Changes to Elliptic Curves problems sheets in 2021-22.

The 2021-22 sheets are the same as those for earlier years, except for the following modifications.

(1) The three new questions whose solutions are given below have been added.

(2) Two easy questions have been removed (old sheet 2 Q6 and old sheet 3 Q6, whose solution is in the notes anyway) and one rather tricky one (old sheet 3 Q4).

(3) Two questions have been moved forward a sheet: old sheet 3 Q2, old sheet 4 Q1.

The reason for doing this were as follows.

(a) I wanted another question on formal groups on the sheets as it is such a long section in the lectures and the topic has started to appear more in exam questions.

(b) The current Sheet 4 covers almost half the course. Moving things forward is tricky, but I've always covered the material for old sheet 4 Q1 by the end of Lecture 10 so it seems safe on Sheet 3.

(c) The new Question 3 on Sheet 4 seems an important result which is apparently used occasionally in exam solutions without much comment. (Whereas the tricky one I removed, old sheet 3 Q4, is rather tangential to everything.)

(d) I thought it good for the problem sheets to contain a descent question for a family of elliptic curves, since these appear so often in exam questions. (So I nicked one randomly from an old paper.)

Elliptic Curves. HT 2021/22. Sheet 3.

5. Let m be a positive integer and $F(X,Y) \in R[[X,Y]]$ a formal group. Prove that the multiplication by m series $[m](T) \in R[[T]]$ is a homomorphism from F to F.

By definition of a homomorphism, we need to show

$$[m]F(X,Y) \stackrel{?}{=} F([m](X),[m]Y).$$

This is true when $m=0$, since $[0](T) := 0$. Now for $m \geq 1$ we can use the recursive definition to rewrite this as

$$F([m-1]F(X,Y),F(X,Y)) \stackrel{?}{=} F(F([m-1](X),X),F([m-1]Y,Y)).$$

By induction we can assume $[m-1]F(X,Y) = F([m-1](X),[m-1]Y)$. Starting from the LHS we compute

$$F([m-1]F(X,Y),F(X,Y)) = F(F([m-1](X),[m-1](Y)),F(X,Y))$$

$$= F([m-1](X),F([m-1](Y),F(X,Y))) = F([m-1](X),F(F(X,Y),[m-1](Y)))$$

$$= F([m-1](X),F(X,F(Y,[m-1](Y)))) = F(F([m-1](X),X),F(Y,[m-1](Y)))$$

which by commutativity equals the RHS. Here we have used, in order, induction, associativity, commutativiity, associativity, associativity.

Elliptic Curves. HT 2021/22. Sheet 4.

3. As in lectures, write $\mathcal{G} = \mathcal{C}(\mathbb{Q})$ and $\mathcal{H} = \mathcal{D}(\mathbb{Q})$. Let a and b be the integers so that

$$\mathcal{G}/\hat{\phi}(\mathcal{H}) \cong C_2^a \text{ and } \mathcal{H}/\phi(\mathcal{G}) \cong C_2^b.$$

(a) Explain why the map

$$\hat{\phi} : \mathcal{H}/\phi(\mathcal{G}) \to \hat{\phi}(\mathcal{H})/2\mathcal{G}, \quad P + \phi(\mathcal{G}) \mapsto \hat{\phi}(P) + 2G$$

is well-defined and surjective. Prove that the kernel of this map is the class $[(0,0)] \in \mathcal{H}/\phi(\mathcal{G})$ of $(0,0) \in \mathcal{H}$.
(b) Hence show that

$$\mathcal{G}/2\mathcal{G} \cong C_2^{a+b} \text{ or } C_2^{a+b-1}$$

according to whether $(0,0) \in \phi(\mathcal{G})$ or $(0,0) \notin \phi(\mathcal{G})$.
(c) Show that $(0,0) \in \phi(\mathcal{G})$ if and only if the 2-torsion of $\mathcal{G}$ is isomorphic to C_2^2. Deduce that the rank of $\mathcal{G}$ is $a + b - 2$.

3.(a) The map is well-defined since $\hat{\phi} \circ \phi = [2]$ and is obviously surjective.

Let $[P] \in \mathcal{H}/\phi(\mathcal{G})$ map to $[o]$, i.e. $\hat{\phi}(P + \phi(G)) = [o]$, that is $\hat{\phi}(P) + 2G = 2G$ so $\hat{\phi}(P) \in 2G$. Then $\hat{\phi}(P) = 2R$ for some $R \in G$. Hence $\hat{\phi}(P - \phi(R)) = o$ as $\hat{\phi} \circ \phi = [2]$. From lectures (Lemma 6.1) we know $P - \phi(R) = o$ or $P - \phi(R) = (0,0)$. Hence $[P]$ in $\mathcal{H}/\phi(\mathcal{G})$ is $[o]$ or $[(0,0)]$.

