**Solution 1.**

We need $m^2 \equiv 7 \pmod{25}$. We have $3^3 = 27 \equiv 7 \pmod 5$. Then $(3+5x)^3 \equiv 27 + 3.3^2.5x \pmod{25}$, giving 7 (mod 25) iff $20 + 135x \equiv 0 \pmod{25}$, iff $x \equiv 3 \pmod 5$, whence $18^3 \equiv 7 \pmod{25}$. Hence $m = 18$ works.

[S; 2 marks]

If $|n^3 - 7|_3 < 3^{-1}$ then $n^3 \equiv 7 \pmod 9$, which has no solutions.

[S; 2 marks]

If $A + B + C = 0$ in a field with a non-archimedean valuation, and $|A| \geq |B| \geq |C|$, then we must have $|A| = |B|$. Indeed we will either have $A = B = C = 0$ or $|A| = |B| > 0$. In our case $|x^3|_2 = 2^{-3a}$ or $= 0$, $|2y^3|_2 = 2^{-1-3b}$ or $= 0$, and $|4z^3|_2 = 2^{-2-3c}$ or $= 0$. Hence two of these can be equal only when they are both zero. It follows that $x = y = z = 0$.

[S; 4 marks]

We have convergence iff $|x^n/n!|_2 \to 0$. There are infinitely many values of $n$ for which $|n!|_2 = 2^{1-n}$, so that we cannot have convergence if $|x|_2 \geq 2^{-1}$. On the other hand, if $|x|_2 \leq 2^{-2}$ then $|x^n/n!|_2 \leq 2^{-2n}.2^{n-1}$, since we are given that $|n!|_2 \geq 2^{-n}$. Thus $|x^n/n!|_2 \to 0$ if $|x|_2 \leq 2^{-2}$. Thus it is necessary and sufficient that $|x|_2 \leq 2^{-2}$.

[B or N (optional question, sheet 3); 4 marks]

Hensel: Let $K$ be a field, complete w.r.t. a non-archimedean valuation $|\dots|$, with valuation ring $R$. Let $f(x) \in R[x]$, and let $a \in R$ satisfy

$$|f(a)| < |f'(a)|^2.$$

Then there is a unique $a^* \in R$ with $f(a^*) = 0$ and

$$|a^* - a| \leq |f(a)|/|f'(a)|.$$

[B; 3 marks]

We use Hasse's bound:

$$|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}$$

for any elliptic curve $E$ over $\mathbb{F}_p$. If $p$ is a prime of good reduction for $y^2 = x^3 + ax + b$ it follows that the congruence $y^2 \equiv x^3 + ax + b \pmod p$ has at least $p - 2\sqrt{p}$ solutions, after allowing for the point at infinity. Since $p \geq 5$

we deduce that there is at least one solution $(u_0, v_0)$ say, which is necessarily non-singular since there is good reduction at $p$. If the partial derivative in $x$ is not divisible by $p$ we apply Hensel's Lemma to $f(t) = x^3 + ax + b - v_1^2$ for any $v_1 \in \mathbb{Z}_p$ with $v_1 \equiv v_0 \pmod{p}$. Thus there is a solution $(u, v_1)$ for each such $v_1$. Similarly if the partial derivative in $y$ is not divisible by $p$ at $(u_0, v_0)$ we may work with $f(t) = t^2 - u_1^3 - au_1 - b$, taking any $u_1 \equiv u_0 \pmod{p}$.

[S; 5 marks]

In the case of bad reduction $x^3 + ax + b$ has a repeated factor modulo $p$.

[B; 1 mark]

The above argument goes through if the reduction to $\mathbb{F}_p$ has at least one smooth point. However the reduction takes the form $y^2 = (x + \alpha)^2(x + \beta)$. If $\alpha \neq \beta$ then $(-\beta, 0)$ is a smooth point, while if $\alpha = \beta$ then $(1 - \alpha, 1)$ is smooth. (In the latter case the partial w.r.t $x$ is 3, while the partial derivative w.r.t $y$ is 2. These cannot both vanish.)

[N; 4 marks]

**Solution 2.**

A formal group is a power series $F(X,Y) \in R[[X,Y]]$ s.t.

(i) $F(X,Y) = X + Y +$ terms of degree 2 or higher.

(ii) $F(X, F(Y,Z)) = F(F(X,Y), Z)$.

(iii) $F(X,Y) = F(Y,X)$.

