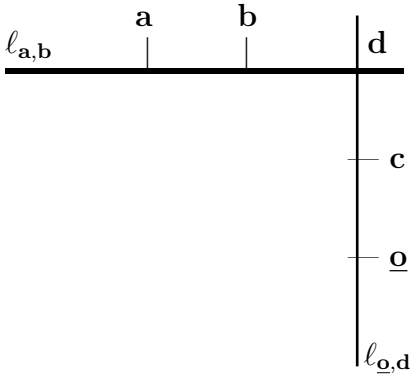
SOLUTIONS TO THE 2009 ELLIPTIC CURVES QUESTIONS

Question 1.

(a) [*Proof from lectures*]. For any two points $\mathbf{a}, \mathbf{b}$ on $\mathcal{C}$, let $\ell_{\mathbf{a},\mathbf{b}}$ denote the line which meets $\mathcal{C}$ at $\mathbf{a}, \mathbf{b}$ [if $\mathbf{a}, \mathbf{b}$ are distinct then $\ell_{\mathbf{a},\mathbf{b}}$ is the unique line through $\mathbf{a}, \mathbf{b}$; if $\mathbf{a} = \mathbf{b}$ then $\ell_{\mathbf{a},\mathbf{b}}$ is the line tangent to $\mathcal{C}$ at $\mathbf{a} = \mathbf{b}$].

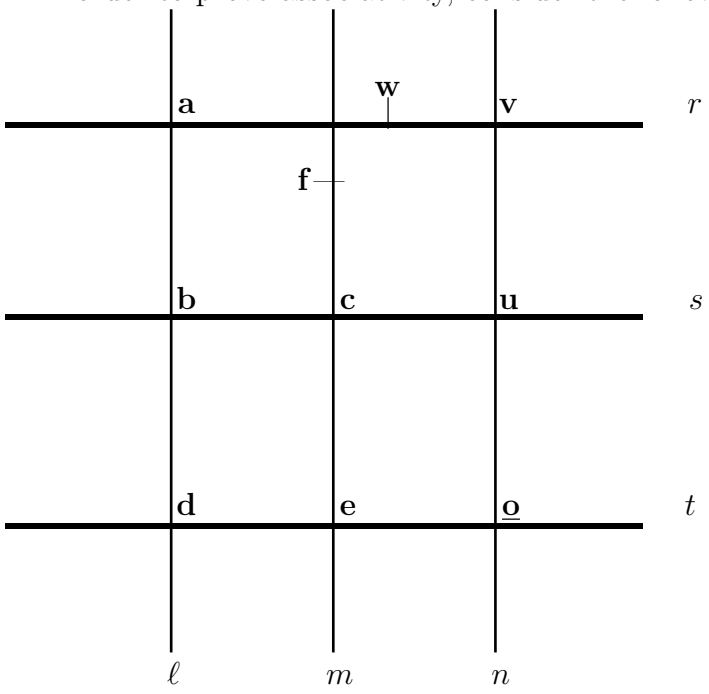


Let $\ell_{\mathbf{a},\mathbf{b}}$ denote the line which meets $\mathcal{C}$ at $\mathbf{a}, \mathbf{b}$.
Then $\ell_{\mathbf{a},\mathbf{b}}$ and $\mathcal{C}$ have 3 points of intersection (Bézout).
Let $\mathbf{d}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\mathbf{a},\mathbf{b}}$.
Now, let $\ell_{\underline{\mathbf{o}},\mathbf{d}}$ denote the line which meets $\mathcal{C}$ at $\underline{\mathbf{o}}$ and $\mathbf{d}$.
Let $\mathbf{c}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\underline{\mathbf{o}},\mathbf{d}}$.
Define $\mathbf{a} + \mathbf{b} = \mathbf{c}$.

We recall from lectures the following lemma.

Lemma. Let $P_1, \ldots, P_8$ be such that no 4 points lie on a line and no 7 points lie on a conic. Then there exists a unique point P_9 which is a 9th point of intersection of any two cubics passing through $P_1, \ldots, P_8$.

In order to prove associativity, consider the following diagram.



