SOLUTIONS TO THE ELLIPTIC CURVES QUESTIONS ON THE 2007 EXAMINATION.

Question 1.

(i) [*Seen similar on problem sheet*]. Let $x_0 = a_0 = 1$. Then $|x_0^2 + 2|_3 = 3^{-1}$. Look for $x_1 = a_0 + 3a_1$ such that $|x_1^2 + 2|_3 \leqslant 3^{-2}$. This is satisfied if: $(1 + 3a_1)^2 \equiv -2 \pmod{3^2}$ $\iff$ $2 \cdot 1 \cdot 3a_1 \equiv -2 - 1 \pmod{3^2}$ $\iff$ $2a_1 \equiv -1 \pmod 3$ $\iff$ $a_1 \equiv 1 \pmod 3$. So, now define: $a_1 = 1$ and $x_1 = a_0 + 3a_1 = 4$. Check that indeed $|x_1^2 + 2|_3 = |18|_3 = 3^{-2}$.
Now, look for $x_2 = a_0 + 3a_1 + 3^2a_2$ such that $|x_2^2 + 2|_3 \leqslant 3^{-3}$. This is satisfied if: $(4 + 3^2a_2)^2 \equiv -2 \pmod{3^3}$ $\iff$ $2 \cdot 4 \cdot 3^2a_2 \equiv -2 - 16 \equiv -18 \pmod{3^3}$ $\iff$ $8a_2 \equiv -2 \pmod 3$ $\iff$ $a_2 \equiv 2 \pmod 3$. So, now define: $a_2 = 2$ and $x_2 = 4 + 3^2a_2 = 22$. Check that indeed $|x_2^2 + 2|_3 = |486|_3 = |3^3 \cdot 18|_3 < 3^{-2}$.

Suppose there were such an $x \in \mathbb{Z}$ such that $|x^2 + 3|_3 < 3^{-2}$, and let $|x|_3 = 3^r$, for some $r \in \mathbb{Z}$. Then $|x^2|_3 = 3^{2r}$. Note that $|-3|_3 = |3|_3 = 3^{-1}$, so that $|x^2|_3 \neq |3|_3$, which means [from the general property for any p-adic valuation that, if $|a|_p \neq |b|_p$ then $|a + b|_p = \max(|a|_p, |b|_p)$] that $|x^2 + 3|_3 = \max(3^{2r}, 3^{-1})$. If $r < 0$ then $3^{2r} < 3^{-1}$ and so this maximum will be 3^{-1}; if $r \geqslant 0$ then $3^{2r} > 3^{-1}$ and so this maximum will be 3^{2r}. In either case, we must always have $|x^2 + 3|_3 \geqslant 3^{-1}$, and so it never happens that $|x^2 + 3|_3 < 3^{-2}$.

[6 marks]

(ii) [*Unseen*]. For prime $p \neq 2$, we have: $\frac{1+2p}{p-p^3} = \frac{1}{p}\frac{1+2p}{1-p^2} = \frac{1}{p}(1 + 2p)(1 + p^2 + p^4 + \ldots) = \frac{1}{p}(1 + 2p + p^2 + 2p^3 + p^4 + 2p^5 \ldots) = \frac{1}{p} + 2 + p + 2p^3 + p^4 + 2p^5 \ldots = 12, \overline{12}$, and so we suspect this is the expansion (or, can find the first few terms and initially guess the pattern). So, now let $\alpha = \frac{1}{p} + 2 + p + 2p^3 + p^4 + 2p^5 \ldots = 12, \overline{12}$, in which case $\alpha - (\frac{1}{p} + 2) = 0, \overline{12} = p^2\alpha$, so that $(1 - p^2)\alpha = \frac{1}{p} + 2$, and so $\alpha = \frac{1+2p}{p-p^3}$, as required. **[5 marks]**

