Elliptic Curves. Solutions to Sheet 0.

1.
(a). There is an identity element $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, but the matrix $\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$, for example, does not have an inverse, since there does not exist a matrix A such that $A\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)A = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$; so, not a group.
(b). This is group, with identity $\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$. Closure and associativity are easy to show. The inverse of $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ is $\left(\begin{smallmatrix}-a&-b\\-c&-d\end{smallmatrix}\right)$.

2.
(a). Not a homomorphism since, for example, $\phi(1+3) = \phi(4) = 17$, but $\phi(1) \times \phi(3) = 2 \times 10 = 20$.
(b). This is a homomorphism since, for all $v, w \in \mathbb{Q}$, we have $\phi(v+w) = \sqrt{2}(v+w) = \sqrt{2}\,v + \sqrt{2}\,w = \phi(v) + \phi(w)$. The map is injective since, for all $v, w \in \mathbb{Q}$, if $\phi(v) = \phi(w)$, then $\sqrt{2}\,v = \sqrt{2}\,w$, and so $v = w$. The map is not surjective since, for example, 2 is not in the image of ϕ (since there is no $v \in \mathbb{Q}$ such that $\sqrt{2}\,v = 2$). Hence the map is not bijective. Finally, $v \in \ker\phi \iff \sqrt{2}\,v = 0 \iff v = 0$, and so $\ker\phi = \{0\}$.
(c). This is a homomorphism since, for all $v, w \in \mathbb{Z}$, we have $\phi(v+w) = 2(v+w) = 2v + 2w = \phi(v) + \phi(w)$. The map is not injective since, for example, the elements 0 and 3 (which are distinct in $\mathbb{Z}$) both map to 0 in $\mathbb{Z}/3\mathbb{Z}$; therefore the map is also not bijective. The map is surjective since $0 \mapsto 0$, $1 \mapsto 2$ and $2 \mapsto 1$ so that all three elements of $\mathbb{Z}/3\mathbb{Z}$ are in the image of ϕ. Finally, $v \in \ker\phi \iff 2v = 0$ in $\mathbb{Z}/3\mathbb{Z} \iff 3|2v \iff 3|v$ in $\mathbb{Z}$. Hence the kernel of ϕ is $\{\ldots -3, 0, 3 \ldots\} = 3\mathbb{Z}$.

3.
(a). $3 = (1/27) \times 81$ and $81 = 9^2 \in (\mathbb{Q}^*)^2$, so $3 = 1/27$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. $-4 = 4 \times (-1)$ and $-1 \notin (\mathbb{Q}^*)^2$, so $-4 \neq 4$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Finally, $3 = (5/6) \times (18/5)$, and $18/5 \notin (\mathbb{Q}^*)^2$, so $3 \neq 5/6$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.
(b). In $\mathbb{Q}^*/(\mathbb{Q}^*)^2$: $-2/27 = (-2/27) \times 9^2 = -6$, $16 = 16 \times (1/4)^2 = 1$, $12 = 12 \times (1/2)^2 = 3$, and $1/3 = (1/3) \times 3^2 = 3$.
(c). In $\mathbb{Q}^*/(\mathbb{Q}^*)^2$: $6 \times 10 = 60 = 60 \times (1/2)^2 = 15$, $10/21 = (10/21) \times 21^2 = 210$, $15^{101} = 15 \times (15^{50})^2 = 15$, and $3^{-1} = 3^{-1} \times 3^2 = 3$.
(d). Whenever p_1, p_2 are distinct primes, we have that $p_1 = p_2 \times (p_1/p_2)$, where $p_1/p_2 \notin (\mathbb{Q}^*)^2$. Hence, $p_1 \neq p_2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. This means that the primes are all distinct in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, and so $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is infinite (note that this does not describe all elements in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, but the above argument is sufficient to show that the size of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is infinite). In $\mathbb{R}^*/(\mathbb{R}^*)^2$, every $r > 0$ is equal to 1 (since such an r is a member of $(\mathbb{R}^*)^2$), and similarly any $r < 0$ is equal to -1. But $1 \neq -1$ in $\mathbb{R}^*/(\mathbb{R}^*)^2$, since $-1 \notin (\mathbb{R}^*)^2$. Hence, $\mathbb{R}^*/(\mathbb{R}^*)^2$ has exactly 2 distinct elements: 1 and -1. Finally, everything in $\mathbb{C}^*$ is in $(\mathbb{C}^*)^2$ (since every complex number is a square of some complex number), and so $\mathbb{C}^*/(\mathbb{C}^*)^2$ has exactly 1 element.

4.
(a). A singular point (x, y) must satisfy the three equations: $f(x,y) = x^4 + y^3 - 3x^2y = 0$, $g(x,y) = (\partial f/\partial X)(x,y) = 4x^3 - 6xy = 0$ and $h(x,y) = (\partial f/\partial Y)(x,y) = 3y^2 - 3x^2 = 0$.

From $h(x,y)=0$, we get $(y+x)(y-x)=0$ and so $y=x$ or $y=-x$, which we now consider as separate cases.

Case 1. $y=x$. In this case, $f(x,y)=0$ becomes $x^3(x-2)=0$ (with solutions $x=0,2$) and $g(x,y)=0$ becomes $2x^2(2x-3)=0$ (with solutions $x=0,3/2$), and so the only simultaneous solution for x is $x=0$. Substituting $x=0$ into $f(x,y)=0$ gives $y^3=0$ and so $y=0$. Hence, $(0,0)$ is the only possibility within case 1.

Case 2. $y=-x$. In this case, $f(x,y)=0$ becomes $x^3(x+2)=0$ (with solutions $x=0,-2$) and $g(x,y)=0$ becomes $2x^2(2x+3)=0$ (with solutions $x=0,-3/2$), and so the only simultaneous solution for x is $x=0$. As before, substituting $x=0$ into $f(x,y)=0$ gives $y^3=0$ and so $y=0$.

In either case, $(0,0)$ is the only possible point which could be singular.

[*Alternative Method (harder than the above, but guaranteed to work for any curve): Let* $\alpha(x)=Res(f,g)$ *with respect to* y, *and* $\beta(x)=Res(g,h)$ *with respect to* y, *and finally use resultants with respect to* x *to show that* $x=0$ *is the only common root of* $\alpha(x)$ *and* $\beta(x)$].

Finally, note that $(0,0)$ does indeed satisfy $f(x,y)=g(x,y)=h(x,y)=0$ and so is a singular point. Conclusion: $(0,0)$ is the only singular point.

$f(X+0,Y+0)=R_3(X,Y)+R_4(X,Y)$, where $R_3(X,Y)=Y^3-3X^2Y=Y(Y-\sqrt{3}\,X)(Y+\sqrt{3}\,X)$. So the three tangents at $(0,0)$ are $Y=0$, $Y=\sqrt{3}\,X$ and $Y=-\sqrt{3}\,X$.

(b). A singular point (x,y) must satisfy the three equations: $f(x,y)=y^2-x(x^2-1)^2=0$, $g(x,y)=(\partial f/\partial X)(x,y)=-(x^2-1)(5x^2-1)=0$ and $h(x,y)=(\partial f/\partial Y)(x,y)=2y=0$. From $h(x,y)=0$ we have $y=0$ and, on substituting this into $f(x,y)=0$ we have $-x(x^2-1)^2=0$, and so the only possible values for x are $x=0,1-1$. But from $g(x,y)=0$ we see that x must also satisfy $x=1-1,\sqrt{1/5},-\sqrt{1/5}$. The only common solutions are: $x=1,-1$. Substituting $x=1$ or $x=-1$ into $f(x,y)=0$ gives that $y=0$, and so the only possible points which could be singular are: $(1,0)$ and $(-1,0)$. Finally, note that $x=1,y=0$ does indeed satisfy $f(x,y)=g(x,y)=h(x,y)=0$ as does $x=-1,y=0$. Conclusion: $(1,0)$ and $(-1,0)$ are the only singular points.

At $(0,0)$, we have $f(X+0,Y+0)=-X+$ terms of degree at least 2, and so there is a unique tangent at the point $(0,0)$, namely the line $X=0$. At $(1,0)$, we note that $f(X+1,Y+0)=(Y^2-4X^2)+$ terms of degree at least 3. Here, $(Y^2-4X^2)=L_1(X,Y)L_2(X,Y)$, where $L_1(X,Y)=Y-2X$ amd $L_2(X,Y)=Y+2X$. Finally, the two tangents to $\mathcal{C}$ at $(1,0)$ are therefore $L_1(X-1,Y-0)=Y-2(X-1)=0$ and $L_2(X-1,Y-0)=Y+2(X-1)=0$.

5. If (x,y) is singular on $Y^2=X^3+AX+B$, then (x,y) satisfies the three equations: $f(x,y)=y^2-(x^3+Ax+B)=0$, $g(x,y)=(\partial f/\partial X)(x,y)=-(3x^2+A)=0$ and $h(x,y)=(\partial f/\partial Y)(x,y)=2y=0$. From $h(x,y)=0$, we have $y=0$; substituting $y=0$ into $f(x,y)=0$, we deduce $x^3+Ax+B=0$. From $g(x,y)=0$, we see that x also satisfies $3x^2+A=0$; that is, x is a common root of $p_1(x)=x^3+Ax+B$ and its derivative $p_2(x)=3x^2+A$; that is, x satisfies: $p_1(x)=x^3+Ax+B=0$ and $p_2(x)=3x^2+A=0$. Then x would satisfy: $p_3(x)=3p_1(x)-xp_2(x)=2Ax+3B=0$, and so: $p_4(x)=2Ap_2(x)-3xp_3(x)=-9Bx+2A^2$, and so: $p_5(x)=9Bp_3(x)+2Ap_4(x)=4A^3+27B^2=0$. But we are told that $4A^3+27B^2\neq 0$ and so no such x can exist; therefore there are no singular points. [The above is from first principles. An easier alternative method is to compute: Disc(x^3+Ax+B) is $4A^3+27B^2$; if this is nonzero, no such x can exist, and so no singular point can exist.]

6.

(a). Let $f(X,Y) = Y^2 - X^5$. Imagine that $f(X,Y) = g(X,Y)h(X,Y)$, where g, h are non-constant polynomials defined over $\mathbb{C}$. Since $f(X,Y)$ has degree 2 in Y, there are three possibilities: g has degree 0 in Y and h has degree 2 in Y; g has degree 1 in Y and h has degree 1 in Y; g has degree 2 in Y and h has degree 0 in Y.

Case 1. g has degree 0 in Y and h has degree 2 in Y. Then we can write: $g(X,Y) = \phi_0(X)$, where $\phi_0(X)$ is a polynomial in X, and $h(X,Y) = \theta_2(X)Y^2 + \theta_1(X)Y + \theta_0(X)$, where each $\theta_i(X)$ is a polynomial in X. Then, equating the coefficients of Y^2 in the equation $f(X,Y) = g(X,Y)h(X,Y)$ gives that $1 = \phi_0(X)\theta_2(X)$, and so both $\phi_0(X)$ and $\theta_2(X)$ must be constants. But then $g(X,Y)$ would be constant, contradicting out initial assumption that g, h are non-constant.

Case 2. g has degree 1 in Y and h has degree 1 in Y. Then we can write: $g(X,Y) = \phi_1(X)Y + \phi_0(X)$, where each $\phi_i(X)$ is a polynomial in X, and $h(X,Y) = \theta_1(X)Y + \theta_0(X)$, where each $\theta_i(X)$ is a polynomial in X. Then, equating the coefficients of Y^2 in the equation $f(X,Y) = g(X,Y)h(X,Y)$ gives that $1 = \phi_1(X)\theta_1(X)$, and so both $\phi_1(X)$ and $\theta_1(X)$ must be constants (and multiplicative inverses); say $\phi_1(X) = r$ and $\theta_1(X) = 1/r$, where $r \in \mathbb{C}$ is a nonzero constant. Then the equation $f(X,Y) = g(X,Y)h(X,Y)$ becomes: $Y^2 - X^5 = Y^2 + \big(r\theta_0(X) + (1/r)\phi_0(X)\big)Y + \theta_0(X)\phi_0(X)$. Equating coefficients of Y gives that $r\theta_0(X) + (1/r)\phi_0(X) = 0$ and so $\phi_0(X) = -r^2\theta_0(X)$. Hence the equation becomes: $Y^2 - X^5 = Y^2 - r^2\big(\theta_0(X)\big)^2$. But, $r^2\big(\theta_0(X)\big)^2$ is a polynomial of even degree in X, whereas X^5 is of odd degree, a contradiction.

Case 3. g has degree 2 in Y and h has degree 0 in Y. This gives the same contradiction as in Case 1, but with g, h interchanged.

In summary, our initial assumption, that $f(X,Y) = g(X,Y)h(X,Y)$, where g, h are non-constant polynomials defined over $\mathbb{C}$, lead to a contradiction in all cases. Hence, it is not possible to write $f(X,Y)$ as such a product, and so $f(X,Y)$ is irreducible over $\mathbb{C}$. Of course, this means that $f(X,Y)$ is irreducible over $\mathbb{Q}$, also.

(b). Let $f(X,Y) = Y^3 - X^3 = (X-Y)(X^2+XY+Y^2) = (X-Y)(X-\omega Y)(X-\omega^2 Y)$, where $\omega = e^{2\pi/3} = (1+\sqrt{-3})/2$. So, the irreducible components over $\mathbb{C}$ are: $X-Y$, $X-\omega Y$ and $X+\omega Y$, whereas the irreducible components over $\mathbb{Q}$ are $X-Y$ and X^2+XY+Y^2 (since t^2+t+1 cannot be factorised over $\mathbb{Q}$).

(c). This is irreducible over $\mathbb{C}$ (and so irreducible over $\mathbb{Q}$) by the same argument as in (a). Note that this argument applies to any curve of the form $Y^2 - Q(X) = 0$, where $Q(X)$ is not the square of a polynomial.

7.

(a). Trying simple substitutions of the form where X, Y are replaced by $aX + bY$ and $cX + dY$ in $2X^2 - Y^2 = 1$ gives: $(2a^2 - c^2)X^2 + (2b^2 - d^2)Y^2 + (4ab - 2cd)XY = 1$; we can now notice that the coefficients on the LHS can be made to be $1, 1, -6$ by taking (for example) $a = 1, b = -1, c = 1, d = 1$. Be careful to note that $(X,Y) \mapsto (X-Y, X+Y)$ is then a birational transformation from $\mathcal{D} : X^2 + Y^2 - 6XY = 1$ to $\mathcal{C} : 2X^2 - Y^2 = 1$ [since $X^2 + Y^2 - 6XY = 1$ can be rewritten as $2(X-Y)^2 - (X+Y)^2 = 1$, and so a point (X,Y) on $\mathcal{D}$ maps to a point $(X-Y, X+Y)$ in $\mathcal{C}$]. The inverse map from $\mathcal{C}$ to $\mathcal{D}$ is $(X,Y) \mapsto \big((X+Y)/2, (Y-X)/2\big)$.

(b). Let $\mathcal{C} : Y^2 = (X+2)^6(X^3+1)$ and $\mathcal{D} : Y^2 = X^3 + 1$. Then $\mathcal{C}$ can be rewritten

as $\big(Y/(X+2)^3\big)^2 = X^3+1$ and so there is a birational map $(X,Y) \mapsto \big(X, Y/(X+2)^3\big)$ from $\mathcal{C}$ to $\mathcal{D}$. This is a birational transformation, since there is the inverse map $(X,Y) \mapsto \big(X, Y(X+2)^3\big)$.

(c). The map $(X,Y) \mapsto (\sqrt{2}\,X, Y)$ give a birational transformation over $\mathbb{C}$ from $Y^2 = 2X^2$ to $Y^2 = X^2$, with inverse map $(X,Y) \mapsto (X/\sqrt{2}, Y)$. There is no birational transformation over $\mathbb{Q}$, since $Y^2 = X^2$ has infinitely many $\mathbb{Q}$-rational points of the form $(a/b, \pm a/b)$, where $a, b \in \mathbb{Z}$, whereas $Y^2 = 2X^2$ has $(0,0)$ as its only $\mathbb{Q}$-rational point (since $\sqrt{2}$ is irrational).

8.

(a). The discriminant of X^4-2 is the same as $\mathrm{Res}(X^4-2, 4X^3)$, which is the determinant of the matrix:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & -2 & 0 \\ 1 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The determinant is $\mathrm{Disc}(X^4-2) = 2^{11}$.

(b). The resultant of $X^3 - a$ and $X^2 - b$ is the determinant of the matrix:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & -a \\ 1 & 0 & 0 & -a & 0 \\ 0 & 0 & 1 & 0 & -b \\ 0 & 1 & 0 & -b & 0 \\ 1 & 0 & -b & 0 & 0 \end{pmatrix}.$$

The determinant is $\mathrm{Res}(X^3 - a, X^2 - b) = a^2 - b^3$.

9. First note that, if there is an intersection point of $X^3 + Y^3 = Z^3$ and $X^2 + Y^2 = Z^2$ with $Z = 0$, then $X^3 = -Y^3$ and $X^2 = -Y^2$; squaring both sides of the first equation, and cubing both sides of the second equation one deduces: $X^6 = Y^6$ and $X^6 = -Y^6$; adding these gives $2X^6 = 0$, and so $X = 0$, and so $Y = 0$. But the point $(0,0,0)$ is not allowed in projective coordinates, so we conclude that there are no points of intersection with $Z = 0$. We can therefore consider only points with $Z \neq 0$.

Given that $Z \neq 0$, we can therefore use the affine models $x^3 + y^3 = 1$ and $x^2 + y^2 = 1$. [Each point (x,y) of intersection on $x^3+y^3 = 1$ and $x^2+y^2 = 1$ will give the point $(x,y,1)$ of intersection on $X^3 + Y^3 = Z^3$ and $X^2 + Y^2 = Z^2$; conversely, each point (X,Y,Z) of intersection on $X^3 + Y^3 = Z^3$ and $X^2 + Y^2 = Z^2$ with $Z \neq 0$ (which we have established must be the case) will give the point $(X/Z, Y/Z)$ of intersection on $x^3 + y^3 = 1$ and $x^2 + y^2 = 1$].

