Solution to Question 1.

(i) [*Easy variation of example from Exercise Sheets.*] Let $x_0 = a_0 = 2$. Then $|x_0^2+6|_5 = 5^{-1}$. Look for $x_1 = a_0 + 5a_1$ such that $|x_1^2+6|_5 \leqslant 5^{-2}$. This is satisfied if: $(2+5a_1)^2 \equiv -6 \pmod{5^2} \iff 2\cdot 2\cdot 5a_1 \equiv -6-2^2 \pmod{5^2} \iff 4a_1 \equiv -2 \pmod 5 \iff a_1 \equiv 2 \pmod 5$. So, now define: $a_1 = 2$ and $x_1 = a_0 + 5a_1 = 12$. Check that indeed $|x_1^2+6|_5 = |150|_5 = 5^{-2}$.

Now, look for $x_2 = a_0 + 5a_1 + 5^2a_2$ such that $|x_2^2+6|_5 \leqslant 5^{-3}$. This is satisfied if: $(12+5^2a_2)^2 \equiv -6 \pmod{5^3} \iff 2\cdot 12\cdot 5^2a_2 \equiv -6-12^2 \pmod{5^3} \iff 24a_2 \equiv -6 \pmod 5 \iff a_2 \equiv 1 \pmod 5$. So, now define: $a_2 = 1$ and $x_2 = 12 + 5^2a_2 = 37$. Check that indeed $|x_2^2+6|_5 = |1375|_5 = 5^{-3}$.

Now, look for $x_3 = a_0 + 5a_1 + 5^2a_2 + 5^3a_3$ such that $|x_3^2+6|_5 \leqslant 5^{-4}$. This is satisfied if: $(37+5^3a_3)^2 \equiv -6 \pmod{5^4} \iff 2\cdot 37\cdot 5^3a_3 \equiv -6-37^2 \pmod{5^4} \iff 74a_2 \equiv -11 \pmod 5 \iff a_3 \equiv 1 \pmod 5$. So, now define: $a_3 = 1$ and $x_3 = 37 + 5^3a_3 = 162$. Check that indeed $|x_3^2+6|_5 = |26250|_5 = 5^{-4}$. **[2 marks]**

(ii) [*Easy variation of example from Exercise Sheets.*] Let $\beta = \alpha - 11/5 = 0,\overline{14}$. Then $5^2\beta = 0,00\overline{14} = \beta - (1\cdot 5^1 + 4\cdot 5^2)$; that is: $24\beta = -105$ and so $\beta = -105/24$. This gives: $\alpha = \beta + 11/5 = -87/40$. **[2 marks]**

(iii) [*Unseen.*] The map $x \mapsto x^2$ on F_p takes $0 \mapsto 0$, and is a 2-to-1 map on $\mathcal{F}_p^*$. It follows that the both of the sets $\{a - y^2 : y \in \mathcal{F}_p\}$ and $\{x^2 : x \in \mathcal{F}_p\}$ have size $(p-1)/2 + 1 = (p+1)/2$.

Since $\mathcal{F}_p$ has only p elements, and the sum of the sizes of these sets is $p+1$, there must be an element common to both sets. That is, there must exist $x, y \in \mathcal{F}_p$ such that $x^2 = a - y^2$, and so $x^2 + y^2 = a$.

Let $a \in \mathcal{F}_p$ be the reduction of b modulo p. Then $a \in \mathcal{F}_p^*$, since $|b|_p = 1$. From above, there exist $x_0, y_0 \in \mathcal{F}_p$ such that $x_0^2 + y_0^2 = a$ in $\mathcal{F}_p$. Since $a \neq 0$, at least one of x_0, y_0 is nonzero; say that $x_0 \neq 0$. Let $y \in \mathbb{Z}$ be any choice of $y \equiv y_0$ modulo p. Then $b - y^2 \in \mathbb{Z}$, satisfies $|b-y^2|_p = 1$ and there exists an x_0 such that $|x_0^2 - (b-y^2)|_p < 1$. Applying Hensel's Lemma to the polynomial $F(T) = T^2 - (b-y^2)$ gives that there must exist an $x \in \mathbb{Z}_p$ such that $F(x) = 0$, as required. **[4 marks]**

(iv) [*Seen similar on an Exercise Sheet.*] The discriminant of $f(X) = X^3 + 2X + 2$ is $4\cdot 2^3 + 27\cdot 2^2 = 140 = 2^2\cdot 5\cdot 7$, so the curve $\widetilde{\mathcal{E}} : Y^2 = X^3 + 2X + 2$ is an elliptic curve over all $\mathcal{F}_p$ except $p = 2, 5, 7$.

