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:
$|f'(a_1) - f'(a_0)| = |f'(a_0 + b_0) - f'(a_0)| = |(\text{poly in } a_0)b_0 + (\text{poly in } a_0)b_0^2 + \ldots|$
$\qquad \leqslant |b_0| < |f'(a_0)|$ (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, bookwork]

(b)
Which of the following numbers has a cube root in $\mathbb{Q}_3$? Be sure to justify your answer.

$$(i) \quad 35 \qquad (ii) \quad 132 \qquad (iii) \quad 10/459.$$

(i) 35 is a unit in $\mathbb{Z}_3$ and $35 \equiv 8 \mod 27$. Thus, for $f(x) = x^3 - 35$, we have

$$|f(2)|_3 \leq 1/27 < 1/9 = |f'(2)|_3^2.$$

Therefore, by Hensel's Lemma, $f(x)$ has a root in $\mathbb{Z}_3$, which is a cube root of 35.

(ii) $132 = 3 \times 44$, so that $v_3(132) = 3^{-1}$. If we had $\alpha^3 = 132$, then we would have $|\alpha|_3 = (1/3)^{1/3}$, which is impossible. So 132 has no cube root in $\mathbb{Q}_3$.

(iii) We have $10/459 = 10 \cdot 17^{-1} \cdot 3^{-3}$. Therefore, $10/459$ has a cube root if and only if $10 \cdot 17^{-1}$ has a cube root. Now, $4^3 = 64 = 10 \mod 27$, so 10 has a cube root in $\mathbb{Z}_3$ by considering the polynomial $x^3 - 10$ and using Hensel's Lemma as in (i). Similarly, $17 = -10 = (-4)^3 \mod 27$ so, 17 has a cube root in $\mathbb{Z}_3$. Therefore, $10/17$ has a cube root in $\mathbb{Q}_3$. **[5 marks, unseen]**

(c)
Prove that $2y^2 = x^4 - 17$ has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p.

[*You may use any of the theorems stated during lectures.*]

$(x^4 - 17)/2$ is positive for x large, so the equation clearly has real solutions. For any algebraically closed field of characteristic different from 2 and 17, $x^4 - 17$ has 4 distinct roots, so $2y^2 = x^4 - 17$ is non-singular over $\mathbb{F}_p$ for all $p \neq 2, 17$. If we denote by N_p the number of solutions in $\mathbb{F}_p$, then Hasse's bound gives

$$N_p \geq p - 1 - 2\sqrt{p}$$

for any $p \neq 2, 17$. Therefore, for any such $p \geq 7$, there is an $\mathbb{F}_p$-solution (a, b). If we put $f(x, y) = 2y^2 - x^4 + 17$, then either $df/dx(a, b) \neq 0$ or $df/dy(a, b) \neq 0$. In the first case, if we put $g(x) = f(x, b)$, then $g'(a) \neq 0$. Therefore, by Hensel's lemma, we can lift (a, b) to a solution to $f(x, y) = 0$ in $\mathbb{Q}_p$. A similar argument using $h(y) = f(a, y)$ gives a $\mathbb{Q}_p$ solution in the second case. So we need only examine for solutions in $\mathbb{Q}_{17}$, $\mathbb{Q}_5$, $\mathbb{Q}_3$, and $\mathbb{Q}_2$.

$\mathbb{Q}_{17}$. If we put $g(y) = y^2 - (1/2)(1 - 17) \in \mathbb{Z}_{17}[x]$, then $g(3) \equiv 0 \mod 17$ and $g'(3) = 6 \in \mathbb{Z}_{17}^*$. So by Hensel's lemma, $g(y)$ has a root $b \in \mathbb{Z}_{17}$. Then $(1, b)$ is a zero of $2y^2 - x^4 + 17$.

$\mathbb{Q}_5$. Now put $g(y) = 2y^2 + 17$. Then $g(2) \equiv 0 \mod 5$ and $g'(2) = 8 \in \mathbb{Z}_5^*$. So $g(y)$ has a zero $b \in \mathbb{Z}_5$ and $(0, b)$ is a zero of $2y^2 - x^4 + 17$.