Let (x,y) be a point of intersection on $x^3+y^3 = 1$ and $x^2+y^2 = 1$. Then $x^6 = (1-y^3)^2$ and $x^6 = (1-y^2)^3$, and so y must satisfy: $(1-y^3)^2 = (1-y^2)^3$, which can be rewritten as:

$$y^2(y-1)^2(2y^2+4y+3) = 0 \qquad (*)$$

[Note that $(*)$ can also be derived as $\mathrm{Res}(x^2+y^2-1, x^3+y^3-1)$ with respect to the variable x].

The solutions in y are: $0, 1, -1+\sqrt{-1/2}, -1-\sqrt{-1/2}$. When $y=0$, then x simultaneously satisfies $x^3 = 1-0^3$ and $x^2 = 1-0^2$ so $x=1$, giving rise to the point of intersection: $P_1 = (1,0)$. When $y=1$, then x simultaneously satisfies $x^3 = 1-1^3$ and $x^2 = 1-1^2$ so $x=0$, giving rise to the point of intersection: $P_2 = (0,1)$. When $y = -1+\sqrt{-1/2}$, then x simultaneously satisfies $x^3 = 1-(-1+\sqrt{-1/2})^3$ and $x^2 = 1-(-1+\sqrt{-1/2})^2$, and so $x = x^3/x^2 = \big(1-(-1+\sqrt{-1/2})^3\big)/\big(1-(-1+\sqrt{-1/2})^2\big) = -1-\sqrt{-1/2}$; this gives rise to the point of intersection: $P_3 = (-1-\sqrt{-1/2}, -1+\sqrt{-1/2})$. Similarly, the final possibility for y, namely $y = -1-\sqrt{-1/2}$ gives rise to the point $P_4 = (-1+\sqrt{-1/2}, -1-\sqrt{-1/2})$. We have shown that P_1, P_2, P_3, P_4 are the only possible points of intersection, and substitution into $x^3+y^3=1$ and $x^2+y^2=1$ shows that they are all indeed points of intersection, so we have a complete list. Bézout's Theorem tells us that there should be 6 points of intersection, so some of the multiplicities must be greater than 1. At $P_1 = (1,0)$, we see that $\mathrm{d}x/\mathrm{d}y = 0$ on both curves, but that $\mathrm{d}^2x/\mathrm{d}y^2$ differ (since $\mathrm{d}^2x/\mathrm{d}y^2 = 0$ on $x^3+y^3=1$ but is nonzero on $x^2+y^2=1$). We conclude that $P_1 = (1,0)$ is a point of intersection of multiplicity exactly 2. Similarly (but using $\mathrm{d}y/\mathrm{d}x$ and $\mathrm{d}^2y/\mathrm{d}x^2$), we see (by symmetry) that $P_2 = (0,1)$ is a point of intersection of multiplicity exactly 2. We can now apply Bézout's Theorem to see that P_3, P_4 must each be points of intersection of multiplicity only 1 (since the total of all multiplicities must be 6); or one can check directly that the value of $\mathrm{d}y/\mathrm{d}x$ on $x^3+y^3=1$ at P_3 is distinct from the value of $\mathrm{d}y/\mathrm{d}x$ on $x^2+y^2=1$ at P_3 (and similarly for P_4).

On the original projective curves, $X^3+Y^3=Z^3$ and $X^2+Y^2=Z^2$, the six points of intersection are therefore:

$(1,0,1)$, with multiplicity 2.
$(0,1,1)$, with multiplicity 2.
$(-1-\sqrt{-1/2}, -1+\sqrt{-1/2}, 1)$, with multiplicity 1.
$(-1+\sqrt{-1/2}, -1-\sqrt{-1/2}, 1)$, with multiplicity 1.

10. (a). From the rule that 2 is a quadratic residue residue mod p ($p \neq 2$) iff $p \equiv \pm 1$ modulo 8, we have that 2 is a quadratic residue modulo 1009 (since 1009 is prime and $1009 \equiv 1$ modulo 8).

By quadratic reciprocity, since 3 and 1009 are both odd primes, and since at least one of them is congruent to 1 modulo 4, we have $(\frac{3}{1009}) = (\frac{1009}{3}) = (\frac{1}{3}) = 1$, since $1 \equiv 1^2$ mod 5. Hence, 3 is a quadratic residue modulo 1009.

Again applying quadratic reciprocity, $(\frac{5}{1009}) = (\frac{1009}{5}) = (\frac{4}{5}) = 1$, since $4 \equiv 2^2$ mod 5. Hence, 5 is a quadratic residue modulo 1009.

$(\frac{10}{1009}) = (\frac{2}{1009})(\frac{5}{1009}) = 1 \cdot 1 = 1$. Hence, 10 is a quadratic residue modulo 1009.
$(\frac{15}{1009}) = (\frac{3}{1009})(\frac{5}{1009}) = 1 \cdot 1 = 1$. Hence, 15 is a quadratic residue modulo 1009.

(b). When $p \equiv 1$ mod 4, we have by quadratic reciprocity that $(\frac{3}{p}) = (\frac{p}{3})$, which is 1 when $p \equiv 1$ mod 3, and is -1 when $p \equiv 2$ mod 3. When $p \equiv 3$ mod 4, we have $(\frac{3}{p}) = -(\frac{p}{3})$, which is -1 when $p \equiv 1$ mod 3, and is 1 when $p \equiv 2$ mod 3. In summary:
$(\frac{3}{p}) = 1$ when p satisfies both $p \equiv 1$ mod 4 and $p \equiv 1$ mod 3, that is, when $p \equiv 1$ mod 12.
$(\frac{3}{p}) = -1$ when p satisfies both $p \equiv 1$ mod 4 and $p \equiv 2$ mod 3, that is, when $p \equiv 5$ mod 12.

$(\frac{3}{p}) = -1$ when p satisfies both $p \equiv 3 \bmod 4$ and $p \equiv 1 \bmod 3$, that is, when $p \equiv 7 \bmod 12$.
$(\frac{3}{p}) = 1$ when p satisfies both $p \equiv 3 \bmod 4$ and $p \equiv 2 \bmod 3$, that is, when $p \equiv 11 \bmod 12$.

Hence, 3 is a quadratic residue mod p when $p \equiv 1$ or $11 \bmod 12$, and 3 is not a quadratic residue mod p when $p \equiv 5$ or $7 \bmod 12$. This describes what happens for all primes apart from $p = 2, 3$ (since any prime $p \neq 2, 3$ must be congruent to one of $1, 5, 7, 11 \bmod 12$). Finally, when $p = 2$ or 3 we have that 3 is a quadratic residue mod p.

It is always true by quadratic reciprocity that, for any prime $p \neq 2$, $(\frac{5}{p}) = (\frac{p}{5})$, since $5 \equiv 1 \bmod 4$; that is 5 is a quadratic residue mod p iff p is a quadratic residue mod 5. But then $(\frac{p}{5}) = 1$ when $p \equiv 1, 4 \bmod 5$ (since $1 \equiv 1^2$ and $4 = 2^2 \bmod 5$) and $(\frac{p}{5}) = -1$ when $p \equiv 2, 3 \bmod 5$ (since none of $0^2, 1^2, 2^2, 3^2, 4^2$ are congruent to either of 2 or 3 mod 5). In summary, 5 is a quadratic residue mod p when $p \equiv 1, 4 \bmod 5$, and 5 is not a quadratic residue mod p when $p \equiv 2, 3 \bmod 5$. This describes what happens for all primes apart from $p = 2, 5$ (since any prime $p \neq 5$ must be congruent to one of $1, 2, 3, 4 \bmod 5$). Finally, when $p = 2$ or 5 we have that 5 is a quadratic residue mod p (since it is congruent mod p to 1^2 and 0^2, respectively).

We know $(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p})$. For $p \neq 2, 5$ we can use the standard rules that $(\frac{2}{p}) = 1$ when $p \equiv 1, 7 \bmod 8$, that $(\frac{2}{p}) = -1$ when $p \equiv 3, 5 \bmod 8$; also, $(\frac{5}{p}) = 1$ when $p \equiv 1, 4 \bmod 5$, and $(\frac{5}{p}) = -1$ when $p \equiv 2, 3 \bmod 5$ (done above). Note that $(\frac{10}{p}) = 1$ when $(\frac{2}{p}) = (\frac{5}{p}) = 1$ or $(\frac{2}{p}) = (\frac{5}{p}) = -1$ and $(\frac{10}{p}) = -1$ when $(\frac{2}{p})$ and $(\frac{5}{p})$ have opposite sign.

In a similar manner to the first example, we therefore have that (for any $p \neq 2, 5$), $(\frac{10}{p}) = 1$ when $p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \bmod 40$, and $(\frac{10}{p}) = -1$ when $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \bmod 40$. This describes what happens for all primes apart from $p = 2, 5$ (since any prime $p \neq 5$ must be congruent to one of $1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39 \bmod 40$). Finally, when $p = 2$ or 5 we have that 10 is a quadratic residue mod p (since it is congruent mod p to 0^2).

11. Suppose there were integers a, b, c, not all 0 such that $2a^2 + 5b^2 = c^2$. Without loss of generality, we can divide through by the square of any common factor of a, b, c, and assume that $\gcd(a, b, c) = 1$. Reducing the equation modulo 5 gives: $2a^2 \equiv c^2 \pmod 5$.

Imagine that 5 does not divide a; then there would exist $\lambda \in \mathbb{Z}$ such that $\lambda a \equiv 1 \pmod 5$; multiplying both sides by λ^2 would then give $2 \equiv (\lambda c)^2 \pmod 5$; but this is a contradiction, since 2 is not a quadratic residue mod 5 [to see this, check that: $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 4$, $4^2 \equiv 1 \pmod 5$]. This contradiction shows that our assumption '5 does not divide a' must be false, and so we conclude that: $5|a$.

Since $5|a$ and $2a^2 + 5b^2 = c^2$, we can deduce that $5|c^2$ and so $5|c$. Therefore $5^2|a^2$ and $5^2|c^2$ and so $5|5b^2$; but only 5^1 divides into 5, and so $5|b^2$, giving $5|b$. We now have that 5 divides all of a, b, c, contradicting the fact that $\gcd(a, b, c) = 1$. This proves that no such a, b, c exist.

12. Define $S(n) = \{x \in \mathbb{N} : 1 \leqslant x \leqslant n \text{ and } \gcd(x, n) = 1\}$, so that $\phi(n) = \#S(n)$.

For any p, to get $S(p^r)$ we remove all multiples of p from the set $\{1, \ldots, p^r\}$, and so $\phi(p^r) = \#S(p^r)$ is $p^r - \frac{1}{p}p^r$; that is: $p^r - p^{r-1}$.

For two distinct primes p_1, p_2, note that $S(p_1p_2)$ can be obtained by removing from the set $\{1, \ldots p_1p_2\}$ all multiples of p_1 (of which there are $\frac{1}{p_1}p_1p_2 = p_2$) and all multiples of

p_2 (of which there are $\frac{1}{p_2}p_1p_2 = p_1$). But note that the element p_1p_2, which is a multiple of both p_1 and p_2, should only be counted once. Hence the total number of elements removed is: $p_2 + p_1 - 1$, so $\phi(p_1p_2) = p_1p_2 - (p_2 + p_1 - 1) = (p_1 - 1)(p_2 - 1)$.

Applying Euler's Theorem, that $a^{\phi(n)} \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$, gives as follows.

$2^{12} \equiv 2^{\phi(13)} \equiv 1 \pmod{13}$, since $\gcd(2, 13) = 1$. $3^{12} \equiv 3^{\phi(13)} \equiv 1 \pmod{13}$, since $\gcd(3, 13) = 1$. Hence, $3^{24} \equiv (3^{12})^2 \equiv 1^2 \equiv 1 \pmod{13}$. Similarly, $3^{12000} \equiv (3^{12})^{1000} \equiv 1^{1000} \equiv 1 \pmod{13}$, and $3^{12002} \equiv (3^{12})^{1000} \cdot 3^2 \equiv 1^{1000} \cdot 9 \equiv 9 \pmod{13}$.

Since $(4, 35) = 1$ and $\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24$, we have $4^{24} \equiv 1 \pmod{35}$. So, $4^{48} \equiv (4^{24})^2 \equiv 1^2 \equiv 1 \pmod{35}$, also. Similarly, $4^{48000001} \equiv 4^{48000000} \cdot 4 \equiv (4^{24})^{2000000} \cdot 4 \equiv 1^{2000000} \cdot 4 \equiv 4 \pmod{35}$.

We cannot do the same thing for 7^r, since $(7, 35) \neq 1$. Note that $7^5 \equiv 7 \pmod{35}$ [this is due to the fact that $7^5 \equiv 7$ modulo each of 5 and 7], and so $7^{24} \equiv (7^5)^4 \cdot 7^4 \equiv 7^4 \cdot 7^4 \equiv 7^5 \cdot 7^3 \equiv 7 \cdot 7^3 \equiv 21 \pmod{35}$. Similarly, $7^{48} \equiv (7^5)^9 \cdot 7^3 \equiv 7^9 \cdot 7^3 \equiv (7^5)^2 \cdot 7^2 \equiv 7^2 \cdot 7^2 \equiv 21 \pmod{35}$. Similarly, $7^{48000000} \equiv 21 \pmod{35}$, so that $7^{48000001} \equiv 21 \cdot 7 \equiv 7 \pmod{35}$.

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 same as that of C_2 ("cyclic 2" group; i.e. the integers modulo 2 under addition), wi replaced by $\mathbf{o}, (0,0)$, respectively.
(b). The only points on $Y^2 = X^3 + 1$ over $\mathbb{F}_5$ are: $\mathbf{o}, (0,1), (0,4), (4,0), (2,2),$ The point $(2,2)$ has order 6, and the group table is the same as that of C_6 ("cyc group; i.e. the integers modulo 6 under addition), with $0, 1, 2, 3, 4, 5$ replac $\mathbf{o}, (2,2), (0,4), (4,0), (0,1), (2,3)$, respectively. Note that it's also correct to say th 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: $(3 \cdot 2^2 + 4)/(2 \cdot 4$ The line tangent to the curve at $(2,4)$ is: $Y = 2X$. The x-coordinate of the third of intersection is therefore: $2^2 - 2 - 2 = 0$, with y-coordinate $y = 2 \cdot 0 = 0$. I $(2,4) + (2,4) + (0,0) = \mathbf{o}$, and so $(2,4) + (2,4) = (0,-0) = (0,0)$. Now, not we always have $-(x,y) = (x,-y)$ and so $-(0,0) = (0,0)$, giving: $2(0,0) = \mathbf{o}$. I $4(2,4) = 2(0,0) = \mathbf{o}$. Also, check that $3(2,4) = 4(2,4) - (2,4) = -(2,4) = (2$ Summarising: the first 4 multiples of $(2,4)$ are: $1(2,4) = (2,4)$, $2(2,4) = (0,0)$, $3(2$ $(2,-4)$, $4(2,4) = \mathbf{o}$, 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 $(X,Y) \mapsto (X/f_m, Y/f_m^{(m}$ [with inverse transformation: $(X,Y) \mapsto (Xf_m, Yf_m^{(m+1)/2})$] maps the given cur $f_m^{(m+1)}Y^2 = f_m^{(m+1)}X^m + \ldots + f_0$, which is the same as: $Y^2 = X^m + c_{m-1}X^{m-1} + \ldots$ where $c_i = f_i/f_m^{m+1-i} \in \mathbb{Q}$ [N.B. our birational transformation is legitimate, since $(m$ is an integer]. So, our new right hand side is monic and is still defined over $\mathbb{Q}$. 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 l least common multiple of $d_0, \ldots d_{(m-1)}$; that is to say, d is the smallest integer ible by all of the denominators of the coefficients c_i. Now, the birational transf tion $(X,Y) \mapsto (Xd^2, Yd^m)$ [with inverse transformation: $(X,Y) \mapsto (X/d^2, Y/d^m)$] 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 sa $Y^2 = X^m + g_{m-1}X^{m-1} + \ldots + g_0$, where $g_i = c_i d^{2(m-i)}$. But now, each $d_i | d$ and s $c_i d \in \mathbb{Z}$, 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 transfor $(X,Y) \mapsto (X, Y/w)$ [with inverse transformation: $(X,Y) \mapsto (X, Yw)$] maps the given to: $f_m Y^2 = f_m X^m + \ldots + f_0$, which is the same as: $Y^2 = X^m + c_{m-1}X^{m-1} + \ldots$ where $c_i = f_i/f_m \in \mathbb{Q}$. We are again in the situation where our right hand side is and is still defined over $\mathbb{Q}$. So now apply the same second birational transformation Case 1.
(b). The birational transformation $(X,Y) \mapsto (5X, 5^2Y)$ [with inverse $(X,Y$ $((1/5)X, (1/5^2)Y)$] maps the given curve to the curve: $Y^2 = X^3 + 75X^2 + 625$. birational transformation $(X,Y) \mapsto (X+25, Y)$ [with inverse $(X,Y) \mapsto (X-25, Y)$] 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 $\lambda, \mu \in \mathbb{Z}$ 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 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 m also a bijection on $\mathbb{F}_p$. Now, rearrange the equation of the curve as: $X^3 = Y^2 - A$. V that, for each $Y = 0, \ldots, p-1$ in $\mathbb{F}_p$, there is precisely one $X \in \mathbb{F}_p$ such that $X^3 = Y$ giving rise to a total of precisely p affine points, which becomes $p+1$ points wh 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 s mod p]. First note that $X = 0$ gives rise to precisely one point $(0, 0)$. Now, pair each X with its negative $-X$ mod p. If $X(X^2 + B) = 0$ then the pair $X, -X$ gives rise to pre two points: $(X, 0), (-X, 0)$. If $X(X^2 + B) \neq 0$ then one of $X(X^2 + B)$ and $-X(X^2$ will be a nonzero quadratic residue mod p and the other will be a quadratic nonr mod p [using the fact that -1 is a quadratic nonresidue mod p and the standard pro 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 cont no points; which one is a residue will contribute two points: $(X, Y), (X, -Y)$. In all each pair $X, -X$ will contribute two points. This gives rise to a total of precisely p points, which becomes $p+1$ points when we include the point at infinity.

