Solution 1

(a) Let $S_N = \sum_{n=1}^{N} x_n$. Assume that $x_n \to 0$ in K. Then:
$|S_N - S_M| = |x_{M+1} + \ldots + x_N| \leqslant \max\big(|x_{M+1}|, \ldots, |x_N|\big) \to 0$ as $M, N \to \infty$. Hence S_N is Cauchy and so convergent (since K is complete), giving that $\sum x_n$ is convergent. Conversely, assume that $\sum x_n$ is convergent, that is, $S_N \to \ell$ for some $\ell \in K$. Then:
$|x_n - 0| = |x_n| = |S_n - S_{n-1}| = |S_n - \ell + \ell - S_{n-1}| \leqslant |S_n - \ell| + |S_{n-1} - \ell| \to 0$ as $n \to \infty$, so that $x_n \to 0$ in K, $|\ |$.

Let $x, y \in K$ satisfy $|x| \neq |y|$; without loss of generality, say $|x| > |y|$. Since $|\ |$ is non-Archimedean, $|x+y| \leq \max(|x|, |y|)$. Imagine $|x+y| < \max(|x|, |y|) = |x|$; then $|x| = |x + y + (-y)| \leq \max(|x + y|, |y|) < |x|$, a contradiction; hence $|x + y| = \max(|x|, |y|)$.

[**5 marks** Bookwork.]

(b) Note that $1+2p+2p^2+2p^3+\ldots = 1+2p(1+p+p^2+\ldots) = 1+2p/(1-p) = (1+p)/(1-p)$, which equals $-9/8$ exactly when $8(1+p) = -9(1-p)$, that is: $p = 17$.

[**2 marks**; Unseen.]

(c) Let $x_0 = a_0 = 2$. Then $|x_0^2 + 3|_7 = 7^{-1}$. Look for $x_1 = a_0 + 7a_1$ such that $|x_1^2 + 3|_7 \leqslant 7^{-2}$. This is satisfied if: $(2 + 7a_1)^2 \equiv -3 \pmod{7^2} \iff 2 \cdot 2 \cdot 7a_1 \equiv -3 - 2^2 \pmod{7^2} \iff 4a_1 \equiv -1 \pmod 7 \iff a_1 \equiv 5 \pmod 7$. So, now define: $a_1 = 5$ and $x_1 = a_0 + 7a_1 = 37$, which satisfies $|x_1^2 + 3|_7 < 7^{-1}$.

For any $x \in \mathbb{Z}$, $|x^2|_7 = 7^{2r}$, for some $r \in \mathbb{Z}$, whereas $|14|_7 = 7^{-1}$, so that $|x^2|_7 \neq |14|_7$. By (a), $|x^2 + 14|_7 = \max(|x^2|_7, |14|_7) \geq 7^{-1}$, and so we cannot have $|x^2 + 14|_7 < 7^{-1}$.

[**5 marks**; Seen similar.]

(d) 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 $|a - a_0| \leq |f(a_0)|/|f'(a_0)|$.

We are given that $p \equiv 1 \pmod 3$. Then $p \neq 2$, so p is odd, and so satisfies either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. In the first case, we have that $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{-1}{3}\right)$ [by quadratic reciprocity] $= \left(\frac{1}{p}\right)\left(\frac{-1}{3}\right) = 1 \cdot 1$ [using the result from notes that $\left(\frac{-1}{p}\right) = 1$ when $p \equiv 1 \pmod 4$]. In the second case, $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = -\left(\frac{p}{3}\right)\left(\frac{-1}{p}\right)$ [by quadratic reciprocity] $= -\left(\frac{1}{3}\right)\left(\frac{-1}{p}\right) = -1 \cdot (-1)$ [using the result from notes that $\left(\frac{-1}{p}\right) = 1$ when $p \equiv 1 \pmod 4$]. In either case, we have that $\left(\frac{-3}{p}\right) = 1$, as required.

We now have that there exists $a_0 \in \mathbb{Z}$ such that $a_0^2 \equiv -3 \pmod p$, and so $|f(a_0)|_p \leq p^{-1}$, where $f(x) = x^2 + 3$; clearly $|a_0|_p = 1$ (since $|a_0^2|_p \equiv |-3|_p = 1$) and so $|f'(a_0)|_p = 2|a_0|_p = 1$; hence $|f(a_0)|_p < |f(a_0)|_p^2$; it follows from Hensel's Lemma that $f(x)$ has a root in $\mathbb{Z}_p$; hence -3 is a cube in $\mathbb{Z}_p$ and so in $\mathbb{Q}_p$.