(iii) [*Unseen*]. Imagine $p = p^p$ in $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^p$. Then $p^{-(p-1)} = p/p^p \in (\mathbb{Q}_p^*)^p$, so that $p^{-(p-1)} = w^p$ for some $w \in \mathbb{Q}_p^*$, and so $p^{p-1} = |p^{-(p-1)}|_p = |w^p|_p = |w|_p^p$. But $|w|_p = p^r$, for some $r \in \mathbb{Z}$ and so $p^{p-1} = p^{rp}$, a contradiction, since the right hand exponent is a multiple of p and the left hand exponent is in the range between 1 and $p - 1$ (and so is not a multiple of p). Hence it is never true (for any p) that $p = p^p$ in $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^p$. **[5 marks]**

(iv) [*Unseen*]. Let $s_n \in \mathbb{Z}$ denote the inverse of r^n mod q^n and let $t_n \in \mathbb{Z}$ denote the inverse of q^n mod r^n (which exist, since q^n, r^n are coprime), so that $s_n r^n \to 1$ with respect to $|\ |_q$ and $t_n q^n \to 1$ with respect to $|\ |_r$. Let $x_n = s_n r^n \alpha + t_n q^n \beta$, which satisfies $x_n \to \alpha$ with respect to $|\ |_q$, and $x_n \to \beta$ with respect to $|\ |_r$, as $n \to \infty$, as required.

Let π_i denote the ith prime, and define $y_n = (\pi_1\pi_2\dots\pi_n)^n/\pi_{n+1}^{n^2+1}$. Then, for any prime $p = \pi_i$, we have $|y_n|_p = p^{-n}$ for all $n \geqslant i$, so that $y_n \to 0$ with respect to $|\ \ |_p$ as $n \to \infty$. Also, $|y_n|_\infty \leqslant 1/\pi_{n+1}$, so that $y_n \to 0$ with respect to $|\ \ |_\infty$ as $n \to \infty$. **[9 marks]**

Question 2.

(i) [*Proof from lectures*]. If $\mathrm{char}(R) \neq 0$ then $|p| = 0$, so assume that $\mathrm{char}(R) = 0$. We have from lectures that $[p](T) = pf(T) + g(T^p)$ for some $f(T) = T + \ldots \in R_T$ and $g(T) \in R_T$. We shall proceed by induction on n.

Suppose $z \neq 0$, $z \in \mathcal{M}$ and $[p](z) = 0$. Then $0 = pf(z) + g(z^p) = p(z + \ldots) + g(z^p)$. We cannot have $|pz| > |z^p|$, since then the term pz would have valuation strictly greater than the valuations all other terms. Hence $|pz| \leqslant |z^p| = |z|^p$, and so $|p| \leqslant |z|^{p-1}$, giving $|z| \geqslant |p|^{\frac{1}{p^1-p^0}}$, proving the result for $n = 1$.

Now, assume the result is true for n, and let $z \in F(\mathcal{M})$ have order p^{n+1}. Then $[p](z)$ has order n, and by the induction hypothesis, $|[p](z)| \geqslant |p|^{\frac{1}{p^n-p^{n-1}}}$. Hence:

$$|p|^{\frac{1}{p^n-p^{n-1}}} \leqslant |[p](z)| = |pf(z) + g(z^p)| \leqslant \max\big(|pz|, |z^p|\big).$$

But $|z| < 1, |p| < 1$, so that $|p|^{\frac{1}{p^n-p^{n-1}}} \geqslant |p| > |pz|$, giving $|p|^{\frac{1}{p^n-p^{n-1}}} \leqslant |z^p|$, and so $|z| \geqslant |p|^{\frac{1}{p^{n+1}-p^n}}$, as required. **[9 marks]**

