Solution 1

$(-3)^3 \equiv 5 \pmod{32}$ so $n = -3$ is acceptable.
[2 marks]

If $|n^3 - 5|_5 < 5^{-3}$ then $n^3 \equiv 5 \pmod{625}$, whence $5|n$ and $125|n$, a contradiction.
[2 marks]

Suppose we are given a finite sequence $a_0, \ldots, a_n$ in R satisfying (i), (ii) and (iii) up to the n-th term. We show how to extend the sequence with an $(n+1)$-th term. We define $a_{n+1} = a_n + b_n$, where $b_n = -f(a_n)/f'(a_n)$. Note that $f'(a_n) \neq 0$, since $|f'(a_n)|^2 = |f'(a_0)|^2 > |f(a_0)|$, whence we cannot have $|f'(a_n)| = 0$. Thus (i) will hold if n is replaced by $n+1$.
[2 marks]

Note that

$$|b_n|^2 = |f(a_n)|^2/|f'(a_n)|^2 \leq |f(a_n)|\frac{|f(a_0)|}{|f'(a_0)|^2} < |f(a_n)| \tag{1}$$

by (ii) and (iii), whence

$$|b_n| < \sqrt{|f(a_n)|} \leq \sqrt{|f(a_0)|} < |f'(a_0)| = |f'(a_n)| \leq 1, \tag{2}$$

by a further application of (ii) and (iii).

A Taylor series expansion gives $f'(a_{n+1}) = f'(a_n+b_n) = f'(a_n)+b_n f''(a_n)+ \ldots$, in which the k-th term takes the form $b_n^k f_k(a_n)$ with a polynomial $f_k(x) \in R[x]$. It follows that $|f_k(a_n)| \leq 1$ for $k \geq 1$. Moreover (2) show that $|b_n^k| < |f'(a_n)|$ for $k \geq 1$. It follows that $|b_n f''(a_n) + b_n^2 f_2(a_n) + \ldots| < |f'(a_n)|$, and hence that $|f'(a_n)+b_n f''(a_n)+b_n^2 f_2(a_n)+\ldots| = |f'(a_n)|$. We therefore deduce that $|f'(a_{n+1})| = |f'(a_n)|$. Thus (ii) above remains true up to $n+1$.
[4 marks]

Finally we have another Taylor expansion $f(a_{n+1}) = f(a_n + b_n) = f(a_n) + b_n f'(a_n) + \ldots$, in which the k-th term now takes the form $b_n^k F_k(a_n)$ with a polynomial $F_k(x) \in R[x]$. Our choice of b_n ensures that $f(a_{n+1}) = b_n^2 F_2(a_n) + \ldots$. As before we have $|F_k(a_n)| \leq 1$ for $k \geq 2$. Moreover (1) yields $|b_n^k F_k(a_n)| < |f(a_n)|$ for $k \geq 2$, whence $|f(a_{n+1})| < |f(a_n)|$ as required for (iii).
[3 marks]

We therefore see that we can produce an infinite sequence satisfying (iii), and since the valuation is discrete this implies that $|f(a_n)| \to 0$. Parts (i) and (ii) then imply that $|a_{n+1} - a_n| \to 0$, which suffices to ensure that the sequence (a_n) is convergent, with limit a^*, say. By continuity of polynomials $f(a^*) = 0$. Moreover

$$|a^* - a_0| = \lim |a_n - a_0| \leq \sup |a_{i+1} - a_i| \leq \sup |f(a_i)|/|f'(a_i)| \leq |f(a_0)|/|f'(a_0)|.$$

Thus $a = a^*$ fulfills the conditions of the question.