(b) We thus get $\hat{\phi}(\mathcal{H})/2\mathcal{G}$ is C_2^a or C_2^{a-1} according to whether the class $[(0,0)]$ is trivial or not. The result now follows from the isomorphism of groups

$$\mathcal{G}/\hat{\phi}(\mathcal{H}) \cong \mathcal{G}/2\mathcal{G} \,/\, \hat{\phi}(\mathcal{H})/2\mathcal{G}.$$

(c) Assume $\phi(P) = (0,0)_{\mathcal{H}}$ for some $P \in \mathcal{G}$. Applying $\hat{\phi}$ to both sides we see $2P = \hat{\phi}((0,0)_{\mathcal{H}}) = o_{\mathcal{G}}$. But P cannot be $(0,0)_{\mathcal{G}}$ for then we'd have $\phi(P) = o_{\mathcal{H}}$. So we have an additional 2-torsion point in $\mathcal{G}$ and the 2-torsion is C_2^2.

Conversely, assume that the 2-torsion in $\mathcal{G}$ is C_2^2 and let $P \in \mathcal{G}$ with $P \neq (0,0)_{\mathcal{G}}$ and $2P = o_{\mathcal{G}}$. Then we have $\hat{\phi}(\phi(P)) = o_{\mathcal{G}}$ and by Lemma 6.1 again we see $\phi(P) = o_{\mathcal{H}}$ or $(0,0)_{\mathcal{H}}$. But since $P \neq (0,0)_{\mathcal{G}}$ we cannot have the former.

Thus either the rank is $a + b - 2$ or $(a + b - 1) - 1$, in the two cases.

5. [2006 paper, Qu 8(ii)] For any prime $p \equiv 5 \bmod 8$ show that the elliptic curve $Y^2 = X^3 + p^2X$ has rank 0.

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

The map $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u,v) \mapsto u$, for $(u,v) \neq (0,0)$, with $q : (0,0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, is an injection with im$q$ contained in $\{d : d \text{ is square free and } d|b_1\} = \{\pm 1, \pm 2, \pm p, \pm 2p\}$. Also, $\mathbf{o} \mapsto 1$, $(0,0) \mapsto -1$, $(2p,0) \mapsto 2p$, $(-2p,0) \mapsto -2p$, so that $\{\pm 1, \pm 2p\} \subset$ im$q \subset \{\pm 1, \pm 2, \pm p, \pm 2p\}$. There is only one coset to check, represented by -2, say. We know that $-2 \in$ im$q$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that:

$(-2)\cdot\ell^4 + a_1\ell^2m^2 + (b_1/(-2))\cdot m^4 = n^2$; that 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 $\ell = p\ell'$, $n = pn'$. Then $-2p^2(\ell')^4 + 2m^4 = (n')^2$. Since also $\left(\frac{2}{p}\right) = -1$, this implies $p|m$, $p|n'$. This gives a contradiction, since $p|\ell, p|m$ and $\gcd(\ell, m) = 1$. Hence $-2 \notin \text{im}q$, giving that $\text{im}q = \{\pm 1, \pm 2p\}$, 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 $(u,v) \neq (0,0)$, with $\hat{q} : (0,0) \mapsto a_1^2 - 4b_1 = b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with $\text{im}\hat{q}$ contained in $\{d : d \text{ is square free and } d|b\}$ $= \{\pm 1, \pm p\}$. Also, $\mathbf{o} \mapsto 1$ and $(0,0) \mapsto p^2 = 1$, so that $\{1\} \subset \text{im}\hat{q} \subset \{\pm 1, \pm p\}$.

We know that $-1 \in \text{im}\hat{q}$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, 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 impossible 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 integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $p\cdot\ell^4 + a\ell^2m^2 + (b/p)\cdot m^4 = n^2$; that is: $p\ell^4 + pm^4 = n^2$, and so $p|n$. Letting $n = pn'$, the equation becomes $\ell^4 + m^4 = p^2(n')^2$, which in turn implies $p|\ell, p|m$, since $-1 \not\equiv a^4$ for any a [as can be seen by taking both sides of $-1 \equiv a^4$ to the power of $(p-1)/4$]. This again contradicts $\gcd(\ell, m) = 1$, and so $p \notin \hat{q}$. 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 $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $\mathbf{o}$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}\big((0,0)\big) = \mathbf{o}$, and $\hat{\phi}\big((2p,0)\big) = (0,0)$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0,0)$, and so is the group C_2. Now $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}(\mathbb{Q})_{tors}/2\mathcal{C})(\mathbb{Q})_{tors} \times C_2^{rank}$, and $\mathcal{C}(\mathbb{Q})_{tors}/2\mathcal{C}(\mathbb{Q})_{tors}$ is isomorphic to the 2-torsion group of $\mathcal{C}(\mathbb{Q})_{tors}$ which is C_2 (consisting only of $\mathbf{o}$ and $(0,0)$), so that $\mathcal{C}(\mathbb{Q})_{tors}/2\mathcal{C}(\mathbb{Q})_{tors}$ is isomorphic to C_2. Conclusion: rank $= 0$.