers $a \in \mathbb{Q}_2$ have cube roots in $\mathbb{Q}_2$?

[*Similar seen in problem sheet*]
Obviously, $a = 0$ has a cube root. If $a \neq 0$, then we will have $a = b^3$ if and only if $a = 2^{3n}u$ where u is a unit in $\mathbb{Z}_2$ that has a cube root. But $u \equiv 1 \mod 2$, so If we put $f(x) = x^3 - u$, then $x = 1$ will be a root of $f \mod 2$, and $f'(1) = 3$. Hence, $|f(1)|_2 < 1$, while $|f'(1)|_2 = 1$. Thus, $|f(1)|_2 < |f'(1)|^2$,

and Hensel's Lemma applies to give us a root α of $f(x)$ in $\mathbb{Z}_2$. That is, all units in $\mathbb{Z}_2$ will have cube roots. Therefore, $a \in \mathbb{Q}_2^\times$ has a cube root if and only if $a = 2^{3n}u$ whre u is any unit.

[2 marks]

(ii)
Which numbers $a \in \mathbb{Q}_3$ have cube roots in $\mathbb{Q}_3$?

[*Similar seen in problem sheet*]
Obviously, $a = 0$ has a cube root. If $a \neq 0$, then a has a cube root if and only if $a = 3^{3n}u$ where $u \in \mathbb{Z}_3$ is a unit that has a cube root. If u has a cube root, then $u \mod 3^m$ has a cube root for every m, and hence, $u \mod 27$ has a cube root. Conversely, suppose $u \mod 27$ has a cube root. So there is a $b \in \mathbb{Z}_3$ such that $b^3 \equiv u \mod 27$. If we define $f(x) = x^3 - u$, then $|f(b)|_3 \leq 3^{-3}$. Now, since u is a unit, b is also a unit. Hence, since $f'(b) = 3b$, we $|f'(b)|_3 = 3^{-1}$. Therefore, $|f(b)|_3 < |f'(b)|^2$. By Hensel's lemma, f would then have a root in $\mathbb{Z}_3$, which would then be a cube root of u. To sum, $a \in \mathbb{Q}_3^\times$ has a cube root if and only if $a = 3^{3n}u$ where u is a unit in $\mathbb{Z}_3$ such that $u \mod 27$ has a cube root. Which units of $\mathbb{Z}/27$ have cube roots? To find this out, first compute the cubes in $(\mathbb{Z}/9)^\times$. We quickly see that the only possibilities are $\pm 1 \mod 9$. Thus, the cubes in $(\mathbb{Z}/27)^\times$ must be among $1, 8, 10, -10, -8, -1$. Clearly, all are cubes except possibly ± 10. But $4^3 \equiv 10 \mod 27$ and $(-4)^3 \equiv -10 \mod 27$. Therefore, $a \in \mathbb{Q}_3^\times$ has a cube root if and only if $a = 3^{3n}u$ where $u \in \mathbb{Z}_3^\times$ is congruent to $\pm 1 \mod 9$.

[3 marks]

(iii)
How many solutions are there to

$$x^{37} - x = 37$$

in $\mathbb{Q}_{37}$?

[*unseen*]
Let $f(x) = x^{37} - x - 37$. For $a = 0, 1, \ldots, 36$, we have $f(a) \equiv 0 \mod 37$. On the other hand, $f'(a) = 37a^{36} - 1 \equiv -1 \mod 37$. Therefore, for each such a, we have $|f(a)|_{37} < 1 = |f'(a)|_{37}^2$. Therefore, for each such a, there exists an α that is a root of $f(x)$ such that $|\alpha - a|_{37} \leq |f(a)|_{37}/|f'(a)|_{37} < 1$. That is, each α is congruent $\mod 37$ to a. In particular, all these roots are distinct. Therefore, $f(x)$ has at least 37 distinct roots. Obviously, it can't have more, since $\mathbb{Q}_{37}$ is a field. Therefore, the equation has exactly 37 solutions.