[B; 3 marks]

Construct $Z_n \in TR[[T]]$ of degree $n$ inductively so that $F(T, Z_n)$ has all terms of degree greater than $n$. By (i) we may start with $Z_1 = -T$. Suppose that $F(T, Z_n) = a_{n+1}T^{n+1} + \ldots$. Then if $Z_{n+1} = Z_n + cT^{n+1}$ we have a Taylor series expansion in powers of $cT^{n+1}$ as

$$F(T, Z_{n+1}) = F(T, Z_n) + cT^{n+1}F_Y(T, Z_n) + \text{ terms of degree} \geq 2n+2,$$

and since

$$F_Y(T, Z_n) = 1 + \text{ higher order terms}$$

by (i), we deduce that $F(T, Z_{n+1}) = F(T, Z_n) + cT^{n+1} +$ higher order terms. It follows that $Z_{n+1}$ has the required properties iff $c = -a_{n+1}$. Finally $i(T)$ has the required property iff it is the limit of such a sequence of polynomials $Z_n$, which we have seen can be chosen in exactly one way.

[B; 3 marks]

It follows in the same way that there is a unique $j(T) \in TR[[T]]$ for which $F(i(T), j(T)) = 0$. We claim that both $j(T) = T$ and $j(T) = F(T,0)$ have this property, which will prove that $T = F(T,0)$. By (iii) we have $F(i(T), T) = F(T, i(T)) = 0$ so that $j(T) = T$ is acceptable. By (ii) $F(i(T), F(T,0)) = F(F(i(T),T),0) = F(0,0) = 0$, by (iii) and (i), so $j(T) = F(T,0)$ is also acceptable, as claimed.

[B; 4 marks]

Suppose $(x,y)$ is a non-trivial torsion point lying in the kernel of reduction, so that $|x|_p, |y|_p > 1$ and hence $|y|_p = |x|_p^{3/2}$. Let $z = -x/y, w = -1/y$, whence $|z|_p, |w|_p < 1$. Then $z$ will be a torsion element for the (formal) group $F_E(p\mathbb{Z}_p)$ associated to $E$. It is a fact from the general theory of formal groups that such a torsion element must have an order which is a power of $p$, say $p^n$. Moreover it is also a general fact that one then has

$$|z|_p \geq |p|_p^{1/(p^n - p^{n-1})}.$$

Except in the case $p^n = 2$ we have $1/(p^n - p^{n-1}) < 1$, which would give $1 > |z|_p > p^{-1}$, a contradiction. Thus the only possibility is that $(x, y)$ has order 2 on $E$. However in this case we will have $y = 0$, contradicting the inequality $|y_p| > 1$.

[B; 8 marks]

If $x$ or $y$ were not in $\mathbb{Z}$ we would have $|x|_p > 1$ or $|y|_p > 1$ (and hence both) for some $p$. Then $(x, y)$ would be in the kernel of reduction, contrary to the above result.

[B; 2 marks]

Over $\mathbb{F}_3$ any singular point of $y^2 = x^3 + ax + b$ would have $y = 0$. Thus, over $\mathbb{Q}$, any torsion points $(x, y)$ with $3 \nmid y$ would be in $E_0(\mathbb{Q})$, as is the point at infinity; and these would be mapped injectively into $E_{\mathrm{ns}}(\mathbb{F}_p)$. However $y^2 = x^3 + ax + b$ has at most 6 finite points over $\mathbb{F}_3$, since there are 3 choices for $x$, each corresponding to at most 2 possible $y$. Thus there are at most 6 non-trivial torsion points with $3 \nmid y$.

[N; 5 marks]

**Solution 3.**

We will show that $q(P+Q) = q(P)q(Q)$ when $P, Q$ lie on $D$ and none of $P, Q$ or $P+Q$ is $(0,0)$ or the point at infinity. Let $P = (u_1, v_1)$, $Q = (u_2, v_2)$ and $P + Q = (u_3, -v_3)$, so that $(u_1, v_1), (u_2, v_2), (u_3, v_3)$ are collinear, lying on $v = mu + c$, say, as well as on $E$. Thus $u_1, u_2, u_3$ the three roots of $u(u^2 + au + b) - (mu + c)^2 = 0$, so that for the constant term we have $c^2 = u_1u_2u_3$. None of $u_1, u_2, u_3$ can vanish, since none of $P, Q, P + Q$ is $(0,0)$. It follows that $q(P)q(Q) = u_1u_2 = u_3(c/u_3)^2$, which is $u_3 = q(P+Q)$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

[B; 6 marks]

