

Elliptic Curves: Solutions to Sheet 4

- (1) Let $\phi : \mathcal{C}(\mathbb{Q}) \rightarrow \mathcal{D}(\mathbb{Q})$ be the usual isogeny, which is a group homomorphism with kernel: $\mathbf{o}, (0, 0)$, and let $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \rightarrow \mathcal{C}(\mathbb{Q})$ be the usual dual isogeny, which is also a group homomorphism with kernel: $\mathbf{o}, (0, 0)$. Now, let $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ be the set of torsion elements of $\mathcal{C}(\mathbb{Q})$ which have odd order. First check that $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ is a subgroup: (1) The identity $\mathbf{o}$ has order 1, which is odd, so $\mathbf{o} \in \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, (2) If P, Q have odd torsion orders m, n , respectively, then $mn(P + Q) = n(mP) + m(nQ) = \mathbf{o}$ and so the order of $P + Q$ divides mn , giving that the order of $P + Q$ is odd, i.e. $P + Q \in \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, (3) The order of $-P$ 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 define $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, 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. Let $R = \phi(P)$. Then $mR = m\phi(P) = \phi(mP) = \phi(\mathbf{o}) = \mathbf{o}$, which means that the order of R divides m , and so the order of R is odd; that is: $R \in \mathcal{D}_{\text{oddtors}}(\mathbb{Q})$. Hence, ϕ gives a map from $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ to $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, which certainly satisfies the homomorphism property $\phi(P + Q) = \phi(P) + \phi(Q)$ for all $P, Q \in \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$, since ϕ satisfies this property on the larger set $\mathcal{C}(\mathbb{Q})$. Furthermore, the kernel of $\phi : \mathcal{C}_{\text{oddtors}}(\mathbb{Q}) \rightarrow \mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ must only contain $\mathbf{o}$ [since $(0, 0) \notin \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$], and so $\phi : \mathcal{C}_{\text{oddtors}}(\mathbb{Q}) \rightarrow \mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ is an injection. We have therefore established that there is an injective homomorphism from $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ to $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$, which implies that $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$. Applying the same argument to $\hat{\phi} : \mathcal{D}_{\text{oddtors}}(\mathbb{Q}) \rightarrow \mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ gives that $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$.

Since $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ and $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ are finite groups, we deduce that we have inequalities $|\mathcal{C}_{\text{oddtors}}(\mathbb{Q})| \leq |\mathcal{D}_{\text{oddtors}}(\mathbb{Q})|$ and $|\mathcal{D}_{\text{oddtors}}(\mathbb{Q})| \leq |\mathcal{C}_{\text{oddtors}}(\mathbb{Q})|$, hence $|\mathcal{C}_{\text{oddtors}}(\mathbb{Q})| = |\mathcal{D}_{\text{oddtors}}(\mathbb{Q})|$. Now $\phi : \mathcal{C}_{\text{oddtors}}(\mathbb{Q}) \rightarrow \mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ is an injective homomorphism between finite groups of the same size, and is hence an isomorphism.

- (2) The preimages of $(0, 0)$ under $\hat{\phi}$ are given by the points of order 2 on $\mathcal{D}$ distinct from $(0, 0)$, namely $Q_1 = ((-a_1 + \sqrt{a_1^2 - 4b_1})/2, 0) = (a + 2\sqrt{b}, 0)$ and $Q_2 = ((-a_1 - \sqrt{a_1^2 - 4b_1})/2, 0) = (a - 2\sqrt{b}, 0)$. Recall the standard map from lectures $q : \mathcal{D}(\mathbb{Q}) \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ which takes $\mathbf{o} \rightarrow 1$, $(0, 0) \rightarrow b_1$, and otherwise takes $(u, v) \rightarrow u$. We know from lectures that this map has kernel precisely $\phi(\mathcal{C}(\mathbb{Q}))$. Now, the multiplication by 2 map on $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi} \circ \phi$, and so $(0, 0) \in 2\mathcal{C}(\mathbb{Q})$ iff either Q_1 or Q_2 is a member of $\phi(\mathcal{C}(\mathbb{Q}))$. In particular, the Q_i need to be in $\mathcal{D}(\mathbb{Q})$ which is equivalent to $b = m^2$ for some $m \in \mathbb{Z}$. The additional condition that $Q_i \in \phi(\mathcal{C}(\mathbb{Q}))$ is equivalent to $q(Q_i) = 1$, or $a \pm 2m \in (\mathbb{Q}^*)^2$. Finally, since $a \pm 2m \in \mathbb{Z}$, this condition is equivalent to the existence of $n \in \mathbb{Z}$ with $a \pm 2m = n^2$. Changing the sign of m if necessary gives the desired result.

(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. $\hat{\phi}(P + \phi(\mathcal{G})) = [o]$, that is $\hat{\phi}(P) + 2\mathcal{G} = 2\mathcal{G}$ so $\hat{\phi}(P) \in 2\mathcal{G}$. Then $\hat{\phi}(P) = 2R$ for some $R \in \mathcal{G}$. 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^b or C_2^{b-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.

Recall that $\mathcal{G}/2\mathcal{G} \cong C_2^{r+t}$ where r is the rank and $\mathcal{G}[2] \cong C_2^t$. We have either $t = 1$ or 2 . In the first case, $(0, 0) \notin \phi(\mathcal{G})$, so the rank is $(a + b - 1) - t = a + b - 2$. In the second case, $(0, 0) \in \phi(\mathcal{G})$, so the rank is $(a + b) - t = a + b - 2$.