5.

(a). We first solve for g_1, g_0 and h_1, h_0 such that $Q(X) = (X^2 + g_1X + g_0)^2 + (h$ h_0). Equating coefficients of X^3 forces $g_1 = f_3/2$. Successiviely equating coefficie X^2, X^1, X^0 now solves for g_0, h_1, h_0, giving:

$$g_1 = f_3/2,\ g_0 = (4f_2 - f_3^2)/8,\ h_1 = f_1 - f_3(4f_2 - f_3^2)/8,\ h_0 = f_0 - (4f_2 - f_3^2)^2/$$

Now define $G(X) = X^2 + g_1X + g_0$ and $H(X) = h_1X + h_0$, where g_1, g_0, h_1, h as in the above equation, and we see that indeed $Q(X) = G(X)^2 + H(X)$. Our can be written as: $(Y + G(X))(Y - G(X)) = H(X)$. The birational transform $(X, Y) \mapsto (Y+G(X), X(Y+G(X))$ [that is: $(X, Y) \mapsto (T, S)$, given in the hint] has i $(X, Y) \mapsto (Y/X, X - G(Y/X))$ and transforms the given curve to: $X(X - 2G(Y/$ $H(Y/X)$. After multiplying both sides by X and expanding, this can be rewritten a

$$2Y^2 + 2g_1XY + h_1Y = X^3 - 2g_0X^2 - h_0X.$$

[You could write this as: $(Y + G(X))(Y - G(X)) = H(X) \leftrightarrow T(T - 2G(S/T)) = H$ [where $T = Y + G(X),\ S = X(Y + G(X)),\ X = S/T,\ Y = T - G(S/T)$], wh turn is: $2S^2 + 2g_1TS + h_1S = T^3 - 2g_0T^2 - h_0T$, if you prefer]. One can now proceed to remove the term $2g_1XY$ by $(X, Y) \mapsto (X, Y + g_1X/2)$ and the term h

$(X,Y) \mapsto (X, Y+h_1/4)$, giving the curve: $Y^2 = (1/2)X^3 + \ldots$. Finally, remove the $X^$ and then make the right hand side monic & defined over $\mathbb{Z}$, exactly as in Question

(b). First apply to $\mathcal{C}_1$ the birational transformation $(X,Y) \mapsto (1/X, Y/X^2)$ [self-in which maps $\mathcal{C}_1$ to: $Y^2 = 9X^4 + 2$. The map $(X,Y) \mapsto (X, Y/3)$ [with inverse $(X,$ $(X, 3Y)$] maps this to $Y^2 = X^4 + 2/9$. In the notation of part (a), we can take $G(X)$ and $H(X) = 2/9$, and so $g_1 = g_0 = h_1 = 0$ and $h_0 = 2/9$. The curve is the birationally equivalent to: $2Y^2 = X^3 - (2/9)X$; that is, $Y^2 = (1/2)X^3 - (1/9)X$. We apply $(X,Y) \mapsto (18X, 108Y)$ [with inverse $(X,Y) \mapsto (X/18, Y/108)$], which map curve to: $(Y/108)^2 = (1/2)(X/18)^3 - (1/9)(X/18)$, which is the same as: $Y^2 = X^3 -$ as required.

For $\mathcal{C}_2$, the important thing to recognise is that it has the $\mathbb{Q}$-rational point which allows us to make the constant term a square after a linear change in X. Na $(X,Y) \mapsto (X-1, Y)$ [with inverse $(X,Y) \mapsto (X+1, Y)$] maps $\mathcal{C}_2$ to the curve: $2(X+1)^4 + 7$; that is, $Y^2 = 2X^4 + 8X^3 + 12X^2 + 8X + 9$. Now, $(X,Y) \mapsto (1/X, Y$ [self-inverse] maps this to $Y^2 = 9X^4 + 8X^3 + 12X^2 + 8X + 2$. Since the coefficient is now a square, we can clearly proceed as for $\mathcal{C}_2$ to get the curve in the required fo

Although the question does not require it, here in fact (for those who are curio a series of birational transformations which transform $Y^2 = 9X^4 + 8X^3 + 12X^2 + 8$ to the form $Y^2 = X^3 + AX + B$. This gives you an idea of how large the numbe become (although the coefficients of the final answer aren't too bad). In the notat part (c), we have: $g_1 = 4/9, g_0 = 46/81, h_1 = 280/729, h_0 = -658/6561$, and so our cu birationally equivalent to: $Y^2 + (4/9)XY + (140/729)Y = (1/2)X^3 - (46/81)X^2 + 329$ One now removes the XY and Y terms by the map $(X,Y) \mapsto (X, Y + (2/9)X + 70$ [with inverse: $(X,Y) \mapsto (X, Y - (2/9)X - 70/729)$], which birationally transform curve to the curve: $Y^2 = (1/2)X^3 - (14/27)X^2 + (203/2187)X + 4900/531441$. apply: $(X,Y) \mapsto (X - 28/81, Y)$ [with inverse $(X,Y) \mapsto (X + 28/81, Y)$], which map curve to the curve: $Y^2 = (1/2)X^3 - (7/81)X$. Finally, the map: $(X,Y) \mapsto (18X,$ [with inverse $(X,Y) \mapsto (X/18, Y/108)$] maps this to the curve: $Y^2 = X^3 - 56X$, is in the required form. In summary: $\mathcal{C}_2 : Y^2 = 2X^4 + 7$ is birationally equival $Y^2 = X^3 - 56X$.

(c). First, the map $(X,Y) \mapsto (X, Y/i)$ [with inverse: $(X,Y) \mapsto (X, iY)$] maps the curve to the curve: $Y^2 = X^4 + 1$. In the notation of part (a), we can take $G(X) = X$ $H(X) = 1$, so that our curve can be birationally transformed over $\mathbb{Q}$ to $2Y^2 = X^3$ that is: $Y^2 = (1/2)X^3 - (1/2)X$. Finally, applying $(X,Y) \mapsto (2X, 4Y)$ [with in $(X,Y) \mapsto (X/2, Y/4)$] birationally transforms this curve to: $Y^2 = X^3 - 4X$, as requ

It is not possible to birationally transform over $\mathbb{R}$ the curve $Y^2 = -X^4 - 1$ form $Y^2 = X^3 + AX + B$, since any such birational transformation would give a between the $\mathbb{R}$-rational points of the two curves; but the second curve has infinitely $\mathbb{R}$-rational points (take all X sufficiently large, e.g. all $X > 2\max(1, |A|, |B|)$), wh the first curve has no $\mathbb{R}$-rational points. [Note that this also implies that there is no birational transformation over $\mathbb{Q}$, either.] The curves $Y^2 = -X^4 - 1$ and $Y^2 = X^3 - 4$ called *twists* of each other, since they are both defined over $\mathbb{Q}$, are birationally equi over $\mathbb{C}$, but are not birationally equivalent over $\mathbb{Q}$].

Over $\mathbb{Q}(\sqrt{-2})$, the curve $Y^2 = -X^4 - 1$ has the $\mathbb{Q}(\sqrt{-2})$-rational point $(1,$
Applying the transformation $(X, Y) \mapsto (X - 1, Y)$ [with inverse $(X, Y) \mapsto (X + 1, Y$
get: $Y^2 = -X^4 - 4X^3 - 6X^2 - 4X - 2$. Now, applying $(X, Y) \mapsto (1/X, Y/X^2)$ [self-in
we get: $Y^2 = -2X^4 - 4X^3 - 6X^2 - 4X - 1$. Now, we apply $(X, Y) \mapsto (X, Y/\sqrt{-2})$
inverse $(X, Y) \mapsto (X, Y\sqrt{-2})$] to get: $Y^2 = X^4 + 2X^3 + 3X^2 + 2X + 1/2$. From pa
we can now say that this is birationally equivalent (over $\mathbb{Q}$ and so over $\mathbb{Q}(\sqrt{-2})$) to a
of the form $Y^2 = X^3 + AX + B$, with $A, B \in \mathbb{Z}$.

Elliptic Curves. Solutions to Sheet 2.

1.

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

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

2. Using $2YY' = 3X^2$, we see that the slope of the curve at $(0,2)$ is $3\cdot 0^2/(2\cdot 2$ and so the tangent to the curve at $(0,2)$ is the line: $Y = 2$. The x-coordinate third point of intersection is then: $0^2 - 0 - 0 = 0$, with corresponding y-coordin In summary: The line $Y = 2$ intersects the curve at $(0,2)$ with multiplicity 3. I $(0,2)+(0,2)+(0,2) = \mathbf{o}$, and so: $3(0,2) = \mathbf{o}$. But, $1(0,2) = (0,2)$ and $2(0,2) = (0$ and so 3 is the smallest $k \geqslant 1$ such that $k(0,2) = \mathbf{o}$; that is, $(0,2)$ has order 3.

3.

(a). As usual, $-(\alpha,0) = (\alpha,0)$, and so $(\alpha,0)+(\alpha,0) = \mathbf{o}$; that is, $(\alpha,0)$ is a po order 2, as required. We now compute $(x',y') = (x,y)+(\alpha,0)$. First, the line th (x,y) and $(\alpha,0)$ is: $Y = (y/(x-\alpha))(X-\alpha)$. Substituting this into the curve $X^3 - (m^2+\alpha-a)X^2 + \ldots = 0$, where $m = y/(x-\alpha)$. The sum of the roots c cubic is: $m^2+\alpha-a$, and so the x-coordinate of the third point of intersection is giv $x' = m^2+\alpha-a-x-\alpha = m^2-x-a = y^2/(x-\alpha)^2 - x - a = (\alpha x + a\alpha + b)/(x$ 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: $(\alpha^2 +$ $b)x/(\alpha^2+a\alpha+b)x$, which is x, as required [Note that $\alpha^2+a\alpha+b \neq 0$, since the $(X-\alpha)(X^2+aX+b)$ 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 fo 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 α_2, α respectively. The formula for T_3 is the same as for T_2, but (again) with $\alpha_1, \alpha_2, \alpha_3$ re 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 fac $\alpha_1-\alpha_2$ from the numerator and denominator), we get the formula for T_3; that is: T T_3. The formula for T_3 is invariant under $\alpha_1 \leftrightarrow \alpha_2$ and so $T_2T_1 = T_3$, also. $T_1T_2 = T_3 = T_2T_1$, and so T_1 and T_2 commute. By symmetry, T_1 and T_3 commute, 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 $T_3^2 : x \mapsto x$; 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.

4. (a). Let L be the tangent line to the curve at P, and let R be the third po intersection; that is, the line and the curve meet at P, P, R. Then $P+P+R = \mathbf{o}$. $3P = \mathbf{o} \iff R = P \iff L$ 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 $(0, 1, 0) =$ which the statement is true, since $3\mathbf{o} = \mathbf{o}$ and $(X_0, X_1, X_2) = (0, 1, 0)$ makes the H determinant 0. When $X_2 \neq 0$, we can write everything in affine form, with $x = X_0/X$ $y = X_1/X_2$, when we see that the Hessian determinant (after dividing through by is 0 exactly when:

$$3Ax^2 + 9Bx + 3xy^2 - A^2 = 0.$$

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

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

Finally, we use the fact the (x, y) is a point on the curve, so that $y^2 = x^3 + Ax + B$, a we can replace y^2 by $x^3 + Ax + B$ in equations (1),(2). This makes both equations b 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 quartic $3x^4 + 6Ax^2 + 12Bx - A^2$, which has at most 4 roots $x_1, \ldots, x_4$. Each x_i giv to at most two points $(x_i, y_i), (x_i, -y_i)$ on the curve, giving at most 8 points of or Together with $\mathbf{o}$, this gives at most 9 points that are 3-torsion.

Elliptic Curves. Solutions to Sheet 3.

1. (a). Let $x, y \in K$ be such that $|x| \neq |y|$, without loss of generality, say that $|x|$
Since K is non-Archimedean, we know that $|x \pm y| \leqslant \max(|x|, |y|) = |y|$, and s
sufficient to show that $|x \pm y| \not< |y|$. Imagine $|x \pm y| < |y|$; then $|y| = |(x \pm y) -$
$\max(|x \pm y|, |x|) < |y|$, a contradiction, as required. [Note that an immediate conseq
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 $x = x_1 + \ldots + x$
$x_{\ell+1} + \ldots + x_n$ and let $y = x_\ell$. Then $|x| \leqslant \max(|x_i| : 1 \leqslant i \leqslant n, i \neq \ell\} < |y|$ a
$|x_1 + \ldots + x_n| = |x + y| = |y| = |x_\ell|$, by part (a).

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

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

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

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

(b). $|3/7|_3 = 3^{-1}$, $|3/7|_7 = 7$. For all other primes p, $\gcd(p, 3) = \gcd(p, 7) = 1$ a
$|3/7|_p = 1$. Note also that $|3/7|_\infty = 3/7$. The given product $\prod |3/7|_i$ has all factors
to 1 apart from the factors: $|3/7|_3 = 3^{-1}$, $|3/7|_7 = 7$ and $|3/7|_3 = 3/7$, whose produc
Hence the given product $\prod |3/7|_i$ is 1. For any $x \in \mathbb{Q}$, write $x = \pm n/d$, where n
are integers with $\gcd(n, d) = 1$, and write n, d in terms of their primes factorisations
$p_1^{s_1} \cdot \ldots p_k^{s_k}$ 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 pr
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 $p = \infty$
$|x|_p = n/d = (p_1^{s_1} \cdot \ldots p_k^{s_k})/(q_1^{t_1} \cdot \ldots q_\ell^{t_\ell})$. For all other primes p, we have $|x|_p = 1$. It f
that the product $\prod |x|_i$ is equal to $(p_1^{-s_1} \cdot \ldots p_k^{-s_k}) \cdot q_1^{t_1} \cdot \ldots q_\ell^{t_\ell} \cdot (p_1^{s_1} \cdot \ldots p_k^{s_k})/(q_1^{t_1} \cdot .$
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 $1/5^$
not converge in $\mathbb{Q}_5$ (since, if $a_n \to \ell$ then $|a_n|_p \to |\ell|_p$).

(b). *Method 1.* $|n|_5 \leqslant 5^{-1}$ for $n = 5, 10, 15, \ldots$ and $|n|_5 = 1$ otherwise; this mean
$|n|_5$ does not converge (since there is a subsequence $|n|_5$ for $5 \not| n$ converging to 1
subsequence $|n|_5$ for $5|n$ and $5^2 \not| n$ converging to $1/5$), and so n does not converge
(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 co
to 0 (using the result from lectures which says that $\sum c_i$ converges iff $|c_i|_n \to 0$).

(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 f
$5, 10, 15, \ldots$) contributes at least one new factor of 5. Hence $|n! - 0|_5 = |n!|_5 < 5^{-(n/5}$
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
(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
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 $\mathbb{Q}_5$
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
approximation for which $|a_0^2 + 1|_5 = |5|_5 = 5^{-1}$. Take $x_1 = a_0 + 5a_1 = 2 + 5a_1$. Th
want $(2 + 5a_1)^2 \equiv -1 \bmod 5^2$, and so $20a_1 \equiv -5 \bmod 5^2$, which is the same as $4a_1$
mod 5, and so $a_1 = 1$. This gives a better approximation: $x_1 = 2 + 1 \cdot 2 = 7$, which sa
$|x_1^2 + 1|_5 = 5^{-2}$. Simlarly, we then find $a_2 = 2$ and so $x_2 = 7 + 2 \cdot 5^2 = 57$. Then, fina
similarly find $a_3 = 1$ and so $x_3 = 57 + 1 \cdot 5^3 = 182$, satisfying $|x^2 + 1|_5 = 5^{-4}$, as req
(b). If there were an integer x such that $|x^2 - 7/8|_3 \leqslant 3^{-7}$, then we would have x^2
mod 3^7 and so $x^2 \equiv 7/8 \bmod 3$. But $7/8 \equiv 2 \bmod 3$, which is not a quadratic r
(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 possib
for $|x^2|_5$. If $|x^2|_5 > |5/4|_5$ then (using the result that $|a + b|_p = \max(|a|_p, |b|_p)$
$|a|_p \neq |b|_p$) we have $|x^2 - 5/4|_5 = \max(|x^2|_5, |5/4|_5) = |x^2|_5 > |5/4|_5 = 5^{-1} >$
contradicting $|x^2 - 5/4|_5 \leqslant 5^{-4}$. If $|x^2|_5 < |5/4|_5$ then (using the same result) we
$|x^2 - 5/4|_5 = \max(|x^2|_5, |5/4|_5) = |5/4|_5 = 5^{-1} > 5^{-4}$, again contradicting $|x^2 - 5/$
5^{-4}. It must then be that $|x^2|_5 = |5/4|_5 = 5^{-1}$, but this is again impossible since $|x^2|$
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) $4 + 7 \cdot (0 + 7 \cdot 4) = 4 + 0 \cdot 7^1 + 4$
$4, 04$.

For $3/14$, it is easier first to write: $3/14 = 7^{-1} \cdot 3/2$. First find the 7-adic expa
of $3/2$, with the idea that the 7-adic expansion of $3/14$ will then just be the 7-adic expa
of $3/2$ shifted one place to the left). Now, $|3/2|_7 = 1$ and so $3/2 = a_0, a_1 a_2 \ldots$.
$2(a_0 + 7a_1 + 7^2 a_2 + \ldots) = 3$, we first find $2a_0 \equiv 3 \bmod 7$ and so $a_0 = 5$. Cont
as usual, we find that $a_1 = 3, a_2 = 3, a_3 = 3 \ldots$. At this point, we suspect that
$5, \overline{3}$. We can prove this rigorously as follows. Let $\alpha = 5, \overline{3}$. Then $\alpha - 5 = 0, \overline{3}$, a
$7^{-1}(\alpha - 5) - 3 = 3, \overline{3} - 3 = 0, \overline{3} = \alpha - 5$. Hence, $\alpha - 5 - 21 = 7\alpha - 35$ and so $\alpha =$
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^{-}
$2) - 3 \cdot 5^{-1} - 4 \cdot 5^0 = 0, \overline{34} = \beta - 2$, 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
n, d in terms of their primes factorisations: $n = p_1^{s_1} \cdot \ldots p_k^{s_k}$ and $d = q_1^{t_1} \cdot \ldots q_\ell^{t_\ell}$,
$p_1, \ldots p_k, q_1, \ldots q_\ell$ are distinct primes. If $x \in \mathbb{Z}$ then $\ell = 0$ (i.e. there are no occur
of q_j) and we see that when $p = p_i$ for some i, $|x|_p = p_i^{-s_i} \leqslant 1$, and otherwise $|x|$
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 occurre 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, no denominator and is in $\mathbb{Z}$.