Here, r, s, t, ℓ, m, n are lines. On each line, the labelled points are the points of intersection between $\mathcal{C}$ and that line. From our construction of the law for adding points:

$$\mathbf{a} + \mathbf{b} = \mathbf{e},$$

and so:

$$(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \text{3rd point of intersection on } \ell_{\underline{\mathbf{o}},\mathbf{f}}.$$

Similarly:

$$\mathbf{b} + \mathbf{c} = \mathbf{v},$$

$$\mathbf{a} + (\mathbf{b} + \mathbf{c}) = \text{3rd point of intersection on } \ell_{\underline{\mathbf{o}},\mathbf{w}}.$$

To show $(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \mathbf{a} + (\mathbf{b} + \mathbf{c})$, it is sufficient to show that $\mathbf{f} = \mathbf{w}$. Let $F_1 = \ell mn$ and $F_2 = rst$, both of which are cubic curves.

$\mathcal{C}$ and F_1 have 8 common points: $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \underline{\mathbf{o}}$.

$\mathcal{C}$ and F_2 also have these 8 common points: $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \underline{\mathbf{o}}$.

From the above lemma, the 9th point of intersection of $\mathcal{C}$ and F_1 must be the same as the 9th point of intersection of $\mathcal{C}$ and F_2; that is, $\mathbf{f} = \mathbf{w}$, as required. **[10 marks]**

(b) [*Seen similar idea on a problem sheet*]. Our curve is $y^2 = h(x) = x^3 - x - 1$. For $p = 2$, take $x = -2$, in which case we want $y \in \mathbb{Z}_2$ such that $y^2 = h(-2) = -7 \pmod 8$, which exists (by the result from lectures that, when $|a|_2 = 1$, we have $a \in (\mathbb{Q}_2^*)^2 \iff a \equiv 1 \pmod 8$). For $p = 3$, any $x \equiv 0, 1$ or 2 mod 3, giving $h(x) \equiv 2 \pmod 3$ in each case, so we require $y^2 \equiv 2 \pmod 3$, which is impossible, since $y \equiv 0, 1, 2$ give $y^2 \equiv 0, 1, 1$, respectively. Hence, there are no such $x, y \in \mathbb{Z}_3$. For $p = 5$, take $x = 0$, in which case we want $y \in \mathbb{Z}_5$ such that $y^2 = h(0) = -1$, which exists since $-1 \equiv 2^2 \pmod 5$ is a quadratic residue mod 5 (by the result from lectures that, when $p \neq 2$ and $|a|_p = 1$, we have $a \in (\mathbb{Q}_p^*)^2 \iff a \in (\mathcal{F}_p^*)^2$). For $p = 7$, take $x = 3$, in which case we want $y \in \mathbb{Z}_7$ such that $y^2 = h(3) = 23$, which exists since $23 \equiv 2 \equiv 3^2 \pmod 7$ is a quadratic residue mod 7 (again, by the result from lectures that, when $p \neq 2$ and $|a|_p = 1$, we have $a \in (\mathbb{Q}_p^*)^2 \iff a \in (\mathcal{F}_p^*)^2$). For $p = 23$, take $x = -2$, in which case we want $y \in \mathbb{Z}_{23}$ such that $y^2 = h(-2) = -7$, which exists since $-7 \equiv 16 \equiv 4^2$ is a quadratic residue mod 23 (again, using the same result as before). For $p \geqslant 11$, $p \neq 23$, the curve is an elliptic curve mod p [since the only bad primes are $2, 23$] and $\#\widetilde{\mathcal{E}}(\mathbb{F}_p) \geqslant p + 1 - 2\sqrt{p} > 5$. At most 4 of these are 2-torsion, so there exists x_0 such that $h(x_0)$ is a nonzero residue mod p; applying the same result as before gives the existence of a corresponding $y \in \mathbb{Z}_p$. In summary, there exist such $x, y \in \mathbb{Z}_p$ for all p except 3. **[6 marks]**

(c) [*Seen similar on a problem sheet*]. The line tangent to $\mathcal{E}$ at $P = (1, 1)$ has slope y' given by $2yy' = 3x^2 + 5$, with $x = 1, y = 1$; that is, the slope is $8/2 = 4$. This tangent line also goes through $(1, 1)$ and so has equation: $Y = 4X - 3$. The x-coordinate of $2P$ is therefore $4^2 - (1 + 1) = 14$, and the y-coordinate is: $-(4 \cdot 14 - 3) = -53 \equiv 168 \pmod{221}$, so that $Q = 2P \equiv (14, 168)$ (modulo $N = 221$). We now wish to compute $3P = P + 2P = P + Q$, and so the first step is to find the line joining $P = (1, 1)$ to $Q = (14, 168)$. We must compute the slope given by $(168 - 1)/(14 - 1) = 167/13$ (modulo $N = 221$), for which the first step

is to find the inverse of 13 (modulo $N = 221$). Using Euclid's Algorithm: $221 = 17 \cdot 13 + 0$ (stops after one step). So, we cannot find the inverse of 13 (modulo $N = 221$), and this step has given us a factor 13 of N. **[6 marks]**