For $p \geqslant 11$, the number of points in $\mathcal{E}(\mathcal{F}_p)$ is at least $p + 1 - 2\sqrt{p} > 4$. Excluding $\mathbf{o}$ and points of the form $(x, 0)$ (of which there are at most 3), there must be at least one point

$(x_0, y_0) \in \mathcal{E}(\mathcal{F}_p)$ such that $y_0 \neq 0$. Let $\alpha = x_0^3 + 2x_0 + 2$; then $|\alpha|_p = 1$ and there exists y_0 such that $|y_0^2 - \alpha|_p < 1$. So, applying Hensel's Lemma to $G(T) = T^2 - \alpha$, there exists $y \in \mathbb{Z}_p$ such that $y^2 = x_0^3 + 2x_0 + 2$.

For $p = 2$, working modulo 8, we see that, for $X = 0, 1, \ldots 7$, we have $f(X)$ congruent to $2, 5, 6, 3, 2, 1, 6, 7$. Taking $x = 5$ then gives $f(x) = 137 \equiv 1 \pmod 8$, and so by a standard instance of Hensel's Lemma from lectures [namely that, when $|a|_2 = 1$, a is a square in $\mathbb{Z}_2$ if and only if $a \equiv 1 \bmod 8$], there exists $y \in \mathbb{Z}_2$ such that $y^2 = 137$, giving $(5, y) \in \mathcal{E}(\mathbb{Z}_2)$.

For $p = 3$, working modulo 3, we see that for $X = 0, 1, 2$, we have $f(X)$ congruent to $2, 2, 2$ modulo 3; but 2 is not a square mod 3. [So there can't be any $(x, y) \in \mathcal{E}(\mathbb{Z}_p)$ since, if there were, the reduction of the point modulo 3 would give a solution to $y^2 = x^3 + 2x + 2$ in $\mathcal{F}_3$].

For $p = 5$, working modulo 5, we see that for $X = 0, 1, 2, 3, 4$, we have $f(X)$ congruent to $2, 0, 4, 0, 4$ modulo 5. Taking, for example, $x = 2$, then gives $f(x) = 14 \equiv 4 \pmod 5$, which is a square in $\mathcal{F}_5$, and so by a standard instance of Hensel's Lemma from lectures [namely that, when $|a|_p = 1$, $p \neq 2$, a is a square in $\mathbb{Z}_p$ if and only if a is a square in $\mathcal{F}_p$], there exists $y \in \mathbb{Z}_5$ such that $y^2 = 14$, giving $(2, y) \in \mathcal{E}(\mathbb{Z}_5)$.

For $p = 7$, working modulo 7, we immediately notice that, taking $x = 0$ gives $f(0) = 2$, which is a square in $\mathcal{F}_7$, and so by the same standard instance of Hensel's Lemma from lectures as above, there exists $y \in \mathbb{Z}_7$ such that $y^2 = 2$, giving $(0, y) \in \mathcal{E}(\mathbb{Z}_7)$.

Conclusion: there exist $x, y \in \mathbb{Z}_p$ such that $y^2 = x^3 + 2x + 2$, for all p except $p = 3$. Finally, there do not exist such $x, y \in \mathbb{Z}$, since $\mathbb{Z} \subset \mathbb{Z}_3$. **[5 marks]**

(v) This part is open ended, and answers will vary from student to student. In a high quality answer, I am looking for a variety of types of examples; particularly interesting are those which have solutions in every $\mathbb{Z}_p$ and those which have no solutions for lots of specific p. The answer should ideally describe methodology for obtaining examples, and a very good answer might notice enough patterns to describe families of curves that have certain local properties. **[7 marks]**

Solution to Question 2.

