Elliptic Curves. Solutions to Sheet 1.

1. (a). The only points on $Y^2 = X^3 + 2X$ over $\mathbb{F}_5$ are: $\mathbf{o}, (0,0)$. The group table is the same as that of C_2 ("cyclic 2" group; i.e. the integers modulo 2 under addition), with $0, 1$ replaced by $\mathbf{o}, (0,0)$, respectively.
(b). The only points on $Y^2 = X^3 + 1$ over $\mathbb{F}_5$ are: $\mathbf{o}, (0,1), (0,4), (4,0), (2,2), (2,3)$. The point $(2,2)$ has order 6, and the group table is the same as that of C_6 ("cyclic 6" group; i.e. the integers modulo 6 under addition), with $0, 1, 2, 3, 4, 5$ replaced by $\mathbf{o}, (2,2), (0,4), (4,0), (0,1), (2,3)$, respectively. Note that it's also correct to say that the group is $C_2 \times C_3$, since $C_2 \times C_3$ is isomorphic to C_6.

2. We have: $2YY' = 3X^2 + 4$, and so the slope at the point $(2,4)$ is: $(3 \cdot 2^2 + 4)/(2 \cdot 4) = 2$. The line tangent to the curve at $(2,4)$ is: $Y = 2X$. The x-coordinate of the third point of intersection is therefore: $2^2 - 2 - 2 = 0$, with y-coordinate $y = 2 \cdot 0 = 0$. Hence, $(2,4) + (2,4) + (0,0) = \mathbf{o}$, and so $(2,4) + (2,4) = (0,-0) = (0,0)$. Now, note that we always have $-(x,y) = (x,-y)$ and so $-(0,0) = (0,0)$, giving: $2(0,0) = \mathbf{o}$. Hence, $4(2,4) = 2(0,0) = \mathbf{o}$. Also, check that $3(2,4) = 4(2,4) - (2,4) = -(2,4) = (2,-4)$. Summarising: the first 4 multiples of $(2,4)$ are: $1(2,4) = (2,4)$, $2(2,4) = (0,0)$, $3(2,4) = (2,-4)$, $4(2,4) = \mathbf{o}$, and so 4 is the smallest positive multiple of $(2,4)$ equal to $\mathbf{o}$.

3.
(a). Case 1. m is odd. The birational transformation $(X,Y) \mapsto (X/f_m, Y/f_m^{(m+1)/2})$ [with inverse transformation: $(X,Y) \mapsto (Xf_m, Yf_m^{(m+1)/2})$] maps the given curve to: $f_m^{(m+1)}Y^2 = f_m^{(m+1)}X^m + \ldots + f_0$, which is the same as: $Y^2 = X^m + c_{m-1}X^{m-1} + \ldots + c_0$, where $c_i = f_i/f_m^{m+1-i} \in \mathbb{Q}$ [N.B. our birational transformation is legitimate, since $(m+1)/2$ is an integer]. So, our new right hand side is monic and is still defined over $\mathbb{Q}$. Now, write each $c_i = n_i/d_i$, where each $n_i, d_i \in \mathbb{Z}$, with each n_i, d_i coprime. Let d be the least common multiple of $d_0, \ldots d_{(m-1)}$; that is to say, d is the smallest integer divisible by all of the denominators of the coefficients c_i. Now, the birational transformation $(X,Y) \mapsto (Xd^2, Yd^m)$ [with inverse transformation: $(X,Y) \mapsto (X/d^2, Y/d^m)$] maps to the curve: $Y^2/d^{2m} = X^m/d^{2m} + c_{m-1}X^{m-1}/d^{2m-2} \ldots + c_0$, which is the same as: $Y^2 = X^m + g_{m-1}X^{m-1} + \ldots + g_0$, where $g_i = c_i d^{2(m-i)}$. But now, each $d_i | d$ and so each $c_i d \in \mathbb{Z}$, giving that each $g_i \in \mathbb{Z}$, as required.

Case 2. f_m is a square. Let w be such that $f_m = w^2$. The birational transformation $(X,Y) \mapsto (X, Y/w)$ [with inverse transformation: $(X,Y) \mapsto (X, Yw)$] maps the given curve to: $f_m Y^2 = f_m X^m + \ldots + f_0$, which is the same as: $Y^2 = X^m + c_{m-1}X^{m-1} + \ldots + c_0$, where $c_i = f_i/f_m \in \mathbb{Q}$. We are again in the situation where our right hand side is monic and is still defined over $\mathbb{Q}$. So now apply the same second birational transformation as in Case 1.
(b). The birational transformation $(X,Y) \mapsto (5X, 5^2Y)$ [with inverse $(X,Y) \mapsto ((1/5)X, (1/5^2)Y)$] maps the given curve to the curve: $Y^2 = X^3 + 75X^2 + 625$. The birational transformation $(X,Y) \mapsto (X+25, Y)$ [with inverse $(X,Y) \mapsto (X-25, Y)$] maps this to the curve: $Y^2 = X^3 - 1875X + 31875$, as required.

4.

(a). Since $p \equiv 2 \pmod 3$, we have $\gcd(3, p-1) = 1$, and so there exist $\lambda, \mu \in \mathbb{Z}$ such that $3\lambda + (p-1)\mu = 1$. For any $x, y \in \mathbb{F}_p^*$, we have $x^{p-1} = y^{p-1} = 1$ [by Fermat's Little Theorem], and so:

$$x^3 = y^3 \Rightarrow \left(x^3\right)^\lambda \cdot 1^\mu = \left(y^3\right)^\lambda \cdot 1^\mu \Rightarrow \left(x^3\right)^\lambda \cdot \left(x^{p-1}\right)^\mu = \left(y^3\right)^\lambda \cdot \left(y^{p-1}\right)^\mu$$
$$\Rightarrow x^{3\lambda+(p-1)\mu} = y^{3\lambda+(p-1)\mu} \Rightarrow x = y.$$

Thus the map $x \mapsto x^3$ is injective on $\mathbb{F}_p^*$ and so is a bijection. Since $0^3 = 0$, the map is also a bijection on $\mathbb{F}_p$. Now, rearrange the equation of the curve as: $X^3 = Y^2 - A$. We see that, for each $Y = 0, \ldots, p-1$ in $\mathbb{F}_p$, there is precisely one $X \in \mathbb{F}_p$ such that $X^3 = Y^2 - A$, giving rise to a total of precisely p affine points, which becomes $p+1$ points when we include the point at infinity.

(b). Since $p \equiv 3 \pmod 4$, we have that $\left(\frac{-1}{p}\right) = -1$ [i.e. -1 is not congruent to a square mod p]. First note that $X = 0$ gives rise to precisely one point $(0, 0)$. Now, pair each $X \in \mathbb{F}_p^*$ with its negative $-X$ mod p. If $X(X^2 + B) = 0$ then the pair $X, -X$ gives rise to precisely two points: $(X, 0), (-X, 0)$. If $X(X^2 + B) \neq 0$ then one of $X(X^2 + B)$ and $-X(X^2 + B)$ will be a nonzero quadratic residue mod p and the other will be a quadratic nonresidue mod p [using the fact that -1 is a quadratic nonresidue mod p and the standard property of Legendre symbols that: $\left(\frac{mn}{p}\right)\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$]. Whichever one is a nonresidue will contribute no points; which one is a residue will contribute two points: $(X, Y), (X, -Y)$. In all cases, each pair $X, -X$ will contribute two points. This gives rise to a total of precisely p affine points, which becomes $p+1$ points when we include the point at infinity.

5.

(a). $(2, 0) + (-(2, 0)) = \mathbf{o}$, where $-(2, 0)$ is the inverse of $(2, 0)$; but we know that $-(2, 0) = (2, -0) = (2, 0)$ and so $(2, 0) + (2, 0) = \mathbf{o}$; that is, $(2, 0)$ is of order 2, as required.

(b). In general, a point (x, y) on $Y^2 = X^3 + f_2X^2 + f_1X + f_0$ has inverse: $(x, -y)$ and so (x, y) is of order 2 exactly when $(x, y) + (x, y) = \mathbf{o} \iff (x, y) = (x, -y)$. But $y = -y$ precisely when $y = 0$. So, we see that all points of order 2 are of the form $(x, 0)$ where x is a root of the cubic $X^3 + f_2X^2 + f_1X + f_0$. There are at most 3 such points over any field, since a cubic has at most 3 roots in any field. In the complex numbers, of course, there will always be exactly 3 such points. Applying this to the curve $Y^2 = X(X^2 - 3)$, we see that $X(X^2 - 3)$ has one $\mathbb{Q}$-rational root $X = 0$, giving $(0, 0)$ as the only $\mathbb{Q}$-rational point of order 2; the other two roots give the points $(\sqrt{3}, 0)$ and $(-\sqrt{3}, 0)$, which are the remaining two $\mathbb{C}$-rational points of order 2. The curve $Y^2 = X^3 - 7$ has no $\mathbb{Q}$-rational point of order 2 (since $X^3 - 7$ has no $\mathbb{Q}$-rational roots); over $\mathbb{C}$, there are the 3 points of order 2 given by: $(\omega_1, 0), (\omega_2, 0), (\omega_3, 0)$, where $\omega_k = 7^{1/3}e^{2\pi ik/3}$, for $k = 0, 1, 2$. Finally, the curve $Y^2 = X(X-1)(X-7)$ has the points of order 2: $(0, 0), (1, 0), (7, 0)$ all of which are both $\mathbb{C}$-rational and $\mathbb{Q}$-rational. Group structures of the 2-torsion groups over $\mathbb{Q}$ for the three curves are clearly: C_2, C_1 and $C_2 \times C_2$, respectively (since all members except $\mathbf{o}$ have order 2).

6. Using $2YY' = 3X^2$, we see that the slope of the curve at $(0, 2)$ is $3 \cdot 0^2/(2 \cdot 2) = 0$, and so the tangent to the curve at $(0, 2)$ is the line: $Y = 2$. The x-coordinate of the

third point of intersection is then: $0^2 - 0 - 0 = 0$, with corresponding y-coordinate 2. In summary: The line $Y = 2$ intersects the curve at $(0, 2)$ with multiplicity 3. Hence: $(0, 2) + (0, 2) + (0, 2) = \mathbf{o}$, and so: $3(0, 2) = \mathbf{o}$. But, $1(0, 2) = (0, 2)$ and $2(0, 2) = (0, -2)$, and so 3 is the smallest $k \geq 1$ such that $k(0, 2) = \mathbf{o}$; that is, $(0, 2)$ has order 3.

7.