(ii) [*Proof from lectures*]. Let $\underline{\mathbf{o}} \neq (x, y) \in \mathcal{E}(\mathbb{Q}_p)$ be in the kernel of reduction, that is, $|x|_p, |y|_p > 1$. Then, from the equation for $\mathcal{E}$, $|y|_p = |x|_p^{3/2}$ and $|z| = |-x/y|_p = |x|_p^{-1/2} < 1, |w| = |-1/y|_p < 1$. If (x, y) were torsion, then z would be a torsion point in $F_{\mathcal{E}}(\mathcal{M}) = F_{\mathcal{E}}(p\mathbb{Z}_p)$. From lectures, it must be of order p^n, and so by (i) must satisfy $1 > |z|_p \geqslant |p|_p^{\frac{1}{p^n-p^{n-1}}}$ [corresponding to $1 < |x|_p \leqslant |p|_p^{\frac{-2}{p^n-p^{n-1}}}$ and $1 < |y|_p \leqslant |p|_p^{\frac{-3}{p^n-p^{n-1}}}$]. Note that, since $|p|_p = p^{-1}$, any p^n apart from 2^1 [so that $p^n - p^{n-1} > 1$] would force $1 > |z|_p > p^{-1}$, contradicting the fact that $|z|_p$ is p^r for some integer r. The only remaining possibility is that (x, y) is of order 2; but then $y = 0$ and x is a root of $x^3 + Ax + B$; this is incompatible with $|x|_p > 1$ [which makes x^3 have strictly larger valuation than Ax and B]. We conclude that x, y cannot be torsion, and that there is no torsion (apart from $\underline{\mathbf{o}}$) in the kernel of reduction.

When $\widetilde{\mathcal{E}}$ is non-singular, $\mathcal{E}_0(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Q}_p)$ and $\widetilde{\mathcal{E}}_{ns}(\mathbb{F}_p) = \widetilde{\mathcal{E}}(\mathbb{F}_p)$ and the reduction map $\sim : \mathcal{E}(\mathbb{Q}_p) \to \widetilde{\mathcal{E}}(\mathbb{F}_p)$ contains no nontrivial torsion, and so is injective when restricted to $\mathcal{E}_{\mathrm{tors}}(\mathbb{Q}_p)$; hence $\mathcal{E}_{\mathrm{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$. **[8 marks]**

(iii) [*Unseen*]. Here, $A = D, B = 0$, so that $2(4A^3 + 27B^2) = 8D^3$ and D is not divisible by 3. So, by (iii), we can take $p = 3$, which does not divide $2(4A^3 + 27B^2)$, and so $\mathcal{E}_{\mathrm{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_3)$. But note that $\widetilde{\mathcal{E}} : Y^2 = X^3 + 2X = X(X+1)(X-1)$, and so $\widetilde{\mathcal{E}}(\mathbb{F}_p) = \{\underline{\mathbf{o}}, (0,0), (1,0), (2,0)\}$, which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Hence $\mathcal{E}_{\mathrm{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. But note that $\underline{\mathbf{o}}, (0,0) \in \mathcal{E}_{\mathrm{tors}}(\mathbb{Q})$ and so $\mathcal{E}_{\mathrm{tors}}(\mathbb{Q})$ must be isomorphic to either $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. But we can exclude the latter, since

$D > 0$ and so $(\sqrt{-D}, 0)$ and $(-\sqrt{-D}, 0)$ are not in $\mathcal{E}_{\text{tors}}(\mathbb{Q})$. Therefore, $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomrphic to $\mathbb{Z}/2\mathbb{Z}$ and $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\underline{\mathbf{o}}, (0,0)\}$. **[8 marks]**

Question 3.

(i) [*Proof from lectures*]. Let $(u_1, v_1), (u_2, v_2), (u_3, v_3)$ be 3 points on $\mathcal{D}(\mathbb{Q})$ which sum to $\underline{\mathbf{o}}$, so that $(u_1, v_1) + (u_2, v_2) = (u_3, -v_3)$. Then there are the 3 points of intersection between $\mathcal{D}$ and some line defined over $\mathbb{Q}$: $Y = \ell X + m$, say. Substituting $Y = \ell X + m$ into $\mathcal{D}$ gives: $X(X^2 + a_1X + b_1) - (\ell X + m)^2$, whose 3 roots must be u_1, u_2, u_3. That is: $X(X^2 + a_1X + b_1) - (\ell X + m)^2 = (X - u_1)(X - u_2)(X - u_3)$. Equating constant terms gives: $u_1u_2u_3 = m^2 = 1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, and so $u_1u_2 = 1/u_3 = u_3$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Therefore, by the definition of q we have: $q\big((u_1, v_1)\big)q\big((u_2, v_2)\big) = q\big((u_3, v_3)\big)$, as required. **[6 marks]**