$\mathbb{Q}_3$. Put $g(y) = 2y^2 - (1 - 17) = 2y^2 + 16$. Then $g(1) \equiv 0 \mod 3$ and $g'(1) = 2 \in \mathbb{Z}_3^*$. So $g(y)$ has a root b in $\mathbb{Z}_3$ by Hensel's Lemma, and $(1, b)$ is a solution of $f(x, y) = 0$.

$\mathbb{Q}_2$. It suffices to show that 17 has a fourth root in $\mathbb{Z}_2$, so consider $g(x) = x^2 - 17$. We have $g(1) = 1 - 17 \equiv 0 \mod 16$, so that $|g(1)|_2 = 2^{-4}$, while $g'(1) = 2$, so $|g'(1)|_2 = 2^{-1}$. Hence, $|g(1)|_2 < |g'(1)|_2^2$, and $g(x)$ has a root in $\alpha \in \mathbb{Z}_2$ such that $|\alpha - 1|_2 \leq |g(1)|_2/|g'(1)|_2 = 2^{-3}$. Now we can consider $h(x) = x^2 - \alpha$. Then $|h(1)|_2 \leq 2^{-3}$, while $|h'(1)|_2 = 2^{-1}$, so that $h(x)$ has a root $\beta \in \mathbb{Z}_2$. Then β is a 4-th root of 17.

[10 marks, seen]

2.
(a)
For the elliptic curve $\mathcal{E}$ with equation $y^2 = x^3 + 1$ compute the groups

(i) $\mathcal{E}(\mathbb{F}_5)$
(ii) $\mathcal{E}(\mathbb{F}_7)$

For case (i) describe directly the group law on the points of the curve.

(i) As we go through the values $0, 1, 2, 3, 4$ for x, we get $1, 2, 4, 3, 0$ for $x^3 + 1$. These correspond to the points

$$P_1 = (0, 1), P_2 = (0, 4), P_3 = (2, 2), P_4 = (2, 3), P_5 = (4, 0),$$

which, together with the origin O make up the group of point. This group is clearly isomorphic to C_6. Note that P_5 is the only point of order 2. We compute $2P_3$ as follows. The slope of the tangent is $y' = 3x^2/2y = 2/4 = 3$. Thus, the equation of the tangent line is $y = 3(x-2)+2 = 3x-4 = 3x+1$. We find the points of intersection using the roots of

$$(3x+1)^2 - x^3 - 1 = 4x^2 + x + 1 + 4x^3 - 1 = x(4x^2+4x+1) = x(2x+1)^2.$$

Thus, $2P_3 = (0,1) = P_1$. We check easily that P_1 and P_2 have order 3. So $4P_3 = 2P_1 = P_2$. Since P_3 must have order 6, we have $3P_3 = P_5$. Hence, we must have $5P_3 = P_4$, the other point of order 6. Finally, $6P_3 = O$. To summarize, the group of points is given by

$$O, \quad P_3, \quad 2P_3 = P_1, \quad 3P_3 = P_5, \quad 4P_3 = P_2, \quad 5P_3 = P_4,$$

which also contains the information for the group table.

[5 marks, seen]

(ii) As we go through the values $0,1,2,3,4,5,6$ for x, we get for x^3+1, $1,2,2,0,2,0,0$ giving us the points

$$(0,\pm 1), (1,\pm 3), (2,\pm 3), (3,0), (4,\pm 3), (5,0), (6,0).$$

Together with the origin, we see that the group has order 12. By examining the points of order two, we see that there is a subgroup isomorphic to $C_2 \times C_2$. Hence, the group is isomorphic to $C_2 \times C_2 \times C_3$.