(a). As usual, $-(\alpha, 0) = (\alpha, 0)$, and so $(\alpha, 0) + (\alpha, 0) = \mathbf{o}$; that is, $(\alpha, 0)$ is a point of order 2, as required. We now compute $(x', y') = (x, y) + (\alpha, 0)$. First, the line through (x, y) and $(\alpha, 0)$ is: $Y = (y/(x - \alpha))(X - \alpha)$. Substituting this into the curve gives: $X^3 - (m^2 + \alpha - a)X^2 + \ldots = 0$, where $m = y/(x - \alpha)$. The sum of the roots of this cubic is: $m^2 + \alpha - a$, and so the x-coordinate of the third point of intersection is given by: $x' = m^2 + \alpha - a - x - \alpha = m^2 - x - a = y^2/(x - \alpha)^2 - x - a = (\alpha x + a\alpha + b)/(x - \alpha)$. So, we have:

$$T : x \mapsto \frac{\alpha x + a\alpha + b}{x - \alpha}.$$

We now check $T^2(x) = T(T(x))$, which is:

$$T : x \mapsto \frac{\alpha(\alpha x + a\alpha + b)/(x - \alpha) + a\alpha + b}{(\alpha x + a\alpha + b)/(x - \alpha) - \alpha}.$$

On multiplying numerator and denominator by $x - \alpha$ and simplifying, we get: $(\alpha^2 + a\alpha + b)x/(\alpha^2 + a\alpha + b)x$, which is x, as required [Note that $\alpha^2 + a\alpha + b \neq 0$, since the cubic $(X - \alpha)(X^2 + aX + b)$ has distinct roots].

(b). For $Y^2 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$, the formula for T_1 is the same as for T in part (a), but with α, a, b replaced by $\alpha_1, -\alpha_2 - \alpha_3, \alpha_2\alpha_3$, respectively. That is:

$$T_1 : x \mapsto \frac{\alpha_1 x - \alpha_1\alpha_2 - \alpha_1\alpha_3 + \alpha_2\alpha_3}{x - \alpha_1}.$$

The formula for T_2 is the same as for T_1, but with $\alpha_1, \alpha_2, \alpha_3$ replaced by $\alpha_2, \alpha_3, \alpha_1$, respectively. The formula for T_3 is the same as for T_2, but (again) with $\alpha_1, \alpha_2, \alpha_3$ replaced by $\alpha_2, \alpha_3, \alpha_1$, respectively. These are then:

$$T_2 : x \mapsto \frac{\alpha_2 x - \alpha_2\alpha_3 - \alpha_2\alpha_1 + \alpha_3\alpha_1}{x - \alpha_2}.$$

$$T_3 : x \mapsto \frac{\alpha_3 x - \alpha_3\alpha_1 - \alpha_3\alpha_2 + \alpha_1\alpha_2}{x - \alpha_3}.$$

On computing $T_1T_2(x) = T_1(T_2(x))$, and simplifying (by removing a common factor of $\alpha_1 - \alpha_2$ from the numerator and denominator), we get the formula for T_3; that is: $T_1T_2 = T_3$. The formula for T_3 is invariant under $\alpha_1 \leftrightarrow \alpha_2$ and so $T_2T_1 = T_3$, also. Hence $T_1T_2 = T_3 = T_2T_1$, and so T_1 and T_2 commute. By symmetry, T_1 and T_3 commute, as do T_2 and T_3. Furthermore, $T_1T_2T_3 = T_3^2$ (since $T_1T_2 = T_3$), and we know from part (a) that $T_3^2 : x \mapsto x$; hence $T_1T_2T_3 : x \mapsto x$, as required.

Finally, the fixed points of T_1 are the solutions to $T_1(x) = x$, that is:

$$\alpha_1 x - \alpha_1\alpha_2 - \alpha_1\alpha_3 + \alpha_2\alpha_3 = (x - \alpha_1)x,$$

which has solutions:

$$x_1 = \alpha_1 + \sqrt{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)}, \quad x_2 = \alpha_1 - \sqrt{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)}.$$

Computing $T_2(x_1)$ and $T_2(x_2)$ gives x_2, x_1, respectively.

8. (a). Let L be the tangent line to the curve at P, and let R be the third point of intersection; that is, the line and the curve meet at P, P, R. Then $P + P + R = \mathbf{o}$. Then, $3P = \mathbf{o} \iff R = P \iff L$ intersects $\mathcal{E}$ only at P (3 times).
(b). The Hessian matrix is:

$$\begin{pmatrix} -6X_0 & 0 & -2AX_2 \\ 0 & 2X_2 & 2X_1 \\ -2AX_2 & 2X_1 & -2AX_0 - 6BX_2 \end{pmatrix}.$$

The determinant is:
$-6X_0\big(2X_2(-2AX_0 - 6BX_2) - (2X_1)(2X_1)\big) - 2AX_2\big(0 - (2X_2)(-2AX_2)\big)$
$= 8(3AX_0^2X_2 + 9BX_0X_2^2 + 3X_0X_1^2 - A^2X_2^3)$.
The only projective point (X_0, X_1, X_2) on the curve with $X_2 = 0$ is $(0, 1, 0) = \mathbf{o}$, for which the statement is true, since $3\mathbf{o} = \mathbf{o}$ and $(X_0, X_1, X_2) = (0, 1, 0)$ makes the Hessian determinant 0. When $X_2 \neq 0$, we can write everything in affine form, with $x = X_0/X_2$ and $y = X_1/X_2$, when we see that the Hessian determinant (after dividing through by $8X_2^3$) is 0 exactly when:

$$3Ax^2 + 9Bx + 3xy^2 - A^2 = 0. \tag{1}$$

Also, the point $P = (x, y) \neq \mathbf{o}$, written in affine form, has order 3 exactly when $2(x, y) = (x, -y)$ which happens if and only if the x-coordinate of $2(x, y)$ is x. But, as usual, the x-coordinate of $2(x, y)$ is $m^2 - 2x$, where $m = (3x^2 + A)/(2y)$ (note that $y \neq 0$ here, since $y = 0$ would make P be of order 2). So, P being of order 3 implies $\big((3x^2 + A)/(2y)\big)^2 - 2x = x$, that is:

$$-9x^4 - 6Ax^2 + 12xy^2 - A^2 = 0. \tag{2}$$

Finally, we use the fact the (x, y) is a point on the curve, so that $y^2 = x^3 + Ax + B$, and so we can replace y^2 by $x^3 + Ax + B$ in equations (1),(2). This makes both equations become the same equation: $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$, as required.

(c). By part (b), the x-coordinate of any point of order 3 must be a root of the quartic $3x^4 + 6Ax^2 + 12Bx - A^2$, which has at most 4 roots $x_1, \ldots, x_4$. Each x_i gives rise to at most two points $(x_i, y_i), (x_i, -y_i)$ on the curve, giving at most 8 points of order 3. Together with $\mathbf{o}$, this gives at most 9 points that are 3-torsion.

Elliptic Curves. Solutions to Sheet 2.

1. (a). Let $x, y \in K$ be such that $|x| \neq |y|$, without loss of generality, say that $|x| < |y|$. Since K is non-Archimedean, we know that $|x \pm y| \leqslant \max(|x|, |y|) = |y|$, and so it is sufficient to show that $|x \pm y| \not< |y|$. Imagine $|x \pm y| < |y|$; then $|y| = |(x \pm y) - x| \leqslant \max(|x \pm y|, |x|) < |y|$, a contradiction, as required. [Note that an immediate consequence is the implication: $|u \pm v| < |u| \Rightarrow |u| = |v|$].

(b). Let $x_1, \ldots, x_n \in K$ be such that $|x_\ell| > |x_i|$ for all $i \neq \ell$. Let $x = x_1 + \ldots + x_{\ell-1} + x_{\ell+1} + \ldots + x_n$ and let $y = x_\ell$. Then $|x| \leqslant \max(|x_i| : 1 \leqslant i \leqslant n, i \neq \ell\} < |y|$ and so: $|x_1 + \ldots + x_n| = |x + y| = |y| = |x_\ell|$, by part (a).

(c). Since $K, |\ |$ satisfies the triangle inequality $|x+y| \leqslant |x|+|y|$, we can apply the standard trick from first year Analysis: $|x| \leqslant |(x-y)+y| \leqslant |x-y|+|y|$ to give: $|x|-|y| \leqslant |x-y|$; similarly $|y|-|x| \leqslant |x-y|$, and so: $|\ |x|-|y|\ |_\infty \leqslant |x-y|$. If $s_n \to s$ in $K, |\ |$ then $|s_n - s| \to 0$ in $\mathbb{R}$, and so $|\ |s_n| - |s|\ |_\infty \leqslant |s_n - s| \to 0$, giving $|s_n| \to |s|$ in $\mathbb{R}, |\ |_\infty$, as required.

Suppose $s \neq 0$; then $|s| > 0$ and taking $\epsilon = |s|$, there exists N such that $|s_n - s| < |s|$ for all $n > N$, so that $|s_n| = |s|$ for all $n > N$ (since if $|s_n| \neq |s|$ then (a) would give $|s_n - s| = \max(|s_n|, |s|) \geqslant |s|$, a contradiction).

2. (a). $3/50 = 5^{-2} \cdot 3/2$ (where 5 has no common factor with either the numerator and denominator of $3/2$) and so $|3/50|_5 = 5^2$. Similarly, $3/50 = 3^1 \cdot 1/50$ and so $|3/50|_3 = 3^{-1}$. Similarly, $3/50 = 7^0 \cdot 3/50$, and so $|3/50|_7 = 7^0 = 1$.

$d_5(2/3, 1/5) = |2/3 - 1/5|_5 = |7/15|_5 = 5$, $d_7(2/3, 1/5) = |7/15|_7 = 7^{-1}$, $d_{11}(2/3, 1/5) = |7/15|_{11} = 1$.

(b). $|3/7|_3 = 3^{-1}$, $|3/7|_7 = 7$. For all other primes p, $\gcd(p, 3) = \gcd(p, 7) = 1$ and so $|3/7|_p = 1$. Note also that $|3/7|_\infty = 3/7$. The given product $\prod |3/7|_i$ has all factors equal to 1 apart from the factors: $|3/7|_3 = 3^{-1}$, $|3/7|_7 = 7$ and $|3/7|_3 = 3/7$, whose product is 1. Hence the given product $\prod |3/7|_i$ is 1. For any $x \in \mathbb{Q}$, write $x = \pm n/d$, where n and d are integers with $\gcd(n, d) = 1$, and write n, d in terms of their primes factorisations: $n = p_1^{s_1} \cdot \ldots p_k^{s_k}$ and $d = q_1^{t_1} \cdot \ldots q_\ell^{t_\ell}$, where $p_1, \ldots p_k, q_1, \ldots q_\ell$ are distinct primes. For any prime p, if $p = p_i$ for some i, then $|x|_p = p_i^{-s_i}$. If $p = q_j$ for some j, then $|x|_p = q_j^{t_j}$. If $p = \infty$, then $|x|_p = n/d = (p_1^{s_1} \cdot \ldots p_k^{s_k})/(q_1^{t_1} \cdot \ldots q_\ell^{t_\ell})$. For all other primes p, we have $|x|_p = 1$. It follows that the product $\prod |x|_i$ is equal to $(p_1^{-s_1} \cdot \ldots p_k^{-s_k}) \cdot q_1^{t_1} \cdot \ldots q_\ell^{t_\ell} \cdot (p_1^{s_1} \cdot \ldots p_k^{s_k})/(q_1^{t_1} \cdot \ldots q_\ell^{t_\ell})$, which is again equal to 1.

3. (a). $|1/5^n|_5 = 5^n \to \infty$; this means that $|1/5^n|_5$ does not converge, and so $1/5^n$ does not converge in $\mathbb{Q}_5$ (since, if $a_n \to \ell$ then $|a_n|_p \to |\ell|_p$).