[3 marks]

(c)
Consider the equation

$$y^2 = x^3 + 6.$$

Find all p for which the equation has a solution in $\mathbb{Z}_p$.
[*Warning: You are not allowed to use the point at 'infinity'.*]
[*You may use standard facts from the lectures as long as they are stated clearly.*]

[*Similar seen in lecture*]
If we take $x = 3$, then we get the equation $y^2 = 33$, which gives $y^2 \equiv 1 \mod 8$. Thus, 33 has a square root mod 8, and hence, a square root in $\mathbb{Z}_2$. Therefore, there is a solution in $\mathbb{Z}_2$.
If we take $x = 1$, then we get $y^2 = 7$, which is $y^2 \equiv 1 \mod 3$. Thus, 7 has a square root mod 3, and hence, a square root in $\mathbb{Z}_3$. So the equation has a solution in $\mathbb{Z}_3$. Taking $x = 0$, we get $y^2 = 6$, which becomes $y^2 \equiv 1 \mod 5$. Hence, 6 has a square root mod 5, and therefore, a square root in $\mathbb{Z}_5$.
If we take $y = 0$, then we get the equation $0 = x^3 + 6$ or $x^3 - 1 \equiv 0 \mod 7$. This clearly has the root 1 mod 7, and hence, has a root in $\mathbb{Z}_7$. Therefore, the equation has a solution in $\mathbb{Z}_7$.

Consider now the situation of $\mathbb{Z}_p$ for $p \geq 11$. The discriminant of the equation is 27×6 so the corresponding elliptic curve only has bad reduction at 2 and 3. Thus, for all prime $p \geq 11$, we will get an elliptic curve upon reduction mod p, which has numbers of point $\geq p + 1 - 2\sqrt{p}$. For $p \geq 11$ this is always greater than 4. Hence, the elliptic curve will have some point (x_0, y_0) in $\mathbb{F}_p$ such that $y_0 \neq 0$. Now let (x, y) be a pair in $\mathbb{Z}_p$ that lifts the pair (x_0, y_0) and consider the polynomial $h(t) = t^2 - (x^3 + 6)$. Clearly, $|h(y)|_p < 1$ and $h'(y) = 2y$ is non-zero mod p, and hence, $|h'(y)|_p = 1$. Therefore, by Hensel's Lemma, $h(t)$ has a root y_1 in $\mathbb{Z}_p$, upon which (x, y_1) will be a solution of our original equation in $\mathbb{Z}_p$.
To conclude, the equation has solutions in $\mathbb{Z}_p$ for all primes p.

[7 marks]

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

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

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 $a = Q(0)$.

□

[8 marks]

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

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. □

[7 marks]

(c) Let $\mathcal{E}$ be given by an equation

$$\mathcal{E} : y^2 = x^3 + (3m+1)x + 9n^2,$$

where the polynomial $x^3 + (3m+1)x + 9n^2$ has no rational root. Prove that $\mathcal{E}(\mathbb{Q})$ is infinite.

[*unseen*]
Reducing mod 3, we get the equation

$$y^2 = x^3 + x$$

which defines an elliptic curve over $\mathbb{F}_3$. This curve has the four points $\underline{\mathbf{o}}, (0,0), (2, \pm 1)$. Since $\mathcal{E}_{tor}(\mathbb{Q})$ admits an injective homomorphism to $\mathcal{E}(\mathbb{F}_3)$, we see that $\mathcal{E}_{tor}(\mathbb{Q})$ has order at most four. Hence, the only possible points of finite order must have order 2 or 4. But $\mathcal{E}(\mathbb{Q})$ clearly has no points of order 2, since $x^3 + (3m+1)x + 9n^2$ is assumed to have no rational roots. Hence, $\mathcal{E}_{tor}(\mathbb{Q}) = \underline{\mathbf{o}}$. On the other hand, the curve has the obvious point $(0, 3n)$, which must then be a point of infinite order.
[5 marks]

(d) Let $\mathcal{E}$ be given by an equation

$$\mathcal{E} : y^2 = x^3 + ax,$$

where a is a non-zero square-free integer. Show that $\mathcal{E}(\mathbb{Q})$ has no element of order 4.

