Question 1.

(a)

We require $m^2 \equiv 2 \pmod{7^3}$. We have $3^2 \equiv 2 \pmod 7$, and $(3+7k)^2 \equiv 9+42k \pmod{7^2}$. Thus $(3+7k)^2 \equiv 2 \pmod{7^2}$ iff $49 \mid 7+42k$ iff $7 \mid 1+6k$ iff $k \equiv 1 \pmod 7$. Hence $10^2 \equiv 2 \pmod{49}$, and $(10+7^2k)^2 \equiv 100+980k \pmod{7^3}$. Thus $(10+49k)^2 \equiv 2 \pmod{7^3}$ iff $7^3 \mid 98+980k$ iff $7 \mid 2+20k$ iff $k \equiv 2 \pmod 7$. Hence $m = 10+49.2 = 108$ is a solution.

[3 marks; S]

If $|n^3-2|_7 \leq 7^{-3}$ then $n^3 \equiv 2 \pmod{7^3}$ and hence $n^3 \equiv 2 \pmod 7$. But $0^3, 1^3, 2^3 \ldots, 6^3 \equiv 0,1,1,6,1,6,6 \pmod 7$ so that we never have $n^3 \equiv 2 \pmod 7$.

[2 marks; S]

Fact: an infinite p-adic series converges iff the individual terms tend to zero. Since $p \mid k$ we have $|k|_p \leq p^{-1}$ and hence $|k^n|_p \leq p^{-n} \to \infty$. The series therefore converges.

[2 marks; S]

We claim the limit is $(1-k)^{-1}$. Note that $1-k \neq 0$ since $p \mid k$. We have $\sum_{n<N} k^n = (1-k^N)/(1-k)$, whence

$$\left| \sum_{n<N} k^n - \frac{1}{1-k} \right|_p = \left| \frac{k^N}{1-k} \right|_p \leq \frac{p^{-N}}{|1-k|_p} \to 0$$

as required.

[3 marks; S]

We claim that $3^{2^n} \equiv 1 \pmod{2^n}$ for all $n \in \mathbb{N}$, which will suffice. This is true for $n=1$, and if $3^{2^n} = 1+2^n k$ with $n \geq 1$ then

$$3^{2^{n+1}} = 1 + 2^{n+1}(k + 2^{n-1}k^2) \equiv 1 \pmod{2^{n+1}}.$$

The claim therefore follows by induction. Hence $|3^{2^n}-1|_2 \leq 2^{-n}$, which tends to zero as n tends to infinity, as required.

[3 marks; N]

The sequence $b + (a-b)3^{2^n}$ therefore converges to a in $\mathbb{Q}_2$ and to b in $\mathbb{Q}_3$.

[2 marks; N]

(b)

One can determine p and q if the calculation involves a multiple jP for which jP is the point at infinity modulo one of the primes but not modulo the other.

[2 marks; B]

We start by computing $2P$ modulo 391, using the tangent line $y = mx+c$ at $(3, 4)$. Thus $m = (3.3^2)/(2.4) \equiv 3.9.49 \equiv 150 \pmod{391}$, since $8.49 = 392 \equiv 1 \pmod{391}$; and $c = 4 - 3m$. This line intersect the curve when $x^3 - 11 - (mx + c)^2$=0, giving three roots $x = 3, 3$ and x_2 say, whose sum is m^2. Thus $x_2 \equiv 150^2 - 6 \equiv 207 \pmod{391}$, and the corresponding y value is $y_2 = mx_2 + c = 4 + m(x_2 - 3) \equiv 4 + 150.204 \equiv 106 \pmod{391}$. Hence $2P = (207, -106)$.

[5 marks; S]

We now compute $3P = P + 2P$, using the line $y = nx + d$ between P and $2P$. Thus $n = (4 - (-106))/(3 - 207) = -110/204$. However 204 does not have an inverse modulo 391. Indeed the highest common factor is found to be 17, and we then find $391 = 17 \times 23$.

[3 marks; S]

Question 2.