(b). *Method 1.* $|n|_5 \leq 5^{-1}$ for $n = 5, 10, 15, \ldots$ and $|n|_5 = 1$ otherwise; this means that $|n|_5$ does not converge (since there is a subsequence $|n|_5$ for $5 \not| n$ converging to 1 and a subsequence $|n|_5$ for $5|n$ and $5^2 \not| n$ converging to $1/5$), and so n does not converge in $\mathbb{Q}_5$ (since, if $a_n \to \ell$ then $|a_n|_p \to |\ell|_p$).

(b). *Method 2.* $n = \sum 1$, which does not converge, since $|1|_5 = 1$ which does not converge to 0 (using the result from lectures which says that $\sum c_i$ converges iff $|c_i|_p \to 0$).

(c). $n! = 5^r \cdot k$, where $r > n/5 - 1$, since every fifth factor of $1 \cdot 2 \cdot \ldots n$ (i.e. the factors $5, 10, 15, \ldots$) contributes at least one new factor of 5. Hence $|n! - 0|_5 = |n!|_5 < 5^{-(n/5-1)} \to 0$, and so $n!$ converges to 0 in $\mathbb{Q}_5$.
(d). $|(3 + 10^n) - 3|_5 = |10^n|_5 = |5^n \cdot 2^n|_5 = 5^{-n} \to 0$, and so $3 + 10^n$ converges to 3 in $\mathbb{Q}_5$.
(e). $|10^n|_5 = |5^n \cdot 2^n|_5 = 5^{-n} \to 0$ in $\mathbb{Q}_5$ and so $\sum 10^n$ converges in $\mathbb{Q}_5$ (using the result from lectures which says that $\sum c_i$ converges iff $|c_i|_p \to 0$).
(f). $|7^n|_5 = 1$ which does not converge to 0, and so $\sum 7^n$ does not converge in $\mathbb{Q}_5$ (using the same result from lectures as used in part (e)).

4. (a). We are looking for x such that $|x^2 + 1|_5 \leqslant 5^{-4}$. Take $x_0 = a_0 = 2$ as the initial approximation for which $|a_0^2 + 1|_5 = |5|_5 = 5^{-1}$. Take $x_1 = a_0 + 5a_1 = 2 + 5a_1$. Then we want $(2 + 5a_1)^2 \equiv -1 \bmod 5^2$, and so $20a_1 \equiv -5 \bmod 5^2$, which is the same as $4a_1 \equiv -1 \bmod 5$, and so $a_1 = 1$. This gives a better approximation: $x_1 = 2 + 1 \cdot 5 = 7$, which satisfies $|x_1^2 + 1|_5 = 5^{-2}$. Simlarly, we then find $a_2 = 2$ and so $x_2 = 7 + 2 \cdot 5^2 = 57$. Then, finally, we similarly find $a_3 = 1$ and so $x_3 = 57 + 1 \cdot 5^3 = 182$, satisfying $|x^2 + 1|_5 = 5^{-4}$, as required.
(b). If there were an integer x such that $|x^2 - 7/8|_3 \leqslant 3^{-7}$, then we would have $x^2 \equiv 7/8 \bmod 3^7$ and so $x^2 \equiv 7/8 \bmod 3$. But $7/8 \equiv 2 \bmod 3$, which is not a quadratic residue (since $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 1 \bmod 3$); this means that no such x can exist.
(c). If there were an integer x such that $|x^2 - 5/4|_5 \leqslant 5^{-4}$ then consider the possibilities for $|x^2|_5$. If $|x^2|_5 > |5/4|_5$ then (using the result that $|a + b|_p = \max(|a|_p, |b|_p)$ when $|a|_p \neq |b|_p$) we have $|x^2 - 5/4|_5 = \max(|x^2|_5, |5/4|_5) = |x^2|_5 > |5/4|_5 = 5^{-1} > 5^{-4}$, contradicting $|x^2 - 5/4|_5 \leqslant 5^{-4}$. If $|x^2|_5 < |5/4|_5$ then (using the same result) we have $|x^2 - 5/4|_5 = \max(|x^2|_5, |5/4|_5) = |5/4|_5 = 5^{-1} > 5^{-4}$, again contradicting $|x^2 - 5/4|_5 \leqslant 5^{-4}$. It must then be that $|x^2|_5 = |5/4|_5 = 5^{-1}$, but this is again impossible since $|x^2|_5 = 5^r$ where r is an even integer. Hence no such x exists.

5. 200 mod 7 is 4, so write: $200 = 4 + 7 \cdot 28 =$ (similarly) $4 + 7 \cdot (0 + 7 \cdot 4) = 4 + 0 \cdot 7^1 + 4 \cdot 7^2 = 4, 04$.

For 3/14, it is easier first to write: $3/14 = 7^{-1} \cdot 3/2$. First find the 7-adic expansion of 3/2, with the idea that the 7-adic expansion of 3/14 will then just be the 7-adic expansion of 3/2 shifted one place to the left). Now, $|3/2|_7 = 1$ and so $3/2 = a_0, a_1 a_2 \ldots$. Using $2(a_0 + 7a_1 + 7^2 a_2 + \ldots) = 3$, we first find $2a_0 \equiv 3 \bmod 7$ and so $a_0 = 5$. Continuing as usual, we find that $a_1 = 3, a_2 = 3, a_3 = 3 \ldots$. At this point, we suspect that $3/2 = 5, \overline{3}$. We can prove this rigorously as follows. Let $\alpha = 5, \overline{3}$. Then $\alpha - 5 = 0, \overline{3}$, and so $7^{-1}(\alpha - 5) - 3 = 3, \overline{3} - 3 = 0, \overline{3} = \alpha - 5$. Hence, $\alpha - 5 - 21 = 7\alpha - 35$ and so $\alpha = 3/2$, proving that $3/2 = 5, \overline{3}$ in $\mathbb{Q}_7$. Finally, $3/14 = 7^{-1} \cdot 3/2 = 53, \overline{3}$.

Let $\beta = 2, \overline{34} \in \mathbb{Q}_5$. Then $\beta - 2 = 0, \overline{34}$ and so $5^{-2}(\beta - 2) = 34, \overline{34}$, giving: $5^{-2}(\beta - 2) - 3 \cdot 5^{-1} - 4 \cdot 5^0 = 0, \overline{34} = \beta - 2$, and so: $\beta = -67/24$.

6. Let $x \in \mathbb{Q}$. Write $x = \pm n/d$, where n and d are integers with $\gcd(n, d) = 1$, and write n, d in terms of their primes factorisations: $n = p_1^{s_1} \cdot \ldots p_k^{s_k}$ and $d = q_1^{t_1} \cdot \ldots q_\ell^{t_\ell}$, where $p_1, \ldots p_k, q_1, \ldots q_\ell$ are distinct primes. If $x \in \mathbb{Z}$ then $\ell = 0$ (i.e. there are no occurrences of q_j) and we see that when $p = p_i$ for some i, $|x|_p = p_i^{-s_i} \leqslant 1$, and otherwise $|x|_p = 1$; hence $|x|_p \leqslant 1$ for all p; that is to say: $x \in \mathbb{Z}_p$ for all p.

Conversely, assume that $x \in \mathbb{Z}_p$ for all p. Then there could not be any occurrence of q_j [since then at $p = q_j$ we would have $|x|_p = q_j^{t_j} > 1$, contradicting $x \in \mathbb{Z}_p$. Hence, x has no denominator and is in $\mathbb{Z}$.

7. First note that $-28 = 2^2 \cdot (-7)$. In $\mathbb{Q}_2$, we know that any integer congruent to 1 mod 8 is a square, and so certainly -7 is a square; hence so is $-28 = 2^2 \cdot (-7)$.

In $\mathbb{Q}_3$, we observe that $|-28|_3 = 1$ and $-28 \equiv 2 \pmod 3$ which is not a quadratic residue mod 3; hence -28 is not a square in $\mathbb{Q}_3$. In $\mathbb{Q}_5$, we observe that $|-28|_5 = 1$ and $-28 \equiv 2 \pmod 5$ which is not a quadratic residue mod 5; hence -28 is not a square in $\mathbb{Q}_5$. In $\mathbb{Q}_7$, if there were an x such that $x^2 = -28$, then $|x^2|_7 = |-28|_7 = 7^{-1}$, contradicting the fact that $|x^2|_7 = 7^r$ where r is an even integer; hence -28 is not a square in $\mathbb{Q}_7$. In $\mathbb{Q}_{11}$, we observe that $|-28|_{11} = 1$ and $-28 \equiv 5 \pmod{11}$ which is a quadratic residue mod 11 since $5 \equiv 4^2 \pmod{11}$; hence -28 is a square in $\mathbb{Q}_{11}$. [The above repeatedly used the result that, when $p \neq 2$ and when $|a|_p = 1$ then a is a square in $\mathbb{Q}_p$ iff it is a square mod p.]

8. In $\mathbb{R}$, we have for example the root $\sqrt{2}$. In $\mathbb{Q}_2$, note that $17 \equiv 1 \bmod 8$, and so 17 is a square in $\mathbb{Q}_2$. In $\mathbb{Q}_{17}$, note that $|2|_{17} = 1$ and 2 is a quadratic residue mod 17, so that 2 is a square in $\mathbb{Q}_{17}$.

Finally, let $p \neq 2, 17$. Then each of $(\frac{2}{p}), (\frac{17}{p}), (\frac{34}{p})$ is 1 or -1. They cannot all be -1 since $(\frac{34}{p}) = (\frac{2}{p})(\frac{17}{p})$ [and $-1 \neq (-1)(-1)$], so at least one of them must be 1. Wlog, say that $(\frac{2}{p}) = 1$. Then $|2|_p = 1$ and 2 is a quadratic residue mod p, so that 2 must be a square in $\mathbb{Q}_p$.

9. Suppose there were an $x \in \mathbb{Q}_3$ such that $x^3 = 4$ in $\mathbb{Q}_3$. Then $|x|_3^3 = |4|_3 = 1$ and so $|x|_3 = 1$, which means that x can be written $x = a_0, a_1 a_2 \ldots$. Reducing x modulo 9 would then give the integer $a_0 + 3a_1$ whose cube is 4 modulo 9. But $0, \ldots 8$ square to give: $0, 1, 8, 0, 1, 8, 0, 1, 8$, respectively, so that $x^3 = 4$ is an impossible congruence mod 9. Hence 4 is not a cube in $\mathbb{Q}_3$.

Let $f(x) = x^3 - 28$ and let $x_0 = 1$. Then $|f(x_0)|_3 = |-27|_3 = 3^{-3}$, whereas $|f'(x_0)|_3 = |3|_3 = 3^{-1}$. Hence $|f(x_0)|_3 < |f'(x_0)|_3^2$, and so by Hensel's Lemma there must be a root of $f(x)$ in $\mathbb{Q}_3$; that is 28 must be a cube in $\mathbb{Q}_3$.

Let $f(x) = x^3 - 13$ and let $x_0 = -1$. Then $|f(x_0)|_7 = |-14|_3 = 7^{-1}$, whereas $|f'(x_0)|_7 = |3|_7 = 1$. Hence $|f(x_0)|_7 < |f'(x_0)|_7^2$, and so by Hensel's Lemma again there must be a root of $f(x)$ in $\mathbb{Q}_7$; that is 13 must be a cube in $\mathbb{Q}_7$.