[**6 marks**; Unseen]

(e) When $p \equiv 2 \pmod 3$, note that 3 is coprime to $p-1$, and so there exist $\lambda, \mu \in \mathbb{Z}$ such that $(p-1)\lambda + 3\mu = 1$. Now, suppose that $v^3 = w^3$ in $\mathbb{F}_p^*$. Then $v^{3\mu} = w^{3\mu}$. Also $(p-1)\lambda$ is a multiple of the order of the group $\mathbb{F}_p^*$ and so $v^{(p-1)\lambda} = w^{(p-1)\lambda}$ (since both are equal to 1). Multiplying these last two equations gives: $v^{(p-1)\lambda+3\mu} = w^{(p-1)\lambda+3\mu}$, and so $v = w$. We have shown that $v^3 = w^3$ implies $v = w$, and so the map $v \mapsto v^3$ is injective, and hence surjective (and hence bijective), from $\mathbb{F}_p^*$ to $\mathbb{F}_p^*$. Since q is not divisible by p (since $q \equiv 1 \pmod{27}$), it follows that there exists $x_0 \in \mathbb{Z}$ such that $x_0^3 \equiv q \pmod p$. This is the same as $|f(x_0)|_p < 1$, where $f(x) = x^3 - q$. But from the fact that q is not divisible by p and $x_0^3 \equiv q \pmod p$ it follows that x_0 is not divisible by p, and so $|x_0|_p = 1$, giving that $|f'(x_0)|_p = |3x_0^2|_p = 1$. Therefore, $|f(x_0)|_p < |f'(x_0)|_p^2$ and so, by Hensel's Lemma, there exists a solution in $\mathbb{Q}_p$ to $x^3 - q = 0$, which is also a solution to $(x^2+3)(x^3-q) = 0$.

When $p \equiv 1 \pmod 3$, we have already established in (d) that $x^2+3=0$ has a solution $\mathbb{Q}_p$, which will also be a solution to $(x^2+3)(x^3-q) = 0$. When $p = 3$, note that we are given $q \equiv 1 \pmod{27}$, so that $|f(x_0)|_3 \leq 3^{-3}$, where $x_0 = 1$ and $f(x) = x^3 - q$. Also, $|f'(x_0)|_3 = |3 \cdot 1^2| = 3^{-1}$, so that $|f(x_0)|_3 < |f'(x_0)|_3^2$. By Hensel's Lemma, it follows that there exists a solution in $\mathbb{Q}_3$ to $x^3 - q = 0$, and so to $(x^2+3)(x^3-q) = 0$. Since $q > 0$, there also exists a solution to $x^3 - q = 0$ in $\mathbb{R}$, and so to $(x^2+3)(x^3-q) = 0$. Hence there is a solution to $(x^2+3)(x^3-q) = 0$ in $\mathbb{R}$ and every $\mathbb{Q}_p$, as required. Finally note that x^2+3 has no solution in $\mathbb{Q}$ (since none in $\mathbb{R}$) and $x^3 - q$ has no solution in $\mathbb{Q}$ (since none in $\mathbb{Q}_q$, since $|x^3|_q = q^{3r}$, whereas $|q|_q = q^{-1}$).

[**7 marks**; Unseen, although they have previously seen the idea of $x \mapsto x^3$ being bijective on $\mathbb{F}_p^*$, when $p \equiv 2 \pmod 3$, in a different problem on a sheet.]

Solution 2

(a) Let $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + 4x$. Then $\mathbf{o}$ and $(0,0)$ [which has order 2] are both members of the torsion subgroup. Furthermore, consider the point $(2,4) \in \mathcal{E}(\mathbb{Q})$; the tangent to $\mathcal{E}$ at $(2,4)$ has slope $(3 \cdot 2^2 + 4)/(2 \cdot 4) = 2$ and has equation $y = 2x$. So, the x-coordinate of $2(2,4)$ is $2^2 - 2 - 2 = 0$, with corresponding y-coordinate 0, giving: $2(2,4) + (0,0) = \mathbf{o}$ and so $2(2,4) = -(0,0) = (0,0)$. Hence $4(2,4) = 2(0,0) = \mathbf{o}$; similarly $4(2,-4) = \mathbf{o}$. We have found 4 torsion elements: $\mathbf{o}, (0,0), (2,4), (2,-4)$, and so the torsion subgroup is of order at least 4. The discriminant of $x^3 + 4x$ is $4 \cdot 4^3 + 27 \cdot 0^2 = 2^8$, and so $\widetilde{\mathcal{E}} : y^2 = x^3 + 4x$ is an elliptic curve for all $p \neq 2$. The elements of $\widetilde{\mathcal{E}}(\mathbb{F}_3)$ are: $\mathbf{o}, (0,0), (2, \pm 1)$, and so $\widetilde{\mathcal{E}}(\mathbb{F}_3)$ has order 4. Since the torsion subgroup of $\mathcal{E}(\mathbb{Q})$ injects into this group, its order must divide 4. Hence the torsion subgroup of $\mathcal{E}(\mathbb{Q})$ consists precisely of the 4 torsion elements already found, namely: $\{\mathbf{o}, (0,0), (2, \pm 4)\}$.