[*Similar seen in lecture*]
First note: the question should also read that $a \neq \pm 1$. If P were a point of order 4, we would have $2P = (0,0)$, since $(0,0)$ is the only point of order 2. This is saying that the tangent line to $\mathcal{E}$ at P must go through $(0,0)$. Hence, we must consider the non-vertical lines through $(0,0)$ and see which ones are tangent to $\mathcal{E}$ at the other point of intersection. Theses lines have the equation $y = mx$. Thus, we get

$$m^2x^2 = x^3 + ax,$$

and the other points of intersection will have x-coordinates that are the roots of $x^2 - m^2x + a$. This polynomial will have multiple roots if and only if $m^4 - 4a = 0$. Hence, we get
$m = \pm\sqrt{2}a^{1/4}, \pm i\sqrt{2}a^{1/4}$. The x-values at the intersection points in these cases are
$x = m^2/2 = \pm\sqrt{a}$. These values will never be rational. Hence, $\mathcal{E}(\mathbb{Q})$ has no point of order 4.
[5 marks]

3.
Let l be a prime and $\mathcal{E}_l$ be the elliptic curve

$$y^2 = x^3 - l^2x.$$

(a) Find the torsion subgroup $\mathcal{E}_{l,\mathrm{tor}}(\mathbb{Q})$ of the Mordell-Weil group.

[*Similar seen in lecture*]
Note the four points $\underline{\mathbf{o}}$, $(0,0)$, $(\pm l, 0)$ of order two. Consider first the case $l \neq 3$.
Then the equation defines an elliptic curve over $\mathbb{F}_3$. In fact, for any $l \neq 3$, the equation over $\mathbb{F}_3$ is

$$y^2 = x^3 - x.$$

This has the four points $\underline{\mathbf{o}}, (0,0), (2,0), (3,0)$. Since the reduction map defines an injection

$$\mathcal{E}_{l,\mathrm{tor}}(\mathbb{Q}) \hookrightarrow \mathcal{E}(\mathbb{F}_3),$$

we get that

$$\mathcal{E}_{l,\mathrm{tor}}(\mathbb{Q}) = \mathcal{E}(\mathbb{Q})[2] \simeq C_2 \times C_2.$$

Now suppose $l = 3$ and consider the equation

$$y^2 = x^3 - 3^2 x = x^3 + x$$

over $\mathbb{F}_5$ (where it has good reduction). It has the points $\underline{\mathbf{o}}, (0,0), (1,0), (4,0)$. Since we still have an injection

$$\mathcal{E}_{3,\mathrm{tor}}(\mathbb{Q}) \hookrightarrow \mathcal{E}_3(\mathbb{F}_5),$$

we again get

$$\mathcal{E}_{3,\mathrm{tor}}(\mathbb{Q}) = \mathcal{E}_3(\mathbb{Q})[2] \simeq C_2 \times C_2.$$

[5 marks]

(b) If l is a prime, show that the rank of

$$\mathcal{E}_l : y^2 = x^3 - l^2 x$$

is at most two.

[*Similar seen in lecture*]
We have the standard isogeny

$$\phi : \mathcal{E}_l \longrightarrow \mathcal{D}$$

where the latter is defined by

$$y^2 = x^3 + 4l^2 x,$$

and the dual isogeny

$$\hat{\phi} : \mathcal{D} \longrightarrow \mathcal{E}_l.$$

The maps are given by

$$\phi(x,y) = (y^2/x^2, y + 25y/x^2)$$

and

$$\phi(x,y) = ((1/4)(y/x)^2, (1/8)(y - 100y/x^2)).$$

There is the map

$$q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{E}_l(\mathbb{Q})) \hookrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

that takes (u,v) to u if $(u,v) \neq (0,0)$ and $q(0,0) = 4l^2 = 1$. Also,

$$\hat{q} : \mathcal{E}_l(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \hookrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

takes (u,v) to u for $(u,v) \neq (0,0)$ and $\hat{q}(0,0) = -l^2 = -1$. Now $Im(\hat{q})$ is given by square-free integers that divide l, and hence, $\pm 1, \pm l$. Also, $Im(q)$ is given by square-free integers dividing $2l$, that is, $\pm 1, \pm 2, \pm l, \pm 2l$. We have $r \in Im(\hat{q})$ if and only if

$$r^2 s^4 - l^2 m^4 = r n^2$$

admits a solution (s,m,n) such that $gcd(s,m) = 1$. But for $r = 1, -1, l, -l$, we will have the corresponding solutions $(1,0,1)$, $(0,1,l)$, $(1,1,0)$ and $(1,1,0)$. Therefore, $Im(\hat{q}) = \{\pm 1, \pm l\}$. On the other hand, $r \in Im(q)$ if and only if

$$r^2 s^4 + 4l^2 m^4 = r n^2$$

has a solution (s,m,n) such that $gcd(s,m) = 1$. Hence, we must have $r > 0$. That is, $Im(q) \subset \{1, 2, l, 2l\}$.