10. The number of positive multiples of an integer $k > 0$ which are $\leqslant n$ is clearly $\left[\frac{n}{k}\right]$. To count the power of p dividing $n!$, since p is prime, it is enough to count the powers of p dividing $1, 2, 3, \ldots, n$ and add these powers up. Now, the number of multiples of p among $1, 2, 3, \ldots, n$ is $[\frac{n}{p}]$. Each multiple of p^2 among $1, 2, 3, \ldots, n$ gives an additional power of p dividing into $n!$, giving $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right]$ so far. Continuing in this way we get that the total power of p is as in the given formula. This gives that $|n!|_p = p^{-M}$, where $M = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots \leqslant \frac{n}{p} + \frac{n}{p^2} + \ldots = \frac{n}{p-1}$. Hence $|n!| \geqslant p^{-\frac{n}{p-1}}$, and so $|1/n!| \leqslant p^{\frac{n}{p-1}}$. Suppose that $|x| < p^{-\frac{1}{p-1}}$ and let $\tau = |x|/p^{-\frac{1}{p-1}} < 1$. Then $\left|\frac{x^n}{n!}\right| = \tau^n p^{-\frac{n}{p-1}} \left|\frac{1}{n!}\right| \leqslant \tau^n p^{-\frac{n}{p-1}} p^{\frac{n}{p-1}} = \tau^n \to 0$.

Hence, $\exp_p(x)$ converges (using the result from lectures which says that $\sum c_i$ converges iff $|c_i|_p \to 0$).

On the other hand, if $|x| \geqslant p^{-\frac{1}{p-1}}$, note that, for any $n = p^\ell$, the above $\frac{n}{p}, \frac{n}{p^2}, \ldots \frac{n}{p^\ell} = p^{\ell-1}, p^{\ell-2}, \ldots, 1 \in \mathbb{Z}$ and so $M = p^{\ell-1} + p^{\ell-2}, \ldots + 1 = \frac{p^\ell - 1}{p-1}$; this means that the subsequence $\left|\frac{x^{p^\ell}}{(p^\ell)!}\right| \geqslant (p^{-\frac{1}{p-1}})^{p^\ell} p^{\frac{p^\ell - 1}{p-1}} = p^{\frac{-1}{p-1}}$, and so $\left|\frac{x^n}{n!}\right| \not\to 0$. Hence $\exp_p(x)$ does not converge when $|x| \geqslant p^{-\frac{1}{p-1}}$.

When $K = \mathbb{Q}_p$ ($p \neq 2$), any $|x|_p < 1$ must satisfy $|x|_p \leqslant p^{-1}$ [since $|x|_p = p^r$ for some $r \in \mathbb{Z}$] $< p^{-\frac{1}{p-1}}$, since $p \geqslant 3$. Any $|x|_p \geqslant 1$ satisfies $|x| \geqslant p^{-\frac{1}{p-1}}$. When $K = \mathbb{Q}_2$, any $|x|_2 < 1/2$ must satisfy $|x|_2 \leqslant 2^{-2}$ [since $|x|_p = p^r$ for some $r \in \mathbb{Z}$] $< p^{-\frac{1}{p-1}} = 2^{-1}$. Any $|x|_p \geqslant 1/2$ satisfies $|x| \geqslant p^{-\frac{1}{p-1}} = 2^{-1}$.

Elliptic Curves. Solutions to Sheet 3.

1 Let $\mathcal{C}$ be the curve $2Y^2 = X^4 - 17$. Over $\mathbb{R}$, the curve has the point $(4, \sqrt{239/2})$. In $\mathbb{Q}_2$, let $x = 11$. Then $11^4 - 17 = 2^5 \cdot 457$; but 457 is an integer congruent to 1 mod 8, and so, from lectures, there exists $\gamma \in \mathbb{Z}_2 \subset \mathbb{Q}_2$ such that $457 = \gamma^2$; then $(11, 4\gamma)$ is a point on the curve over $\mathbb{Q}_2$. For the next few primes, we shall repeatedly use the result from lectures that, if $p \neq 2$ and $|a|_p = 1$, then a is a square in $\mathbb{Q}_p$ iff it is a square mod p. Now, note that $-8, -34, -34, -8, 10, -8$ are quadratic residues modulo $p = 3, 5, 7, 11, 13, 17$, respectively, and so there exists $\gamma \in \mathbb{Q}_p$ such that $\gamma^2 = -8, -34, -34, -8, 10, -8$, respectively; this gives the $\mathbb{Q}_p$-rational points on the curve: $(1, \gamma), (0, \gamma/2), (0, \gamma/2), (1, \gamma), (4, \gamma/2), (1, \gamma)$, respectively. Hence $\mathcal{C}$ has $\mathbb{Q}_p$-rational points for all primes up to and including $p = 17$ [in fact, it was only necessary to do here $p = 2, 3, 5, 7, 11, 17$ here].

Let p be any prime $p \geqslant 13$ and $p \neq 17$. Our curve $\mathcal{C}$ (after multiplying both sides by 2) is birationally equivalent to $V^2 = 2X^4 - 34$, where $V = 2Y$; note that $2X^4 - 34$ has discriminant $-2^{11}17^3$. Recall Theorem 1.15 from lectures, that any curve $y^2 = Q(x)$, where $Q(x) = f_4x^4 + \ldots + f_0$ has nonzero discriminant over $\mathbb{F}_p$, has at least $p - 1 - 2\sqrt{p} > 4$ affine points over $\mathbb{F}_p$, and so at least 5 affine points. At most 4 of these can have $2x^4 - 34 \equiv 0 \pmod{p}$, and so there exists $x_0 \in \mathbb{Z}$ such that $2(x_0^4 - 17)$ is a nonzero quadratic residue mod p. As above, there exists $\gamma \in \mathbb{Q}_p$ such that $\gamma^2 = 2(x_0^4 - 17)$, and so $(x_0, \gamma/2)$ is a $\mathbb{Q}_p$-rational point on our original curve $\mathcal{C}$. Hence $\mathcal{C}$ has points in $\mathbb{R}$ and every $\mathbb{Q}_p$.

Alternative method for the above parts: Note that for $p \nmid 2\Delta$ (that is: $p \neq 2, 17$, so that $\widetilde{\mathcal{C}}$ is still an elliptic curve mod p) and $p \geqslant 5$, we have $\#\widetilde{\mathcal{C}}(\mathbb{F}_p) \geqslant p + 1 - 2\sqrt{p} > 1$, and so the number of affine points is > 0; these are non-singular, since $\widetilde{\mathcal{C}}$ is still an elliptic curve mod p. Also, by a theorem from lectures, any non-singular point on $\widetilde{\mathcal{C}}(\mathbb{F}_p)$ lifts to a point on $\mathcal{C}(\mathbb{Q}_p)$; also, any affine non-singular point on $\widetilde{\mathcal{C}}(\mathbb{F}_p)$ lifts to an affine point on $\mathcal{C}(\mathbb{Q}_p)$ (since the point at infinity on $\mathcal{C}(\mathbb{Q}_p)$ maps to the point at infinity on $\widetilde{\mathcal{C}}(\mathbb{F}_p)$ under the reduction map mod p). This shows the existence of such $x, y \in \mathbb{Q}_p$ for all p except $p = 2, 3$ and bad primes, so only still need to consider $p = 2, 3, 17$. Also, note that for $p = 3$ there is the non-singular affine point $(1, 1)$ on $\widetilde{\mathcal{C}}(\mathbb{F}_3)$, and for $p = 17$ there is the non-singular affine point $(1, 3)$ on $\widetilde{\mathcal{C}}(\mathbb{F}_{17})$, and as before these must lift to affine points $(x, y) \in \mathcal{C}(\mathbb{Q}_p)$. Over $\mathbb{R}$, the curve has the point $(4, \sqrt{239/2})$. In $\mathbb{Q}_2$, let $x = 11$. Then $11^4 - 17 = 2^5 \cdot 457$; but 457 is an integer congruent to 1 mod 8, and so, from lectures, there exists $\gamma \in \mathbb{Z}_2 \subset \mathbb{Q}_2$ such that $457 = \gamma^2$; then $(11, 4\gamma)$ is a point on the curve over $\mathbb{Q}_2$. This completes the alternative method of showing that $\mathcal{C}$ has points in $\mathbb{R}$ and every $\mathbb{Q}_p$.

Now, imagine that $\mathcal{C}$ had a $\mathbb{Q}$-rational point; that is, imagine that there exist $X, Y \in \mathbb{Q}$ such that $2Y^2 = X^4 - 17$. Let $X = t/r$, where $r, t \in \mathbb{Z}$ and $\gcd(r, t) = 1$. Then $2(r^2Y)^2 = t^4 - 17r^4 \in \mathbb{Z}$. For any prime p, this gives that $|2|_p |r^2Y|_p^2 \leqslant 1$. When $p \neq 2$, we have $|2|_p = 1$ and so $|r^2Y|_p^2 \leqslant 1$ and so $|r^2Y|_p \leqslant 1$. When $p = 2$, we have $2^{-1}|r^2Y|_2^2 \leqslant 1$; but this still gives $|r^2Y|_2 \leqslant 1$ [since $|r^2Y|_2 > 1$ would mean $|r^2Y|_2 \geqslant 2^1$ and so $2^{-1}|r^2Y|_2^2 \geqslant 2^{-1}2^2 > 1$]. Overall, we have shown that $|r^2Y|_p \leqslant 1$ for all p; since also $r^2Y \in \mathbb{Q}$, this gives that $r^2Y \in \mathbb{Z}$; let us say: $s = r^2Y \in \mathbb{Z}$. Therefore $r, s, t \in \mathbb{Z}$ satisfy $2s^2 = t^4 - 17r^4$ and $\gcd(r, t) = 1$.

Let q be any prime such that $q|s$. Note that $q \neq 17$ [since if $17|s$ then our equation

$2s^2 = t^4 - 17r^4$ would force $17|t$, and so $17^2|2s^2$ and $17^2|t^4$, which would give $17^2|17r^4$, forcing $17|r$, which would contradict $\gcd(r,t) = 1$]. Note also that we must not then have $q|r$ [since if $q|s$ and $q|r$, then our equation $2s^2 = t^4 - 17r^4$ would force $q|t$, which would contradict $\gcd(r,t) = 1$]. Reducing our equation modulo q gives that $0 \equiv t^4 - 17r^4$ and so $(t^2/r^2)^2 \equiv 17 \bmod q$ [note that division by r^2 is allowable mod q since r is not divisible by q]. Hence 17 is a nonzero quadratic residue mod q. For $q \neq 2$, quadratic reciprocity then allows us to deduce that q is a quadratic residue mod 17 [since $17 \equiv 1 \pmod 4$]. Furthermore, one can check directly that 2 is a quadratic residue mod 17, since $2 \equiv 6^2 \bmod 17$. Overall, we have shown that every prime q dividing s must be a quadratic residue mod 17, and we can take $s > 0$ (if necessary, replacing s by $-s$), so that s is the product of its prime factors. It follows that s itself must be a quadratic residue mod 17, since it is a product of quadratic residues mod 17. Hence s^2 is a nonzero fourth power [also known as a *quartic residue*] mod 17. Note also that reducing our equation mod 17 gives $2s^2 \equiv t^4 \pmod{17}$, so that $2s^2$ is also a nonzero fourth power mod 17. Since $s, 2s^2$ are both nonzero fourth powers mod 17, it follows that $2 = (2s^2)/s^2$ is also a fourth power mod 17. On the other hand, one can compute directly that $0^4, 1^4, 2^4, 3^4, 4^4, 5^4, 6^4, 7^4, 8^4, 9^4, 10^4, 11^4, 12^4, 13^4, 14^4, 15^4, 16^4$ are congruent mod 17 to: $0, 1, 16, 13, 1, 13, 4, 4, 16, 16, 4, 4, 13, 1, 13, 16, 1$, respectively, so that in fact 2 is not a fourth power mod 17. This contradication show that our original curve $\mathcal{C}$ has no $\mathbb{Q}$-rational points.