7. The number of positive multiples of an integer $k > 0$ which are $\leqslant n$ is clearly $\left[\frac{n}{k}\right.$ count the power of p dividing $n!$, since p is prime, it is enough to count the power dividing $1, 2, 3, \ldots, n$ and add these powers up. Now, the number of multiples of p a $1, 2, 3, \ldots, n$ is $[\frac{n}{p}]$. Each multiple of p^2 among $1, 2, 3, \ldots, n$ gives an additional pow 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 of p is as in the given formula. This gives that $|n!|_p = p^{-M}$, where $M = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] +$ $\frac{n}{p} + \frac{n}{p^2} + \ldots = \frac{n}{p-1}$. Hence $|n!| \geqslant p^{-\frac{n}{p-1}}$, and so $|1/n!| \leqslant p^{\frac{n}{p-1}}$. Suppose that $|x| <$ and let $\tau = |x|/p^{-\frac{1}{p-1}} < 1$. Then $\left|\frac{x^n}{n!}\right| = \tau^n p^{-\frac{n}{p-1}} \left|\frac{1}{n!}\right| \leqslant \tau^n p^{-\frac{n}{p-1}} p^{\frac{n}{p-1}} = \tau^n$ Hence, $\exp_p(x)$ converges (using the result from lectures which says that $\sum c_i$ con 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 $\frac{n}{p}, \frac{n}{p^2}, \ldots$ $p^{\ell-1}, p^{\ell-2}, \ldots, 1 \in \mathbb{Z}$ and so $M = p^{\ell-1} + p^{\ell-2}, \ldots + 1 = \frac{p^\ell - 1}{p-1}$; this means that th sequence $\left|\frac{x^{p^\ell}}{(p^\ell)!}\right| \geqslant (p^{-\frac{1}{p-1}})^{p^\ell} p^{\frac{p^\ell - 1}{p-1}} = p^{\frac{-1}{p-1}}$, and so $\left|\frac{x^n}{n!}\right| \not\to 0$. Hence $\exp_p(x)$ do 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 $r \in \mathbb{Z}] < p^{-\frac{1}{p-1}}$, since $p \geqslant 3$. Any $|x|_p \geqslant 1$ satisfies $|x| \geqslant p^{-\frac{1}{p-1}}$. When $K = \mathbb{Q}$ $|x|_2 < 1/2$ must satisfy $|x|_2 \leqslant 2^{-2}$ [since $|x|_p = p^r$ for some $r \in \mathbb{Z}] < p^{-\frac{1}{p-1}} = 2^{-1}$ $|x|_p \geqslant 1/2$ satisfies $|x| \geqslant p^{-\frac{1}{p-1}} = 2^{-1}$.

Elliptic Curves. Solutions to Sheet 4.

1. First note that $-28 = 2^2 \cdot (-7)$. In $\mathbb{Q}_2$, we know that any integer congruent to 1 i
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 qua
residue mod 3; hence -28 is not a square in $\mathbb{Q}_3$. In $\mathbb{Q}_5$, we observe that $|-28|_5 =$
$-28 \equiv 2 \pmod 5$ which is not a quadratic residue mod 5; hence -28 is not a square
In $\mathbb{Q}_7$, if there were an x such that $x^2 = -28$, then $|x^2|_7 = |-28|_7 = 7^{-1}$, contrad
the fact that $|x^2|_7 = 7^r$ where r is an even integer; hence -28 is not a square in $\mathbb{Q}$
$\mathbb{Q}_{11}$, we observe that $|-28|_{11} = 1$ and $-28 \equiv 5 \pmod{11}$ which is a quadratic r
mod 11 since $5 \equiv 4^2 \pmod{11}$; hence -28 is a square in $\mathbb{Q}_{11}$. [The above repeatedl
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 s
mod p.]

2. In $\mathbb{R}$, we have for example the root $\sqrt{2}$. In $\mathbb{Q}_2$, note that $17 \equiv 1 \bmod 8$, and so
square in $\mathbb{Q}_2$. In $\mathbb{Q}_{17}$, note that $|2|_{17} = 1$ and 2 is a quadratic residue mod 17, so th
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
since $(\frac{34}{p}) = (\frac{2}{p})(\frac{17}{p})$ [and $-1 \neq (-1)(-1)$], so at least one of them must be 1. Wlo
that $(\frac{2}{p}) = 1$. Then $|2|_p = 1$ and 2 is a quadratic residue mod p, so that 2 must be a s
in $\mathbb{Q}_p$.

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

Let $f(x) = x^3 - 28$ and let $x_0 = 1$. Then $|f(x_0)|_3 = |-27|_3 = 3^{-3}$, w
$|f'(x_0)|_3 = |3|_3 = 3^{-1}$. Hence $|f(x_0)|_3 < |f'(x_0)|_3^2$, and so by Hensel's Lemma there
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 $|f(x_0)|_7 = |-14|_3 = 7^{-1}$, w
$|f'(x_0)|_7 = |3|_7 = 1$. Hence $|f(x_0)|_7 < |f'(x_0)|_7^2$, and so by Hensel's Lemma again
must be a root of $f(x)$ in $\mathbb{Q}_7$; that is 13 must be a cube in $\mathbb{Q}_7$.

4. Let $\mathcal{C}$ be the curve $2Y^2 = X^4 - 17$. Over $\mathbb{R}$, the curve has the point $(4, \sqrt{239/2})$.
let $x = 11$. Then $11^4 - 17 = 2^5 \cdot 457$; but 457 is an integer congruent to 1 mod 8, a
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
curve over $\mathbb{Q}_2$. For the next few primes, we shall repeatedly use the result from le
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, not
$-8, -34, -34, -8, 10, -8$ are quadratic residues modulo $p = 3, 5, 7, 11, 13, 17$, respec
and so there exists $\gamma \in \mathbb{Q}_p$ such that $\gamma^2 = -8, -34, -34, -8, 10, -8$, respectively
gives the $\mathbb{Q}_p$-rational points on the curve: $(1, \gamma), (0, \gamma/2), (0, \gamma/2), (1, \gamma), (4, \gamma/2),$
respectively. Hence $\mathcal{C}$ has $\mathbb{Q}_p$-rational points for all primes up to and including $p =$
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 by 2) is birationally equivalent to $V^2 = 2X^4 - 34$, where $V = 2Y$; note that $2X^4$ has discriminant $-2^{11}17^3$. Recall Theorem 1.15 from lectures, that any curve $y^2 =$ where $Q(x) = f_4x^4 + \ldots + f_0$ has nonzero discriminant over $\mathbb{F}_p$, has at least $p-1-2$ affine points over $\mathbb{F}_p$, and so at least 5 affine points. At most 4 of these can have $2x^4$ - 0 (mod p), and so there exists $x_0 \in \mathbb{Z}$ such that $2(x_0^4 - 17)$ is a nonzero quadratic r mod p. As above, there exists $\gamma \in \mathbb{Q}_p$ such that $\gamma^2 = 2(x_0^4 - 17)$, and so $(x_0, \gamma/2$ $\mathbb{Q}_p$-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: $p \neq 2,$ that $\widetilde{\mathcal{C}}$ is still an elliptic curve mod p) and $p \geqslant 5$, we have $\#\widetilde{\mathcal{C}}(\mathbb{F}_p) \geqslant p + 1 - 2\sqrt{}$ and so the number of affine points is > 0; these are non-singular, since $\widetilde{\mathcal{C}}$ is still an e curve mod p. Also, by a theorem from lectures, any non-singular point on $\widetilde{\mathcal{C}}(\mathbb{F}_p)$ l 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 po $\mathcal{C}(\mathbb{Q}_p)$ (since the point at infinity on $\mathcal{C}(\mathbb{Q}_p)$ maps to the point at infinity on $\widetilde{\mathcal{C}}(\mathbb{F}_p)$ the reduction map mod p). This shows the existence of such $x, y \in \mathbb{Q}_p$ for all p $p = 2, 3$ and bad primes, so only still need to consider $p = 2, 3, 17$. Also, note th $p = 3$ there is the non-singular affine point $(1, 1)$ on $\widetilde{\mathcal{C}}(\mathbb{F}_3)$, and for $p = 17$ there non-singular affine point $(1, 3)$ on $\widetilde{\mathcal{C}}(\mathbb{F}_{17})$, and as before these must lift to affine $(x, y) \in \mathcal{C}(\mathbb{Q}_p)$. Over $\mathbb{R}$, the curve has the point $(4, \sqrt{239/2})$. In $\mathbb{Q}_2$, let $x = 11$. $11^4 - 17 = 2^5 \cdot 457$; but 457 is an integer congruent to 1 mod 8, and so, from lectures, 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 $\mathbb{Q}_2$ 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 $X,$ such that $2Y^2 = X^4 - 17$. Let $X = t/r$, where $r, t \in \mathbb{Z}$ and $\gcd(r, t) = 1$. Then $2(r^2$ $t^4 - 17r^4 \in \mathbb{Z}$. For any prime p, this gives that $|2|_p |r^2Y|_p^2 \leqslant 1$. When $p \neq 2$, we have $|2$ 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 th gives $|r^2Y|_2 \leqslant 1$ [since $|r^2Y|_2 > 1$ would mean $|r^2Y|_2 \geqslant 2^1$ and so $2^{-1}|r^2Y|_2^2 \geqslant 2^{-1}2^2$ Overall, we have shown that $|r^2Y|_p \leqslant 1$ for all p; since also $r^2Y \in \mathbb{Q}$, this give $r^2Y \in \mathbb{Z}$; let us say: $s = r^2Y \in \mathbb{Z}$. Therefore $r, s, t \in \mathbb{Z}$ satisfy $2s^2 = t^4 - 17r$ $\gcd(r, t) = 1$.

Let q be any prime such that $q|s$. Note that $q \neq 17$ [since if $17|s$ then our eq $2s^2 = t^4 - 17r^4$ would force $17|t$, and so $17^2|2s^2$ and $17^2|t^4$, which would give 17^2 forcing $17|r$, which would contradict $\gcd(r, t) = 1$]. Note also that we must not have $q|r$ [since if $q|s$ and $q|r$, then our equation $2s^2 = t^4 - 17r^4$ would force $q|t$, would contradict $\gcd(r, t) = 1$]. Reducing our equation modulo q gives that $0 \equiv$ $17r^4$ and so $(t^2/r^2)^2 \equiv 17 \bmod q$ [note that division by r^2 is allowable mod q r is not divisible by q]. Hence 17 is a nonzero quadratic residue mod q. For q quadratic reciprocity then allows us to deduce that q is a quadratic residue mod 17 $17 \equiv 1 \pmod 4$]. Furthermore, one can check directly that 2 is a quadratic r mod 17, since $2 \equiv 6^2 \bmod 17$. Overall, we have shown that every prime q divi must be a quadratic residue mod 17, and we can take $s > 0$ (if necessary, repla by $-s$), so that s is the product of its prime factors. It follows that s itself mu a quadratic residue mod 17, since it is a product of quadratic residues mod 17.

s^2 is a nonzero fourth power [also known as a *quartic residue*] mod 17. Note als reducing our equation mod 17 gives $2s^2 \equiv t^4 \pmod{17}$, so that $2s^2$ is also a n fourth power mod 17. Since $s, 2s^2$ are both nonzero fourth powers mod 17, it f that $2 = (2s^2)/s^2$ is also a fourth power mod 17. On the other hand, one can co 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 cong mod 17 to: $0, 1, 16, 13, 1, 13, 4, 4, 16, 16, 4, 4, 13, 1, 13, 16, 1$, respectively, so that in fa not a fourth power mod 17. This contradication show that our original curve $\mathcal{C}$ h $\mathbb{Q}$-rational points.

5. Since $p \equiv 2 \pmod 3$, we have $\gcd(3, p-1) = 1$, and so there exist $\lambda, \mu \in \mathbb{Z}$ 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 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 $p \nmid a$. From above, there must exist $x_0 \in \mathbb{Z}$ such $x_0^3 \equiv a \pmod p$; clearly $p \nmid x_0$. Let $f(x) = x^3 - a$. Then $|f(x_0)|_p = |x_0^3 - a|_p$ since $x_0^3 - a \equiv 0 \pmod p$. Also, $|f'(x_0)|_p = |3x_0^2|_2 = 1$, since $|3|_p = 1$ and $p \nmid x_0$. $|f(x_0)|_p < |f'(x_0)|_p^2$, and so by Hensel's Lemma, there exists $x \in \mathbb{Z}_p$ with $f(x) = 0$ is, $x^3 = a$, as required.

6. Recall the standard fact about resultants (stated in Section 0, the preliminary ing), that there exist polynomials $p(x), q(x) \in R[x]$ such that: $p(x)f(x) + q(x)g$ $\mathrm{Res}\big(f(x), g(x)\big)$ Since the discriminant D is the resultant of $f(x)$ and $f'(x)$, there mu ist polynomials $p(x), q(x) \in R[x]$ such that $p(x)f(x)+q(x)f'(x) = D$, and so: $p(a_0)f$ $q(a_0)f'(a_0) = D$. Since $|a_0| \leqslant 1$, and since $p(x), q(x), f(x), f'(x) \in R[x]$, we mus $|p(a_0)|, |f(a_0)|, |q(a_0)|, |f'(a_0)| \leqslant 1$ and so $|D| \leqslant \max(|p(a_0)f(a_0)|, |q(a_0)f'(a_0)|)$ which also implies $|D^2| = |D|^2 \leqslant |D|$. Now, we are given that $|f(a_0)| < |D|^2$ $|p(a_0)f(a_0)| \leqslant |f(a_0)| < |D^2| \leqslant |D|$. Hence $|D| \neq |p(a_0)f(a_0)|$, and so $|q(a_0)f'(a$ $|D - p(a_0)f(a_0)| = \max(|D|, |p(a_0)f(a_0)|) = |D|$ [using the fact that, if $|u| \neq |v$ $|u \pm v| = \max(|u|, |v|)$]. Since also $|q(a_0)| \leqslant 1$, this gives that $|f'(a_0)| \geqslant |D|$. F $|f(a_0)| < |D|^2 \leqslant |f'(a_0)|^2$, and so $f(X)$ has a root $a \in R$ by Hensel's Lemma.

7. Let $f(X) = 5X^3 - 7X^2 + 3X + 6$, so that $f'(X) = 15X^2 - 14X + 3$. Let $x_0 = a$ Then $|f(x_0)|_7 = |7|_7 = 7^{-1}$ and $|f'(x_0)|_7 = |4|_7 = 1$. Then Hensel's Lemma tells u there exists $\alpha \in \mathbb{Z}_7$ with $|\alpha - 1|_7 < 1$, and the proof tells us to construct a sequence x $x_n - f(x_n)/f'(x_n)$ which will converge to α, with each $f(x_n) \equiv 0 \pmod{7^{n+1}}$, so that x will satisfy $|\alpha - a|_7 \leqslant 7^{-4}$. Now compute $x_1 = x_0 - f(x_0)/f'(x_0) = 1 - 7/4 = -3/4$ $\pmod{7^2}$. Then compute $x_2 = x_1 - f(x_1)/f'(x_1) = 152494/6313 \equiv 36 \pmod{7^3}$. F compute $x_3 = x_2 - f(x_2)/f'(x_2) = 152494/6313 \equiv 379 \pmod{7^4}$. As a check, not $f(x_3) = f(379) = 271195351 = 7^4 \cdot 112951 \equiv 0 \pmod{7^4}$, and all $|f(x_n)|_7 \leqslant 7^{-4}$ for So, for all $n \geqslant 3$, the process $x_{n+1} = x_n - f(x_n)/f'(x_n)$ will not affect $x_n \bmod 7^4$; t $x_n \equiv 379 \bmod 7^4$ [and so $|x_n - 379|_7 \leqslant 7^{-4}$] for all $n \geqslant 3$. Since $x_n \to \alpha$ in $\mathbb{Z}_7$ it f that $|\alpha - 379|_7 \leqslant 7^{-4}$, as required.

Elliptic Curves. Solutions to Sheet 5.

1. 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 w
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 define
$\mathbb{Z}_p$, 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
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-s
and $b \neq 0$).

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

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

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

4.
(a). Let $\mathcal{E} : Y^2 = X^3 + p^2$. Then the point $(0, p)$ on $\mathcal{E}$ reduces modulo p to the cusp
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
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 node $(0, 0)$ on $\widetilde{\mathcal{E}} : Y^2 = X^3 + X^2$, which is another way of saying that $(0, 0)$ on $\widetilde{\mathcal{E}}$ l 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 $\widetilde{\mathcal{E}}$ not lift to any point in $\mathcal{E}(\mathbb{Q}_p)$ by the same argument as in Question 2.

