Question 1.

(a)
To see this, note that if $|y| > 1$, then from the equation

$$|y|^2 = |x^3 + Ax + B| > 1,$$

we must have $|x| > 1$. On the other hand, if $|x| > 1$, then
$|x^3 + Ax + B| = |x^3| = |y|^2$, so $|y| > 1$. That is, we have $|x| > 1$ and $|y| > 1$ if and only if $|x| > 1$ or $|y| > 1$.
Now if $(x, y) = (x : y : 1)$ reduces to $(0 : 1 : 0)$ modulo p, then either $|x| > 1$ or $|y| > 1$, since otherwise, the reduction would be $(\tilde{x} : \tilde{y} : 1)$. Now suppose that $|x| > 1$ or $|y| > 1$. Then from $|y|^2 = |x^3 + Ax + B| = |x|^3$, we see that $|y| > 1$, $|x| > 1$, and $|y| > |x|$. So the reduction is
$(\widetilde{x/y} : 1 : \widetilde{1/y}) = (0 : 1 : 0)$.
[7 marks. Similar to bookwork.]

(b)
If $a \in \mathbb{Q}^*$ has a square root in $\mathbb{Q}_p^*$ for all p then a has a square root in $\mathbb{Q}$.

Proof. Write $a = \pm \prod_p p^{n_p}$ for distinct primes p and integers n_p. For each p, since $a = x^2$ in $\mathbb{Q}_p$, we have that n_p is even. Thus, we can write $a = \pm \prod_p p^{2m_p}$ for integers m_p. But then, since $\prod_p p^{-n_p}$ has a square root $\prod_p p^{-m_p}$ in $\mathbb{Q}$, $a \prod_p p^{-n_p} = \pm 1$ would have a square root in each $\mathbb{Q}_p$. But -1 does not have a square root in, say, $\mathbb{Q}_3$, since any square root would be in $\mathbb{Z}_3$, giving rise to a square root of -1 in $\mathbb{Z}/3$, which doesn't exist. Thus, we must have $a \prod_p p^{-n_p} = 1$, and hence, $a = \prod_p p^{2m_p}$, which has the square root $\prod_p p^{m_p}$ in $\mathbb{Q}$.
[7 marks. Unseen, but similar seen.]

(c)
Hensel: Let K be a field, complete w.r.t. a non-archimedean valuation $|\cdot|$, 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

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

[2 marks. Bookwork]

(d) Let $p \neq 2$. Suppose a has a square root. Then clearly $n = 2m$, so that $u = ap^{-2m}$ has a square root. Conversely, suppose $a = p^n u$ with n even

such that $u \in \mathbb{Z}_p^*$ has a square root modulo p. Then clearly, p^n has a square root, so it suffices to show that u has a square root. For this, consider $f(x) = x^2 - u$ and let $a \in \mathbb{Z}_p$ such that $f(a) \equiv 0 \mod p$. Then $a \in \mathbb{Z}_p^*$, so $f'(a) = 2a \in \mathbb{Z}_p^*$. Hence, $|f'(a)|^2 = 1 > |f(a)|$. Hence, by Hensel's Lemma, there is a $b \in \mathbb{Z}_p s$ such that $b \equiv a \mod p$ and $f(b) = 0$, which then is a square root of u.
When $p = 2$, $a \in \mathbb{Q}_2^*$ has a square root if and only if $a = 2^n u$ where n is even and where $u \in \mathbb{Z}_2^*$has a square root modulo 8. That the condition is necessary is clear exactly as in the $p \neq 2$ case. To show that it is sufficient, note again that it suffices to show that $u \in \mathbb{Z}_2^*$ has a square root. Again, put $f(x) = x^2 - u$ and let a be a square root of u modulo 8. Then $a \in \mathbb{Z}_s^*$ and $f'(a) = 2a$. So $|f'(a)|^2 = 2^{-2} > |f(a)| = 2^{-3}$. Therefore, Hensel's Lemma applies again to give us a $b \in \mathbb{Z}_2$ such that $f(b) = 0$.
[4 marks. Seen in example in lecture.]

(e) First, since 11 has a square root in $\mathbb{R}$, it is clear that the polynomial has a root in $\mathbb{R}$. In $\mathbb{Q}_2$, we have $-7 \equiv 1 \mod 8$, so that -7 has a square root in $\mathbb{Z}/8$, and hence, in $\mathbb{Z}_2$ by Hensel's lemma. In $\mathbb{Q}_7$, $11 \equiv 4 = 2^2 \mod 7$, so 11 has a square root in $\mathbb{Z}_7$ by Hensel's lemma. Also, $-7 \equiv 4 \equiv 2^2 \mod 11$, so that -7 has a square root in $\mathbb{Z}_{11}$. Now, let p be any prime other than 2, 7 and 11. Then -7 and 11 are units in $\mathbb{Z}_p$, and

$$(-77/p) = (-7/p)(11/p),$$

so that at least one of -77, -7 and 11 must have a square root mod p. Hence, by Hensel's lemma, one of them must have a square root in $\mathbb{Z}_p$.
[5 marks. Unseen, but similar seen.]

Question 2.

(a) A formal group over R is a power series $F(X, Y) \in R[[X, Y]]$ such that

$$F(X, Y) = X + Y + \text{terms of degree} \geq 2;$$
$$F(F(X, Y), Z) = F(X, F(Y, Z));$$
$$F(X, Y) = F(Y, X).$$

Given an elliptic curve $y^2 = x^3 + Ax + B$, there is a formal group $F_{\mathcal{E}}(X, Y) \in \mathbb{Z}[A, B][[X, Y]]$ such that $p\mathbb{Z}_p$ with the group law induced by $F_{\mathcal{E}}$ is isomorphic to $\mathcal{E}_1(\mathbb{Q}_p)$ with the elliptic curve group law.
[2 marks.]