[3 marks]

Under the new hypothesis we may proceed as before, to get a sequence satisfying (i) with n replace by $n+1$. Instead of (1) we have

$$|b_n|^2 = |f(a_n)|^2/|f'(a_n)|^2 \le |f(a_n)|\frac{|f(a_0)|}{|f'(a_0)|^2} \le |f(a_n)|,$$

and instead of (2),

$$|b_n| \le \sqrt{|f(a_n)|} \le \sqrt{|f(a_0)|} \le |f'(a_0)| = |f'(a_n)| < 1.$$

This suffices to show that $|b_n^k f_k(a_n)| < |f'(a_n)|$ for $k \ge 2$, while for $k = 1$ we have $f_1(x) = \frac{1}{2}f''(x)$, whence $|b_n f_1(a_n)| \le |f'(a_n) f_1(a_n)| < |f'(a_n)|$. The treatment of (ii) then goes through as before.

For (iii) we see from the above estimate that $|b_n^k| < |f(a_n)|$ if $k \ge 3$, so that $|b_n^k F_k(a_n)| < |f(a_n)|$. For $k = 2$ we have $F_2(x) = \frac{1}{2}f''(x)$, whence $|b_n^2 F_2(a_n)| \le |f(a_n) F_2(a_n)| < |f(a_n)|$. The proof may now be completed as before.

[5 marks]

Let $f(x) = x^3 + 3x + y^3 + 3y - n$, so that $f'(x) = 3x^2 + 3$ and $\frac{1}{2}f''(x) = 3x$. It follows that $|f'(b)| = 3^{-1}$ and $|\frac{1}{2}f''(b)| < 1$ for any $b \in \mathbb{Z}_3$. Thus if there exist a_0 and y such that $|f(a_0)| \le 3^{-2}$, then $f = 0$ is solvable. Hence it is sufficient (and clearly necessary) that $x^3 + 3x + y^3 + 3y \equiv n \pmod 9$ should be solvable. The required n are therefore those congruent to 0, 1, 4, 5 or 8 $\pmod 9$.

[4 marks]

Solution 2

Either $|x|_p \leqslant 1, |y|_p \leqslant 1$ or $|x|_p, |y|_p > 1$. Assume the latter, for a contradiction. Then the parameters $z = -x/y$ and $w = -1/y$ satisfy $|z|_P = |x|_p^{-1/2} < 1$ and $|w|_p < 1$, by the equation for $\mathcal{E}$. If (x, y) were torsion, then z would be a torsion point in $F_{\mathcal{E}}(p\mathbb{Z}_p)$. Thus it has order p^n for some $n \geq 1$, and $|z|_p \geq p^{-1/(p^n - p^{n-1})}$. However, $p^n - p^{n-1} > 1$ for $n \geq 1$, unless $p = 2$ and $n = 1$. If (x, y) has order 2 we have $y = 0$, contradicting the assumption that $|y|_p > 1$. Otherwise $1 > |z|_p > p^{-1}$, which is also impossible.
[4 marks]

When $\widetilde{\mathcal{E}}$ is non-singular the group $\widetilde{\mathcal{E}_{\text{ns}}}$ is the whole of $\widetilde{\mathcal{E}}$, and the reduction map is a group homomorphism from $\mathcal{E}(\mathbb{Q}_p)$ to $\widetilde{\mathcal{E}}(\mathbb{F}_p)$. The result just proved shows that no non-trivial torsion points of $\mathcal{E}(\mathbb{Q}_p)$ are mapped to zero by the reduction map, whence it is an injection on $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$. Thus $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$.
[4 marks]

If $y^2 = x^3 + ax + b$ is defined over $\mathbb{Z}$ and $(x_1, y_1) \in \mathbb{Q}^2$ is a non-trivial torsion point, then $|x_1|_p \leq 1$, $|y_1|_p \leq 1$ for every prime p, whence $x_1, y_1 \in \mathbb{Z}$.
[1 mark]