[**5 marks**; Seen similar.]

(b) Let $\mathcal{E}$ be the elliptic curve $y^2 = x(x+1)(x+n^2) = x^3 + (n^2+1)x^2 + n^2 x$. The tangent to $\mathcal{E}$ at $(n, n(n+1))$ has slope $(3n^2 + 2(n^2+1)n + n^2)/(2n(n+1)) = n + 1$, and so equation $y = (n+1)x + c$ for some c; the line must pass through $(n, n(n+1))$ so that $c = 0$ and the equation of the tangent is: $y = (n+1)x$. The x-coordinate of $P = 2(n, n(n+1))$ is $(n+1)^2 - (n^2+1) - 2n = 0$, with y-coordinate $(n+1) \cdot 0 = 0$. Hence $2(n, n(n+1)) + (0,0) = \mathbf{o}$, so that $2(n, n(n+1)) = -(0,0) = (0,0)$, giving $4(n, n(n+1)) = \mathbf{o}$. So $(n, n(n+1))$ is torsion, as must be $(n, -n(n+1)) = -(n, n(n+1))$. Replacing every occurrence of n with $-n$ gives that the tangent to $\mathcal{E}$ at $(-n, n(n-1))$ has equation $y = (-n+1)x$ and $2(-n, n(n-1)) = (0,0)$; we deduce, as before, that $(-n, \pm n(n-1))$ are torsion elements. Therefore there are at least 8 members of the torsion subgroup of $\mathcal{E}(\mathbb{Q})$, namely: $\mathbf{o}, (0,0), (-1,0), (-n^2, 0)$ and the above 4 points of order 4. Finally, let $n \equiv 2$ (modulo 5), so that $n^2 \equiv 4$ (modulo 5). Then $\widetilde{\mathcal{E}}$ modulo 5 is: $y^2 = x(x+1)(x+4)$, and the cubic has no repeated roots, so that $\mathcal{E}$ has good reduction at 5. The elements of $\widetilde{\mathcal{E}}(\mathbb{F}_5)$ are: $\mathbf{o}, (0,0), (1,0), (2, \pm 1), (3, \pm 2), (4, 0)$, and so $\widetilde{\mathcal{E}}(\mathbb{F}_5)$ has order 8. Since the torsion subgroup of $\mathcal{E}(\mathbb{Q})$ injects into this groups, its order must divide 8. Hence the torsion subgroup of $\mathcal{E}(\mathbb{Q})$ consists precisely of the 8 torsion elements already found, namely: $\{\mathbf{o}, (0,0), (-1,0), (-n^2, 0), (n, \pm n(n+1)), (-n, \pm n(n-1))\}$.

[**7 marks**; Unseen.]

(c) 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 in the question, $y^2|(\phi_1(x)\psi_1(x) + \phi_2(x)\psi_2(x)) = \Delta$, as required.

[**7 marks**; Bookwork.]

(d) The disciminant of $x^3 - k^2x + k^3$ is $4\cdot(-k^2)^3 + 27\cdot(k^3)^2 = 23k^6$. If (x, y) is a torsion point in $\mathcal{E}(\mathbb{Q})$, then we know by Nagell-Lutz that $x, y \in \mathbb{Z}$ with $y^2|23k^6$ and so $|y|^2 \leq 23|k|^6$; that is: $|y| \leq \sqrt{23}|k|^3 \leq 5|k|^3$.