(a)

We require

(i) $F(X,Y) = X + Y +$ higher order terms;

(ii) $F(X,Y) = F(Y,X)$; and

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

[3 marks; B]

We will prove by induction that there is a unique series of polynomials $Z_n(T)$ of degree $\leq n$ such that (a) Z_n and Z_{n+1} agree up to degree n, and (b) $F(X,Z_n)$ has only terms of degree $> n$. This suffices since we may take $i(T)$ as the formal limit of the polynomials $Z_n(T)$; and this is clearly the only admissible choice, since if $F(T,i(T)) = 0$ we may take $Z_n(T)$ as the terms of $i(T)$ of degree $\leq n$, giving an admissible sequence Z_n.

[3 marks; B]

For the induction we see that $Z_1(T) = -T$ is admissible by (i). Generally suppose $F(T,Z_n) = cT^{n+1} + \ldots$, and consider $Z_{n+1} = Z_n + dT^{n+1}$. We have $F(T,Z+W) = F(T,Z) + WF_Y(T,Z) +$terms involving higher powers of W, and $F_Y(T,Z) = 1+$higher order terms, by (i). Hence $F(T,Z_n + dT^{n+1}) = F(T,Z_n) + dZ^{n+1} +$higher order terms, so that $F(T,Z_n + dT^{n+1}) = (c + d)Z^{n+1} +$higher order terms. We therefore see that there is exactly one possible choice for d, namely $d = -c$.

[3 marks; B]

We require that $P(F(T,S))F_X(T,S) = P(T)$ identically in T and S.

[1 mark; B]

For $P(T) = F_X(0,T)^{-1}$ we first note that $F_X(0,T) = 1+$higher order terms, by (i) above, whence $F_X(0,T)^{-1}$ exists as a power series. It then suffices to check that $F_X(0,F(T,S))^{-1}F_X(T,S) = F_X(0,T)^{-1}$, or equivalently that $F_X(T,S)F_X(0,T) = F_X(0,F(T,S))$. However $F(X,F(T,S)) = F(F(X,T),S)$ by (iii) above, and the result follows on differentiating with respect to X and setting $X = 0$.

[4 marks; B]

(b)

Theorem: The kernel of the reduction map $\mathcal{E}(\mathbb{Q}_p) \to \tilde{\mathcal{E}}(\mathbb{F}_p)$ is torsion-free.

[2 marks; B]

Hence if we restrict the reduction map to the subgroup $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ the kernel is trivial, giving us an injection into $\tilde{\mathcal{E}}(\mathbb{F}_p)$, which is finite. It follows that $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ must also be finite.

[3 marks; B]

(c)

The discriminant is $4n^6$ and hence there is good reduction for any prime ≥ 5 which does not divide n. For $p \equiv 5 \pmod 6$ the congruence $x^3 \equiv y^2 - n^2 \pmod p$ has exactly one solution x for each y modulo p. Thus the elliptic curve has $p+1$ points modulo p, allowing for the point at infinity.

[3 marks; S]

It follows that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ divides $p+1$. Since $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is a subgroup of $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ we deduce that its order, t say, also divides $p+1$. If $k = (p+1)/6$ there is a prime $p_1 \equiv 5 \pmod 6$ for which $(p_1+1)/6$ is coprime to k. But then t divides both $p+1$ and p_1+1, and hence divides their highest common factor, which is 6.

[3 marks; N]

Question 3.

One defines $q : \mathcal{H} \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ by taking $q(\mathbf{0})$ to be the identity coset, by taking $q(0,0)$ to be the coset of b_1, and by taking $q(u,v)$ to be the coset of u for all other elements (u,v) of $\mathcal{H}$.