(d) [*Unseen*]. Define x_n to be the sequence $1, p, \ldots$ [p times] $\ldots, p, p^2, \ldots$ [p^2 times] $\ldots, p^2, \ldots$ Then the sequence of $|x_n|_p$ is: $1, p^{-1}, \ldots$ [p times] $\ldots, p^{-1}, p^{-2}, \ldots$ [p^2 times] $\ldots, p^{-2}, \ldots$ giving that $x_n \to 0$, and so $\sum_{n=1}^{\infty} x_n$ is convergent (using the result from lectures that, for a field complete with respect to a non-Archimedean valuation, $\sum_{n=1}^{\infty} x_n$ is convergent if and only if $x_n \to 0$).

$\sum_{n=1}^{\infty} |x_n|_p = 1 + (p^{-1} + \ldots$ [p times] $\ldots + p^{-1}) + (p^{-2} + \ldots$ [p^2 times] $\ldots + p^{-2}) + \ldots =$ $1 + 1 + 1 + \ldots$ which is not convergent in $\mathbb{R}$. **[3 marks]**

Question 2.

(a) 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 $\omega(T) = P(T)\mathrm{d}T$. Note that $F_X(0,T) = 1 + \ldots$ is invertible, so that $P(T)$ is indeed a member of $R[[T]]$. Furthermore, $P(0) = 1$, so that it is normalised.

We need to show that ω is an invariant differential; that is, $\omega \circ F(T,S) = \omega(T)$, which is equivalent to: $P\big(F(T,S)\big)F_X(T,S) = P(T)$ so, in our 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 $F\big(U, F(T,S)\big) = F\big(F(U,T), S\big)$ [associativity] with respect to U to get: $F_X\big(U, F(T,S)\big) = F_X\big(F(U,T), S\big)F_X(U,T)$ and 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 $Q(T)$ satisfies $Q\big(F(T,S)\big)F_X(T,S) = Q(T)$. Substituting $T = 0$ gives $Q(S)F_X(0,S) = Q(0)$, so that $Q(S) = Q(0)F_X(0,S)^{-1}$. It follows that $\hat{\omega} = a\omega$, where $a = Q(0)$. **[7 marks]**

(ii) [*Proof from lectures*]. First, note that $\omega_G \circ f\big(F(T,S)\big) = \omega_G\big(G(f(T), f(S)\big) = \omega_G \circ f(T)$, so that $\omega_G \circ f$ is an inviariant differential on G. From part (a), it follows that $\omega_G \circ f = a\,\omega_F$, for some $a \in R$. Since ω_F, ω_G are normalised, $(1 + \ldots)\mathrm{d}f(T) = a(1 + \ldots)\mathrm{d}T$, and so $(1 + \ldots)f'(T)\mathrm{d}T = a(1 + \ldots)\mathrm{d}T$; equating constant terms gives $a = f'(0)$, as required.

Let ω be the normalised invariant differential on F. Since $[p](T) = pT + \ldots$, it satisfies $[p]'(0) = p$. Applying the previous result to $[p]$, a homomorphism from F to itself, gives: $\omega \circ [p] = [p]'(0)\omega = p\omega$, 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 $[p](T)$ must then satisfy $p | n a_n$ and so $p|n$ or $p|a_n$, as required. **[7 marks]**

(b) [*Seen similar on a problem sheet*]. The elliptic curve has $2\Delta = 2(4A^3+27B^2) = 2(4\cdot(0)^3+27\cdot(-9)^2) = 2\cdot 3^5$, and so has good reduction at all primes p except $p = 2, 3$. Taking $p = 5$, we find that $\widetilde{\mathcal{E}}(\mathbb{F}_5) = \{\underline{\mathbf{o}}, (0,1), (0,4), (2,2), (2,3), (4,0)\}$, and since $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_5)$, this gives, by Lagrange's Theorem, that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid 6$. Taking $p = 7$, we find that $\widetilde{\mathcal{E}}(\mathbb{F}_7) = \{\underline{\mathbf{o}}, (3,2), (3,5), (5,2), (5,5), (6,2), (6,5)\}$, and since $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_7)$, this gives that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid 7$. Hence, $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \gcd(6,7) = 1$. Hence $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\underline{\mathbf{o}}\}$. **[5 marks]**