Since $k \in \mathbb{Z}$, and we are given $k \neq 0$, we have $|k| \geqslant 1$ and so: $|k|^2 \leqslant |k|^4$ and $|k|^3 \leqslant |k|^6$.
Imagine $|x| > 3|k|^2$.
Then: $|x^2 - k^2| \geq |x^2| - |k^2| > 9|k|^4 - |k^2| \geqslant 9|k|^4 - |k^4| = 8|k|^4$, so:
$|y|^2 = |x(x^2-k^2) + k^3| \geq |x(x^2-k^2)| - |k^3| = |x||x^2-k^2| - |k^3| > 3|k|^2 8|k|^4 - |k|^6 = 23|k|^6$, contradicting $|y|^2 \leq 23|k|^6$ (above). Hence $|x| \leq 3|k|^2$, as required.

[**6 marks**; Unseen]

Solution 3

(a) Let $\mathcal{C} : Y^2 = X(X^2 + X + 2)$. Here, $a = 1, b = 2$ and so $a_1 = -2a = -2, b_1 = a^2 - 4b = -7$, giving $\mathcal{D} : V^2 = U(U^2 - 2U - 7)$. The isogeny $\phi : \mathcal{C} \to \mathcal{D}$ is given by $\phi(x, y) = \Big(\big(\frac{y}{x}\big)^2, y - \frac{by}{x^2}\Big) = \Big(\big(\frac{y}{x}\big)^2, y - \frac{2y}{x^2}\Big)$. The isogeny $\hat{\phi} : \mathcal{D} \longrightarrow \mathcal{C}$ is given by $\hat{\phi}(u, v) = \Big(\frac{1}{4}\big(\frac{v}{u}\big)^2, \frac{1}{8}\big(v - \frac{b_1 v}{u^2}\big)\Big) = \Big(\frac{1}{4}\big(\frac{v}{u}\big)^2, \frac{1}{8}\big(v + \frac{7v}{u^2}\big)\Big)$.

Step 1. Find $\mathcal{D}(\mathbb{Q})/\hat{\phi}(\mathcal{C}(\mathbb{Q}))$. We need to consider $r|b_1 = -7, r \in \mathbb{Z}$, r square free, that is, $r = \pm 1, \pm 7$, so that im $q \leqslant \{\pm 1, \pm 7\}$. But $q(\mathbf{o}) = 1,\ q(0, 0) = b_1 = -7,\ q(-1, 2) = -1,\ q(7, 14) = 7$ [note that $(7, 14)$ can be found as $(0, 0)+(-1, 2)$ without needing to search], so that im $q = \{\pm 1, \pm 7\}$ and $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\mathbf{o}, (0, 0), (-1, 2), (7, 14)\} = \langle (0, 0), (-1, 2)\rangle$.

Step 2. Find $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$. We need to consider $r|b = 2, r \in \mathbb{Z}$, r square free, that is, $r = \pm 1, \pm 2$. Also, $\hat{q}(\mathbf{o}) = 1,\ \hat{q}(0, 0) = b = 2$, so that $\{1, 2\} \leqslant$ im $\hat{q} \leqslant \{\pm 1, \pm 2\}$. Note that $-1 \in$ im $\hat{q} \iff -2 \in$ im $\hat{q}$, and so it is only necessary to check one member of the coset $\{-1, -2\}$.

Choose $r = -1$. Then $\widehat{W}_{-1}$, $r\ell^4 + a\ell^2 m^2 + (b/r)m^4 = n^2$ becomes:

$$\widehat{W}_{-1} : -\ell^4 + \ell^2 m^2 - 2m^4 = n^2, \quad \text{for some } \ell, m, n \in \mathbb{Z}, \text{ not all 0, with } \gcd(\ell, m) = 1.$$

On multiplying both sides by 4 and completing the square, we obtain:

$$-(2\ell^2 - m^2)^2 - 7m^4 = 4n^2. \qquad (1)$$

This gives $-(2\ell^2 - m^2)^2 \equiv 4n^2 \pmod 7$.

Imagine $7 \nmid (2\ell^2 - m^2)$; then $2\ell^2 - m^2$ would have an inverse α mod 7, and so $-1 \equiv (2\alpha n)^2 \pmod 7$, contradicting the fact that -1 is not a quadratic residue mod 7.

Hence, by reductio, $7|(2\ell^2 - m^2)$ and so $7|n$ [since $7|4n^2$ and $7 \nmid 4$], giving also that $7^2|(2\ell^2 - m^2)^2$ and $7^2|4n^2$, so that, from (1), $7^2|7m^4$, and so $7|m$. But combining $7|m$ with $7|2\ell^2 - m^2$ gives $7|2\ell^2$, so that $7|\ell$. We have shown that $7|\ell$ and $7|m$, contradicting $\gcd(\ell, m) = 1$. Hence there are no solutions to $\widehat{W}_{-1}$, giving that $-1 \notin$ im $\hat{q}$.