If $y_1 = 0$ then the result is immediate. Otherwise (x_1, y_1) is not 2-torsion and we consider $(x_2, y_2) = 2(x, y)$, with $(x_2, y_2) \neq \mathbf{0}$, whence $x_2, y_2 \in \mathbb{Q}$. However (x_2, y_2) is also a torsion point, so that $x_2, y_2 \in \mathbb{Z}$. The line tangent to $\mathcal{E}$ at (x_1, y_1) has slope $(3x_1^2 + a)/(2y_1)$, from which we have $x_2 = \big((3x_1^2 + a)/(2y_1)\big)^2 - 2x_1$. Since $x_2, x \in \mathbb{Z}$ we have $\big((3x_1^2 + a)/(2y_1)\big)^2 \in \mathbb{Z}$. It follows that $4y_1^2 | (3x_1^2 + a)^2$ and so $y_1^2 | (3x_1^2 + a)^2 = \psi_1(x_1)$. Also, $y_1^2 = x_1^3 + ax_1 + b = \psi_2(x_1)$. Using the identity given we conclude that $y_1^2 | (\phi_1(x_1)\psi_1(x_1) + \phi_2(x_1)\psi_2(x_1)) = \Delta$, as required.
[7 marks]

(a) $(1/4\,,\, a + 1/8)$ is on the curve, but is non-integral, and hence cannot be a torsion point.

[2 marks]

(b) $\Delta = 4.1^3 + 27.2^2 = 112$, so there is good reduction at 5, where the points in $\mathbb{F}_5$ are $(1, \pm 2), (4, 0)$ and $\mathbf{0}$. Only one of these has order 2 (with $y = 0$) so this is C_4. Globally the point $(-1, 0)$ has order 2, and if $P = (1, 2)$ calculation shows that $x(2P) = -1$, so that $2P$ must be $(-1, 0)$. Hence the $\mathbb{Q}$-torsion is $\{(1, 2), (1, -2), (-1, 0), \mathbf{0}\}$ of type C_4.

[3 marks]

(c) $\Delta = 4a^3 + 27b^2 \not\equiv 0 \pmod 5$ so there is good reduction at 5. Moreover $\widetilde{\mathcal{E}}$ is given by $y^2 = x^3 + x$, which has the points $\mathbf{0}, (\pm 2, 0)$ and $(0,0)$ over $\mathbb{F}_5$. Thus the rational torsion group has order dividing 4. Hence if there is non-trivial torsion there would be a rational point $(\alpha, 0)$ of order 2. Then α would be an integer root of $x^3 + ax + b \equiv x^3 + x + 1 \pmod 2$. This is impossible as $x^3 + x + 1$ is irreducible modulo 2.

[4 marks]

Solution 3

As coset representatives for $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ we may take non-zero square-free values $r \in \mathbb{Z}$. Such an r arises from $q(x, y)$ if and only if $x = ru^2$ and $x^2+ax+b = rv^2$ for some rational u, v. If $u = l/m$ in lowest terms, then $r^2l^4+ral^2m^2+bm^4 = rn^2$ with integers l, m for which $(l, m) = 1$ and $m \neq 0$. Since rn^2 is an integer and r is square-free it follows that n is also an integer. We claim that $r|b$. Otherwise there would be a prime $p|r$ with $p \nmid b$. Then $p|r(n^2-rl^4-al^2m^2) = bm^4$, whence $p|m$. This entails $p^2|r^2l^4 + ral^2m^2 + bm^4$, whence $p|rn^2$, from which we deduce that $p|n$. Finally we would have $p^3|rn^2 - ral^2m^2 - bm^4 = r^2l^4$, which imples that $p|l$. This contradicts our assumption that $(l, m) = 1$, and therefore shows that no such p can exist. It therefore follows that $r|b$, so that q must have finite image.