(c) [*Unseen*]. Since n is not divisible by 15 (and so is not divisible by at least one of 3 or 5) and since $2\Delta = 4n^3$, the curve has good reduction at either 3 or 5. When n is not divisible by 3, there is good reduction at 3 and either $n \equiv 2$ or $-n \equiv 2 \pmod 3$; in the first case the reduction of $\mathcal{E}$ mod 3 is: $Y^2 = X^3 + 2X$, with points: $\{\underline{\mathbf{o}}, (0,0), (1,0), (2,0)\} \cong C_2 \times C_2$; in the second case the reduction of $\mathcal{F}$ mod 3 is isomorphic to $C_2 \times C_2$. When n is not divisible by 5, there is good reduction at 5 and either $n \equiv 1, 2$ or $-n \equiv 1, 2 \pmod 5$; in the first case the reduction of $\mathcal{E}$ mod 5 is: $Y^2 = X^3 + X$ or $Y^2 = X^3 + 2X$, with points: $\{\underline{\mathbf{o}}, (0,0), (2,0), (3,0)\} \cong C_2 \times C_2$ or $\{\underline{\mathbf{o}}, (0,0)\} \cong C_2$, respectively; in the second case the reduction of $\mathcal{F}$ mod 5 is isomorphic to $C_2 \times C_2$ or C_2. In all case, $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ or $\mathcal{F}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $C_2 \times C_2$. But since $\mathcal{E}(\mathbb{Q})[2] = \mathcal{F}(\mathbb{Q})[2] = \{\underline{\mathbf{o}}, (0,0)\}$ (since $n, -n$ are nonsquare) it follows that $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\underline{\mathbf{o}}, (0,0)\}$ or $\mathcal{F}_{\text{tors}}(\mathbb{Q}) = \{\underline{\mathbf{o}}, (0,0)\}$. **[6 marks]**

Question 3.

(a) [*Seen similar on a problem sheet*]. Let $\mathcal{C} : Y^2 = X(X^2+aX+b) = X(X^2+5X-5)$, where $a = 5, b = -5$, and isogenous curve $\mathcal{D} : Y^2 = X(X^2+a_1X+b_1) = X(X^2-10X+45)$, where $a_1 = -10, b_1 = 45$, with the usual isogeny $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x,y) \mapsto (y^2/x^2, y + 5y/x^2)$, and dual isogeny $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) : (u,v) \mapsto (\frac{1}{4}v^2/u^2, \frac{1}{8}(v - 45v/u^2))$.

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u,v) \mapsto u$, for $(u,v) \neq (0,0)$, with $q : (0,0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, is an injection with im$q$ contained in $\{d : d \text{ is square free and } d|b_1\} = \{\pm 1, \pm 3, \pm 5, \pm 15\}$. Also, $\mathbf{o} \mapsto 1$, $(0,0) \mapsto 45 = 5$. Hence, $\{1, 5\} \subset \text{im}q \subset \{\pm 1, \pm 3, \pm 5, \pm 15\}$.

There are only three cosets to check, represented by $-1, 3, -3$, say. We know that $-1 \in \text{im}q$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1)\cdot\ell^4 + a_1\ell^2m^2 + (b_1/(-1))\cdot m^4 = n^2$ that is: $-\ell^4 - 10\ell^2m^2 - 45m^4 = n^2$. We can see that the LHS is $\leqslant 0$ and the RHS is $\geqslant 0$, and there is equality iff $\ell = m = n = 0$, a contradiction. Hence $-1 \notin \text{im}q$. Similarly $-3 \notin \text{im}q$. We know that $3 \in \text{im}q$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $3\cdot\ell^4 + a_1\ell^2m^2 + (b_1/3)\cdot m^4 = n^2$ that is: $3\ell^4 - 10\ell^2m^2 + 15m^4 = n^2$. Rewrite as: $(3\ell^2 - 5m^2)^2 + 20m^4 = 3n^2$. Reducing modulo 5 gives: $(3\ell^2 - 5m^2)^2 \equiv 3n^2$ (modulo 5). If n were coprime to 5, then this would give: $(3\ell^2/n)^2 = 3$ in $\mathcal{F}_5$, contradicting the fact that 3 is not a quadratic residue modulo 5. So, $5|n$ and so $5|(3\ell^2 - 5m^2)$, also. Hence 5^2 divides $(3\ell^2 - 5m^2)^2$ and $3n^2$ and so must divide $20m^4$; but 20 is only divisible by 5 (not by 5^2) so that 5 must divide m^4; hence 5 divides m. Furthermore, the fact (already found)

that $5|(3\ell^2-5m^2)$ gives that $5|3\ell^2$, and so $5|\ell$ also. We've shown that 5 divides both of ℓ, m, which contradicts the fact that $\gcd(\ell,m)=1$. Hence $3 \notin \mathrm{im}\hat{q}$.