2. Since $p \equiv 2 \pmod 3$, we have $\gcd(3, p-1) = 1$, and so there exist $\lambda, \mu \in \mathbb{Z}$ such that $3\lambda + (p-1)\mu = 1$. For any $x, y \in \mathbb{F}_p^*$, we have $x^{p-1} = y^{p-1} = 1$ [by Fermat's Little Theorem], and so:

$$x^3 = y^3 \Rightarrow \left(x^3\right)^\lambda \cdot 1^\mu = \left(y^3\right)^\lambda \cdot 1^\mu \Rightarrow \left(x^3\right)^\lambda \cdot \left(x^{p-1}\right)^\mu = \left(y^3\right)^\lambda \cdot \left(y^{p-1}\right)^\mu$$

$$\Rightarrow x^{3\lambda+(p-1)\mu} = y^{3\lambda+(p-1)\mu} \Rightarrow x = y.$$

Thus the map $x \mapsto x^3$ is injective on $\mathbb{F}_p^*$ and so is a bijection.

Now, let $a \in \mathbb{Z}$ be such that $p \not| a$. From above, there must exist $x_0 \in \mathbb{Z}$ such that $x_0^3 \equiv a \pmod p$; clearly $p \not| x_0$. Let $f(x) = x^3 - a$. Then $|f(x_0)|_p = |x_0^3 - a|_p < 1$, since $x_0^3 - a \equiv 0 \pmod p$. Also, $|f'(x_0)|_p = |3x_0^2|_2 = 1$, since $|3|_p = 1$ and $p \not| x_0$. Hence $|f(x_0)|_p < |f'(x_0)|_p^2$, and so by Hensel's Lemma, there exists $x \in \mathbb{Z}_p$ with $f(x) = 0$, that is, $x^3 = a$, as required.

3. Recall the standard fact about resultants (stated in Section 0, the preliminary reading), that there exist polynomials $p(x), q(x) \in R[x]$ such that: $p(x)f(x) + q(x)g(x) = \mathrm{Res}\big(f(x), g(x)\big)$ Since the discriminant D is the resultant of $f(x)$ and $f'(x)$, there must exist polynomials $p(x), q(x) \in R[x]$ such that $p(x)f(x) + q(x)f'(x) = D$, and so: $p(a_0)f(a_0) + q(a_0)f'(a_0) = D$. Since $|a_0| \leqslant 1$, and since $p(x), q(x), f(x), f'(x) \in R[x]$, we must have $|p(a_0)|, |f(a_0)|, |q(a_0)|, |f'(a_0)| \leqslant 1$ and so $|D| \leqslant \max(|p(a_0)f(a_0)|, |q(a_0)f'(a_0)|) \leqslant 1$, which also implies $|D^2| = |D|^2 \leqslant |D|$. Now, we are given that $|f(a_0)| < |D|^2$ and so $|p(a_0)f(a_0)| \leqslant |f(a_0)| < |D^2| \leqslant |D|$. Hence $|D| \neq |p(a_0)f(a_0)|$, and so $|q(a_0)f'(a_0)| = |D - p(a_0)f(a_0)| = \max(|D|, |p(a_0)f(a_0)|) = |D|$ [using the fact that, if $|u| \neq |v|$ then

$|u \pm v| = \max(|u|, |v|)]$. Since also $|q(a_0)| \leqslant 1$, this gives that $|f'(a_0)| \geqslant |D|$. Finally, $|f(a_0)| < |D|^2 \leqslant |f'(a_0)|^2$, and so $f(X)$ has a root $a \in R$ by Hensel's Lemma.

4. We first (as suggested in the hint) show:
Lemma (*). For any $\alpha = a + b\sqrt{d} \in \mathbb{Q}_p(\sqrt{d})$, $|\alpha|_p \leqslant 1 \Rightarrow |\alpha + 1|_p \leqslant 1$.
Proof. Assume $|\alpha|_p \leqslant 1$, so that $|a^2 - b^2 d|_p \leqslant 1$. The result is trivial for $b = 0$, so we can assume $b \neq 0$. Let:
$f(x) = \big(x - (a + b\sqrt{d})\big)\big(x - (a - b\sqrt{d})\big) = x^2 - 2ax + a^2 - b^2 d$.

Imagine $|2a|_p > 1$. Then $g(x) = f(x)/(2a) = \frac{x^2}{2a} - x + \frac{a^2 - b^2 d}{2a}$ would be defined over $\mathbb{Z}_p$, with $|g(0)|_p = |\frac{a^2 - b^2 d}{2a}|_p < 1 = |-1|_p^2 = |g'(0)|_p^2$, so by Hensel's Lemma, there would exist a root in $\mathbb{Z}_p$, contradicting the fact that $a + b\sqrt{d}, a - b\sqrt{d} \notin \mathbb{Z}_p$ (since d is non-square and $b \neq 0$).

Hence $|2a|_p \leqslant 1$. So:
$|\alpha + 1|_p = |a + 1 + b\sqrt{d}|_p = |(a+1)^2 - b^2 d|_p^{1/2} = |(a^2 - b^2 d) + 2a + 1|_p^{1/2} \leqslant 1$ (since $|a^2 - b^2 d|_p, |2a|_p, |1|_p \leqslant 1$), completing the proof of Lemma (*).

For any $\alpha = a + b\sqrt{d} \in \mathbb{Q}_p(\sqrt{d})$, let $\overline{\alpha}$ denote $a - b\sqrt{d}$; also, let:
$\alpha_1 = a_1 + b_1\sqrt{d},\ \alpha_2 = a_2 + b_2\sqrt{d} \in \mathbb{Q}_p(\sqrt{d})$, where $a, b, a_1, b_1, a_2, b_2 \in \mathbb{Q}_p$.

Note that $|\alpha|_p = |a^2 - b^2 d|_p^{1/2} \geqslant 0$, and that:
$|\alpha|_p = 0 \iff a^2 - b^2 d = 0 \iff a = b = 0 \iff \alpha = 0$ (since d is non-square).

$|\alpha_1\alpha_2|_p = |\alpha_1\alpha_2\overline{\alpha_1\alpha_2}|_p^{1/2} = |\alpha_1\overline{\alpha}_1\alpha_2\overline{\alpha}_2|_p^{1/2} = |\alpha_1\overline{\alpha}_1|_p^{1/2}|\alpha_2\overline{\alpha}_2|_p^{1/2} = |\alpha_1|_p|\alpha_2|_p$.

Also, without loss of generality, $|\alpha_1|_p \leqslant |\alpha_2|_p$, so that $|\frac{\alpha_1}{\alpha_2}|_p \leqslant 1$. Then:
$|\alpha_1 + \alpha_2|_p = |\frac{\alpha_1}{\alpha_2} + 1|_p|\alpha_2|_p \leqslant$ [by Lemma (*)] $|\alpha_2|_p = \max\big(|\alpha_1|_p, |\alpha_2|_p\big)$.

Hence, $|\ |_p$ is a non-Archimedean valuation on $\mathbb{Q}_p(\sqrt{d})$. Finally, note that when $\alpha = a$ [with $b = 0$], our definition of $|\ |_p$ on $\mathbb{Q}_p(\sqrt{d})$ gives $|\alpha|_p = |a^2 - 0^2 d|_p^{1/2} = |a^2|_p^{1/2} = |a|_p$, which agrees with the usual $|\ |_p$ on $\mathbb{Q}_p$, so that our non-Archimedean valuation on $\mathbb{Q}_p(\sqrt{d})$ extends that on $\mathbb{Q}_p$.

5. In projective form, the point is: $(-64/25, 59/125, 1)$. The coordinate with largest 5-adic value is $59/125$, and on dividing all coordinates through by this, we can also represent the point as: $(-320/59, 1, 125/59)$, which is in 5-adic standard form (that is, 1 is the maximum of the 5-adic valuations of the coordinates). Reducing mod 5 gives $(0, 1, 0)$ on $\widetilde{\mathcal{E}}$, which is the point at infinity.

6. Suppose that (x, y) on $\mathcal{E}$ reduces mod p to $(0, 0)$ on $\widetilde{\mathcal{E}}$. Then $|x|_p, |y|_p < 1$, indeed $|x|_p, |y|_p \leqslant p^{-1}$ (since any p-adic value is one of: $\ldots..., p^{-2}, p^{-1}, 1, p^1, p^2, \ldots$, so that if a p-adic value is < 1 then it must be $\leqslant p^{-1}$), so that $|x|_p^3 \leqslant p^{-3}$. But $|p|_p = p^{-1}$ and so $|x|_p^3 \neq |p|_p$ which means that $|x^3 + p|_p = \max(|x|_p, |p|_p) = p^{-1}$. Since x, y satisfy $y^2 = x^3 + p$, we must therefore have: $|y|_p^2 = p^{-1}$, which contradicts the fact that $|y|_p^2 = p^{2r}$ for some integer r.

7.
(a). Let $\mathcal{E} : Y^2 = X^3 + p^2$. Then the point $(0, p)$ on $\mathcal{E}$ reduces modulo p to the cusp $(0, 0)$ on $\widetilde{\mathcal{E}} : Y^2 = X^3$, which is another way of saying that $(0, 0)$ on $\widetilde{\mathcal{E}}$ lifts to the point $(0, p)$ in $\mathcal{E}(\mathbb{Q}_p)$.

(b). Question 3 is an example of this.
(c). Let $\mathcal{E} : Y^2 = X^3 + X^2 + p^2$. Then the point $(0, p)$ on $\mathcal{E}$ reduces modulo p to the node $(0, 0)$ on $\widetilde{\mathcal{E}} : Y^2 = X^3 + X^2$, which is another way of saying that $(0, 0)$ on $\widetilde{\mathcal{E}}$ lifts to the point $(0, p)$ in $\mathcal{E}(\mathbb{Q}_p)$.
(d). Let $\mathcal{E} : Y^2 = X^3 + X^2 + p$ and $\widetilde{\mathcal{E}} : Y^2 = X^3 + X^2$. Then the node $(0, 0)$ on $\widetilde{\mathcal{E}}$ does not lift to any point in $\mathcal{E}(\mathbb{Q}_p)$ by the same argument as in Question 2.