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

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

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

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

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

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

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

6. Recall from lectures that the first step in deriving the formal group of an elliptic is to write the equation $\mathcal{E} : Y^2 = X^3 + AX + B$ as: $\mathcal{E}' : w = f(z, w) = z^3 + Aw^2z +$ where $z = -x/y, w = -1/y$. We then Inductively define $f_n(z, w)$ by: $f_1(z, w) = f$ 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 $f_1(z, w) = z^3 + Aw^2z + Bw^3$ al weighted degree $\equiv 3$ [where we give z weight 1, w weight 3, A weight -4 and B weigh Suppose that this is also true of $f_m(z, w)$; then $f_{m+1}(z, w) = f_m(z, z^3 + Aw^2z +$ where z has weighted degree 1, $z^3 + Aw^2z + Bw^3$ is homogeneous of weighted deg and so the same will be true of f_{m+1}. So, by induction, all terms of every f_m and terms of $w(z)$ will have weighted degree 3, and so $w(z) = \sum c_n z^n$, where $c_n = 0$ $n \equiv 3 \bmod 4$. We now perform the addition $(z_1, w_1) + (z_2, w_2)$. As usual, we first the line $z = \lambda w + \mu$ through the points, given by $\lambda = (w(z_1) - w(z_2))/(z_1 - z_2$ $\mu = (z_1w(z_2) - z_2w(z_1))/(z_1 - z_2)$, both in $\mathbb{Z}[A, B][[z_1, z_2]]$. Letting z_1 and z_2 each weight 1, the numerator $w(z_1) - w(z_2)$ is homogeneous of weighted degree 3, and s homogeneous of weighted degree 2. Similarly, μ is homogeneous of weighted degree in lectures, substituting $w = \lambda z + \mu$ into $\mathcal{E}'$ gives $\lambda z + \mu = z^3 + A(\lambda z + \mu)^2 z + B(\lambda z$ 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 $z = \lambda u$ 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 so is an invertible power series, with $1/(1 + \phi(z)) = 1 - \phi(z) + \phi(z)^2 + \ldots]$. Th $(z_1, w_1)+(z_2, w_2)+(z_3, w_3) =$ the identity, and so $(z_1, w_1)+(z_2, w_2) = -(z_3, w_3)$. Ne $(x, y) \mapsto (x, -y)$ induces $(z, w) \mapsto (-z, -w)$ [since $z = -x/y, w = -1/y$], so that 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 homoge of weighted degree 1, and the fraction whose numerator $2A\lambda\mu + 3B\lambda^2\mu$ is homoge of weighted degree 1, and whose denominator $1 + A\lambda^2 + B\lambda^3$ is homogeneous of we degree 0. Therefore the final power series giving the formal group must be homoge of weighted degree 1.

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

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

Elliptic Curves. Solutions to Sheet 6.

1. In all of the following, we use the result from lectures that (when the coefficient are in $\mathbb{Z}$) $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}$ mod p, where $p \neq 2$ is a prin dividing the discriminant. Note that this typically gives a much faster way of comp $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ than the Nagell-Lutz result. N.B. (a),(b),(c) are about the level that co 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 orde $\mathcal{E}_{\text{tors}}(\mathbb{Q})$, which generate a subgroup of $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ of size 6 (namely, the 6 points mP for $0 \leqslant m \leqslant 2$ and $0 \leqslant n \leqslant 1$). Further, $\Delta = 4A^3 + 27B^2 = 27$, so we can reduce m any prime except 2 (which must always be avoided) and 3. Over $\mathbb{F}_5$, there are or points: $\mathbf{o}, (0, \pm 1), (2, \pm 3), (4, 0)$. So, we conclude that $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ has size at most 6, means that it consists of precisely the $C_6 = C_2 \times C_3$ group of points we have found al

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

(b). Here, the (birational over $\mathbb{Q}$) transformation $(X, Y) \mapsto (X - 1, Y)$ takes the curve to: $Y^2 = X(X + 1)(X - 1) = X^3 - X$, which has discriminant -4, and so w reduce modulo the prime 3 Over $\mathbb{F}_3$ there are the points: $\mathbf{o}, (0, 0), (1, 0), (2, 0)$ givin $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ has size at most 4. But, in fact, $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ contains $\mathbf{o}, (0, 0), (-1, 0), (1, 0)$, means the this $C_2 \times C_2$ group gives all of $\mathcal{E}_{\text{tors}}(\mathbb{Q})$. [*Alternatively, even without u birational transformation to the form* $Y^2 = X^3 + AX + B$*, we could just work entirel the given equation of the curve, noting that the original cubic* $X(X - 1)(X - 2)$ *h repeated roots mod* 3*, so that* $Y^2 = X(X - 1)(X - 2)$ *is an elliptic curve mod* 3*, an 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 to: $Y^2 = X^3 + 1$ which we have already seen in part (a) to have a $C_2 \times C_3$ group torsion group.

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

(d). **[optional]** The discriminant of $X^3 - 219X + 1654$ is $\Delta = 4(-219)^3 + 27 \cdot 16$ $31850496 = 2^{17}3^5$, so we need only avoid the primes 2, 3 (alternatively, it would be suf to compute that $\Delta \not\equiv 0 \bmod 5$, since that is all we shall require). Reducing modulo 5 the nine points: $\mathbf{o}, (0, \pm 2), (1, \pm 1), (2, \pm 2), (3, \pm 2)$, and so $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ has size at most short integer search for possible x-coordinates reveals the point $P = (11, 24)$ of orde can be checked by computing $P, 2P, 3P, \ldots, 9P = \mathbf{o}$). Hence, $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is just the C_9 consisting of these points.

Note that, if $P = (11, 24)$, then the complete list of torsion points is: $\mathbf{o}$ $(11, 24), 2P = (-13, 48), 3P = (3, -32), 4P = (35, -192), 5P = (35, 192), 6$ $(3, 32), 7P = (-13, -48), 8P = (11, -24)$.

2. Let $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q})$ be the usual isogeny, which is a group homomorphism 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

homomorphism with kernel: $\mathbf{o}, (0,0)$. Now, let $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ be the set of torsion ele
of $\mathcal{C}(\mathbb{Q})$ which have odd order. First check that $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ is a subgroup: (1) The id
$\mathbf{o}$ has order 1, which is odd, so $\mathbf{o} \in \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, (2) If P, Q have odd torsion orders
respectively, then $mn(P+Q) = n(mP) + m(nQ) = \mathbf{o}$ and so the order of $P+Q$ d
mn, giving that the order of $P+Q$ is odd, i.e. $P+Q \in \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, (3) The order
is the same as the order of $-P$, so $P \in \mathcal{C}_{\text{oddtors}}(\mathbb{Q}) \Rightarrow -P \in \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$. Similarly
$\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, a subgroup of $\mathcal{D}(\mathbb{Q})$.

Now, consider any $P \in \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$. Then P must have odd order m, say
$R = \phi(P)$. Then $mR = m\phi(P) = \phi(mP) = \phi(\mathbf{o}) = \mathbf{o}$, which means that the orde
divides m, and so the order of R is odd; that is: $R \in \mathcal{D}_{\text{oddtors}}(\mathbb{Q})$. Hence, ϕ g
map from $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ to $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, which certainly satisfies the homomorphism
erty $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, since ϕ satisfies this prope
the larger set $\mathcal{C}(\mathbb{Q})$. Furthermore, the kernel of $\phi : \mathcal{C}_{\text{oddtors}}(\mathbb{Q}) \to \mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ mus
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 inj
[any homomorphism with trivial kernel is an injection]. We have therefore establishe
there is an injective homomorphism (namely ϕ) from $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ to $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$,
implies that $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, namely the sub
$\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q}))$ [note, since $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ are finite, it follows from thi
$\#\mathcal{C}_{\text{oddtors}}(\mathbb{Q}) = \#\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q}))) \leqslant \#\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$]. (We have just used here the g
fact that if θ is a homomorphism from group G to group H, then $G/\ker\theta$ is isomorp
$\text{im}\theta$, which is the same as $\theta(G)$; when θ is injective, $\ker\theta$ contains only the identity el
and $G/\ker\theta$ can be replaced by G). Applying the same argument to $\hat{\phi} : \mathcal{D}_{\text{oddtors}}($
$\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ gives that $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, n
$\hat{\phi}(\mathcal{D}_{\text{oddtors}}(\mathbb{Q}))$ [and consequently $\#\mathcal{D}_{\text{oddtors}}(\mathbb{Q}) = \#\hat{\phi}(\mathcal{D}_{\text{oddtors}}(\mathbb{Q})) \leqslant \#\mathcal{C}_{\text{oddtors}}(\mathbb{Q}$
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
ber of elements. Combining the fact that $\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q})))$ is a subgroup of $\mathcal{D}_{\text{oddt}}$
and the fact that $\#\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q}))) = \#\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ gives that $\phi(\mathcal{C}_{\text{oddtors}}(\mathbb{Q})))$ m
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 eq
$\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$; 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 $\mathcal{D}$ d
from $(0,0)$, namely $Q_1 = ((-a_1 + \sqrt{a_1^2 - 4b_1})/2, 0) = (a + 2\sqrt{b}, 0)$ and $Q_2 = ((-$
$\sqrt{a_1^2 - 4b_1})/2, 0) = (a - 2\sqrt{b}, 0)$. Recall the standard map from lectures $q : \mathcal{D}($
$\mathbb{Q}^*/(\mathbb{Q}^*)^2$ which takes $\mathbf{o} \to 1$, $(0,0) \to b_1$, and otherwise takes $(u,v) \to u$. We know
lectures that this map has kernel precisely $\phi(\mathcal{C}(\mathbb{Q}))$. Now, the multiplication by 2 m
$\mathcal{C}(\mathbb{Q})$ is $\hat{\phi} \circ \phi$, and so $(0,0) \in 2\mathcal{C}(\mathbb{Q})$ iff either Q_1 or Q_2 is a member of $\phi(\mathcal{C}(\mathbb{Q})) \iff q($
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 $a -$
$(\mathbb{Q}^*)^2 \iff b = m^2$ and $a + 2m = n^2$, for some $m, n \in \mathbb{Q}$; but in fact m, n must b
since $a, b \in \mathbb{Z}$.

4. First let us suppose that our elliptic curve $Y^2 = X^3 + AX + B$ has a point (
of order 4. Performing the birational transformation $(X,Y) \mapsto (X - x_0, Y - y_0)$
corresponds to replacing the variables X, Y by $X + x_0, Y + y_0$] maps (x_0, y_0) to $(0$
the birationally equivalent curve if the form: $Y^2 + 2y_0Y + y_0^2 = (\text{monic cubic in } X)$,

is of the form: $Y^2 + 2y_0Y = X^3 + f_2X^2 + f_1X$ [after absorbing $-y_0^2$ into the cubic
The fact that there is no constant term f_0 is a consequence of the fact that our new
contains the point $(0,0)$. We perform the further birational transformation $(X,$
$(X, Y - f_1X/(2y_0))$ [which corresponds to replacing the variable Y by $Y + f_1X/$
which maps to the new birationally equivalent curve $Y^2 + bXY + aY = X^3 + cX^2,$
$b = f_1/y_0, a = 2y_0, c = f_2 - (f_1/(2y_0))^2]$. Note that, for any r, the birational transforn
$(X, Y) \mapsto (r^2X, r^3Y)$ [which corresponds to replacing the variables X, Y by $X/r^2,$
maps to the birationally equivalent curve: $Y^2 + brXY + ar^3Y = X^3 + cr^2X^2$. Ch
$r = c/a$ forces the coefficients of Y and X^2 both to be c^3/a^2. So, let $r = c/a, v =$
and $w = br = b^2/c$. Note that $y_0 \neq 0$, since (x_0, y_0) is not of order 2, and so $a = 2y$
Also, $c \neq 0$ (since if $c = 0$ then $Y = 0$ would meet the curve $Y^2 + bXY + aY = X^3$
3 times at $(0,0)$ making $(0,0)$ of order 3, and so (x_0, y_0) of order 3 on the original
a contradiction). Hence, it was legitimate to have divided by a and c. Our curve is
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
contained a rational point (x_0, y_0) [not of order 2 or 3], which we have mapped to $(0,$
now use the fact that $(0,0)$ is of order 4 on $\mathcal{E}$ to see what condition this gives on v, w.
perform the addition $(0,0) + (0,0)$. The line tangent to $\mathcal{E}$ at $(0,0)$ is $Y = 0$. Substi
this into $\mathcal{E}$ gives: $X^3 + vX^2$, which has roots $0, 0, -v$, and so $(0,0), (0,0), (-v,0)$ a
three points of intersection of $Y = 0$ and $\mathcal{E}$, so that $(0,0) + (0,0) + (-v,0) = \mathbf{o}$, g
$2(0,0) = -(-v,0)$. Now, since $\mathbf{o}$ is the point at infinity, the negative of $(-v,0)$ is the
point on $\mathcal{E}$ with X-coordinate $-v$. Substituting $X = -v$ into $\mathcal{E}$ gives: $Y^2 - vwY + v$
and so: $Y(Y - v(w-1))$, which has roots $0, v(w-1)$. So, the negative of $(-v$
$(-v, v(w-1))$, giving: $2(0,0) = (-v, v(w-1))$. Now, $(0,0)$ is of order 4 iff $2(0,0$
order 2 iff $2(0,0)$ equals its own inverse (since it is not the identity). But $(-v, v(w -$
the inverse of $(-v,0)$ and so equals its own inverse iff $v(w-1) = 0$. Now, we canno
$v = 0$, since then $\mathcal{E}$ would be singular and so would not be an elliptic curve. So,
having order 4 on $\mathcal{E}$ is equivalent to $w = 1$. Substutuing $w = 1$ into $\mathcal{E}$ gives the re
form.

Elliptic Curves. Solutions to Sheet 7.

1.

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

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u$, for $(u, v) \neq$ with $q : (0, 0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, is an injection with im$q$ contained in d is square free and $d|b_1\} = \{\pm 1, \pm 2\}$. Also, $\mathbf{o} \mapsto 1$, $(0, 0) \mapsto -8 = -2$, so $\{1, -2\} \subset \text{im}q \subset \{\pm 1, \pm 2\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in$ i there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a_1\ell$ $(b_1/(-1)) \cdot m^4 = n^2$ that is: $-\ell^4 - 4\ell^2m^2 + 8m^4 = n^2$. Rewrite as: $-(\ell^2 + 2m^2)^2 + 12m^4$ Reducing modulo 3 gives $-(\ell^2 + 2m^2)^2 \equiv n^2$ (modulo 3). If n were coprime to 3, the would give: $((\ell^2 + 2m^2)/n)^2 = -1$ in $\mathbb{F}_3$, contradicting the fact that -1 is not a qua residue modulo 3. So, $3|n$ and so $3|(\ell^2 + 2m^2)$ also. This means that $9|(\ell^2 + 2m^2)$ $9|n^2$, which can be combined with $-(\ell^2 + 2m^2)^2 + 12m^4 = n^2$ to give: $9|12m^4$ a $3|m$. Combining $3|m$ with $3|(\ell^2 + 2m^2)$ gives that $3|\ell$. This contradicts the fac $\gcd(\ell, m) = 1$. Hence our equation is impossible in $\mathbb{Q}_3$, and so impossible in $\mathbb{Q}$. $-1 \notin \text{im}q$.

We conclude that 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 $(x, y) \neq$ with $\hat{q} : (0, 0) \mapsto b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with im$\hat{q}$ contained in d is square free and $d|b\} = \{\pm 1, \pm 3\}$. Also, $\mathbf{o} \mapsto 1$ and $(0, 0) \mapsto 3$, so that $\{1$ im$\hat{q} \subset \{\pm 1, \pm 3\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in$ i there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a\ell$ $(b/(-1)) \cdot m^4 = n^2$; that is: $-\ell^4 + 2\ell^2m^2 - 3m^4 = n^2$. Rewrite as: $-(\ell^2 - m^2)^2 - 2m^4$ This is impossible in $\mathbb{R}$ (the left hand side is $\leqslant 0$ and the right hand side is $\geqslant 0$, and eq only occurs when $\ell^2 - m^2 = m^4 = n^2 = 0$, implying $\ell = m = n = 0$, which is not allo Hence $-1 \notin \text{im}\hat{q}$.

We conclude that 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 $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ i erated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $(0, 0)$] together with the images $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0, 0)\big) = \mathbf{o}$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}$ 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 is phic to $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q}) \times C_2^r$, which is isomorphic to $\mathcal{C}(\mathbb{Q})[2] \times C_2^r$, where $\mathcal{C}(\mathbb{Q}$ the 2-torsion group and r is the rank. The 2-torsion points on $\mathcal{C} : Y^2 = X(X^2 + 2X$ are $\mathbf{o}$ together with the points of the form $(x, 0)$, where x is a root of $X(X^2 + 2X$ that is: $(0, 0)$, $(-1 + \sqrt{-2}, 0)$ and $(-1 + \sqrt{-2}, 0)$, of which only $\mathbf{o}$ and $(0, 0)$ are in $\mathcal{C}($ giving that $\mathcal{C}(\mathbb{Q})[2]$ is isomorphic to C_2. Combining this with the facts (already f 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 r

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

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

There is only one coset to check, represented by -1, say. We know that $-1 \in$ i
there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1)\cdot\ell^4 + a_1\ell$
$(b_1/(-1))\cdot m^4 = n^2$ that is: $-\ell^4 - 28\ell^2m^2 - 192m^4 = n^2$. We can see that the LHS is $\leqslant$
the RHS is $\geqslant 0$, and there is equality iff $\ell = m = n = 0$, a contradiction. Hence $-1 \notin$
We conclude that im$q = \{1, 2, 3, 6\}$ and that $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\mathbf{o}, (0, 0), (8, 16), (24, -$
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 $(u, v) \neq (0, 0)$
$\hat{q} : (0, 0) \mapsto a_1^2 - 4b_1 = b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with im$\hat{q}$ contained in
d is square free and $d|b\} = \{\pm1\}$. Also, $\mathbf{o} \mapsto 1$ and $(0, 0) \mapsto 1$, so that $\{1\} \subset$ im$\hat{q} \subset$

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

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

Finally, since multiplication by 2 in $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi} \circ \phi$, we have that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ i
erated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $\mathbf{o}$] together with the images unde
generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0, 0)\big) = \mathbf{o}$ and $\hat{\phi}\big((8, 16)\big) = (1, -4)$]. Concl
$\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(1, -4)$, and so is the group C_2. Now $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is is

phic 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-t
group of $\mathcal{C}_{\text{tors}}(\mathbb{Q})$ which is C_2 (consisting only of $\mathbf{o}$ and $(0,0)$), so that $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{t}}$
is isomorphic to C_2. Conclusion: rank $= 0$. [If this seems surprising, then not
$(1,4), (1,-4)$ are points of order 4 in $\mathcal{C}(\mathbb{Q})$].

2. We are given that $A, +$ is an Abelian group, and that $h : A \to \mathbb{R}_{\geqslant 0}$ satisfies:
(I) There exists a constant C, independent of P, Q, such that
$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| \leqslant C$, for all $P, Q \in A$,
(II) For any $B \in \mathbb{R}$, the set $\{P \in A : h(P) \leqslant B\}$ is finite.