Let $(u, v) \in D(\mathbb{Q})$ and let $q(u, v)$ be represented in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ by a square-free integer $r$, which could have either sign. We claim that $r|b_1$, which will show that $q$ has finite image. The claim is trivial if $u = 0$, since $q(u, v) = b_1$ in this case. Otherwise $r, u$ and $u^2 + a_1u + b_1 = u(v/u)^2$ are the same modulo squares, so that we can write $u = rs^2$ and $u^2 + a_1u + b_1 = rt^2$ for some $s, t \in \mathbb{Q}$, with $s \neq 0$. Then

$$r^2s^4 + a_1rs^2 + b_1 = rt^2. \quad (*)$$

To show that $r|b_1$ we show that there can be no prime $p$ for which $p|r$ but $p \not| b_1$. If there were such a $p$, there would be integers $e, f$ with $|r^2s^4|_p = p^{2+4e}$, $|b_1|_p = 1$, and $|rt^2|_p = p^{1+2f}$ or 0. Thus these three terms have different valuations. Moreover for any positive real $x \neq 1$ we have $\sqrt{x} < \max(x, 1)$, whence

$$|a_1rs^2|_p \leq |rs^2|_p < \max(|r^2s^4|_p, 1) = \max(|r^2s^4|_p, |b_1|_p.)$$

This provides the required contradiction, since in (*) the two largest terms would have the same valuation.

[B; 7 marks]

We have $A^2 + C^2 = 2B^2$ and $B^2 + D^2 = 2C^2$. So if $x = -2B^2C^{-2}$ we have

$$x(x^2 + 5x + 4) = x(x + 1)(x + 4) = (-2B^2C^{-2})(1 - 2B^2C^{-2})(4 - 2B^2C^{-2})$$

$$= (-2B^2C^{-2})(-A^2C^{-2})(2D^2C^{-2}) = (2ABDC^{-3})^2,$$

giving a point $(x, y)$ with $x = -2B^2C^{-2}$ and $y = 2ABDC^{-3}$.

[N; 2 marks]

There is a 2-isogeny $\phi : E \to F$ where $F : V^2 = U(U^2 + a_1U + b_1)$ with $a_1 = -2.5 = -10$ and $b_1 = 5^2 - 4.4 = 9$. The map $q$ above (on $F(\mathbb{Q})$ rather than $D(\mathbb{Q})$) has kernel $\phi(E(\mathbb{Q}))$. We claim that the image is trivial. A coset in the image has a representative $r|b_1 = 9$ which is square-free, so that $r = \pm 1$ or $\pm 3$. Moreover (*) is solvable, leading to

$$rs^4 - 10s^2 + 9r^{-1} = t^2.$$

We shall show that only $r = 1$ is possible. If $r < 0$ the equation cannot hold, since the LHS is negative. If $r = 3$ we would get, putting $s = l/m$ in lowest terms, that $3l^4 - 10l^2m^2 + 3m^4 = n^2$ with integers $l, m, n$ in which $l, m$ are coprime. Then $-10(lm)^2 \equiv n^2 \pmod 3$, which is possible only if 3 divides both $n$ and $lm$. Then 9 divides $10(lm)^2$ and $n^2$, whence $3|l^4 + m^4$. This can happen only when both $l$ and $m$ are divisble by 3, a contradiction to our assumption that $l$ and $m$ were coprime. Thus the image of $q$ is trivial, and so $\#F(\mathbb{Q})/\phi(E(\mathbb{Q})) = 1$.

[S; 5 marks]

There is an analogous homomorphism $\hat{q}$ from $E(\mathbb{Q})$ to $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ in which any point in the image has a representative $r$, which is a square-free integer dividing $b = 4$. Thus $r = \pm 1$ or $\pm 2$, so that the image has size at most 4. As above we deduce that $\#E(\mathbb{Q})/\hat{\phi}(F(\mathbb{Q})) \leq 4$.

[S; 1 mark]

Since $\hat{\phi} \circ \phi = [2]$ it now follows that $\#E(\mathbb{Q})/2E(\mathbb{Q}) \leq 4$. However $E(\mathbb{Q})$ has 4 points of order dividing 2, so that $E_{\text{tors}}(\mathbb{Q})/2E_{\text{tors}}(\mathbb{Q})$ has order 4. The rank is therefore zero.

[S; 2 marks]

It follows that the only points are the torsion points, which have $X = 0, -1, -4$ or $-2$. Thus when $X = -2B^2C^{-2}$ as above we must have $B = C$ and hence $A, B, C, D$ are all equal.

[N; 2 marks]