8. Take $F(X, Y) = X + Y + tXY^p$, clearly non-commutative. One only has to check associativity.

$$F(F(X,Y),Z) = F(X+Y+tXY^p, Z) = X+Y+tXY^p+Z+t(X+Y+tXY^p)Z^p$$

$$= X+Y+tXY^p+Z+tXZ^p+tYZ^p,$$

since the remaining term $t^2XY^pZ^p \in I = t^2\mathbb{F}_p[t]$ and so $t^2XY^pZ^p = 0$ in $R = \mathbb{F}_p[t]/I$. Also:

$$F(X,F(Y,Z)) = X+F(Y,Z)+tXF(Y,Z)^p = X+Y+Z+tYZ^p+tX(Y+Z+tYZ^p)^p$$

$$= X+Y+Z+tYZ^p+tX(Y^p+Z^p+(tYZ^p)^p),$$

since all other terms in the binomial expansion of $(Y + Z + tYZ^p)^p$ are divisible by p and so are equal to 0 in R, which has characteristic p. But $(tYZ^p)^p = t^2(t^{p-2}Y^pZ^{p^2}) \in I$ and so $(tYZ^p)^p = 0$ in R, so that the above are the same, giving associativity, as required.

9. Recall from lectures that the first step in deriving the formal group of an elliptic curve is to write the equation $\mathcal{E} : Y^2 = X^3 + AX + B$ as: $\mathcal{E}' : w = f(z, w) = z^3 + Aw^2z + Bw^3$, where $z = -x/y, w = -1/y$. We then Inductively define $f_n(z, w)$ by: $f_1(z, w) = f(z, w)$ and $f_{m+1}(z, w) = f_m(z, f(z, w))$ and define

$$w(z) = \lim_{m\to\infty} f_m(z, 0) \in \mathbb{Z}[A, B][[z]],$$

which satisfies $w(z) = f\big(z, w(z)\big)$. The terms of $f_1(z, w) = z^3 + Aw^2z + Bw^3$ all have weighted degree $\equiv 3$ [where we give z weight 1, w weight 3, A weight -4 and B weight -6]. Suppose that this is also true of $f_m(z, w)$; then $f_{m+1}(z, w) = f_m(z, z^3 + Aw^2z + Bw^3)$, where z has weighted degree 1, $z^3 + Aw^2z + Bw^3$ is homogeneous of weighted degree 3, and so the same will be true of f_{m+1}. So, by induction, all terms of every f_m and so all terms of $w(z)$ will have weighted degree 3, and so $w(z) = \sum c_n z^n$, where $c_n = 0$ unless $n \equiv 3 \bmod 4$. We now perform the addition $(z_1, w_1) + (z_2, w_2)$. As usual, we first write the line $z = \lambda w + \mu$ through the points, given by $\lambda = (w(z_1) - w(z_2))/(z_1 - z_2)$ and $\mu = (z_1w(z_2) - z_2w(z_1))/(z_1 - z_2)$, both in $\mathbb{Z}[A, B][[z_1, z_2]]$. Letting z_1 and z_2 each have weight 1, the numerator $w(z_1) - w(z_2)$ is homogeneous of weighted degree 3, and so λ is homogeneous of weighted degree 2. Similarly, μ is homogeneous of weighted degree 3. As in lectures, substituting $w = \lambda z + \mu$ into $\mathcal{E}'$ gives $\lambda z + \mu = z^3 + A(\lambda z + \mu)^2 z + B(\lambda z + \mu)^3$, and so:

$$(1 + A\lambda^2 + B\lambda^3)z^3 + (2A\lambda\mu + 3B\lambda^2\mu)z^2 + \ldots = 0.$$

Let $(z_3, w(z_3))$ be the third point of intersection of $\mathcal{E}'$ and the line $z = \lambda w + \mu$, so that z_1, z_2, z_3 are the roots of the above cubic, giving that $z_1 + z_2 + z_3 = -(\text{coeff of } z^2)/(\text{coeff of } z^3)$, so:

$$z_3 = -z_1 - z_2 - \frac{2A\lambda\mu + 3B\lambda^2\mu}{1 + A\lambda^2 + B\lambda^3} \in \mathbb{Z}[A, B][[z_1, z_2]],$$

since the denominator is of the form $1 + \phi(z)$, where $\phi(z)$ has no constant term [and so is an invertible power series, with $1/(1 + \phi(z)) = 1 - \phi(z) + \phi(z)^2 + \ldots$]. The sum $(z_1, w_1) + (z_2, w_2) + (z_3, w_3) =$ the identity, and so $(z_1, w_1) + (z_2, w_2) = -(z_3, w_3)$. Negation $(x, y) \mapsto (x, -y)$ induces $(z, w) \mapsto (-z, -w)$ [since $z = -x/y, w = -1/y$], so that the z-coordinate of $(z_1, w_1) + (z_2, w_2)$ is given by $F_{\mathcal{E}}(z_1, z_2)$, where:

$$F_{\mathcal{E}}(z_1, z_2) = z_1 + z_2 + (\text{ terms of degree } \geqslant 2) \in \mathbb{Z}[A, B][[z_1, z_2]].$$

But note that the expression for z_3 above consists of the terms z_1, z_2, both homogeneous of weighted degree 1, and the fraction whose numerator $2A\lambda\mu + 3B\lambda^2\mu$ is homogeneous of weighted degree 1, and whose denominator $1 + A\lambda^2 + B\lambda^3$ is homogeneous of weighted degree 0. Therefore the final power series giving the formal group must be homogeneous of weighted degree 1.

For the case when our curve is of the form $Y^2 = X^3 + AX$ (so that $B = 0$), each term of the formal group must be an integer multiple of $A^k z_1^{n_1} z_2^{n_2}$. Since the weighted degree is 1 and since A has weight -4, we see that the degree purely in z_1, z_2 must by $\equiv 1 \bmod 4$, as required.

When our curve is of the form $Y^2 = X^3 + B$ (so that $A = 0$) the fact that B has weight -6 similarly gives that each term of the formal group has degree $\equiv 1 \bmod 6$ in z_1, z_2.

Elliptic Curves. Solutions to Sheet 4.

1. In all of the following, we use the result from lectures that (when the coefficients of $\mathcal{E}$ are in $\mathbb{Z}$) $\mathcal{E}_{\rm tors}(\mathbb{Q})$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}$ mod p, where $p \neq 2$ is a prime not dividing the discriminant. Note that this typically gives a much faster way of computing $\mathcal{E}_{\rm tors}(\mathbb{Q})$ than the Nagell-Lutz result. N.B. (a),(b),(c) are about the level that could be asked as part of a 3-hour exam.

(a). There are the obvious points $P = (0,1)$ of order 3 and $Q = (-1,0)$ of order 2 in $\mathcal{E}_{\rm tors}(\mathbb{Q})$, which generate a subgroup of $\mathcal{E}_{\rm tors}(\mathbb{Q})$ of size 6 (namely, the 6 points $mP + nQ$ for $0 \leqslant m \leqslant 2$ and $0 \leqslant n \leqslant 1$). Further, $\Delta = 4A^3 + 27B^2 = 27$, so we can reduce modulo any prime except 2 (which must always be avoided) and 3. Over $\mathbb{F}_5$, there are only six points: $\mathbf{o}, (0, \pm 1), (2, \pm 3), (4, 0)$. So, we conclude that $\mathcal{E}_{\rm tors}(\mathbb{Q})$ has size at most 6, which means that it consists of precisely the $C_6 = C_2 \times C_3$ group of points we have found already.

Note that, if $P = (0,1)$ and $Q = (-1,0)$, then the complete list of torsion points is: $\mathbf{o}, P = (0,1), 2P = (0,-1), Q = (-1,0), P+Q = (2,-3), 2P+Q = (2,3)$.

(b). Here, the (birational over $\mathbb{Q}$) transformation $(X,Y) \mapsto (X-1, Y)$ takes the given curve to: $Y^2 = X(X+1)(X-1) = X^3 - X$, which has discriminant -4, and so we can reduce modulo the prime 3 Over $\mathbb{F}_3$ there are the points: $\mathbf{o}, (0,0), (1,0), (2,0)$ giving that $\mathcal{E}_{\rm tors}(\mathbb{Q})$ has size at most 4. But, in fact, $\mathcal{E}_{\rm tors}(\mathbb{Q})$ contains $\mathbf{o}, (0,0), (-1,0), (1,0)$, which means the this $C_2 \times C_2$ group gives all of $\mathcal{E}_{\rm tors}(\mathbb{Q})$. [*Alternatively, even without using a birational transformation to the form* $Y^2 = X^3 + AX + B$*, we could just work entirely with the given equation of the curve, noting that the original cubic* $X(X-1)(X-2)$ *has no repeated roots mod* 3*, so that* $Y^2 = X(X-1)(X-2)$ *is an elliptic curve mod* 3*, and then noting that the only points are:* $\mathbf{o}, (0,0), (1,0), (2,0)$.]

(c). The (birational over $\mathbb{Q}$) transformation $(X,Y) \mapsto (3^2X, 3^3Y)$ takes the given curve to: $Y^2 = X^3 + 1$ which we have already seen in part (a) to have a $C_2 \times C_3$ group as its torsion group.

Note that, if $P = (0, 1/27)$ and $Q = (-1/9, 0)$ then the complete list of torsion points is given by: $\mathbf{o}, P = (0,1/27), 2P = (0,-1/27), Q = (-1/9,0), P+Q = (2/9,-1/9), 2P+Q = (2/9, 1/9)$.

2. Let $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q})$ be the usual isogeny, which is a group homomorphism with kernel: $\mathbf{o}, (0,0)$, and let $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q})$ be the usual dual isogeny, which is also a group homomorphism with kernel: $\mathbf{o}, (0,0)$. Now, let $\mathcal{C}_{\rm oddtors}(\mathbb{Q})$ be the set of torsion elements of $\mathcal{C}(\mathbb{Q})$ which have odd order. First check that $\mathcal{C}_{\rm oddtors}(\mathbb{Q})$ is a subgroup: (1) The identity $\mathbf{o}$ has order 1, which is odd, so $\mathbf{o} \in \mathcal{C}_{\rm oddtors}(\mathbb{Q})$, (2) If P, Q have odd torsion orders m, n, respectively, then $mn(P+Q) = n(mP) + m(nQ) = \mathbf{o}$ and so the order of $P+Q$ divides mn, giving that the order of $P+Q$ is odd, i.e. $P+Q \in \mathcal{C}_{\rm oddtors}(\mathbb{Q})$, (3) The order of $-P$ is the same as the order of $-P$, so $P \in \mathcal{C}_{\rm oddtors}(\mathbb{Q}) \Rightarrow -P \in \mathcal{C}_{\rm oddtors}(\mathbb{Q})$. Similarly define $\mathcal{D}_{\rm oddtors}(\mathbb{Q})$, a subgroup of $\mathcal{D}(\mathbb{Q})$.