(i) [*Seen similar on Exercise Sheets (although this one is computationally harder).*]

There are the obvious points: $\mathbf{o}, (0, 0), (-1, 0), (-4, 0)$, all of order 2 in $\mathcal{E}_{\text{tors}}(\mathbb{Q})$. There's a further obvious point: $(2, 6)$, and note that $2(2, 6) = (0, 0)$ so that $(2, 6) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$ also, and is of order 4. The points $P = (-1, 0)$ and $Q = (2, 6)$ generate a $C_2 \times C_4$ group in $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ whose members are: $mP + nQ$ for $0 \leqslant m \leqslant 1$ and $0 \leqslant n \leqslant 3$. So, this group of size 8 is a subgroup of $\mathcal{E}_{\text{tors}}(\mathbb{Q})$. Now, over $\mathbb{Q}$, we can transform $\mathcal{E}$ (after the map: $(x, y) \mapsto (9x + 15, 27y)$) to the curve: $Y^2 = X^3 - 351X + 1890$. This new cubic has discriminant $4(-351)^3 + 27(1890)^3 = -76527504 = 2^4 3^{14}$, and so we only need to avoid the

primes $2, 3$. [N.B. If you don't like the idea of factorising a number like 76527504, you can just observe that a map $x \mapsto kx+\ell$ only changes the discriminant of a polynomial by a power of k, and so we only need to avoid the primes dividing the discriminant of $X(X+1)(X+4)$ which is 144 (i.e. the primes $2, 3$) plus any primes dividing the coefficient 9 in "$9x + 15$". This gives a computationally easier way to see that we only need to avoid the primes $2, 3$]. Reducing $Y^2 = X^3 - 351X + 1890$ modulo 5 gives: $Y^2 = X^3 - X$ [N.B. The fact that $4(-1)^3 + 27 \cdot 0^2 \not\equiv 0 \bmod 5$ gives a further independent proof that 5 is a legitimate choice of prime]. This has the points: $\mathbf{o}, (0,0), (1,0), (2,\pm 1), (3,\pm 2), (4,0)$ over $\mathcal{F}_5$, and so $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ has size at most 8. Hence, $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is precisely the $C_2 \times C_4$ group of points given above. **[6 marks]**

(ii). [*Unseen and open-ended.*] Answers will vary. The students should try reducing at several primes, and notice that the number of points mod p (where p is a prime not dividing the discriminant) is always divisible by 8. On the other hand, a search only reveals the four torsion points: $\mathbf{o}, (0,0), (1,0), (4,0)$, and Nagell-Lutz reveals that these are the only ones. So, it appears that the group orders mod p. They may recognise a more delicate argmuent using the homomorphism property, using different primes to show, in turn, that $(0,0), (1,0), (4,0)$ are not in $2\mathcal{E}(\mathbb{Q})$. This gives an argument to determine the torsion group completely, using only finite field reductions (but an argument of a type different than any they have used previously). A very high quality answer will recognise the relevance of whether $[1,-1], [1,-3], [1,3]$ give a pair of quadratic residues, respectively, and use this to prove that the group orders are always divisible by 8. For other examples of similar type, they might merely adjust the numbers on the given example to obtain another example of exactly the same type, or they might discuss (for example) curves of the form $Y^2 = X(X^2 + aX + b)$ where modulo some primes the group is C_4 and modulo other primes is $C_2 \times C_2$. **[14 marks]**

Solution to Question 3.

(i). [*Seen similar on an Exercise Sheet.*] They have already had this question on an Exercise Sheet for the case $N = 4$, where the argument was that any elliptic curve with a point (x_0, y_0) of order N can be birationally mapped to a curve of the form:

$$\mathcal{E} : Y^2 + wXY + vY = X^3 + vX^2,$$

where (x_0, y_0) is mapped to $(0,0)$, which is now a point of order 4 on $\mathcal{E}$. We can also compute $2(0,0) = -(-v, 0) = (-v, v(w-1))$. Now compute: $3(0,0) = 2(0,0) + (0,0) = (-v, v(w-1)) + (0,0)$, for which we first take the line through $(-v, v(w-1)) + (0,0)$, namely: $Y = (1-w)X$. Substituting this into $\mathcal{E}$ gives a cubic in x with roots $0, -v, 1-w$, so that the intersection of the line $Y = (1-w)X$ and $\mathcal{E}$ is: $(0,0), (-v, v(w-1)), (1-w, (1-w)^2)$. Hence: $3(0,0) = (-v, v(w-1)) + (0,0) = -(1-w, (1-w)^2)$. But $-(1-w, (1-w)^2)$ is the

other point on $\mathcal{E}$ with X-coordinate $1-w$, that is: $(1-w, w-v-1)$. Now, $5(0,0)=\mathbf{o}$ when $3(0,0)=-2(0,0)$, that is, when: $(1-w, w-v-1)=(-v,0)$, which happens precisely when $w=1+v$; substituting this into $\mathcal{E}$ gives the required form. **[7 marks]**