From (I) we obtain: $h(P+Q) + h(P-Q) - 2h(P) - 2h(Q) \leqslant C$ and so
$h(P-Q) \geqslant 0$): $h(P+Q) \leqslant h(P+Q) + h(P-Q) \leqslant 2h(P) + 2h(Q) + C \leqslant 2h(P) + C$
where $C_1(Q) = 2h(Q) + C$. Hence Property (1) in the definition of height funct
satisfied.

Letting $Q = P$ in (I), we obtain:
$$|h(2P) + h(e) - 4h(P)| \leqslant C, \quad (*)$$
where e denotes the identity element of the group A. This gives: $h(2P) + h(e) - 4h$
$-C$, and so: $h(2P) \geqslant 4h(P) - C_2$, where $C_2 = C + h(e)$. Hence Property (2)
definition of height function is satisfied. Furthermore, (II) is the same as Property
the definition of height function. Hence all 3 required properties are satisfied, giving
is a height function, as required.

Replacing P, Q in (I) with $2P, P$, respectively, gives:
$$|h(3P) - 2h(2P) - h(P)| \leqslant C.$$
Multiplying $(*)$ by 2 gives:
$$|2h(2P) + 2h(e) - 8h(P)| \leqslant 2C.$$
These last two equations then give:
$$|h(3P) - 9h(P)| = |h(3P) - 2h(2P) - h(P) + 2h(2P) + 2h(e) - 8h(P) - 2h(e)|$$
$$\leqslant |h(3P) - 2h(2P) - h(P)| + |2h(2P) + 2h(e) - 8h(P)| + 2|h(e)| \leqslant C_3,$$
where $C_3 = 3C + 2|h(e)|$ (which is independent of P).

3. In all of the following, each step multiplies numbers $\leqslant N$ (followed by a p
reduction modulo N), and so we are guaranteed that everything can be done on an
calculator, since N^2 has only 9 digits.
(a). First compute (modulo $N = 10481$): $2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 256$, $2^{16} \equiv$
$2^{32} \equiv 230$ (where each of these was obtained be squaring the previous one, and re
modulo N). Now, we write 46 in base 2: $46 = 2 + 4 + 8 + 32$ and so $2^{46} \equiv 2^2 2^4 2^8$
$4 \cdot 16 \cdot 256 \cdot 230 \equiv 64 \cdot 6475 \equiv 5641$ modulo N, so that $2^{46} - 1 \equiv 5640$ modulo N.

Now, compute $\gcd(5640, N)$ by Euclid's Algorithm: $10481 = 1 \cdot 5640 + 4841$; 5
$1 \cdot 4841 + 799$; $4841 = 6 \cdot 799 + 47$, $799 = 17 \cdot 47 + 0$. So, 47 is a factor of N. Co
$10481/47 = 223$, giving the factorisation $N = 10481 = 47 \cdot 223$.
(b). The line tangent to $\mathcal{E}$ at $P = (5, 11)$ has slope y' given by $2yy' = 3x^2 - 1$
$x = 5, y = 11$; that is, the slope is $74/22 = 37/11$. This tangent line also goes th
$(5, 11)$ and so has equation: $Y = (37/11)X - 64/11$. The x-coordinate of $2P$ is the
$(37/11)^2 - (5 + 5) = 159/121$. [It will turn out not to be necessary to evaluat
mod N, although if this is done using EA, then it is 7364], and the y-coordina

$-((37/11)\cdot(159/121)-(64/11)) = 1861/1331$ [again, although unnecessary in this exa
this can be computed by EA to be: 6679 mod N], so that $Q = 2P = (159/121, 1861/$
We now wish to compute $3P = P + Q$, and so again the first step is to find the line j
P and Q. This has slope given by $(1861/1331 - 11)/(159/121 - 5) = 6930/2453$, a
we need to compute $6930/2453$ (modulo $N = 10481$), for which the first step is to fi
inverse of 2453 (modulo $N = 10481$). Using Euclid's Algorithm: $10481 = 4 \cdot 2453 +$
$2453 = 3 \cdot 669 + 446$; $669 = 1 \cdot 446 + 223$; $446 = 2 \cdot 223 + 0$. So, we cannot find the i
of 2453 (modulo $N = 10481$), and this step has given us a factor 223 of N. As b
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 $d =$
and $\phi(N)$, we see: $10212 = 2 \cdot 4085 + 2042$; $4085 = 2 \cdot 2042 + 1$, so that $\gcd(10212, 4085$
Reversing the steps: $1 = 4085 - 2 \cdot 2042 = 4085 - 2 \cdot (10212 - 2 \cdot 4085) = 5 \cdot 4085 - 2 \cdot$
Hence, 5 is the inverse of 4085 modulo 10212. The decoding operation is therefore
$X^5 \bmod N$. Computing $6012^5 = (6012^2)^2 \cdot 6012 \equiv 5656^2 \cdot 6012 \equiv 2324 \cdot 6012 \equiv$
(modulo $N = 10481$). Also: $3236^5 = (3236^2)^2 \cdot 3236 \equiv 1177^2 \cdot 3236 \equiv 1837 \cdot 3236 \equiv$
(modulo $N = 10481$). The decoded message is therefore: 0715, 1805; that is: GORI

Elliptic Curves. Solutions to Sheet 8.
Solutions to the Exam-style Questions.

Question 1.

(i). Let $x_0 = a_0 = 2$. Then $|x_0^2 + 3|_7 = 7^{-1}$. Look for $x_1 = a_0 + 7a_1$ such $|x_1^2 + 3|_7 \leqslant 7^{-2}$. This is satisfied if: $(2 + 7a_1)^2 \equiv -3 \pmod{7^2} \iff 2 \cdot 2 \cdot$ $-3 - 2^2 \pmod{7^2} \iff 4a_1 \equiv -1 \pmod 7 \iff a_1 \equiv 5 \pmod 7$. So, now define: a and $x_1 = a_0 + 7a_1 = 37$. Check that indeed $|x_1^2 + 3|_7 = |1372|_7 = 7^{-3} < 7^{-1}$. **[5 ma**

(ii). Compute $1, \overline{2} = 1 + 2p + 2p^2 + 2p^3 + \ldots = 1 + 2p(1 + p + p^2 + \ldots) = 1 + 2p/(1 -$ $(1+p)/(1-p)$. So, $1, \overline{2} = -9/8 \iff (1+p)/(1-p) = -9/8 \iff 8(1+p) = -9(1-p)$ $p = 17$. **[3 marks]**

(iii). We are given that $p \equiv 1 \pmod 3$. Then $p \neq 2$, so p is odd, and so satisfies $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. In the first case, we have that $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{p}{3}\right.$ [by quadratic reciprocity] $= \left(\frac{1}{p}\right)\left(\frac{-1}{3}\right) = 1 \cdot 1$ [using the result from notes that $\left(\frac{-1}{p}\right.$ when $p \equiv 1 \pmod 4$]. In the second case, $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = -\left(\frac{p}{3}\right)\left(\frac{-1}{p}\right)$ [by qua reciprocity] $= -\left(\frac{1}{3}\right)\left(\frac{-1}{p}\right) = -1 \cdot (-1)$ [using the result from notes that $\left(\frac{-1}{p}\right) = 1$ $p \equiv 1 \pmod 4$]. In either case, we have that $\left(\frac{-3}{p}\right) = 1$, as required. We may app general rule from lectures (which follows easily from Hensel's Lemma) that, if $p \neq$ $|a|_p = 1$, then a is a square in $\mathbb{Q}_p^*$ iff a is a quadratic residue in $\mathbb{F}_p$. Hence -3 is a s in $\mathbb{Q}_p^*$. **[6 marks]**

(iv). For $p \equiv 2 \pmod 3$, note that 3 is coprime to $p - 1$, and so there exist λ, such that $(p-1)\lambda + 3\mu = 1$. Now, suppose that $v^3 = w^3$ in $\mathbb{F}_p^*$. Then $v^{3\mu} = w^{3\mu}$ $(p-1)\lambda$ is a multiple of the order of the group $\mathbb{F}_p^*$ and so $v^{(p-1)\lambda} = w^{(p-1)\lambda}$ (since are equal to 1). Multiplying these last two equations gives: $v^{(p-1)\lambda+3\mu} = w^{(p-1)\lambda+3}$ so $v = w$. We have shown that $v^3 = w^3$ implies $v = w$, and so the map $v \mapsto v^3$ is inj and hence surjective (and hence bijective), from $\mathbb{F}_p^*$ to $\mathbb{F}_p^*$. Since also $0 \mapsto 0^3$, th $v \mapsto v^3$ must also be a bijection from $\mathbb{F}_p$ to $\mathbb{F}_p$. For any $d \in \mathbb{Z}$ not divisible by 3, it f that there exists $x_0 \in \mathbb{Z}$ such that $x_0^3 \equiv d \pmod p$. This is the same as $|f(x_0)|_p$ where $f(x) = x^3 - d$. But from the fact that d is not divisible by p and $x_0^3 \equiv d \pmod$ follows that x_0 is not divisible by p, and so $|x_0|_p = 1$, giving that $|f'(x_0)|_p = |3x_0^2|$ Therefore, $|f(x_0)|_p < |f'(x_0)|_p^2$ and so, by Hensel's Lemma, there exists a solution to $x^3 - d$; that is, d is a cube in $\mathbb{Q}_p$, for any $d \in \mathbb{Z}$ not divisible by 3.

We have already established in (c) that $X^2 + 3 = 0$ has a solution $\mathbb{Q}_p$ for $p \equiv 1 \pmod 3$, and we have already established (immediately above), since the g is not divisible by 3, that $X^3 - q = 0$ has a solution $\mathbb{Q}_p$ for every $p \equiv 2 \pmod 3$ $p = 3$, note that we are given $q \equiv 1 \pmod{27}$, so that $|f(x_0)|_3 \leqslant 3^{-3}$, where $x_0 =$ $f(x) = x^3 - q$. Also, $|f'(x_0)|_3 = |3 \cdot 1^2| = 3^{-1}$, so that $|f(x_0)|_3 < |f'(x_0)|_3^2$. By H Lemma, it follows that there exists a solution in $\mathbb{Q}_3$ to $X^3 - q = 0$. Finally note since $q > 0$, there exists a solution to $X^3 - q = 0$ in $\mathbb{R}$. Hence there is a solut $(X^2 + 3)(X^3 - q) = 0$ in $\mathbb{R}$ and every $\mathbb{Q}_p$, as required. **[11 marks]**

Question 2.

(i). Let $\mathcal{C}$ be the elliptic curve $Y^2 = X^3+3$. The discriminant of X^3+3 is $4\cdot 0^3+27\cdot 3^2$ and so $\widetilde{\mathcal{C}} : Y^2 = X^3 + 3$ is an elliptic curve for all $p \neq 2, 3$. The elements of are: $\mathbf{o}, (1, \pm 2), (2, \pm 1), (3, 0)$, and so $\widetilde{\mathcal{C}}(\mathbb{F}_5)$ has order 6. The elements of $\widetilde{\mathcal{C}}(\mathbb{F}_7$ $\mathbf{o}, (1, \pm 2), (2, \pm 2), (3, \pm 3), (4, \pm 2), (5, \pm 3), (6, \pm 3)$, and so $\widetilde{\mathcal{C}}(\mathbb{F}_7)$ has order 13. Since tl sion subgroup of $\mathcal{C}(\mathbb{Q})$ injects into both of these groups, its order must divide $\gcd(6, 1$ and so equal 1. Hence the torsion subgroup of $\mathcal{C}(\mathbb{Q})$ is precisely $\{\mathbf{o}\}$. **[5 marks]**

(ii). Let $\mathcal{D}$ be the elliptic curve $Y^2 = X^3 + 4X$. Then $\mathbf{o}$ and $(0, 0)$ [which has or are both members of the torsion subgroup. Furthermore, consider the point $(2, 4) \in$ the tangent to $\mathcal{D}$ at $(2, 4)$ has slope $(3 \cdot 2^2 + 4)/(2 \cdot 4) = 2$ and has equation $Y =$ So, the x-coordinate of $2(2, 4)$ is $2^2 - 2 - 2 = 0$, with corresponding y-coordin giving: $2(2, 4) + (0, 0) = \mathbf{o}$ and so $2(2, 4) = -(0, 0) = (0, 0)$. Hence $4(2, 4) = 2(0, 0$ similarly $4(2, -4) = \mathbf{o}$. We have found 4 torsion elements: $\mathbf{o}, (0, 0), (2, 4), (2, -4),$ a the torsion subgroup is of order at least 4. The discriminant of X^3+4X is $4\cdot 4^3+27\cdot 0^2$ and so $\widetilde{\mathcal{D}} : Y^2 = X^3 + 4X$ is an elliptic curve for all $p \neq 2$. The elements of $\widetilde{\mathcal{D}}(\mathbb{F}_3$ $\mathbf{o}, (0, 0), (2, \pm 1)$, and so $\widetilde{\mathcal{D}}(\mathbb{F}_3)$ has order 4. Since the torsion subgroup of $\mathcal{D}(\mathbb{Q})$ injec this groups, its order must divide 4. Hence the torsion subgroup of $\mathcal{D}(\mathbb{Q})$ consists pr of the 4 torsion elements already found, namely: $\{\mathbf{o}, (0, 0), (2, \pm 4)\}$. **[6 marks]**

(iii). Let $\mathcal{F}$ be the elliptic curve $Y^2 = X(X + 1)(X + n^2) = X^3 + (n^2 + 1)X^2 +$ The tangent to $\mathcal{D}$ at $(n, n(n + 1))$ has slope $(3n^2 + 2(n^2 + 1)n + n^2)/(2n(n + 1)) =$ and so equation $Y = (n + 1)X + c$ for some c; the line must pass through $(n, n(n$ so that $c = 0$ and the equation of the tangent is: $Y = (n + 1)X$. The x-coor of $P = 2(n, n(n + 1))$ is $(n + 1)^2 - (n^2 + 1) - 2n = 0$, with y-coordinate $(n + 1)$ 0. Hence $2(n, n(n + 1)) + (0, 0) = \mathbf{o}$, so that $2(n, n(n + 1)) = -(0, 0) = (0, 0)$, $4(n, n(n+1)) = \mathbf{o}$. So $(n, n(n+1))$ is torsion, as must be $(n, -n(n+1)) = -(n, n(n$ Replacing every occurrence of n with $-n$ gives that the tangent to $\mathcal{D}$ at $(-n, n(n$ has equation $Y = (-n + 1)X$ and $2(-n, n(n - 1)) = (0, 0)$; we deduce, as before $(-n, \pm n(n - 1))$ are torsion elements. Therefore there are at least 8 members torsion subgroup of $\mathcal{F}(\mathbb{Q})$, namely: $\mathbf{o}, (0, 0), (-1, 0), (-n^2, 0)$ and the above 4 poi order 4. Finally, let $n \equiv 2$ (modulo 5), so that $n^2 \equiv 4$ (modulo 5). Then $\widetilde{\mathcal{F}}$ modul $Y^2 = X(X+1)(X+4)$, and the cubic has no repeated roots, so that f has good red at 5. The elements of $\widetilde{\mathcal{F}}(\mathbb{F}_5)$ are: $\mathbf{o}, (0, 0), (1, 0), (2, \pm 1), (3, \pm 2), (4, 0)$, and so $\widetilde{\mathcal{F}}(\mathbb{F}$ order 8. Since the torsion subgroup of $\mathcal{F}(\mathbb{Q})$ injects into this groups, its order must di Hence the torsion subgroup of $\mathcal{F}(\mathbb{Q})$ consists precisely of the 8 torsion elements a found, namely: $\{\mathbf{o}, (0, 0), (-1, 0), (-n^2, 0), (n, \pm n(n + 1)), (-n, \pm n(n - 1))\}$. **[7 mar**

(iv). The disciminant of $X^3 - k^2X + k^3$ is $4 \cdot (-k^2)^3 + 27 \cdot (k^3)^2 = 23k^6$. If (x, y) i rational torsion point on $\mathcal{E} : Y^2 = X^3-k^2X+k^3$, then we know by Nagell-Lutz that x, with $y^2|23k^6$ and so $|y|^2 \leqslant 23|k|^6$; that is: $|y| \leqslant \sqrt{23}|k|^3 = (4.79583\ldots)|k|^3 \leqslant 5|k|^3$.

We cannot have $k = 0$ since then the discriminant would be 0 and $\mathcal{E}$ would not elliptic curve. Since $k \in \mathbb{Z}$, we have $|k| \geqslant 1$ and so: $|k|^2 \leqslant |k|^4$ and $|k|^3 \leqslant |k|^6$.

Imagine $|x| > 3|k|^2$. Then: $|x^2 - k^2| \geqslant |x^2| - |k^2| > 9|k|^4 - |k^2| \geqslant 9|k|^4 - |k^4| = 8|k$ $|y|^2 = |x(x^2-k^2)+k^3| \geqslant |x(x^2-k^2)|-|k^3| = |x||x^2-k^2|-|k^3| > 3|k|^2 8|k|^4-|k|^6 =$ contradicting $|y|^2 \leqslant 23|k|^6$ (above). Hence $|x| \leqslant 3|k|^2$, as required. **[7 marks]**

Question 3.