[2 marks; B]

For any non-zero rational number u we may write $u = rw^2$ with r being a square-free integer, and $w \in \mathbb{Q}$. Then if $v^2 = u(u^2 + a_1u + b_1)$ we must have $u^2 + a_1u + b_1 = rs^2$ for some rational number s, and $v = rsw$. Suppose there is a prime with $p \mid r$ for which $p \nmid b_1$. We consider two cases. If $|u|_p < 1$ then $|u^2|_p < 1$ and $|a_1u|_p < 1$, since $|a_1|_p \le 1$. Thus $|u^2 + a_1u + b_1|_p = 1$, since $|b_1|_p = 1$. This is impossible, since rs^2 is either zero, or contains p to an odd power. On the other hand if $|u|_p \ge 1$ then in fact $|u|_p > 1$, since $u = rw^2$ contains p to an odd power. Thus $|u^2|_p > |u|_p \ge |a_1u|_p$, and $|u^2|_p > 1 = |b_1|_p$, whence $|u^2 + a_1u + b_1|_p = |u|_p^2$. Again this is impossible, since rs^2 is either zero, or contains p to an odd power. It follows that $p|b_1$ whenever $p|r$, so that $r|b_1$.

[8 marks; S]

The maps ϕ and $\hat{\phi}$ are group homomorphisms, and $\hat{\phi}\phi = [2]$.

[1 mark; B]

Let $g_1, \dots, g_m$ be distinct coset representatives for $\mathcal{G}/\hat{\phi}(\mathcal{H})$, and $h_1, \dots, h_n$ similarly for $\mathcal{H}/\phi(\mathcal{G})$. Then for any $g \in G$ we have $g = g_i + \hat{\phi}(h)$ for some $h \in \mathcal{H}$, and $h = h_j + \phi(g')$ for some $g' \in \mathcal{G}$. Hence $g = g_i + \hat{\phi}(h_j) + \hat{\phi}(\phi(g')) = g_i + \hat{\phi}(h_j) + 2g'$. It follows that the set of all combinations $g_i + \hat{\phi}(h_j)$ form a set of (not necessarily distinct) coset representatives for $\mathcal{G}/2\mathcal{G}$. Hence

$$\#\left(\frac{\mathcal{G}}{2\mathcal{G}}\right) \le mn = \#\left(\frac{\mathcal{G}}{\hat{\phi}(\mathcal{H})}\right)\#\left(\frac{\mathcal{H}}{\phi(\mathcal{G})}\right).$$

[5 marks; B]

The image of q consists of cosets $r(\mathbb{Q}^\times)^2$ with integers r dividing b_1, for which the equation

$$r\ell^4 + a_1\ell^2m^2 + b_1r^{-1}m^4 = n^2$$

has an integral solution with ℓ, m, n not all zero. Such a class corresponds to a point (u,v) with $u = r\ell^2/m^2$. There is an entirely analogous map from $\mathcal{G}/\hat{\phi}(\mathcal{H})$ to $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, where the corrsponding integers r divide b, and the equation

$$r\ell^4 + a\ell^2m^2 + br^{-1}m^4 = n^2$$

is solvable.

For $\mathcal{C}$ this latter equation is $r\ell^4 + 5\ell^2m^2 + 3r^{-1}m^4 = n^2$ with $r|3$. The point $(0,0)$ produces $r = b = 3$, while the points $(1,3)$ and $(-3,3)$ produce $r = 1$ and $r = -3$ respectively. Thus these 3 points, together with the point at infinity, form a complete set of coset representatives for $\mathcal{G}/\hat{\phi}(\mathcal{H})$.

[4 marks; S/N]

Similarly for $\mathcal{D} : v^2 = u(u^2 - 10u + 13)$ we have equations $r\ell^4 - 10\ell^2m^2 + 13r^{-1}m^4 = n^2$ with $r|13$. Clearly there are no solutions with when $r < 0$, and $r = 1$ and $r = 13$ arise from the point at infinity and $(0,0)$ respectively. These two points are therefore coset representatives for $\mathcal{H}/\phi(\mathcal{G})$.

[3 marks; S/N]

Since $\hat{\phi}(0) = \hat{\phi}(0,0) = \mathbf{0}$ the argument above shows that $\mathcal{G}/(2\mathcal{G})$ consists of the cosets of $\mathbf{0}, (0,0), (1,3)$ and $(-3,3)$, so that the group has order 4.

[2 marks; S/N]