(ii). [*Open-ended.*] It is up to the students how far they want to push the same idea. The computations and parametrisations becomes harder as N increases. For $N=1,\ldots,10$ and 12, one gets curve in v,w which can be parametrised, although recognising the parametrisation becomes increasingly difficult. A fantastic answer would notice that $N=11$ is the first value which is different in quality, since the condition on v,w can be birationally transformed to the elliptic curve $Y^2+Y=X^3-X^2$, and the question of whether any elliptic curve over $\mathbb{Q}$ has a point of order 11 comes down to deciding whether this particular elliptic curves has nonzero rank (I would not expect them to compute this rank, since it would require a rank computation using number fields, which they have not seen). **[13 marks]**

Solution to Question 4.

(i). [*Seen similar on an Exercise Sheet.*] Let $\mathcal{C}: Y^2=X(X^2+aX+b)=X(X^2+6X+1)$, where $a=6, b=1$, and isogenous curve $\mathcal{D}: Y^2=X(X^2+a_1X+b_1)=X(X^2-12X+32)$, where $a_1=-12, b_1=32$, with the usual isogeny $\phi:\mathcal{C}(\mathbb{Q})\to\mathcal{D}(\mathbb{Q}):(x,y)\mapsto(y^2/x^2, y-y/x^2)$, and dual isogeny $\hat{\phi}:\mathcal{D}(\mathbb{Q})\to\mathcal{C}(\mathbb{Q}):(u,v)\mapsto(\frac{1}{4}v^2/u^2, \frac{1}{8}(v-32v/u^2))$.

The map $q:\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))\mapsto\mathbb{Q}^*/(\mathbb{Q}^*)^2:(u,v)\mapsto u$, for $(u,v)\neq(0,0)$, with $q:(0,0)\mapsto b_1$ and $q:\mathbf{o}\mapsto 1$, is an injection with im$q$ contained in $\{d: d \text{ is square free and } d|b_1\}=\{\pm1,\pm2,\}$. Also, $\mathbf{o}\mapsto 1$, $(0,0)\mapsto 2$. Hence, $\{1,2\}\subset \text{im}q\subset\{\pm1,\pm2,\}$.

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: $-\ell^4-12\ell^2m^2-32m^4=n^2$. We can see that the LHS is $\leqslant 0$ and the RHS is $\geqslant 0$, and there is equality iff $\ell=m=n=0$, a contradiction. Hence $-1\notin\text{im}q$. We conclude that im$q=\{1,2\}$ and that $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))=\{\mathbf{o},(0,0)\}$, and so $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ is generated by $(0,0)$.

The map $\hat{q}:\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))\mapsto\mathbb{Q}^*/(\mathbb{Q}^*)^2:(u,v)\mapsto u$, for $(u,v)\neq(0,0)$, with $\hat{q}:(0,0)\mapsto a_1^2-4b_1=b$ and $\hat{q}:\mathbf{o}\mapsto 1$, is an injection with im$\hat{q}$ contained in $\{d: d \text{ is square free and } d|b\}=\{\pm1\}$. Also, $\mathbf{o}\mapsto 1$, $(0,0)\mapsto 1$, and the obvious point $(-1,2)\mapsto -1$, so that $\{\pm1\}\subset\text{im}\hat{q}\subset\{\pm1\}$. We conclude that im$\hat{q}=\{\pm1\}$ and that $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))=\{\mathbf{o},(-1,2)\}$, so that so that $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ is generated by $(-1,2)$. [N.B. $(0,0)$ should not be included as a generator of $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ even though it is a rational point; $(0,0)$ maps to 1 under $\hat{q}$, and so $(0,0)\in\hat{\phi}(\mathcal{D}(\mathbb{Q}))$; that is $(0,0)=\mathbf{o}$ in $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$].

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: $(-1,2)$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0,0)\big)=\mathbf{o}$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated

by $(-1,2)$, and so is the group C_2. Now $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q}) \times C_2^{rank}$, and $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q})$ is isomorphic to the 2-torsion group of $\mathcal{C}_{\text{tors}}(\mathbb{Q})$ which is C_2 (consisting only of $\mathbf{o}$ and $(0,0)$), so that $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q})$ is C_2. Conclusion: rank = 0. [If this seems surprising, then note that $(-1,2), (-1,-2)$ are points of order 4 in $\mathcal{C}(\mathbb{Q})$]. **[7 marks]**

(ii). [*Open-ended.*]