We conclude that im $\hat{q} = \{1, 2\}$ and $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \{\mathbf{o}, (0, 0)\} = \langle (0, 0)\rangle$.

Step 3. Find $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$. This is by $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \{\mathbf{o}, (0, 0)\}$, together with $\hat{\phi}\big(\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))\big) = \{\hat{\phi}(\mathbf{o}), \hat{\phi}(0, 0), \hat{\phi}(-1, 2), \hat{\phi}(7, 14)\}$

$$= \{\mathbf{o}, \mathbf{o}, \Big(\frac{1}{4}\big(\frac{2}{-1}\big)^2, \frac{1}{8}\big(2 + \frac{7 \cdot 2}{(-1)^2}\big)\Big), \Big(\frac{1}{4}\big(\frac{14}{7}\big)^2, \frac{1}{8}\big(14 + \frac{7 \cdot 14}{7^2}\big)\Big)\}$$

$= \{\mathbf{o}, \mathbf{o}, (1, 2), (1, 2)\} = \{\mathbf{o}, (1, 2)\}$. Therefore $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is:
$\{\mathbf{o}, (0, 0), (1, 2), (0, 0) + (1, 2) = (2, -4)\} = \langle (0, 0), (1, 2)\rangle \cong C_2 \times C_2$.

Finally, use the result: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}) \cong \mathcal{C}(\mathbb{Q})[2] \times C_2^r$, and $\mathcal{C}(\mathbb{Q})[2] = \{\mathbf{o}, (0, 0)\} \cong C_2$ (since the other points of order 2 are $((-1 \pm \sqrt{-7})/2, 0)$), to deduce that the rank $r = 1$.

[**11 marks**; Seen similar.]

(b) We are given that $A/2A$ is finite, so let $A/2A = S = \{Q_1, \ldots Q_r\} \subset A$. Let P be any element of A. Then $P = Q_{i_1}$ in $A/2A$ for some $Q_{i_1} \in S$ and so we can write: $P = 2P_1 + Q_{i_1}$, for some $P_1 \in A$. Inductively, continue to write: $P_1 = 2P_2 + Q_{i_2}, P_2 = 2P_3 + Q_{i_3}, \ldots$, where each $P_j \in A$ and each $Q_{i_j} \in S$. Now: $h(P_j) \leq \frac{1}{4}\big(h(2P_j) + C_2\big)$ [by (2)] $= \frac{1}{4}\big(h(P_{j-1} - Q_{i_j}) + C_2\big) \leq \frac{1}{4}\big(2h(P_{j-1}) + C_1' + C_2\big)$ [by (1)], where:
$C_1' = \max\{C_1(-Q) : Q \in S\}$. So, if $h(P_{j-1}) > (C_1' + C_2)/2$ then:
$h(P_j) < \frac{1}{4}\big(2h(P_{j-1}) + 2h(P_{j-1})\big) = h(P_{j-1})$.

Imagine that $h(P) > (C_1' + C_2)/2$ and $h(P_j) > (C_1' + C_2)/2$ for all j. Then the sequence $h(P), h(P_1), h(P_2), \ldots$ would be strictly decreasing, giving infinitely many distinct members of A with height $\leq h(P)$, which would contradict (3). This contradiction shows that there must exist an n such that $h(P_n) \leq (C_1' + C_2)/2$. So, we can write: $P = 2P_1 + Q_{i_1} = 2(2P_2 + Q_{i_2}) + Q_{i_1} = \ldots$, and after n steps P will be written as a linear combination of P_n and members of S. Let $T = \{Q \in A : h(Q) \leq (C_1' + C_2)/2\}$. We have shown (since $P_n \in T$) that any $P \in A$ is a linear combination of members of $S \cup T$. Furthermore, T is finite, by (3). In conclusion: A is generated by the finite set $S \cup T$, and so is finitely generated.

[**9 marks**; Bookwork.]

(c) Imagine that $h(P) > \frac{1}{3}C_2$. Then $C_2 < 3h(P)$ and so by (2): $h(2P) \geq 4h(P) - C_2 > 4h(P) - 3h(P) = h(P)$. Inductively: $h(P) < h(2P) < h(4P) < \ldots$, so that $P, 2P, 4P, \ldots$ are all distinct, which forces P to have infinite order (since otherwise P would generate a finite group). Hence, if P is a torsion element then $h(P) \leq \frac{1}{3}C_2$.

[**5 marks**; Unseen.]