(ii) [*Proof from lectures*]. Given $(u, v) \in \mathcal{D}(\mathbb{Q})$, with $(u, v) \neq (0, 0)$, we can see that (x, y) (not necessarily $\mathbb{Q}$-rational) on $\mathcal{C}$, a preimage of (u, v) under ϕ, satisfies: $y/x = \pm\sqrt{u}$ [since $u = y^2/x^2$]. Combining this with: $(x/y)v = x - b/x$ and $u = x + b/x + a$ [since $u = y^2/x^2 = x(x^2 + ax + b)/x^2$] gives: $x = (u \pm v/\sqrt{u} - a)/2$, and so $y = (y/x)x = \pm\sqrt{u}(u \pm v/\sqrt{u} - a)/2$. Clearly, $(u, v) \in \phi(\mathcal{C}(\mathbb{Q})) \iff$
$\big((u + v/\sqrt{u} - a)/2, \sqrt{u}(u + v/\sqrt{u} - a)/2\big)$ or $\big((u - v/\sqrt{u} - a)/2, -\sqrt{u}(u - v/\sqrt{u} - a)/2\big)$ is in $\mathcal{C}(\mathbb{Q})$
$\iff \sqrt{u} \in \mathbb{Q} \iff q\big((u, v)\big) = 1$, as required. Also, note that the preimages under ϕ of $(0, 0)$ are $(-a/2 + \sqrt{b_1}/2, 0)$, $(-a/2 - \sqrt{b_1}/2, 0)$ and so $(0, 0) \in \phi(\mathcal{C}(\mathbb{Q})) \iff b_1 \in (\mathbb{Q}^*)^2 \iff q\big((0, 0)\big) = 1$.

[5 marks]

(iii) [*Seen similar on a problem sheet*].

Let $\mathcal{C} : Y^2 = X(X^2 + aX + b) = X(X^2 + X - 2)$, where $a = 1, b = -2$, and isogenous curve $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1) = X(X^2 - 2X + 9)$, where $a_1 = -2, b_1 = 9$, with the usual isogeny $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto (y^2/x^2, y + 2y/x^2)$, and dual isogeny $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) : (u, v) \mapsto (\frac{1}{4}v^2/u^2, \frac{1}{8}(v - 9v/u^2))$.

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u$, for $(u, v) \neq (0, 0)$, with $q : (0, 0) \mapsto b_1$ and $q : \underline{\mathbf{o}} \mapsto 1$, is an injection with im$q$ contained in $\{d : d \text{ is square free and } d | b_1\} = \{\pm 1, \pm 3\}$. Also, $\underline{\mathbf{o}} \mapsto 1$, $(0, 0) \mapsto 9 = 1$ and $(3, 6) \mapsto 3$, so that $\{1, 3\} \subset \text{im}q \subset \{\pm 1, \pm 3\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in \text{im}q$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a_1\ell^2m^2 + (b_1/(-1)) \cdot m^4 = n^2$ that is: $-\ell^4 - 2\ell^2m^2 - 9m^4 = n^2$. This is impossible in $\mathbb{R}$, and so impossible in $\mathbb{Q}$. Hence $-1 \notin \text{im}q$.

We conclude that im$q = \{1, 3\}$, and so $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ is generated by $(3, 6)$.