[7 marks]

The maps $\phi : \mathcal{C} \to \mathcal{D}$ and $\hat{\phi} : \mathcal{D} \to \mathcal{C}$ are homomomorphisms with $\phi\hat{\phi}$ and $\hat{\phi}\phi$ being [2] on the respective groups $\mathcal{D}$ and $\mathcal{C}$. We are told that $\ker(q) = \hat{\phi}(\mathcal{D})$, and we have a similar map $\hat{q}$ on $\mathcal{D}$ with $\ker(\hat{q}) = \phi(\mathcal{C})$. We then obtain induced injective homomorphisms from $\mathcal{C}/\hat{\phi}(\mathcal{D})$ and $\mathcal{D}/\phi(\mathcal{C})$ into $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, each with finite image, as above. Thus $\mathcal{C}/\hat{\phi}(\mathcal{D})$ and $\mathcal{D}/\phi(\mathcal{C})$ are finite.

Let $\{g_1, \ldots, g_k\}$ be coset representatives for $\mathcal{C}/\hat{\phi}(\mathcal{D})$, and similarly $\{h_1, \ldots, h_l\}$ for $\mathcal{D}/\phi(\mathcal{C})$. Given $g \in \mathcal{C}$ there is a g_i and an $h \in \mathcal{D}$ such that $g = g_i + \hat{\phi}(h)$. Similarly there is an h_j and a $g' \in \mathcal{C}$ so that $h = h_j + \phi(g')$. Since $\hat{\phi}$ is a homomorphism, and $\hat{\phi}\phi = [2]$ we have

$$g = g_i + \hat{\phi}(h) = g_i + \hat{\phi}(h_j + \phi(g')) = g_i + \hat{\phi}(h_j) + \hat{\phi}\phi(g') = g_i + \hat{\phi}(h_j) + 2g'.$$

Thus the cosets $g_i + \hat{\phi}(h_j) + 2\mathcal{C}(\mathbb{Q})$ cover $\mathcal{C}$, whence $\mathcal{C}/2\mathcal{C}$ is finite.

[7 marks — Bookwork to here]

For $y^2 = x(x^2 - p^2)$ we have $s = 2$. The image of q corresponds to solvable equations $r^2l^4 - p^2m^4 = rn^2$, with $r|p$; and since $\mathcal{E}'$ is given by $y^2 = x(x^2 + 4p^2)$ the image of $\hat{q}$ corresponds to solvable equations $r^2l^4 + 4p^2m^4 = rn^2$, with $r|2p$. For $r^2l^4 - p^2m^4 = rn^2$ there are solutions $(1, 0, 1), (0, 1, p), (1, 1, 0)$ and $(1, 1, 0)$ for $r = 1, -1, p$ and $-p$ respectively. For $r^2l^4 + 4p^2m^4 = rn^2$ we must clearly have $r > 0$. Thus there are at most 4 possibilities for r, namely $1, 2, p$ and $2p$. Hence, from the above,

$$2^{R+2} = \#\mathcal{C}/2\mathcal{C} \leq \big(\#\mathcal{C}/\hat{\phi}(\mathcal{D})\big)\big(\#\mathcal{D}/\phi(\mathcal{C})\big) \leq 4 \times 4,$$

so that the rank is always at most 2.

[5 marks]

If $x^4+p^2y^4 = 2z^2$ has a non-trivial integral solution we may choose a minimal one. If $p|z$ we would have $p|x$ and so $y^4 + p^2(x/p)^4 = 2(z/p)^2$, contradicting minimality. Hence $p \nmid z$. However $2z^2 \equiv x^4 \pmod{p}$, and therefore $(\frac{2}{p}) = +1$.

[2 marks]

Thus if $r^2l^4 + 4p^2m^4 = rn^2$ and $r = 2$ then $p \equiv \pm 1 \pmod{8}$. Thus for $p \equiv 3$ or $5 \pmod{8}$ the case $r = 2$ cannot occur, giving $\#\mathcal{D}/\phi(\mathcal{C}) \leq 3$, whence $R < 2$.

[2 marks]

For $p = 5$ the curve C has a point $(x, y) = (25/4, 75/8)$, which is non-integral and therefore of infinite order. Thus $R \geq 1$, and hence $R = 1$.

[2 marks — Unseen, but similar to previous exam questions]