Now, consider any $P \in \mathcal{C}_{\rm oddtors}(\mathbb{Q})$. Then P must have odd order m, say. Let $R = \phi(P)$. Then $mR = m\phi(P) = \phi(mP) = \phi(\mathbf{o}) = \mathbf{o}$, which means that the order of R divides m, and so the order of R is odd; that is: $R \in \mathcal{D}_{\rm oddtors}(\mathbb{Q})$. Hence, ϕ gives a

map from $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ to $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, which certainly satisfies the homomorphism property $\phi(P+Q)=\phi(P)+\phi(Q)$ for all $P,Q\in\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, since ϕ satisfies this property on the larger set $\mathcal{C}(\mathbb{Q})$. Furthermore, the kernel of $\phi:\mathcal{C}_{\text{oddtors}}(\mathbb{Q})\to\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ must only contain $\mathbf{o}$ [since $(0,0)\notin\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$], and so $\phi:\mathcal{C}_{\text{oddtors}}(\mathbb{Q})\to\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ is an injection [any homomorphism with trivial kernel is an injection]. We have therefore established that there is an injective homomorphism (namely ϕ) from $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ to $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, which implies that $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, namely the subgroup $\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q})))$ [note, since $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ are finite, it follows from this that $\#\mathcal{C}_{\text{oddtors}}(\mathbb{Q})=\#\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q})))\leqslant\#\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$]. (We have just used here the general fact that if θ is a homomorphism from group G to group H, then $G/\ker\theta$ is isomorphic to $\text{im}\theta$, which is the same as $\theta(G)$; when θ is injective, $\ker\theta$ contains only the identity element and $G/\ker\theta$ can be replaced by G). Applying the same argument to $\hat{\phi}:\mathcal{D}_{\text{oddtors}}(\mathbb{Q})\to\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ gives that $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, namely $\hat{\phi}(\mathcal{D}_{\text{oddtors}}(\mathbb{Q}))$ [and consequently $\#\mathcal{D}_{\text{oddtors}}(\mathbb{Q})=\#\hat{\phi}(\mathcal{D}_{\text{oddtors}}(\mathbb{Q}))\leqslant\#\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$]. So, all of $\mathcal{C}_{\text{oddtors}}(\mathbb{Q}),\mathcal{D}_{\text{oddtors}}(\mathbb{Q}),\hat{\phi}(\mathcal{D}_{\text{oddtors}}(\mathbb{Q})),\hat{\phi}(\mathcal{D}_{\text{oddtors}}(\mathbb{Q}))$ must have the same number of elements. Combining the fact that $\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q})))$ is a subgroup of $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ and the fact that $\#\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q})))=\#\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ gives that $\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q})))$ must be equal to $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$. But $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ is isomorphic to $\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q})))$ which is equal to $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$; hence $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ is isomorphic to $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, as required.

3. The preimages of $(0,0)$ under $\hat{\phi}$ are given by the points of order 2 on $\mathcal{D}$ distinct from $(0,0)$, namely $Q_1=((-a_1+\sqrt{a_1^2-4b_1})/2,0)=(a+2\sqrt{b},0)$ and $Q_2=((-a_1-\sqrt{a_1^2-4b_1})/2,0)=(a-2\sqrt{b},0)$. Recall the standard map from lectures $q:\mathcal{D}(\mathbb{Q})\to\mathbb{Q}^*/(\mathbb{Q}^*)^2$ which takes $\mathbf{o}\to1$, $(0,0)\to b_1$, and otherwise takes $(u,v)\to u$. We know from lectures that this map has kernel precisely $\phi(\mathcal{C}(\mathbb{Q}))$. Now, the multiplication by 2 map on $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi}\circ\phi$, and so $(0,0)\in2\mathcal{C}(\mathbb{Q})$ iff either Q_1 or Q_2 is a member of $\phi(\mathcal{C}(\mathbb{Q}))\iff q(Q_1)=1$ or $q(Q_2)=1\iff a+2\sqrt{b}$ or $a-2\sqrt{b}=1\in\mathbb{Q}^*/(\mathbb{Q}^*)^2\iff a+2\sqrt{b}$ or $a-2\sqrt{b}\in(\mathbb{Q}^*)^2\iff b=m^2$ and $a+2m=n^2$, for some $m,n\in\mathbb{Q}$; but in fact m,n must be in $\mathbb{Z}$ since $a,b\in\mathbb{Z}$.

4.

(a). Let $\mathcal{C}:Y^2=X(X^2+aX+b)=X(X^2+2X+3)$, where $a=2,b=3$, and isogenous curve $\mathcal{D}:Y^2=X(X^2+a_1X+b_1)=X(X^2-4X-8)$, where $a_1=-4,b_1=-8$, with the usual isogeny $\phi:\mathcal{C}(\mathbb{Q})\to\mathcal{D}(\mathbb{Q}):(x,y)\mapsto(y^2/x^2,y-3y/x^2)$, and dual isogeny $\hat{\phi}:\mathcal{D}(\mathbb{Q})\to\mathcal{C}(\mathbb{Q}):(u,v)\mapsto(\frac{1}{4}v^2/u^2,\frac{1}{8}(v+8v/u^2))$.

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 $q:\mathbf{o}\mapsto1$, is an injection with im$q$ contained in $\{d:d\text{ is square free and }d|b_1\}=\{\pm1,\pm2\}$. Also, $\mathbf{o}\mapsto1$, $(0,0)\mapsto-8=-2$, so that $\{1,-2\}\subset\text{im}q\subset\{\pm1,\pm2\}$.

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: $-\ell^4-4\ell^2m^2+8m^4=n^2$. Rewrite as: $-(\ell^2+2m^2)^2+12m^4=n^2$. Reducing modulo 3 gives $-(\ell^2+2m^2)^2\equiv n^2$ (modulo 3). If n were coprime to 3, then this would give: $((\ell^2+2m^2)/n)^2=-1$ in $\mathbb{F}_3$, contradicting the fact that -1 is not a quadratic

residue modulo 3. So, $3|n$ and so $3|(\ell^2+2m^2)$ also. This means that $9|(\ell^2+2m^2)^2$ and $9|n^2$, which can be combined with $-(\ell^2+2m^2)^2+12m^4=n^2$ to give: $9|12m^4$ and so $3|m$. Combining $3|m$ with $3|(\ell^2+2m^2)$ gives that $3|\ell$. 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 $-1\notin \mathrm{im}q$.

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

The map $\hat{q}:\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))\to\mathbb{Q}^*/(\mathbb{Q}^*)^2:(x,y)\mapsto x$, for $(x,y)\neq(0,0)$, with $\hat{q}:(0,0)\mapsto b$ and $\hat{q}:\mathbf{o}\mapsto 1$, is an injection with $\mathrm{im}\hat{q}$ contained in $\{d: d \text{ is square free and } d|b\}=\{\pm1,\pm3\}$. Also, $\mathbf{o}\mapsto 1$ and $(0,0)\mapsto 3$, so that $\{1,3\}\subset \mathrm{im}\hat{q}\subset\{\pm1,\pm3\}$.

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: $(-1)\cdot\ell^4+a\ell^2m^2+(b/(-1))\cdot m^4=n^2$; that is: $-\ell^4+2\ell^2m^2-3m^4=n^2$. Rewrite as: $-(\ell^2-m^2)^2-2m^4=n^2$. This is impossible in $\mathbb{R}$ (the left hand side is $\leqslant 0$ and the right hand side is $\geqslant 0$, and equality only occurs when $\ell^2-m^2=m^4=n^2=0$, implying $\ell=m=n=0$, which is not allowed). Hence $-1\notin\mathrm{im}\hat{q}$.

We conclude that $\mathrm{im}\hat{q}=\{1,3\}$, 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, $\hat{\phi}\big((0,0)\big)=\mathbf{o}$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0,0)$, and so is isomorphic to C_2. We also know that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})/2\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})\times C_2^r$, which is isomorphic to $\mathcal{C}(\mathbb{Q})[2]\times C_2^r$, where $\mathcal{C}(\mathbb{Q})[2]$ is the 2-torsion group and r is the rank. The 2-torsion points on $\mathcal{C}:Y^2=X(X^2+2X+3)$ are $\mathbf{o}$ together with the points of the form $(x,0)$, where x is a root of $X(X^2+2X+3)$, that is: $(0,0)$, $(-1+\sqrt{-2},0)$ and $(-1+\sqrt{-2},0)$, of which only $\mathbf{o}$ and $(0,0)$ are in $\mathcal{C}(\mathbb{Q})[2]$, giving that $\mathcal{C}(\mathbb{Q})[2]$ is isomorphic to C_2. Combining this with the facts (already found) that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic both to C_2 and to $\mathcal{C}(\mathbb{Q})[2]\times C_2^r$, give that $\mathcal{C}(\mathbb{Q})$ has rank 0.

(b). Let $\mathcal{C}:Y^2=X(X^2+aX+b)=X(X^2+14X+1)$, where $a=14,b=1$, and isogenous curve $\mathcal{D}:Y^2=X(X^2+a_1X+b_1)=X(X^2-28X+192)$, where $a_1=-28,b_1=192$, 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 $\hat{\phi}:\mathcal{D}(\mathbb{Q})\to\mathcal{C}(\mathbb{Q}):(u,v)\mapsto(\frac{1}{4}v^2/u^2,\frac{1}{8}(v-192v/u^2))$.

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 $\mathrm{im}q$ contained in $\{d: d \text{ is square free and } d|b_1\}=\{\pm1,\pm2,\pm3,\pm6\}$. Also, $\mathbf{o}\mapsto 1$, $(0,0)\mapsto 192=3$ and the obvious point $(8,16)\mapsto 2$ [N.B. when searching for a point in $\mathcal{D}(\mathbb{Q})$ which might map to 2 under q, one need only try points with x-coordinate equal to 2 modulo squares, e.g. 2,8,1/2,18,etc, so one should find the point $(8,16)$ quickly; also, its a good idea at the outset just to look for "obvious" members of $\mathcal{D}(\mathbb{Q})$ with x coordinates being integers in the range from -10 to 10; doing this at the outset would also reveal the point $(8,16)$.] This means that $1,3,2\in\mathrm{im}q$; but $\mathrm{im}q$ is a group, so $6\in\mathrm{im}q$ also, and indeed we can just take: $(0,0)+(8,16)=(24,-48)$, which maps to 6 under q. Hence, $\{1,2,3,6\}\subset\mathrm{im}q\subset\{\pm1,\pm2,\pm3,\pm6\}$.

There is only one coset to check, represented by -1, say. We know that $-1\in\mathrm{im}q$ 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: $-\ell^4 - 28\ell^2m^2 - 192m^4 = n^2$. 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 $\text{im}q = \{1, 2, 3, 6\}$ and that $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\mathbf{o}, (0,0), (8,16), (24,-48)\}$, and so $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ is generated by $(0,0)$ and $(8,16)$.

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 $\text{im}\hat{q}$ contained in $\{d : d \text{ is square free and } d|b\} = \{\pm 1\}$. Also, $\mathbf{o} \mapsto 1$ and $(0,0) \mapsto 1$, so that $\{1\} \subset \text{im}\hat{q} \subset \{\pm 1\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in \text{im}\hat{q}$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1)\cdot\ell^4 + a\ell^2m^2 + (b/(-1))\cdot m^4 = n^2$; that is: $-\ell^4 + 14\ell^2m^2 - m^4 = n^2$. Rewrite as: $-(\ell^2 - 7m^2)^2 + 48m^4 = n^2$. Reducing modulo 3 gives: $-(\ell^2 - 7m^2)^2 \equiv n^2$ (modulo 3). If n were coprime to 3, then this would give: $((\ell^2 - 7m^2)/n)^2 = -1$ in $\mathbb{F}_3$, contradicting the fact that -1 is not a quadratic residue modulo 3. So, $3|n$ and so $3|(\ell^2 - 7m^2)$, also. Hence 9 divides $(\ell^2 - 7m^2)^2$ and n^2 and so must divide $48m^4$; but 48 is only divisible by 3 (not by 9) so that 3 must divide m^4; hence 3 divides m. Combining this with the fact (already found) that $3|(\ell^2 - 7m^2)$ gives that $3|\ell$ also. We've shown that 3 divides all of ℓ, m, n, a contradiction. Hence $-1 \notin \text{im}\hat{q}$.