The map $\hat{q} : \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x, y) \mapsto u$, for $(x, y) \neq (0, 0)$, with $\hat{q} : (0, 0) \mapsto b$ and $\hat{q} : \underline{\mathbf{o}} \mapsto 1$, is an injection with im$\hat{q}$ contained in $\{d : d \text{ is square free and } d | b\} = \{\pm 1, \pm 2\}$. Also, $\underline{\mathbf{o}} \mapsto 1$ and $(0, 0) \mapsto -2$, so that $\{1, -2\} \subset \text{im}\hat{q} \subset \{\pm 1, \pm 2\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in \mathrm{im}\hat{q}$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a\ell^2 m^2 + (b/(-1)) \cdot m^4 = n^2$; that is: $-\ell^4 + \ell^2 m^2 + 2m^4 = n^2$. Multiply both sides by 4 and rewrite as: $-(2\ell^2 - m^2)^2 + 9m^4 = 4n^2$. Reducing modulo 3 gives: $-(2\ell^2 - m^2)^2 \equiv n^2$ (modulo 3). If n were coprime to 3, then this would give: $((2\ell^2 - m^2)/n)^2 = -1$ in $\mathcal{F}_3$, contradicting the fact that -1 is not a quadratic residue modulo 3. So, $3|n$ and so $3|(2\ell^2 - m^2)$, also. Then $2\ell^2 \equiv m^2$ and so by the same reasoning (since 2 is not a quadratic residue modulo 3) we have that $3|\ell$ and $3|m$. This contradicts the fact that $\gcd(\ell, m) = 1$. Hence our equation is impossible in $\mathbb{Q}_3$, and so impossible in $\mathbb{Q}$. Hence $-1 \notin \mathrm{im}\hat{q}$.

We conclude that $\mathrm{im}\hat{q} = \{1, -2\}$, and so $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ is generated by $(0, 0)$.

Finally, since multiplication by 2 in $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi} \circ \phi$, we have that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $(0, 0)$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((3, 6)\big) = (1, 0)$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0, 0)$ and $(1, 0)$, both of which are points of finite order (order 2, in fact). Conclusion: $\mathcal{C}(\mathbb{Q})$ has rank 0. **[14 marks]**

Question 4.

(i) [*Seen similar on a problem sheet*]. The line tangent to $\mathcal{E}$ at $P = (2, 1)$ has slope y' given by $2yy' = 3x^2 - 1$, with $x = 2, y = 1$; that is, the slope is $11/2$. This tangent line also goes through $(2, 1)$ and so has equation: $Y = (11/2)X - 10$. Note that $2 \cdot 5287 = 10574 \equiv 1$, so that 5287 is the inverse of 2 mod N, and the the tangent line has equation: $Y = (11 \cdot 5287)X - 10 \equiv 5292X - 10$. The x-coordinate of $2P$ is therefore $5292^2 - (2 + 2) \equiv 7956$, and the y-coordinate is: $-(5292 \cdot 7956 - 10) = 42103142 \equiv 1456$, so that $Q = 2P \equiv (7956, 1456)$ (modulo $N = 10573$). We now wish to compute $3P = P + 2P = P + Q$, and so the first step is to find the line joining $P = (2, 1)$ to $Q = (7956, 1456)$. We must compute the slope given by $(1456 - 1)/(7956 - 2) = 1455/7954$ (modulo $N = 10573$), for which the first step is to find the inverse of 7954 (modulo $N = 10573$). Using Euclid's Algorithm: $10573 = 1 \cdot 7954 + 2619$; $7954 = 3 \cdot 2619 + 97$, $2619 = 27 \cdot 97 + 0$. So, we cannot find the inverse of 7954 (modulo $N = 10573$), and this step has given us a factor 97 of N.

[8 marks]

(ii) [*Unseen*]. Let $P = (s, t)$, where $s = c/d$, with $c, d \in \mathbb{Z}$ and $\gcd(c, d) = 1$, so that $h_x(P) = \log(\max(|c|, |d|))$. Then $\phi(P) = (y^2/x^2, y - by/x^2) = ((x^2 + ax + b)/x, y - by/x^2)$, and $(x^2 + ax + b)/x = (c^2 + acd + bd^2)/cd$, and reducing this to lowest terms will only decrease the height, so that: $h_x(\phi(P)) \leqslant \log(\max(|c^2 + acd + bd^2|, |cd|)) \leqslant \log(\max((1 + |a| + |b|)\max(|c|, |d|)^2, \max(|c|, |d|)^2)) = \log((1 + |a| + |b|)\max(|c|, |d|)^2) = \log((1 + |a| + |b|) + 2\log(\max(|c|, |d|)) = k + 2h_x(\phi(P))$, where $k = \log(1 + |a| + |b|)$. Recall that $\hat{\phi} : \mathcal{D} \to \mathcal{C} : (u, v) \mapsto (\frac{1}{4}\frac{v^2}{u^2}, \frac{1}{8}(v - b_1 v/u^2))$. Similarly, for any $Q \in \mathcal{D}(\mathbb{Q})$, we have $h_x(\hat{\phi}(Q)) \leqslant \log(4(1 + |a_1| + |b_1|)) + 2h_x(Q)$, and so $h_x(2P) = h_x(\hat{\phi}(\phi(P))) \leqslant \log(4(1 + |a_1| + |b_1|)) + 2h_x(\phi(P)) \leqslant$