(b) Let $\omega = F_X(0,T)^{-1}dT$, where the subcript refers to the derivative with respect to the first variable. Then

$$\omega \circ F(T,S) = F_X(0,F(T,S))^{-1}F_X(T,S)dT.$$

So we must show

$$F_X(0,F(T,S))^{-1}F_X(T,S) = F_X(0,T)^{-1},$$

or

$$F_X(0,T)F_X(T,S) = F_X(0,F(T,S)).$$

But we have

$$F(U,F(T,S)) = F(F(U,T),S).$$

Differentiation with respect to U yields

$$F_X(U,F(T,S)) = F_X(F(U,T),S)F_X(U,T).$$

Setting $U = 0$, we get

$$F_X(0,F(T,S)) = F_X(T,S)F_X(0,T),$$

which is what we wanted. Hence, ω is an invariant differential form. Since $F(X,Y) \equiv X + Y$ up to terms of higher order, it is clear ω is normalized, i.e., of the form

$$\omega = a(T)dT,$$

where $a(T) = 1 + Tb(T)$ and $b(T) \in \mathbb{Z}_p[T]$.

Let $\alpha = P(T)dT$ be an invariant differential form. Then

$$P(F(T,S))F_X(T,S)dT = P(T)dT.$$

So

$$P((F(T,0))F_X(T,0) = P(0),$$

or

$$P(T) = P(0)F_X(T,0)^{-1}.$$

That is $\alpha = P(0)\omega$. Hence, if α is normalized, then $\alpha = \omega$.
[3 marks]

(c) We put $[0](T) = 0$, $[1](T) = T$ and $[m](T) = F([m-1](T),T)$ for $m > 1$. Also, $[m](T) = F([m+1](T),i(T))$ for $m < 1$, where $i(T) \in T\mathbb{Z}_p[[T]]$ is the unique power series such that $F(T,i(T)) = 0$.

We see by induction that $[m](T) = mT + h(T)$ where $T^2|h(T)$. Now, from

$$F([m](X), [m](Y)) = [m](F(X, Y)),$$

we see that

$$F_X([m](X), [m](Y))[m]'(X) = [m]'(F(X, Y))F_X(X, Y).$$

Setting $X = 0$, we get

$$F_X(0, [m](Y))[m]'(0) = [m]'(Y)F_X(0, Y),$$

so that

$$[m]'(Y)F_X(0, [m](Y))^{-1} = [m]'(0)F_X(0, Y)^{-1}.$$

That is,

$$\omega \circ [m] = [m]'(0)\omega.$$

Applying this to $[p]$, we get

$$\omega \circ [p] = p\omega.$$

If we put $\omega = P(T)dT$, where $P(T) = 1 + Th(T)$, this implies $p|[p]'(T)$. Writing

$$[p](T) = pT + \sum_{n=2}^{\infty} a_n T^n,$$

we get $p|na_n$ for all n. Thus, we can group the terms for which $p|n$ into $g(T^p)$ to get the form we want.
[5 marks]

(d) We have the isomorphism

$$(p\mathbb{Z}_p, F_{\mathcal{E}}(X, Y)) \simeq (\mathcal{E}, +_{\mathcal{E}}).$$

So the torsion subgroups will be isomorphic. If m is not divisible by p, then

$$[m](T) = mT + T^2 g(T),$$

is an isomorphism (since m is a unit in $\mathbb{Z}_p$), so no non-trivial element is killed by $[m]$. If $p|m$, and p^a is the largest power of p that divides m, then $m = p^a m_0$ for $(m_0, p) = 1$. Therefore, for any point x of order m, $m_0 x$ has order p^a. So by induction on a, it suffices to show there is no p-torsion. If $p = 2$, then the 2 torsion points in $\mathcal{E}(\mathbb{Q}_p)$ satisfy $y = 0$, so they cannot

reduce mod p to the origin. Hence, we assume $p > 2$. Let $z \in p\mathbb{Z}_p$ correspond to a p-torsion point in $\mathcal{E}_1(\mathbb{Q}_p)$. If $[p](z) = 0$, then we have

$$pz = z^p r(z)$$

for some power series $r \in \mathbb{Z}_p[[T]]$. Thus,

$$p^{-1}|z| = |z|^p |r(z)| \leq |z|^p.$$

If $|z| \neq 0$, then we get $1/p^{1/(p-1)} \leq |z| \leq 1/p$, which is a contradiction for $p > 2$. So we must have $z = 0$.
[7 marks. Bookwork to here.]

(e) Note that $(1, 2)$ is a rational point. We compute $2(1, 2) = (a, b)$. The slope of the tangent line is $y' = 3x^2/2y = 3/4$ at$(1, 2)$. Thus, the tangent line is $y = 3x/4 + 5/4$. To find the point of intersection, we substitute

$$x^3 - (3x/4 + 5/4)^2 + 3.$$

The x^2 term has coefficient $-9/16$. Thus $1 + 1 + a = 9/16$. Therefore, $a = -23/16$ has non-integral coordinates. But then, $(a, b) \in \mathcal{E}_1(\mathbb{Q}_2)$ and (a, b) is not torsion. Hence, $\mathcal{E}(\mathbb{Q})$ is infinite.
[8 marks. Unseen.]

Question 3.

(a)
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]

(b)

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]

(c)
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]

(d)
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]

(e)
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]