[5 marks, seen]

(b) Compute the torsion subgroups of the rational points of the elliptic curves over $\mathbb{Q}$ given by the equations

$$D_1: \quad y^2 = x^3 + x^2 + 2x + 1; \qquad D_2 : y^2 = x^3 + 64.$$

[*You may use any of the theorems stated during lectures.*]

D_1.
We have the point $(0,1)$. The slope of the tangent line there is $y' = 2/2 = 1$, so that the tangent line is $y = x+1$. To find the points of intersection, we solve

$$x^3 + x^2 + 2x + 1 = (x+1)^2,$$

which has a triple root $x = 0$. Therefore, $(0,1)$ is a point of order 3.
Now we consider the points in $\mathbb{F}_3$. Over $\mathbb{F}_3$, we have

$$(x^3 + x^2 + 2x + 1)' = 2x + 2,$$

which has only $x = 2$ as zero. But $2^3 + 2^2 + 2 \times 2 + 1 = 2 \neq 0$, so the curve has good reduction. In fact, using the same computation, we see that the only points are

$$(0,\pm 1), O.$$

But we have the injection

$$D_1(\mathbb{Q})_{tor} \hookrightarrow D_1(\mathbb{F}_3).$$

Therefore, we must have $D_1(\mathbb{Q})_{tor} = C_3$, generated by $(0,1)$.

[5 marks, unseen]

D_2.

We have the point $(0,8)$, which is again easily seen to have order 3. There is also the point $(-4,0)$ of order 2. Thus, $D_2(\mathbb{Q})_{tor}$ has order at least 6.
Now we compute the points over $\mathbb{F}_5$, where the curve takes the form $y^2 = x^3 - 1$, which is non-singular. As we run through, $x = 0, 1, 2, 3, 4$, we get $x^3 - 1 = 4, 0, 2, 1, 3$. Thus, we get the points

$$(0, \pm 2), (1, 0), (3, \pm 1), O.$$

That is, $D_2(\mathbb{F}_5)$ has order 6. Hence, since

$$D_2(\mathbb{Q})_{tor} \hookrightarrow D_2(\mathbb{F}_5),$$

we see that $D_2(\mathbb{Q})_{tor} = C_6$, generated by $(-4,0) + (0,8)$.

[5 marks, unseen]

(c) Let $\mathcal{E}$ be the elliptic curve over $\mathbb{Q}$ given by the equation

$$y^2 = x^3 + 8.$$

Prove or disprove: $\mathcal{E}$ has infinitely many rational points.

[*You may use any of the theorems stated during lectures.*]

We examine the point $(1,3)$. Compute $2(1,3)$. The tangent line at $(1,3)$ has slope $(3x^2/2y)|_{(1,3)} = 1/2$. Thus, the equation of the tangent line is $y = (1/2)x + (5/2)$. To find the point of intersection, we substitute

$$(1/4)(x+5)^2 = x^3 + 8.$$

Thus, the x-coordinate α of the intersection point satisfies $\alpha + 1 + 1 = 1/4$, and hence $\alpha = -7/4$. Thus, by the Nagell-Lutz theorem, $2(1,3)$ is not a torsion point. Hence $(1,3)$ is not a torsion point. Therefore, the curve has infinitely many rational points. **[5 marks, unseen]**

3.
(a)
Find the structure of the Mordell-Weil group of

$$\mathcal{C}: \quad y^2 = x^3 - 10x.$$

First we compute the points over $\mathbb{F}_3$. For $x = 0, 1, 2$, we get $x^3 - 10x = x^3 - x = 0, 0, 0$. Thus, all the $\mathbb{F}_3$ points are 2-torsion points, and

$$\mathcal{C}(\mathbb{F}_3) = C_2 \times C_2.$$

Now, $\mathcal{C}(\mathbb{Q})_{tor} \hookrightarrow C_2 \times C_2$ via reduction modulo 3. Thus, $\mathcal{C}(\mathbb{Q})_{tor}$ must also consist entirely of 2-torsion points. However, since $x^3 - 10x = x(x^2 - 10)$ and 10 does not have a rational square root, we see that

$$\mathcal{C}(\mathbb{Q})_{tor} = \langle (0,0) \rangle \simeq C_2.$$

[5 marks, unseen, but similar seen]