$\log(4(1+|a_1|+|b_1|))+2(k+h_x(P))=\ell+4h_x(P)$, where $\ell=\log(4(1+|a_1|+|b_1|))+2k=\log(4(1+|2a|+|a^2-4b|))+2\log(1+|a|+|b|)$. **[8 marks]**

(iii) [*Unseen*]. Let $n=m^2$. Since $p\neq 2$, we must have $p\equiv 1$ or $3 \pmod 4$. First consider the case when $p\equiv 3 \pmod 4$, so that $\left(\frac{-1}{p}\right)=-1$ and so, for any u, $\left(\frac{-u(u^2+n)}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{u(u^2+n)}{p}\right)=-\left(\frac{u(u^2+n)}{p}\right)$. Now, let $u\neq 0, u\in\mathcal{F}_p$. If u is a root of X^2+n then so is $-u$, giving the two points $(u,0),(-u,0)\in\mathcal{E}(\mathcal{F}_p)$. If u is not a root of X^2+n then $u(u^2+n)\neq 0$ and from the identity we have just shown, exactly one of $\left(\frac{-u(u^2+n)}{p}\right)$ and $\left(\frac{u(u^2+n)}{p}\right)$ is equal to 1 and the other is equal to -1. Without loss of generality, say that $\left(\frac{u(u^2+n)}{p}\right)=1$ and $\left(\frac{-u(u^2+n)}{p}\right)=-1$. Then there exists $v\neq 0, v\in\mathcal{F}_p$ such that $v^2=u(u^2+n)$, but there does not exist v such that $v^2=-u(u^2+n)$. This gives the two points (u,v) and $(u,-v)$ in $\mathcal{E}(\mathcal{F}_p)$ with X-coordinate u and no points in $\mathcal{E}(\mathcal{F}_p)$ with X-coordinate u. So, in all cases, there are two points in $\mathcal{E}(\mathcal{F}_p)$ with X-coordinate u or $-u$. Divide the $p-1$ nonzero elements of $\mathcal{F}_p$ into pairs $u,-u$, each pair contributing two members of $\mathcal{E}(\mathcal{F}_p)$; this gives so far a total of $p-1$ members of $\mathcal{E}(\mathcal{F}_p)$ with nonzero X-coordinate. When we also include the points $\mathbf{o},(0,0)\in\mathcal{E}(\mathcal{F}_p)$, then we finally obtain $\#\mathcal{E}(\mathcal{F}_p)=p+1$, as required. Since $p\equiv 3 \pmod 4$, it is immediate that $4|(p+1)$; that is: $4|\#\mathcal{E}(\mathcal{F}_p)$, as required.

For the case when $p\equiv 1 \pmod 4$, we have $\left(\frac{-1}{p}\right)=1$ and so there exists $w\in\mathcal{F}_p$ such that $w^2=-1$. Then $\mathcal{E}: Y^2=X(X^2+m^2)=X(X+wm)(X-wm)$, and so $\{\underline{\mathbf{o}},(0,0),(-wm,0),(wm,0)\}$ is a subgroup of $\mathcal{E}(\mathcal{F}_p)$, which again means that $4|\#\mathcal{E}(\mathcal{F}_p)$, as required. **[9 marks]**

General Comment: In the above solutions, I have given everything in full pedantic detail, in order to make every step as clear as possible to a non-specialist. Students could gain full marks from intelligently shortened versions of the above answers.