(i). Let $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2, r \in \operatorname{im} q, r \in \mathbb{Z}, r$ square free. We want to prove that $r|b_1$. Su
$r = q(u,v)$, where $(u,v) \in \mathcal{D}(\mathbb{Q})$, which must exist since $r \in \operatorname{im} q$. Then: $r = q(u$
$u = u^2 + a_1u + b_1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ [since $u(u^2 + a_1u + b_1) = v^2$]. So, $r, u, u^2 + a_1u + b_1$
the same modulo squares, which means we can write:

$$u^2 + a_1u + b_1 = rs^2, \quad u = rt^2, \quad \text{for some } s,t \in \mathbb{Q}.$$

Hence: $(rt^2)^2 + a_1(rt^2) + b_1 = rs^2$. Let $t = \ell/m$, where $\ell, m \in \mathbb{Z}$ and $\gcd(\ell, m)$
Then: $r^2\ell^4/m^4 + a_1r\ell^2/m^2 + b_1 = rs^2$, and so: $r^2\ell^4 + a_1r\ell^2m^2 + b_1m^4 = r(m^2s)^2$.
$a_1, b_1, r, \ell, m \in \mathbb{Z}$, so the LHS of this last equation is in $\mathbb{Z}$, and so the RHS is also
that is: $r(m^2s)^2 \in \mathbb{Z}$. Since r is square free, we must therefore have $m^2s \in \mathbb{Z}$. I
$n = m^2s \in \mathbb{Z}$. Then our equation becomes:

$$r^2\ell^4 + a_1r\ell^2m^2 + b_1m^4 = rn^2, \quad \text{for some } \ell, m, n \in \mathbb{Z},\ \gcd(\ell, m) = 1.$$

We want to show that $r|b_1$, and we know that r is square free. It is sufficient to sho
any prime p, that $p|r \Rightarrow p|b_1$.

Imagine $p|r$ and $p \nmid b_1$, for some prime p. Then $p|r^2\ell^4, a_1r\ell^2m^2, rn^2$ and so b
$p|b_1m^4$, which in turn gives: $p|m$ [since $p \nmid b_1$]. Hence, since now $p|r$ and $p|$
have: $p^2|r^2\ell^4, a_1r\ell^2m^2, b_1m^4$, and so by (†), $p^2|rn^2$, which in turn gives: $p|n$ [s
is square free]. Hence, since now $p|r, m, n$, we have: $p^3|a_1r\ell^2m^2, b_1m^4, rn^2$, and
(†), $p^3|r^2\ell^4$, which in turn gives: $p|\ell$ [since r is square free]. This is a contradi
since $p|\ell$ and $p|m$ but $\gcd(\ell, m) = 1$.

The above assumption that $p|r$ and $p \nmid b_1$ let to a contradiction, and so it is impossil
any prime p to satisfy $p|r$ and $p \nmid b_1$. This is the same as saying that $p|r \Rightarrow p|b_1$ fo
prime p. Since r is square free, we conclude that $r|b_1$, as required **[13 marks]**

(ii) Let $\mathcal{C} : Y^2 = X(X^2 + aX + b) = X(X^2 + 2X + 3)$, where $a = 2, b = 3$, and isog
curve $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1) = X(X^2 - 4X - 8)$, where $a_1 = -4, b_1 = -8$
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 is
$\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) : (u,v) \mapsto (\frac{1}{4}v^2/u^2, \frac{1}{8}(v + 8v/u^2))$.

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u,v) \mapsto u$, for $(u,v) \neq$
with $q : (0,0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, is an injection with im$q$ contained in
d is square free and $d|b_1\} = \{\pm 1, \pm 2\}$. Also, $\mathbf{o} \mapsto 1$, $(0,0) \mapsto -8 = -2$, so
$\{1, -2\} \subset \text{im}q \subset \{\pm 1, \pm 2\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in$ i
there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1)\cdot\ell^4 + a_1\ell$
$(b_1/(-1))\cdot m^4 = n^2$ that is: $-\ell^4 - 4\ell^2m^2 + 8m^4 = n^2$. Rewrite as: $-(\ell^2 + 2m^2)^2 + 12m^4$
Reducing modulo 3 gives $-(\ell^2 + 2m^2)^2 \equiv n^2$ (modulo 3). If n were coprime to 3, the
would give: $((\ell^2 + 2m^2)/n)^2 = -1$ in $\mathbb{F}_3$, contradicting the fact that -1 is not a qua
residue modulo 3. So, $3|n$ and so $3|(\ell^2 + 2m^2)$ also. This means that $9|(\ell^2 + 2m^2)$
$9|n^2$, which can be combined with $-(\ell^2 + 2m^2)^2 + 12m^4 = n^2$ to give: $9|12m^4$ a
$3|m$. Combining $3|m$ with $3|(\ell^2 + 2m^2)$ gives that $3|\ell$. This contradicts the fac

$\gcd(\ell, m) = 1$. Hence our equation is impossible in $\mathbb{Q}_3$, and so impossible in $\mathbb{Q}$. $-1 \notin \text{im}q$.

We conclude that $\text{im}q = \{1, -2\}$, 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 $(x, y) \neq$ with $\hat{q} : (0, 0) \mapsto b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with $\text{im}\hat{q}$ contained in d is square free and $d|b\} = \{\pm 1, \pm 3\}$. Also, $\mathbf{o} \mapsto 1$ and $(0, 0) \mapsto 3$, so that $\{1$ $\text{im}\hat{q} \subset \{\pm 1, \pm 3\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in$ i there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a\ell$ $(b/(-1)) \cdot m^4 = n^2$; that is: $-\ell^4 + 2\ell^2 m^2 - 3m^4 = n^2$. Rewrite as: $-(\ell^2 - m^2)^2 - 2m^4$ This is impossible in $\mathbb{R}$ (the left hand side is $\leqslant 0$ and the right hand side is $\geqslant 0$, and eq only occurs when $\ell^2 - m^2 = m^4 = n^2 = 0$, implying $\ell = m = n = 0$, which is not allo Hence $-1 \notin \text{im}\hat{q}$.

We conclude that $\text{im}\hat{q} = \{1, 3\}$, 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 $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ i erated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $(0, 0)$] together with the images $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0, 0)\big) = \mathbf{o}$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}$ 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 is phic to $\mathcal{C}_{tors}(\mathbb{Q})/2\mathcal{C}_{tors}(\mathbb{Q}) \times C_2^r$, which is isomorphic to $\mathcal{C}(\mathbb{Q})[2] \times C_2^r$, where $\mathcal{C}(\mathbb{Q}$ the 2-torsion group and r is the rank. The 2-torsion points on $\mathcal{C} : Y^2 = X(X^2 + 2X$ are $\mathbf{o}$ together with the points of the form $(x, 0)$, where x is a root of $X(X^2 + 2X$ that is: $(0, 0)$, $(-1 + \sqrt{-2}, 0)$ and $(-1 + \sqrt{-2}, 0)$, of which only $\mathbf{o}$ and $(0, 0)$ are in $\mathcal{C}($ giving that $\mathcal{C}(\mathbb{Q})[2]$ is isomorphic to C_2. Combining this with the facts (already f 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 r

[12 m

Question 4.

(i). First compute (modulo $N = 10001$): $2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 256$, $2^{16} \equiv$ $2^{32} \equiv 7843$, $2^{64} \equiv 6499$ (where each of these was obtained be squaring the previou and reducing modulo N). Now, we write 68 in base 2: $68 = 4 + 64$ and so $2^{68} \equiv 2^4$ $16 \cdot 6499 \equiv 3974$ modulo N, so that $2^{68} - 1 \equiv 3973$ modulo N.

Now, compute $\gcd(3973, N)$ by Euclid's Algorithm: $10001 = 2 \cdot 3973 + 2055$; 3 $1 \cdot 2055 + 1918$; $2055 = 1 \cdot 1918 + 137$, $1918 = 14 \cdot 137 + 0$. So, 137 is a factor of N. Co $10001/137 = 73$, giving the factorisation $N = 10001 = 73 \cdot 137$. **[5 marks]**

(ii). Since $N = 73 \cdot 137$, we have $\phi(N) = 72 \cdot 136 = 9792$. Computing the gcd of $d =$ and $\phi(N)$, we see: $9792 = 2 \cdot 4451 + 890$; $4451 = 5 \cdot 890 + 1$, so that $\gcd(9792, 4451$ Reversing the steps: $1 = 4451 - 5 \cdot 890 = 4451 - 5 \cdot (9792 - 2 \cdot 4451) = -5 \cdot 9792 + 11$ Hence, 11 is the inverse of 4451 modulo 9792. The decoding operation is therefore X^{11} mod N. Computing $6847^{11} = ((6847^2)^2)^2 \cdot (6847^2 \cdot 6847) \equiv (6722^2)^2 \cdot (6722 \cdot 68$ $766^2 \cdot 932 \equiv 6698 \cdot 932 \equiv 1912$. (modulo $N = 10001$). Also: $2577^{11} = ((2577^2)^2)^2 \cdot (2$ $2577) \equiv (265^2)^2 \cdot (265 \cdot 2577) \equiv 218^2 \cdot 2837 \equiv 7520 \cdot 2837 \equiv 2107$ (modulo $N = 1$ The decoded message is therefore: 1912, 2107; that is: SLUG. **[5 marks]**

(iii). We are given that $A/2A$ is finite, so let $A/2A = S = \{Q_1, \ldots Q_r\} \subset A$. Let P l
element of A. Then $P = Q_{i_1}$ in $A/2A$ for some $Q_{i_1} \in S$ and so we can write: $P = 2P_1$
for some $P_1 \in A$. Indusctively, continue to write: $P_1 = 2P_2 + Q_{i_2}, P_2 = 2P_3 + Q$
where each $P_j \in A$ and each $Q_{i_j} \in S$. Now:
$h(P_j) \leqslant \frac{1}{4}\big(h(2P_j) + C_2\big)$ [by (2)] $= \frac{1}{4}\big(h(P_{j-1} - Q_{i_j}) + C_2\big) \leqslant \frac{1}{4}\big(2h(P_{j-1}) + C_1'$
[by (1)], where:
$C_1' = \max\{C_1(-Q) : Q \in S\}$. So, if $h(P_{j-1}) > (C_1' + C_2)/2$ then $h(P_j) < \frac{1}{4}\big(2h(P_j$
$2h(P_{j-1})\big) = h(P_{j-1})$.

Imagine that $h(P) > (C_1' + C_2)/2$ and $h(P_j) > (C_1' + C_2)/2$ for all j.
$h(P), h(P_1), h(P_2), \ldots$ would be a strictly decreasing sequence, giving infinitely mar
tinct members of A with height $\leqslant h(P)$, which would contradict (3). This contrad
show that there must exists an n such that $h(P_n) \leqslant (C_1' + C_2)/2$. So, we can
$P = 2P_1 + Q_{i_1} = 2(2P_2 + Q_{i_2}) + Q_{i_1} = \ldots$, and after n steps P will be written as a
combination of P_n and members of S. Let $T = \{Q \in A : h(Q) \leqslant (C_1' + C_2)/2\}$
have shown (since $P_n \in T$) that any $P \in A$ is a linear combination of members of $
Furthermore, T is finite, by (3). In conclusion: A is generated by the finite set $S \cup T$
so is finitely generated. **[10 marks]**

(iv). Suppose that $h(P) > \frac{1}{3}C_2$. Then $C_2 < 3h(P)$ and so by (2): $h(2P) \geqslant 4h(P) -$
$4h(P) - 3h(P) = h(P)$. Inductively: $h(P) < h(2P) < h(4P) < \ldots$, so that $P, 2P,$
are all distinct, which forces P to have infinite order (since otherwise P would gene
finite group). Hence, if P is a torsion element then $h(P) \leqslant \frac{1}{3}C_2$. **[5 marks]**

Solutions to the 2006 Examination Questions.

Question 1.

(i) [*Proof from lectures*]. Define $f_j(x)$ by:

$$f(x+y) = f_0(x) + f_1(x)y + f_2(x)y^2 + \ldots,$$

so that $f_0(x) = f(x), f_1(x) = f'(x)$. Define $b_0 = -f(a_0)/f'(a_0)$. By $(*)$, $|b_0| < 1$.

Define $a_1 = a_0 + b_0 = a_0 - f(a_0)/f'(a_0)$. Then:

$$|f'(a_1) - f'(a_0)| = |f'(a_0 + b_0) - f'(a_0)| = |(\text{poly in } a_0)b_0 + (\text{poly in } a_0)b_0^2 + \ldots$$
$$\leqslant |b_0| < |f'(a_0)|,$$

so that $|f'(a_1)| = |f'(a_0)|$.

Also, $|f(a_1)| = |f(a_0 + b_0)||f_0(a_0) + f_1(a_0)b_0 + f_2(a_0)b_0^2 + \ldots|$
$= |f_2(a_0)b_0^2 + \ldots|$ [since $f_0(a_0) + f_1(a_0)b_0 = 0$]
$\leqslant \max_{j \geqslant 2}|f_j(a_0)||b_0|^j \leqslant |b_0|^2 = \frac{|f(a_0)|^2}{|f'(a_0)|^2} = \rho|f(a_0)| < |f(a_0)|,$

where $\rho = \frac{|f(a_0)|}{|f'(a_0)|^2} < 1$.

Summarising: $|f'(a_1)| = |f'(a_0)|$ and $|f(a_1)| \leqslant \rho|f(a_0)| < |f(a_0)|$, where
$\frac{|f(a_0)|}{|f'(a_0)|^2} < 1$.

Given $a_n \in R$, define $b_n = -f(a_n)/f'(a_n)$ and $a_{n+1} = a_n + b_n = a_n - f(a_n)/f'(a_n)$

Assume, as induction hypothesis, that:

$|f'(a_n)| = \ldots = |f'(a_1)| = |f'(a_0)|$ and $|f(a_n)| \leqslant \rho|f(a_{n-1})| \leqslant \ldots \leqslant \rho^n|f(a_0)|$.

Then, as above: $|f'(a_{n+1})| = \ldots = |f'(a_1)| = |f'(a_0)|$.

Then $|f(a_{n+1})| \leqslant |b_n|^2$ [justified as for the case $n = 0$ above]

$= \frac{|f(a_n)|^2}{|f'(a_n)|^2} = \frac{|f(a_n)|^2}{|f'(a_0)|^2}$ [by (1), the induction hypothesis]

$\leqslant \frac{|f(a_0)|^2}{|f'(a_0)|^2}|f(a_0)|$ [since $|f(a_n)| \leqslant |f(a_0)|$ by (1), the ind

hypothesis]

$= \rho|f(a_0)| \leqslant \rho^{n+1}|f(a_0)|$ [by (1), the induction hypothesis].

By induction, $\forall n$, $|f'(a_n)| = |f'(a_0)|$ and $|f(a_n)| \leqslant \rho^n|f(a_0)|$ which $\to 0$ as $n \to \infty$.

Now, $|b_n| = |f(a_n)|/|f'(a_n)| = |f(a_n)|/|f'(a_0)| \to 0$, so [by the theorem from lecture a series converges in a non-Archimedean field iff its terms converge to 0]:

$a_n = a_0 + b_0 + b_1 + \ldots + b_n$ converges to a, say.

By continuity of polynomials, $f(a) = \lim f(a_n) = 0$ [by (2)].

Furthermore: $|a - a_0| = |\sum b_n| \leqslant \max|b_n| = \max \frac{|f(a_n)|}{|f'(a_n)|} = \max \frac{|f(a_n)|}{|f'(a_0)|} = \frac{|f(a_0)|}{|f'(a_0)|}$ required.

Imagine that $\hat{a} \neq a$ also satisfied $f(\hat{a}) = 0$ and $|\hat{a} - a_0| \leqslant |f(a_0)|/|f'(a_0)|$. Let $\hat{b} = \hat{a}$

Then $0 = f(\hat{a}) - f(a) = f(a + \hat{b}) - f(a) = \hat{b}f_1(a) + \hat{b}^2 f_2(a) + \ldots$ (3)

But $|\hat{b}| = |\hat{a} - a_0 + a_0 - a| \leqslant \max(|\hat{a} - a_0|, |a - a_0|) \leqslant |f(a_0)|/|f'(a_0)|$

$< |f'(a_0)| = |f_1(a_0)| = |f_1(a)|$ [by (1) and continuity of $|f'(x)|$].

This gives $|\hat{b}^j f_j(a)| \leqslant |\hat{b}^j| \leqslant |\hat{b}^2| < |\hat{b}f_1(a)|$ for $j \geqslant 2$, so that the leading term sum in (3) has valuation strictly greater than the valuations of the other terms, wh inconsistent with the sum being 0. Hence a is unique. **[10 m**

(ii) [*They have seen a variation on an exercise sheet, although this one is substa harder*]. For $p = 2$, can see the equation becomes $-y^2 \equiv 2 \pmod 4$, which is impo since $y \equiv 0, 1, 2, 3$ give $y^2 \equiv 0, 1, 0, 1$, respectively. Hence, there are no such x, y For $p = 3$, take $x = 1$, in which case we want $y \in \mathbb{Z}_3$ such that $3y^2 = -6$, t $f(y) = y^2 + 2 = 0$. But $a_0 = 1$ gives $|f(a_0)|_3 = 3^{-1}$ and $|f'(a_0)| = 1$, so by H Lemma, there exists $y \in \mathbb{Z}_3$ which is a root of f. For $p = 5$, take $x = 2$, in whic we want $y \in \mathbb{Z}_5$ such that $g(y) = 3y^2 - 22 = 0$. But $a_0 = 2$ gives $|g(a_0)|_5 = 5^-$ $|g'(a_0)| = 1$, so by Hensel's Lemma, there exists $y \in \mathbb{Z}_5$ which is a root of g. For take $y = 0$, in which case we want $x \in \mathbb{Z}_7$ such that $h(x) = (4x^3 - 10)/3 = 0$. But a_0 gives $|h(a_0)|_7 = 7^{-1}$ and $|h'(a_0)| = 1$, so by Hensel's Lemma, there exists $x \in \mathbb{Z}_7$ w a root of h. For $p \geqslant 11$, the curve is an elliptic curve mod p [since the only bad prim $2, 3, 5$] and $\#\widetilde{\mathcal{E}}(\mathbb{F}_p) \geqslant p + 1 - 2\sqrt{p} > 5$. At most 4 of these are 2-torsion, so there exi such that $h(x_0)$ is a nonzero residue mod p; applying Hensel's Lemma to $y^2 - h(x_0)$ the existence of a corresponding $y \in \mathbb{Z}_p$. In summary, there exist such $x, y \in \mathbb{Z}_p$ fo except 2. **[7 m**

(iii) [*Unseen*]. We may apply the general rule from lectures (which follows easily Hensel's Lemma) that, if $p \neq 2$ and $|\alpha|_p = 1$, then α is a square in $\mathbb{Q}_p^*$ iff α is a qua residue in $\mathbb{F}_p$. An element $\alpha \in (\mathbb{Q}_p^*)^2$ iff (both $|\alpha|_p = p^r$ for r even and the leadin a_r of α is a quadratic residue mod p) [N.B. if $|\alpha|_p = p^r$ for r odd, then $\alpha \neq \beta^2$ f β, since $|\beta|_p = p^s$ for some integer s]. Let $H_1 = (\mathbb{Q}_p^*)^2$, and fix a quadratic nonr

mod 5, say γ. Let $H_2 = \gamma H_1$, $H_3 = pH_1$, $H_4 = \gamma pH_1$. Since any nonresidue $= \gamma$(re
and vice versa, these give all the cases when (a_r is a residue and r is even) [H1],
a nonresidue and r is even) [H2], (a_r is a residue and r is odd) [H3], (a_r is a nonr
and r is odd) [H4], which partition $\mathbb{Q}_p^*$. Hence there are precisely 4 distinct eleme
$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, when $p \neq 2$.