We go on to compute the rank. We have dual isogenies

$$\phi : \mathcal{C} \mapsto \mathcal{D}$$

$$\psi : \mathcal{D} \mapsto \mathcal{C}$$

where

$$\mathcal{D} : V^2 = U(U^2 + 40),$$

and an exact sequence

$$\mathcal{D}(\mathbb{Q})/\phi \mapsto^{\psi} \mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}) \mapsto \mathcal{C}(\mathbb{Q})/\psi \mapsto 0.$$

$\mathcal{D}(\mathbb{Q})/\phi$. This is isomorphic to the subgroup $Im(q') \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ represented by 1, 40, and square-free $r|40 = 2^3 \cdot 5$ for which there are l, m, n not all zero $(l, m) = 1$ such that

$$rl^4 + (40/r)m^4 = n^2.$$

We have to consider $r \in \{\pm 1, \pm 2, \pm 5, \pm 10.\}$.

-1,-2,-5,-10: In these cases, there are clearly no solutions by positivitiy.

$r = 5$:

$$5l^4 + 8m^4 = n^2.$$

Reducing modulo 5, we get

$$3m^4 = n^2.$$

Since 3 has no square root in $\mathbb{F}_5$, we must have both m and n zero. Thus, $5|m$ and $5|n$. But then, $5^2|5l^4$, so that $5|l$. Therefore, there are no solutions with $(l, m) = 1$ and $5 \notin Im(q')$. Since $10 = 40/2^2 \in Im(q')$, we see that $2 \notin Im(q')$. Therefore, $Im(q') = \{1, 10\} \simeq C_2$.

Now we consider $\mathcal{C}(\mathbb{Q})/\psi$. This is isomorphic to the subgroup $Im(q) \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ represented by 1, -10, and square-free $r|10 = 2 \cdot 5$ for which there are l, m, n not all zero $(l, m) = 1$ such that

$$rl^4 - (10/r)m^4 = n^2.$$

We have to consider $r \in \{\pm 1, \pm 2, \pm 5, \pm 10.\}$.

$r = 5$:

$$5l^4 - 2m^4 = n^2.$$

Reducing modulo 5, we get

$$3m^4 = n^2.$$

Since 3 has no square root in $\mathbb{F}_5$, we see that $5|m$ and $5|n$. As above, we see that $5|l$ so that there is no solution with $(l, m) = 1$. Once again, since $-10 \in Im(q)$, we see that $-2 \notin Im(q)$.
$r = -5$:

$$-5l^4 + 2m^4 = n^2.$$

Reducing modulo 5, we get

$$2m^4 = n^2.$$

Since 2 has no square root in $\mathbb{F}_5$, we see that $5|m$ and $5|n$. As above, we see that $5|l$ so that there is no solution with $(l, m) = 1$. This also implies that 2 is not in the image.
$r = -1$.

$$-l^4 + 10m^4 = n^2.$$

In this case, we see the solution $(1, 1, 3)$. Therefore, we see that

$$\mathcal{C}(\mathbb{Q})/\psi \simeq \{\pm 1, \pm 10\} \simeq C_2 \times C_2.$$

Now, $\mathcal{D}(\mathbb{Q})/\phi$ is represented by $O, (0, 0)$, which then goes to $O \in \mathcal{C}(\mathbb{Q})/2$ under the map $\psi : \mathcal{D}(\mathbb{Q})/\phi \mapsto \mathcal{C}(\mathbb{Q})/2$. Therefore,

$$\mathcal{C}(\mathbb{Q})/2 \simeq \mathcal{C}(\mathbb{Q})/\psi \simeq C_2 \times C_2.$$

Hence,

$$\mathcal{C}(\mathbb{Q}) \simeq C_2 \times \mathbb{Z}.$$

A point of infinite order is $(-1, 3)$.

[10 marks, unseen, but similar seen]

(b)
Let p be a prime such that $p \equiv 5 \mod 8$. Show that

$$\mathcal{E}_p : \quad y^2 = x^3 + px$$

has rank at most 1.