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

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

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

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 $\hat{q} : \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x, y) \mapsto x$, for $(x, y) \neq (0, 0)$, with $\hat{q} : (0, 0) \mapsto b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with $\text{im} \hat{q}$ contained in

$\{d : d \text{ is square free and } d|b\} = \{\pm 1, \pm 3\}$. Also, $\mathbf{o} \mapsto 1$ and $(0, 0) \mapsto 3$, so that $\{1, 3\} \subset \text{im} \hat{q} \subset \{\pm 1, \pm 3\}$.

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

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 $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $(0, 0)$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}((0, 0)) = \mathbf{o}$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(0, 0)$, and so is isomorphic to C_2 . We also know that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q}) \times C_2^r$, which is isomorphic to $\mathcal{C}(\mathbb{Q})[2] \times C_2^r$, where $\mathcal{C}(\mathbb{Q})[2]$ is the 2-torsion group and r is the rank. We know that $(0, 0) \in \mathcal{C}(\mathbb{Q})[2]$, so we deduce that $r = 0$.

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

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

There is only one coset to check, represented by -1 , say. We know that $-1 \in \text{im} q$ iff there are integers ℓ, m, n , not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a_1\ell^2 m^2 + (b_1/(-1)) \cdot m^4 = n^2$ that is: $-\ell^4 - 28\ell^2 m^2 - 192m^4 = n^2$. We can see that the LHS is ≤ 0 and the RHS is ≥ 0 , and there is equality iff $\ell = m = n = 0$, a contradiction. Hence $-1 \notin \text{im} q$. We conclude that $\text{im} q = \{1, 2, 3, 6\}$ and that $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) = \{\mathbf{o}, (0, 0), (8, 16), (24, -48)\}$, and so $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ is generated by $(0, 0)$ and $(8, 16)$.

The map $\hat{q} : \mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u$, for $(u, v) \neq (0, 0)$, with $\hat{q} : (0, 0) \mapsto a_1^2 - 4b_1 = b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with $\text{im} \hat{q}$ contained in $\{d : d \text{ is square free and } d|b\} = \{\pm 1\}$. Also, $\mathbf{o} \mapsto 1$ and $(0, 0) \mapsto 1$, so that $\{1\} \subset \text{im} \hat{q} \subset \{\pm 1\}$.

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

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

Finally, since multiplication by 2 in $\mathcal{C}(\mathbb{Q})$ is $\hat{\phi} \circ \phi$, we have that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by: generators for $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ [namely: $\mathbf{o}$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ [namely, $\hat{\phi}((0, 0)) = \mathbf{o}$ and $\hat{\phi}((8, 16)) = (1, -4)$]. Conclusion: $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is generated by $(1, -4)$, and so is the group C_2 . Now $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is isomorphic to $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q}) \times C_2^{\text{rank}}$, and $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q})$ is isomorphic to the 2-torsion group of $\mathcal{C}_{\text{tors}}(\mathbb{Q})$ which is C_2 (consisting only of $\mathbf{o}$ and $(0, 0)$), so that $\mathcal{C}_{\text{tors}}(\mathbb{Q})/2\mathcal{C}_{\text{tors}}(\mathbb{Q})$ is isomorphic to C_2 . Conclusion: $\text{rank} = 0$. [If this seems surprising, then note that $(1, 4), (1, -4)$ are points of order 4 in $\mathcal{C}(\mathbb{Q})$].

- (5) 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 $\phi : \mathcal{C}(\mathbb{Q}) \rightarrow \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto (y^2/x^2, y - p^2y/x^2)$, and dual isogeny $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \rightarrow \mathcal{C}(\mathbb{Q}) : (u, v) \mapsto (\frac{1}{4}v^2/u^2, \frac{1}{8}(v + 4p^2v/u^2))$.

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 $\text{im}q$ 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 $\{\pm 1, \pm 2p\} \subset \text{im}q \subset \{\pm 1, \pm 2, \pm p, \pm 2p\}$. There is only one coset to check, represented by -2 , say. We know that $-2 \in \text{im}q$ 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 $p \equiv 5 \pmod{8}$, $(\frac{-2}{p}) = -1$, and so $p|\ell, p|n$. Let $\ell = p\ell', n = pn'$. Then $-2p^2(\ell')^4 + 2m^4 = (n')^2$. Since also $(\frac{2}{p}) = -1$, 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 $\mathbf{R}$. 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, $\hat{\phi}((0, 0)) = \mathbf{o}$, and $\hat{\phi}((2p, 0)) = (0, 0)$]. 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: $\text{rank} = 0$.

(6) We are given that $A, +$ is an Abelian group, and that $h : A \rightarrow \mathbf{R}_{\geq 0}$ satisfies:

(I) There exists a constant C , independent of P, Q , such that

$$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| \leq C, \text{ for all } P, Q \in A,$$

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

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

Letting $Q = P$ in (I), we obtain:

$$|h(2P) + h(e) - 4h(P)| \leq C, \quad (*)$$

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

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

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

Multiplying $(*)$ by 2 gives:

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

These last two equations then give:

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

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

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

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

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

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

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