It is up to them what examples they choose to compute, where at least three primes divide $b(a^2-4b)$. A prudent student will try to make life easier by constructing the curve so that the isogenous curve has few bad primes. For the large rank example, the student should explain how the example was found (for example, biasing towards large rank by choosing a, b so that the curve contains a certain point). **[9 marks]**

(iii). [*Open-ended.*] They should first see that there is a crude upper bound of $2k$ on the rank, since the q maps in each direction are into the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by $-1, p_1, \ldots, p_k$, giving a bound of $2k+2$, but then subtracting 2 for the effects of $(0,0)$ on the curve and the isogenous curve. When $a<0$ and $b>0$, one of the homogeneous spaces will be: $(-1)\cdot\ell^4 + a\ell^2m^2 + (b/(-1))\cdot m^4 = n^2$, which is impossible in $\mathbb{R}$, and so the bound on the rank can be reduced to $2k-1$. They might now at this point think of other conditions on a, b which force specific homogeneous spaces to have no points, for reasons in $\mathbb{R}$ or some $\mathbb{Q}_p$. **[9 marks]**

Solution to Question 5.

(i). [*Unseen.*] From the usual isogeny, the usual isogenous curve is $Y^2 = X(X^2 - 2(\lambda_1+\lambda_2)X + (\lambda_1-\lambda_2)^2)$. Making this the same as: $Y^2 = X(X-\mu_1)(X-\mu_1)$ gives:

$$\mu_1 = (\sqrt{\lambda_1}+\sqrt{\lambda_2})^2,\ \mu_2 = (\sqrt{\lambda_1}-\sqrt{\lambda_2})^2,$$

Suppose that $(0,0)$ is in $2\mathcal{E}(\mathbb{Q})$. Since $\hat{\phi}\circ\phi$ is duplication, this forces the preimages of $(0,0)$ under $\hat{\phi}$, namely $(\mu_1,0), (\mu_2,0) = (\mu_1,0)+(0,0)$ to be $\mathbb{Q}$-rational and in $\phi(\mathcal{E}(\mathbb{Q}))$, so that $q(\mu_1,0) = \mu_1$ and $q(\mu_2,0) = \mu_2$ are in $(\mathbb{Q}^*)^2$. That is: $(\sqrt{\lambda_1}+\sqrt{\lambda_2})^2$ and $(\sqrt{\lambda_1}-\sqrt{\lambda_2})^2$, which forces $\lambda_1, \lambda_2, \mu_1, \mu_2$ to be in $(\mathbb{Q}^*)^2$. as required. **[7 marks]**

(ii). [*Unseen and somewhat open-ended.*] There is a naive bound of at most 12 points of order 4, using the fact that the multiplication by 2 map [2] is 4-to-1, and so the 4-torsion group has at most order 16, of which 4 are members of the 2-torsion group. It is up to the students how far to try to push applying the previous result to the problem of bounding the points of order 4. One way is first to observe that, if an elliptic curve has more than 4 points of order 4, then (since duplication is 4-to-1) at most four of them can be preimages of the same point of order 2, and so there must be at least two $\mathbb{Q}$-rational points of order 2, both in $2\mathcal{E}(\mathbb{Q})$. Their sum must also be in $\mathcal{E}(\mathbb{Q})$, and so $\mathcal{E}(\mathbb{Q})$ would then have all three

points of order 2, and can be written in the form $Y^2 = X(X + \lambda_1)(X + \lambda_2)$, where $(0, 0)$ and $(-\lambda_1, 0)$ are in $2\mathcal{E}(\mathbb{Q})$. As above, this forces $\lambda_1, \lambda_2, \mu_1, \mu_2$ to be in $(\mathbb{Q}^*)^2$. However, if we map $(X, Y) \mapsto (X + \lambda_1, Y)$ [so that $(0, 0) \mapsto (\lambda_1, 0)$ and $(-\lambda_1, 0)$ maps to $(0, 0)$] the curve becomes: $Y^2 = X(X - \lambda_1)(X + \lambda_2 - \lambda_1)$ and the same argument gives that $-\lambda_1$ is in $(\mathbb{Q}^*)^2$, contradicting $\lambda_1 \in (\mathbb{Q}^*)^2$. Hence there can only be at most 4 points of order 4. The student might also try to construct an actual example where there are 4 points of order 4, such that $Y^2 = X(X+1)(X+4)$, to see that the bound is sharp. Anything remotely along those lines would be a very high quality answer, as they have not seen this style of argument before. [**8 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.