We conclude that $\text{im}\hat{q} = \{1\}$, and so $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ contains only $\mathbf{o}$. [N.B. $(0,0)$ should not also be included as a separate member 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 $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$; the same comment applies to the obvious point $(1,4)$; in general, for each distinct member r of $\text{im}\hat{q}$, you should only include exactly one point in $\mathcal{C}(\mathbb{Q})$ which maps to r].

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: $\mathbf{o}$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0,0)\big) = \mathbf{o}$ and $\hat{\phi}\big((8,16)\big) = (1,-4)$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(1,-4)$, 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 isomorphic to C_2. Conclusion: rank = 0. [If this seems surprising, then note that $(1,4), (1,-4)$ are points of order 4 in $\mathcal{C}(\mathbb{Q})$].

5. We are given that $A, +$ is an Abelian group, and that $h : A \to \mathbb{R}_{\geq 0}$ satisfies:

(I) There exists a constant C, independent of P, Q, such that
$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| \leq C$, for all $P, Q \in A$,

(II) For any $B \in \mathbb{R}$, the set $\{P \in A : h(P) \leq B\}$ is finite.

From (I) we obtain: $h(P+Q) + h(P-Q) - 2h(P) - 2h(Q) \leq C$ and so (since $h(P-Q) \geq 0$): $h(P+Q) \leq h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + C \leq 2h(P) + C_1(Q)$, where $C_1(Q) = 2h(Q) + C$. Hence Property (1) in the definition of height function is satisfied.

Letting $Q = P$ in (I), we obtain:
$|h(2P) + h(e) - 4h(P)| \leq C, \quad (*)$
where e denotes the identity element of the group A. This gives: $h(2P) + h(e) - 4h(P) \geq -C$, and so: $h(2P) \geq 4h(P) - C_2$, where $C_2 = C + h(e)$. Hence Property (2) in the

definition of height function is satisfied. Furthermore, (II) is the same as Property (3) in the definition of height function. Hence all 3 required properties are satisfied, giving that h is a height function, as required.

Replacing P, Q in (I) with $2P, P$, respectively, gives:

$$|h(3P) - 2h(2P) - h(P)| \leq C.$$

Multiplying $(*)$ by 2 gives:

$$|2h(2P) + 2h(e) - 8h(P)| \leq 2C.$$

These last two equations then give:

$$\begin{aligned} |h(3P) - 9h(P)| &= |h(3P) - 2h(2P) - h(P) + 2h(2P) + 2h(e) - 8h(P) - 2h(e)| \\ &\leq |h(3P) - 2h(2P) - h(P)| + |2h(2P) + 2h(e) - 8h(P)| + 2|h(e)| \leq C_3, \end{aligned}$$

where $C_3 = 3C + 2|h(e)|$ (which is independent of P).

6. In all of the following, each step multiplies numbers $\leqslant N$ (followed by a possible reduction modulo N), and so we are guaranteed that everything can be done on an 9-digit calculator, since N^2 has only 9 digits.

(a). First compute (modulo $N = 10481$): $2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 256$, $2^{16} \equiv 2650$, $2^{32} \equiv 230$ (where each of these was obtained be squaring the previous one, and reducing modulo N). Now, we write 46 in base 2: $46 = 2 + 4 + 8 + 32$ and so $2^{46} \equiv 2^2 2^4 2^8 2^{32} \equiv 4 \cdot 16 \cdot 256 \cdot 230 \equiv 64 \cdot 6475 \equiv 5641$ modulo N, so that $2^{46} - 1 \equiv 5640$ modulo N.

Now, compute $\gcd(5640, N)$ by Euclid's Algorithm: $10481 = 1 \cdot 5640 + 4841$; $5640 = 1 \cdot 4841 + 799$; $4841 = 6 \cdot 799 + 47$, $799 = 17 \cdot 47 + 0$. So, 47 is a factor of N. Compute $10481/47 = 223$, giving the factorisation $N = 10481 = 47 \cdot 223$.

(b). The line tangent to $\mathcal{E}$ at $P = (5, 11)$ has slope y' given by $2yy' = 3x^2 - 1$, with $x = 5, y = 11$; that is, the slope is $74/22 = 37/11$. This tangent line also goes through $(5, 11)$ and so has equation: $Y = (37/11)X - 64/11$. The x-coordinate of $2P$ is therefore $(37/11)^2 - (5 + 5) = 159/121$. [It will turn out not to be necessary to evaluate this mod N, although if this is done using EA, then it is 7364], and the y-coordinate is: $-((37/11)\cdot(159/121) - (64/11)) = 1861/1331$ [again, although unnecessary in this example, this can be computed by EA to be: 6679 mod N], so that $Q = 2P = (159/121, 1861/1331)$. We now wish to compute $3P = P + Q$, and so again the first step is to find the line joining P and Q. This has slope given by $(1861/1331 - 11)/(159/121 - 5) = 6930/2453$, and so we need to compute $6930/2453$ (modulo $N = 10481$), for which the first step is to find the inverse of 2453 (modulo $N = 10481$). Using Euclid's Algorithm: $10481 = 4 \cdot 2453 + 669$; $2453 = 3 \cdot 669 + 446$; $669 = 1 \cdot 446 + 223$; $446 = 2 \cdot 223 + 0$. So, we cannot find the inverse of 2453 (modulo $N = 10481$), and this step has given us a factor 223 of N. As before, compute $10481/223 = 47$, giving the factorisation $N = 10481 = 47 \cdot 223$.

(c). Since $N = 47 \cdot 223$, we have $\phi(N) = 46 \cdot 222 = 10212$. Compute the gcd of $d = 4085$ and $\phi(N)$, we see: $10212 = 2 \cdot 4085 + 2042$; $4085 = 2 \cdot 2042 + 1$, so that $\gcd(10212, 4085) = 1$. Reversing the steps: $1 = 4085 - 2 \cdot 2042 = 4085 - 2 \cdot (10212 - 2 \cdot 4085) = 5 \cdot 4085 - 2 \cdot 10212$. Hence, 5 is the inverse of 4085 modulo 10212. The decoding operation is therefore $X \mapsto X^5 \bmod N$. Computing $6012^5 = (6012^2)^2 \cdot 6012 \equiv 5656^2 \cdot 6012 \equiv 2324 \cdot 6012 \equiv 715$. (modulo $N = 10481$). Also: $3236^5 = (3236^2)^2 \cdot 3236 \equiv 1177^2 \cdot 3236 \equiv 1837 \cdot 3236 \equiv 1805$ (modulo $N = 10481$). The decoded message is therefore: 0715, 1805; that is: GORE.

7. First let us suppose that our elliptic curve $Y^2 = X^3 + AX + B$ has a point (x_0, y_0) of order 4. Performing the birational transformation $(X, Y) \mapsto (X - x_0, Y - y_0)$ [which corresponds to replacing the variables X, Y by $X + x_0, Y + y_0$] maps (x_0, y_0) to $(0, 0)$ on the birationally equivalent curve if the form: $Y^2 + 2y_0Y + y_0^2 =$ (monic cubic in X), and so is of the form: $Y^2 + 2y_0Y = X^3 + f_2X^2 + f_1X$ [after absorbing $-y_0^2$ into the cubic in X]. The fact that there is no constant term f_0 is a consequence of the fact that our new curve contains the point $(0, 0)$. We perform the further birational transformation $(X, Y) \mapsto (X, Y - f_1X/(2y_0))$ [which corresponds to replacing the variable Y by $Y + f_1X/(2y_0)$] which maps to the new birationally equivalent curve $Y^2 + bXY + aY = X^3 + cX^2$, where $b = f_1/y_0, a = 2y_0, c = f_2 - (f_1/(2y_0))^2$]. Note that, for any r, the birational transformation $(X, Y) \mapsto (r^2X, r^3Y)$ [which corresponds to replacing the variables X, Y by $X/r^2, Y/r^3$] maps to the birationally equivalent curve: $Y^2 + brXY + ar^3Y = X^3 + cr^2X^2$. Choosing $r = c/a$ forces the coefficients of Y and X^2 both to be c^3/a^2. So, let $r = c/a, v = c^3/a^2$ and $w = br = b^2/c$. Note that $y_0 \neq 0$, since (x_0, y_0) is not of order 2, and so $a = 2y_0 \neq 0$. Also, $c \neq 0$ (since if $c = 0$ then $Y = 0$ would meet the curve $Y^2 + bXY + aY = X^3 + cX^2$ 3 times at $(0, 0)$ making $(0, 0)$ of order 3, and so (x_0, y_0) of order 3 on the original curve, a contradiction). Hence, it was legitimate to have divided by a and c. Our curve is now of the form:

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

and $(0, 0)$ is our point of order 4. So far, we have only used the fact that our original curve contained a rational point (x_0, y_0) [not of order 2 or 3], which we have mapped to $(0, 0)$. We now use the fact that $(0, 0)$ is of order 4 on $\mathcal{E}$ to see what condition this gives on v, w. First perform the addition $(0, 0) + (0, 0)$. The line tangent to $\mathcal{E}$ at $(0, 0)$ is $Y = 0$. Substituting this into $\mathcal{E}$ gives: $X^3 + vX^2$, which has roots $0, 0, -v$, and so $(0, 0), (0, 0), (-v, 0)$ are the three points of intersection of $Y = 0$ and $\mathcal{E}$, so that $(0, 0) + (0, 0) + (-v, 0) = \mathbf{o}$, giving: $2(0, 0) = -(-v, 0)$. Now, since $\mathbf{o}$ is the point at infinity, the negative of $(-v, 0)$ is the other point on $\mathcal{E}$ with X-coordinate $-v$. Substituting $X = -v$ into $\mathcal{E}$ gives: $Y^2 - vwY + vY = 0$ and so: $Y(Y - v(w - 1))$, which has roots $0, v(w - 1)$. So, the negative of $(-v, w)$ is $(-v, v(w - 1))$, giving: $2(0, 0) = (-v, v(w - 1))$. Now, $(0, 0)$ is of order 4 iff $2(0, 0)$ is of order 2 iff $2(0, 0)$ equals its own inverse (since it is not the identity). But $(-v, v(w - 1))$ is the inverse of $(-v, 0)$ and so equals its own inverse iff $v(w - 1) = 0$. Now, we cannot have $v = 0$, since then $\mathcal{E}$ would be singular and so would not be an elliptic curve. So, $(0, 0)$ having order 4 on $\mathcal{E}$ is equivalent to $w = 1$. Substutuing $w = 1$ into $\mathcal{E}$ gives the required form.