We conclude that $\mathrm{im}q = \{1,5\}$ and that $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\mathbf{o},(0,0)\}$, and so $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ is generated by $(0,0)$.

The map $\hat{q}: \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x,y) \mapsto x$, for $(x,y) \neq (0,0)$, with $\hat{q}:(0,0) \mapsto a_1^2-4b_1 = b$ and $\hat{q}:\mathbf{o} \mapsto 1$, is an injection with $\mathrm{im}\hat{q}$ contained in $\{d : d \text{ is square free and } d|b\} = \{\pm 1, \pm 5\}$. Also, $\mathbf{o} \mapsto 1$, $(0,0) \mapsto -5$, and the obvious point $(-1,3) \mapsto -1$, which imply that $(0,0)+(-1,3) = (5,15) \mapsto 5$, so that $\{\pm 1, \pm 5\} \subset \mathrm{im}\hat{q} \subset \{\pm 1, \pm 5\}$.

We conclude that $\mathrm{im}\hat{q} = \{\pm 1, \pm 5\}$ and $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) = \{\mathbf{o},(0,0),(-1,3),(5,15)\}$, so that $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ is generated by $(0,0),(-1,3)$.

Finally, since multiplication by 2 in $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi}\circ\phi$, we have that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $(0,0),(-1,3)$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0,0)\big) = \mathbf{o}$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0,0),(-1,3)$, and is the group $C_2 \times C_2$. Now $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})/2\mathcal{C}_{\mathrm{tors}}(\mathbb{Q}) \times C_2^{rank}$, and $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})/2\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})$ is isomorphic to the 2-torsion group of $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})$ which is C_2 (consisting only of $\mathbf{o}$ and $(0,0)$, since x^2+5x-5 has no $\mathbb{Q}$-rational roots), so that $\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})/2\mathcal{C}_{\mathrm{tors}}(\mathbb{Q})$ is C_2. Conclusion: rank $= 1$. **[13 marks]**

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

The map $q: \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u,v) \mapsto u$, for $(u,v) \neq (0,0)$, with $q: (0,0) \mapsto b_1 = -4p = -p$ and $q: \mathbf{o} \mapsto 1$, is an injection with $\mathrm{im}q$ contained in $\{d : d \text{ is square free and } d|b_1\} = \{\pm 1, \pm 2, \pm p, \pm 2p\}$. Hence, $\{1,-p\} \subset \mathrm{im}q \subset \{\pm 1, \pm 2, \pm p, \pm 2p\}$.

So $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ is isomorphic to a subgroup of $C_2 \times C_2 \times C_2$.

The map $\hat{q}: \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x,y) \mapsto x$, for $(x,y) \neq (0,0)$, with $\hat{q}:(0,0) \mapsto a_1^2-4b_1 = b$ and $\hat{q}:\mathbf{o} \mapsto 1$, is an injection with $\mathrm{im}\hat{q}$ contained in $\{d : d \text{ is square free and } d|b\} = \{\pm 1, \pm p\}$. Also, $\mathbf{o} \mapsto 1$, $(0,0) \mapsto p$, so that $\{1,p\} \subset \mathrm{im}\hat{q} \subset \{\pm 1, \pm p\}$. There is only one coset to check, represented by -1, say. We know that $-1 \in \mathrm{im}q$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell,m)=1$, such that: $(-1)\cdot\ell^4 + a\ell^2m^2 + (b/(-1))\cdot m^4 = n^2$ that is: $-\ell^4 - pm^4 = n^2$. We can see that the LHS is $\leqslant 0$ and the RHS is $\geqslant 0$, and there is equality iff $\ell = m = n = 0$, a contradiction. Hence $-1 \notin \mathrm{im}q$.