In this case, the there are isogenies

$$\phi : E_p \mapsto E'_p$$

and

$$\psi : E'_p \mapsto E_p,$$

where

$$E'_p : V^2 = U^3 - 4pU.$$

We first consider E_p. $E_p(\mathbb{Q})/\psi$ is isomorphic to the subgroup $Im(q) \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ represented by 1, p, and square-free $r|p$ for which there are l, m, n not all zero $(l, m) = 1$ such that

$$rl^4 + (p/r)m^4 = n^2.$$

We need to consider $r \in \{\pm 1, \pm p\}$. Clearly, no negative r will work. So

$$E_p(\mathbb{Q})/\psi \simeq C_2.$$

$E'_p(\mathbb{Q})/\phi$ is isomorphic to the subgroup $Im(q') \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ represented by 1, $-4p \equiv -p$, and square-free $r|4p$ for which there are l, m, n not all zero $(l, m) = 1$ such that

$$rl^4 - (4p/r)m^4 = n^2.$$

We need to consider $r \in \{\pm 1, \pm 2, \pm p, \pm 2p\}$.

$r = 2$.

$$2l^4 - 2pm^4 = n^2.$$

Reducing modulo p, we get that $2l^4 = n^2$. But since $p \equiv 5 \mod 8$, 2 has no square root in $\mathbb{F}_p$. Hence, $p|l$ and $p|n$. Therefore, $p|m$, and there is no solution such that $(l, m) = 1$. Thus, $2 \notin Im(q')$.

$r = -2$.

$$-2l^4 + 2pm^4 = n^2.$$

Reducing modulo p, we get that $-2l^4 = n^2$. But since $p \equiv 5 \mod 8$, we also have $p \equiv 1 \mod 4$. So -1 has a square root in $\mathbb{F}_p$. Hence, -2 has no square root in $\mathbb{F}_p$. Hence, $p|l$ and $p|n$. Therefore, $p|m$, and there is no solution such that $(l, m) = 1$. Thus, $-2 \notin Im(q')$.
From this, we also conclude that $\pm 2p \notin Im(q')$.
Now we consider $r = p$. Then we have the equation

$$pl^4 - 4m^4 = n^2.$$

If there is a non-trivial solution, then $p \in Im(q')$, so $-1 \in Im(q')$. Thus,

$$E'_p(\mathbb{Q})/\phi \simeq \{\pm 1, \pm p\} \simeq C_2 \times C_2.$$

Since the class of $(0,0)$ goes to zero in $E_p(\mathbb{Q})/2$, we get that $\dim_{\mathbb{F}_2} E_p(\mathbb{Q})/2 = 2$. Therefore, in this case, the rank of $E_p(\mathbb{Q})$ is 1.

If there is no non-trivial solution, then $p \notin Im(q')$ so $-1 \notin Im(q')$. Hence,

$$E'_p(\mathbb{Q})/\phi \simeq \{1, -p\} \simeq C_2$$

and $E'_p(\mathbb{Q})/\phi$ goes to zero in $E_p(\mathbb{Q})/2$. Therefore, $E_p(\mathbb{Q})/2 \simeq E_p(\mathbb{Q})/\psi \simeq C_2$ and $E_p(\mathbb{Q})$ has rank zero. In any case, the rank is at most 1.

[7 marks, unseen]

(c)
What is the rank of $\mathcal{E}_p$ for $p = 5$, $p = 13$,and $p = 29$?

For $p = 5$, the determining equation becomes

$$5l^4 - 4m^4 = n^2$$

so that we get the solution $(l, m, n) = (1, 1, 1)$. Therefore, $E_5(\mathbb{Q})$ has rank 1.

For $p = 13$, the equation is

$$13l^4 - 4m^4 = n^2$$

and we get the solution $(l, m, n) = (1, 1, 3)$. Therefore, $E_{13}(\mathbb{Q})$ has rank 1.

For $p = 29$, we have

$$29l^4 - 4m^4 = n^2$$

with the solution $(1, 1, 5)$. Therefore, $E_{29}(\mathbb{Q})$ has rank 1.

[3 marks, unseen]