We conclude that $\mathcal{E}_l(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ has rank 2 and $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{E}_l(\mathbb{Q}))$ has rank at most 2. Therefore, $\mathcal{E}_l(\mathbb{Q})/2\mathcal{E}_l(\mathbb{Q})$ has rank at most 4. Then, since $\mathcal{E}_l(\mathbb{Q})[2] = C_2 \times C_2$, we get that the Mordell-Weil rank is at most 2.

[5 marks]

(c) Compute the rank of

$$\mathcal{E}_5 : y^2 = x^3 - 25x.$$

[*Similar seen in lecture*]
We have seen already that $\mathcal{E}_5(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ has rank 2. Consider $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{E}_5(\mathbb{Q}))$. For each of $r \in \{2, 5, 10\}$ we must consider the equation

$$r^2s^4 + 100m^4 = rn^2.$$

When $r = 2$, this becomes

$$4s^4 + 100m^4 = 2n^2.$$

After replacing r by 2×2^2 and dividing by 4, we get the equation

$$s^4 + 25m^4 = 2n^2.$$

If there were a solution, then we could find one of minimal length. Now, suppose $5 \mid n$. Then we would have $5|s$, after which we would get

$$m^4 + 25(s/5)^4 = 2(n/5)^2,$$

contradicting the minimality. Therefore, 5 does not divide n. But then, reducing mod 5 would give us a square root of 2 in $\mathbb{F}_5$, a contradiction. Therefore, the equation has no solution, that is, $2 \notin Im(q)$.
On the other hand, if we try $r = 5$, we get

$$25s^4 + 100m^4 = 5n^2$$

which clearly has the solution $(1, 1, 5)$. Therefore, $Im(q) = \{1, 5\}$ and $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{E}_5(\mathbb{Q}))$ has rank 1. The point on $\mathcal{D}$ corresponding to $r = 5$ is $(5, 25)$ and we calculate quickly that $\hat{\phi}(5, 25) = (25/4, -75/8)$. This is not a torsion point and contributes a generator to $\mathcal{E}_5/2\mathcal{E}_5$. Therefore, $\mathcal{E}_5/2\mathcal{E}_5$ has rank 3 and $\mathcal{E}_5$ has rank one.

[10 marks]

(d) For $l \equiv 3 \mod 8$, show that $\mathcal{E}_l$ has rank zero.

[*unseen*]
The key again is to analyze $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{E}_l(\mathbb{Q}))$, that is, the equation

$$r^2s^4 + 4l^2m^4 = rn^2,$$

for $r \in \{2, l, 2l\}$. First consider $r = 2$. Then we get as above,

$$s^4 + l^2m^4 = 2n^2.$$

Also as above, we get that when the solution is chosen to have minimal length, $l \nmid n$. Then reducing mod l, 2 would have a square root in $\mathbb{F}_l$, which cannot happen since $l \equiv 3 \mod 8$. Therefore, $2 \notin Im(q)$.

For $r = l$, the equation eventually reduces to

$$s^4 + 4m^4 = ln^2.$$

Again, take a solution of minimal length. If $2|n$, then $2|s$, and we get the equation

$$m^4 + 4(s/2)^4 = l(n/2)^2,$$

contradicting minimality. Therefore, $2 \nmid n$. But then reducing mod 4 would give us a square root of 3 mod 4, a contradiction. Therefore, $l \notin Im(q)$.
Now suppose $2l \in Im(q)$. This gives a solution to the equation

$$4l^2s^4 + 4l^2m^4 = 2ln^2,$$

which then reduces to

$$s^4 + m^4 = 2ln^2,$$

to which we can assume we have a minimal solution. Since, furthermore, $gcd(s, m) = 1$, they cannot both be divisible by l. Hence, neither is divisible by l (by the equation). Thus, we can reduce mod l and get a non-trivial solution in $\mathbb{F}_l$ to the equation

$$s^4 + m^4 = 0.$$

But then, -1 would have a fourth root in $\mathbb{F}_l$ and, a fortiori, a square root. This is impossible for $l \equiv 3$ mod 4. Therefore, $Im(q) = 1$ and $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{E}_l(\mathbb{Q}))$ is trivial. We conclude that

$$\mathcal{E}_l(\mathbb{Q})/2\mathcal{E}_l(\mathbb{Q})$$

has rank 2, and hence, that the Mordell-Weil rank of $\mathcal{E}_l$ is zero.

[5 marks]