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

Finally, since multiplication by 2 in $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi}\circ\phi$, we have that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $(0,0)$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [which contributes at most $C_2 \times C_2$ since $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \cong$ at most $C_2 \times C_2 \times C_2$ and $\hat{\phi}((0,0)) = \mathbf{o}$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is is isomorphic to a

subgroup of $C_2 \times C_2 \times C_2$. Now $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{\rm tors}(\mathbb{Q})/2\mathcal{C}_{\rm tors}(\mathbb{Q}) \times C_2^{rank}$, and $\mathcal{C}_{\rm tors}(\mathbb{Q})/2\mathcal{C}_{\rm tors}(\mathbb{Q})$ is isomorphic to the 2-torsion group of $\mathcal{C}_{\rm tors}(\mathbb{Q})$ which is C_2 (consisting only of $\mathbf{o}$ and $(0,0)$, since x^2+p has no $\mathbb{Q}$-rational roots), so that $\mathcal{C}_{\rm tors}(\mathbb{Q})/2\mathcal{C}_{\rm tors}(\mathbb{Q})$ is C_2. Conclusion: rank is at most 2. **[6 marks]**

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

The map $\hat{q} : \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x,y) \mapsto x$, for $(x,y) \neq (0,0)$, with $\hat{q} : (0,0) \mapsto a_1^2 - 4b_1 = b = -\alpha$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection, from which it follows that $(1,1) \in \hat{\phi}(\mathcal{D}(\mathbb{Q}))$. If $\hat{\phi}(u,v) = (1,1)$ then $\frac{1}{4}v^2/u^2 = 1$, giving $v = \pm 2u$; substituting this into $\mathcal{D}$ gives $4u^2 = u(u^2 - 2\alpha u + (\alpha^2+4\alpha))$ and so $0 = u(u-\alpha)(u-(\alpha-4))$. We can discount $u=0$ since $\hat{\phi} : (0,0) \mapsto \mathbf{o}$, so the possibilities are: $(\alpha, \pm 2\alpha)$ and $(\alpha+4, \pm 2(\alpha+4))$, Substituting these into $\hat{\phi}$ gives that $(\alpha, -2\alpha)$ and $(\alpha+4, 2(\alpha+4))$ are the preimages of $(1,1)$ under $\hat{\phi}$ (with the other two points being the preimages of $(1,-1)$).

$(1,1) \in 2\mathcal{C}(\mathbb{Q}) = \hat{\phi}(\phi(\mathcal{C}(\mathbb{Q}))) \iff (\alpha, -2\alpha) \in \phi(\mathcal{C}(\mathbb{Q}))$ or $(\alpha+4, 2(\alpha+4)) \in \phi(\mathcal{C}(\mathbb{Q}))$. We now use the injection $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u,v) \mapsto u$, for $(u,v) \neq (0,0)$, with $q : (0,0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, to see that this is the case exactly when α or $\alpha+4$ is square in $\mathbb{Q}$ (and so square in $\mathbb{Z}$, since $\alpha \in \mathbb{Z}$). **[6 marks]**

General Comments. In the above solutions, I have given everything in full pedantic detail, in order to make every step as clear as possible to a non-specialist. Students could gain full marks from intelligently shortened versions of the above answers.

In some of the questions, there are parts (a),(b),... of the same question from different parts of the course, rather than having the same theme necessarily throughout the whole question. The students are told in advance that, on this exam, parts of questions need not be related, and furthermore this has also been the case on the previous exams on this lecture course, so the students will already be aware of this. The motivation for this style is that there are several standard techniques, such as finding torsion, finding the rank, cryptographic applications, applying Hensel's Lemma, etc, which reward hard-working but not necessarily highest-mark students, who are able to perform some of these. Having a substantial number of these standard techniques represented, gives a reward to conscientious students. In addition, I have also included parts of each question which require more creativity. This style of exam for this lecture course has, for the last 3 years, provided a nice spread of marks from 55 to 90, quite close to the average the same groups of students have obtained elsewhere

(with slightly over half of the students each year obtaining raw marks of at least 70, again compatible with the typical strength of the class).

The students have been told in advance that two of the three questions will include bookwork. The geometric lemma (*Let* $P_1, \ldots, P_8$ *be such that no* 4 *points lie on a line and no* 7 *points lie on a conic; then there exists a unique point* P_9 *which is a 9th point of intersection of any two cubics passing through* $P_1, \ldots, P_8$) used in the bookwork of Question 1, was given to them in lectures without proof, and was given to them as something whose statement they should know, and which they should feel free to use. The proof expected for Question 1 (using this geometric lemma) is precisely as given in lectures. I did not include any statement such as *standard geometric results may be assumed if clearly stated*, on the grounds that the result requested is itself such a result. I could, in principle state this specific geometric lemma and mention that it is something they may assume; however, I felt that remembering the statement of the lemma is part of what they should know, and it should not cause a problem as stated, as the proof is precisely what is done in lectures.