Similarly, 1,3,5,7 are all distinct in $(\mathbb{Q}_2{}^*)^2$, since for $|\alpha|_2 = 1$, Hensel's Lemma
that $\alpha \in (\mathbb{Q}_2{}^*)^2$ iff $\alpha \equiv 1 \pmod 8$. Furthermore, any $\alpha \equiv 1$ is equal to prrecise
of $1, 3, 5, 7$ in $\mathbb{Q}_2{}^*/(\mathbb{Q}_2{}^*)^2$. For any α, if $|\alpha|_2 = 2^r$ with r even, then $\alpha = \alpha \cdot 2^r = 1, 3,$
in $\mathbb{Q}_2{}^*/(\mathbb{Q}_2{}^*)^2$, since $|\alpha \cdot 2^r|_2 = 1$. If r is odd, then $\alpha/2 = 2^r\alpha = 1, 3, 5$ or 7 in $\mathbb{Q}_2{}^*/($
and so $\alpha = 2, 6, 10$ or 14 in $\mathbb{Q}_2{}^*/(\mathbb{Q}_2{}^*)^2$. So, there are 8 elements when $p = 2$, repres
say, by $1, 3, 5, 7, 2, 6, 10, 14$ (generated by $3, 5, 2$). **[8 m**

Question 2. Let R be any ring, and let F, G be formal groups over R.
(i) [*Proof from lectures*]. Let $P(T) = F_X(0,T)^{-1}$, so that $\omega(T) = P(T)\mathrm{d}T$. Not
$F_X(0,T) = 1 + \ldots$ is invertible, so that $P(T)$ is indeed a member of $R[[T]]$. Furthe
$P(0) = 1$, so that it is normalised.

We need to show that ω is an invariant differential; that is, $\omega \circ F(T,S) = \omega(T)$,
is equivalent to: $P\big(F(T,S)\big)F_X(T,S) = P(T)$ so, in out case, it is sufficient to show

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

which is true iff:

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

But this last statement is immediate from differentiating $F\big(U, F(T,S)\big) = F\big(F(U,$
[associativity] with respect to U to get: $F_X\big(U, F(T,S)\big) = F_X\big(F(U,T),S\big)F_X(U,T$
setting $U = 0$. Hence ω is an invariant differential.

Suppose that $\hat{\omega} = Q(T)\mathrm{d}T \in R[[T]]\mathrm{d}T$ is also an invariant differential, so that
satisfies $Q\big(F(T,S)\big)F_X(T,S) = Q(T)$. Substituting $T = 0$ gives $Q(S)F_X(0,S) = Q($
that $Q(S) = Q(0)F_X(0,S)^{-1}$. It follows that $\hat{\omega} = a\omega$, where $a = Q(0)$. **[9 m**
(ii) [*Proof from lectures*]. First, note that $\omega_G \circ f\big(F(T,S)\big) = \omega_G\big(G(f(T), f(S)\big) = \omega_G \circ$
so that $\omega_G \circ f$ is an inviariant differential on G. From part (a), it follows that $\omega_G \circ f =$
for some $a \in R$. Since ω_F, ω_G are normalised, $(1 + \ldots)\mathrm{d}f(T) = a(1 + \ldots)\mathrm{d}T$, a
$(1 + \ldots)f'(T)\mathrm{d}T = a(1 + \ldots)\mathrm{d}T$; equating constant terms gives $a = f'(0)$, as requir

Let ω be the normalised invariant differential on F. Since $[p](T) = pT + \ldots$, it sa
$[p]'(0) = p$. Applying the previous result to $[p]$, a homomorphism from F to itself,
$\omega \circ [p] = [p]'(0)\omega = p\omega$, and so

$$p\omega(T) = \omega \circ [p](T) = (1 + \ldots)\mathrm{d}([p](T)) = (1 + \ldots)[p]'(T)\mathrm{d}T.$$

Hence $[p]'(T) \in p\,R_T$. Each term $a_n T^n$ in $[p](T)$ msut then satisfy $p|na_n$ and so
$p|a_n$, as required. **[8 m**
(iii) [*Unseen*]. Let $\mathcal{E}$ be the given curve, which is of the form $Y^2 = X^3 - M^2X$
where $M = m^2 + 1$ and $N = 3n$. First note that for $m \equiv 0, 1, 2 \pmod 3$,

$1, 2, 2 \pmod 3$, so that M is never divisible by 3. Hence $\Delta = 4(-M^2)^3 + 27(N$
$-4M^6 + 27N^4$ is never 0, and so the curve is non-singular and is an elliptic cur
has the obvious point $(0, N)$. Let $P = 2(0, N) \in \mathcal{E}(\mathbb{Q})$. The tangent to $\mathcal{E}$ at
has slope $(3 \cdot 0^2 - M^2)/(2 \cdot N) = -M^2/2N$, and so the x-coordinate of $P = 2(0,$
$\left(-M^2/2N\right)^2 - 2 \cdot 0$, which is not an integer, since the numerator is not divisible by
the denominator $N = 3n$ is divisible by 3. Therefore P is not a torsion point (usi
result from lectures that any torsion point in $\mathcal{E}(\mathbb{Q})$ must have both coordinates in $\mathbb{Z}$
so must be of infinite order, giving that $\mathcal{E}(\mathbb{Q})$ is infinite, as required. **[8 m**

Question 3.

(i) [*Seen similar on an exercise sheet*]. The line tangent to $\mathcal{E}$ at $P = (1, 1)$ has sl
given by $2yy' = 3x^2 + 7$, with $x = 1, y = 1$; that is, the slope is $10/2 = 5$. This ta
line also goes through $(1, 1)$ and so has equation: $Y = 5X - 4$. The x-coordinate
is therefore $5^2 - (1 + 1) = 23$, and the y-coordinate is: $-(5 \cdot 23 - 4) = -111 \equiv 14$
that $Q = 2P \equiv (23, 1406)$ (modulo $N = 1517$). We now wish to compute $4P =$
$2(23, 1406)$, and so the first step is to find the line tangent to $\mathcal{E}$ at Q. This has sl
given by $2yy' = 3x^2 + 7$, with $x = 23, y = 1406$, that is, $y' = 1594/2812$. In or
compute this modulo $N = 1517$, we must first find the inverse of 2812 modulo 1517.
Euclid's Algirithm: $2812 = 1 \cdot 1517 + 1295$, $1517 = 1 \cdot 1295 + 222$, $1295 = 5 \cdot 222$
$222 = 1{\cdot}185{+}37$, $185 = 5{\cdot}37{+}0$. So, we cannot find the inverse of 2812 (modulo $N =$
and this step has given us a proper factor 37 of N. **[8 m**

(ii) [*Seen similar on an exercise sheet*]. The elliptic curve has $\Delta = 4A^3 + 27$
$4 \cdot (-2)^3 + 27 \cdot 0^2 = -32$, and so has good reduction at all primes p except p
Taking $p = 3$, we find that $\mathcal{E}(\mathbb{F}_3) = \{\mathbf{o}, (0, 0), (2, 1), (2, 2)\}$, and since $\mathcal{E}_{\text{tors}}(\mathbb{Q})$
morphic to a subgroup of $\mathcal{E}(\mathbb{F}_3)$, this gives that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid 4$. Taking $p =$
find that $\mathcal{E}(\mathbb{F}_5) = \{\mathbf{o}, (0, 0), (1, 2), (1, 3), (2, 2), (2, 3), (3, 1), (3, 4), (4, 1), (4, 4)\}$, and
$\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{E}(\mathbb{F}_5)$, this gives that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid 10$. I
$\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \gcd(4, 10) = 2$. However, there are the obvious torsion points: $\mathbf{o}$ and
and so $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\mathbf{o}, (0, 0)\}$.

[7 m

(iii) [*Unseen*]. Using $2YY' = 3X^2$, we see that the slope of the curve at any $(x$
$3x^2/(2y)$, and so the tangent to the curve at (x, y) is the line: $Y = \left(\frac{3x^2}{2y}\right)X + c$, for s
The x-coordinate of the third point of intersection is then: $\left(\frac{3x^2}{2y}\right)^2 - x - x = \frac{9x^4-8}{4y}$
$\frac{9x^4-8x(x^3+k)}{4(x^3+k)} = \frac{x(x^3-8k)}{4(x^3+k)}$. Furthermore $3(x, y) = \mathbf{o} \iff 2(x, y) = -(x, y) = (x, -y)$
$\left(\frac{x(x^3-8k)}{4(x^3+k)}, ?\right) = (x, -y) \iff \frac{x(x^3-8k)}{4(x^3+k)} = x$ [the $\Rightarrow$ of the last step is trivial; for $\Leftarrow$
that if $2(x, y)$ has that same x-coordinate as (x, y) then $2(x, y) = (x, -y)$ or $(x, y$
the latter would imply $(x, y) = \mathbf{o}$, which we have excluded]. Note further that th
condition on x is satisfied when $x(x^3 - 8k) = 4x(x^3 + k)$, that is: $x(x^3 + 4k) = 0$.
gives on $\mathcal{E}_k(\mathbb{C})$ the points $(0, \sqrt{k})$ and $(-\sqrt[3]{4k}, i\sqrt{3k})$. But it is impossible for bo
and $i\sqrt{3k}$ to be in $\mathbb{Q}$ (indeed they cannot both be in $\mathbb{R}$), so that at least one of these
of order 3 is not in $\mathcal{E}_k(\mathbb{Q})$. **[10 m**

Question 4.

(i) [*Seen similar on an Exercise Sheet*]. Let $\mathcal{C} : Y^2 = X(X^2 + aX + b) = X(X^2 + 3X$ where $a = 3, b = 5$, and isogenous curve $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1) = X(X^2 - 6X$ where $a_1 = -2a = -6, b_1 = a^2 - 4b = -11$, with the usual isogeny $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}$ $(x, y) \mapsto (y^2/x^2, y - 5y/x^2)$, and dual isogeny $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) : (u, v) \mapsto (\frac{1}{4}v^2/u^2,$ $11v/u^2)$).

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u$, for $(u, v) \neq$ with $q : (0, 0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, is an injection with im$q$ contained in d is square free and $d|b_1\} = \{\pm 1, \pm 11\}$. Also, $\mathbf{o} \mapsto 1$, $(0, 0) \mapsto -11$ and the ol point $(-1, 2) \mapsto -1$, so that $1, -11, -1 \in$ im$q$; but im$q$ is a group, so $11 \in$ im$q$ and indeed we can just take: $(0, 0) + (-1, 2) = (11, 22)$, which maps to 11 un Hence, $\{\pm 1, \pm 11\} \subset$ im$q \subset \{\pm 1, \pm 11\}$, that is im$q = \{\pm 1, \pm 11\}$, and so $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}($ $\{\mathbf{o}, (0, 0), (-1, 2), (11, 22)\}$, that is, $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ is generated by $(0, 0), (-1, 2)$.

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 $(u, v) \neq (0, 0)$ $\hat{q} : (0, 0) \mapsto a_1^2 - 4b_1 = b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with im$\hat{q}$ contained in d is square free and $d|b\} = \{\pm 1, \pm 5\}$. Also, $\mathbf{o} \mapsto 1$ and $(0, 0) \mapsto 5$, so that $\{1, 5\} \subset$ $\{\pm 1, \pm 5\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in$ i there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a\ell$ $(b/(-1)) \cdot m^4 = n^2$; that is: $-\ell^4 + 3\ell^2m^2 - 5m^4 = n^2$. Multiply both sides by 4 and r as: $-(2\ell^2 - 3m^2)^2 - 11m^4 = 4n^2$. We can see that the LHS is $\leqslant 0$ and the RHS i and the equation is satisfied iff $(2\ell^2 - 3m^2) = 11m^4 = 4n^2 = 0$. From this we se $m = n = 0$, which when combined with $2\ell^2 - 3m^2 = 0$ gives that $\ell = 0$, also, whic contradiction. Hence $-1 \notin$ im$\hat{q}$.

We conclude that im$\hat{q} = \{1, 5\}$, 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 $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ i erated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $(0, 0)$] together with the images $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0, 0)\big) = \mathbf{o}$ and $\hat{\phi}\big((-1, 2)\big) = (1, 3)$]. clusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0, 0)$ and $(1, 3)$ and so is the group $C_2 \times C_2$. $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{tors}(\mathbb{Q})/2\mathcal{C}_{tors}(\mathbb{Q}) \times C_2^{rank}$, and $\mathcal{C}_{tors}(\mathbb{Q})/2\mathcal{C}_{tors}(\mathbb{Q})$ morphic to the 2-torsion group of $\mathcal{C}_{tors}(\mathbb{Q})$ which is C_2 (consisting only of $\mathbf{o}$ and $(0,$ that $\mathcal{C}_{tors}(\mathbb{Q})/2\mathcal{C}_{tors}(\mathbb{Q})$ is isomorphic to C_2. Conclusion: rank $= 1$. **[13 m**

(ii) [*Unseen*]. Let $\mathcal{C} : Y^2 = X(X^2 + aX + b) = X(X^2 + p^2)$, where $a = 0, b = p^2$ isogenous curve $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1) = X(X^2 - 4p^2)$, where $a_1 = -2a = 0$ $a^2 - 4b = -4p^2$, with the usual isogeny $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto (y^2/x^2, y - p^2$ and dual isogeny $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) : (u, v) \mapsto (\frac{1}{4}v^2/u^2, \frac{1}{8}(v + 4p^2v/u^2))$.

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u$, for $(u, v) \neq$ with $q : (0, 0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, is an injection with im$q$ contained in d is square free and $d|b_1\} = \{\pm 1, \pm 2, \pm p, \pm 2p\}$. Also, $\mathbf{o} \mapsto 1$, $(0, 0) \mapsto -1$, $(2p, 0)$ $(-2p, 0) \mapsto -2p$, so that $\{\pm 1, \pm 2p\} \subset$ im$q \subset \{\pm 1, \pm 2, \pm p, \pm 2p\}$. There is only one to check, represented by -2, say. We know that $-2 \in$ im$q$ iff there are integers $\ell, m,$ all 0, and with $\gcd(\ell, m) = 1$, such that: $(-2) \cdot \ell^4 + a_1\ell^2m^2 + (b_1/(-2)) \cdot m^4 = n^2$ is: $-2\ell^4 + 2p^2m^4 = n^2$. Since $p \equiv 5 \pmod 8$, $\left(\frac{-2}{p}\right) = -1$, and so $p|\ell$, $p|n$. Let ℓ

$n = pn'$. Then $-2p^2(\ell')^4 + 2m^4 = (n')^2$. Since also $\left(\frac{2}{p}\right) = -1$, this implies $p|m$
This gives a contradiction, since $p|\ell, p|m$ and $\gcd(\ell, m) = 1$. Hence $-2 \notin \text{im}q$, givin
$\text{im}q = \{\pm 1, \pm 2p\}$, and $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\mathbf{o}, (0,0), (2p,0), (-2p,0)\}$.

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 $(u,v) \neq (0,0)$
$\hat{q} : (0,0) \mapsto a_1^2 - 4b_1 = b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with $\text{im}\hat{q}$ contained i
d is square free and $d|b\} = \{\pm 1, \pm p\}$. Also, $\mathbf{o} \mapsto 1$ and $(0,0) \mapsto p^2 = 1$, so that
$\text{im}\hat{q} \subset \{\pm 1, \pm p\}$.

We know that $-1 \in \text{im}\hat{q}$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m$
such that: $(-1)\cdot\ell^4 + a\ell^2m^2 + (b/(-1))\cdot m^4 = n^2$; that is: $-\ell^4 - p^2m^4 = n^2$, clearly impo
in $\mathbb{R}$. Hence $-1 \notin \text{im}\hat{q}$. Similarly, $-p \notin \text{im}\hat{q}$. We know that $p \in \text{im}\hat{q}$ iff there are in
ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $p \cdot \ell^4 + a\ell^2m^2 + (b/p)\cdot m^4 = n^2$
is: $p\ell^4 + pm^4 = n^2$, and so $p|n$. Letting $n = pn'$, the equation becomes $\ell^4 + m^4 = p^2$
which in turn implies $p|\ell, p|m$, since $-1 \not\equiv a^4$ for any a [as can be seen by taking both
of $-1 \equiv a^4$ to the power of $(p-1)/4$]. This again contradicts $\gcd(\ell, m) = 1$, and so

We conclude that $\text{im}\hat{q} = \{1\}$, and so $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \{\mathbf{o}\}$.

Finally, since multiplication by 2 in $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi} \circ \phi$, we have that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ i
erated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $\mathbf{o}$] together with the images unde
generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0,0)\big) = \mathbf{o}$, and $\hat{\phi}\big((2p,0)\big) = (0,0)$]. Concl
$\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0,0)$, and so is the group C_2. Now $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is is
phic to $\mathcal{C}_{tors}(\mathbb{Q})/2\mathcal{C}_{tors}(\mathbb{Q}) \times C_2^{rank}$, and $\mathcal{C}_{tors}(\mathbb{Q})/2\mathcal{C}_{tors}(\mathbb{Q})$ is isomorphic to the 2-t
group of $\mathcal{C}_{tors}(\mathbb{Q})$ which is C_2 (consisting only of $\mathbf{o}$ and $(0,0)$), so that $\mathcal{C}_{tors}(\mathbb{Q})/2\mathcal{C}_t$
is isomorphic to C_2. Conclusion: rank $= 0$. **[12 m**