=1200

Elliptic Curves. Solutions to Sheet 4.

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

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

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

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

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

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

2. Let $\phi : \mathcal{C}(\mathbf{Q}) \to \mathcal{D}(\mathbf{Q})$ be the usual isogeny, which is a group homomorphism with kernel: $\mathbf{o}, (0,0)$, and let $\hat{\phi} : \mathcal{D}(\mathbf{Q}) \to \mathcal{C}(\mathbf{Q})$ be the usual dual isogeny, which is also a group homomorphism with kernel: $\mathbf{o}, (0,0)$. Now, let $\mathcal{C}_{\text{oddtors}}(\mathbf{Q})$ be the set of torsion elements of $\mathcal{C}(\mathbf{Q})$ which have odd order. First check that $\mathcal{C}_{\text{oddtors}}(\mathbf{Q})$ is a subgroup: (1) The identity $\mathbf{o}$ has order 1, which is odd, so $\mathbf{o} \in \mathcal{C}_{\text{oddtors}}(\mathbf{Q})$, (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. $P+Q \in \mathcal{C}_{\text{oddtors}}(\mathbf{Q})$, (3) The order of $-P$ is the same as the order of $-P$, so $P \in \mathcal{C}_{\text{oddtors}}(\mathbf{Q}) \Rightarrow -P \in \mathcal{C}_{\text{oddtors}}(\mathbf{Q})$. Similarly define $\mathcal{D}_{\text{oddtors}}(\mathbf{Q})$, a subgroup of $\mathcal{D}(\mathbf{Q})$.

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

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

$(\mathbf{Q}^*)^2 \iff b = m^2$ and $a + 2m = n^2$, for some $m, n \in \mathbf{Q}$; but in fact m, n must be in $\mathbf{Z}$ since $a, b \in \mathbf{Z}$.

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

The map $q : \mathcal{D}(\mathbf{Q})/\phi(\mathcal{C}(\mathbf{Q})) \to \mathbf{Q}^*/(\mathbf{Q}^*)^2 : (u, v) \mapsto u$, 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 $\{d : d \text{ is square free and } d|b_1\} = \{\pm1, \pm2\}$. Also, $\mathbf{o} \mapsto 1$, $(0, 0) \mapsto -8 = -2$, so that $\{1, -2\} \subset \text{im}q \subset \{\pm1, \pm2\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in \text{im}q$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1)\cdot\ell^4 + a_1\ell^2m^2 + (b_1/(-1))\cdot m^4 = n^2$ that is: $-\ell^4 - 4\ell^2m^2 + 8m^4 = n^2$. Rewrite as: $-(\ell^2 + 2m^2)^2 + 12m^4 = n^2$. Reducing modulo 3 gives $-(\ell^2 + 2m^2)^2 \equiv n^2$ (modulo 3). If n were coprime to 3, then this would give: $((\ell^2 + 2m^2)/n)^2 = -1$ in $\mathbf{F}_3$, 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 $\mathbf{Q}_3$, and so impossible in $\mathbf{Q}$. Hence $-1 \notin \text{im}q$.

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

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

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: $-\ell^4 + 2\ell^2m^2 - 3m^4 = n^2$. 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 $\mathcal{C}(\mathbf{Q})/\hat{\phi}(\mathcal{D}(\mathbf{Q}))$ is generated by $(0, 0)$.

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

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

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

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

The map $\hat{q} : \mathcal{C}(\mathbf{Q})/\hat{\phi}(\mathcal{D}(\mathbf{Q})) \mapsto \mathbf{Q}^*/(\mathbf{Q}^*)^2 : (u, v) \mapsto u$, 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 im$\hat{q}$ contained in $\{d : d \text{ is square free and } d|b\} = \{\pm1\}$. Also, $\mathbf{o} \mapsto 1$ and $(0, 0) \mapsto 1$, so that $\{1\} \subset$ im$\hat{q} \subset \{\pm1\}$.

There is only one coset to check, represented by -1, say. We know that $-1 \in$ im$\hat{q}$ iff there are integers ℓ, m, n, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1)\cdot\ell^4+a\ell^2m^2+(b/(-1))\cdot m^4 = n^2$; that is: $-\ell^4+14\ell^2m^2-m^4 = n^2$. Rewrite as: $-(\ell^2 - 7m^2)^2 + 48m^4 = n^2$. Reducing modulo 3 gives: $-(\ell^2 - 7m^2)^2 \equiv n^2$ (modulo 3). If n were coprime to 3, then this would give: $((\ell^2 - 7m^2)/n)^2 = -1$ in $\mathbf{F}_3$, 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 $-1 \notin$ im$\hat{q}$.

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

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

5. We are given that $A,+$ is an Abelian group, and that $h : A \to \mathbf{R}_{\geq 0}$ satisfies:
(I) There exists a constant C, independent of P, Q, such that
$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| \leq C$, 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:

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

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:

$$|h(3P)-9h(P)| = |h(3P)-2h(2P)-h(P)+2h(2P)+2h(e)-8h(P)-2h(e)|$$
$$\leq |h(3P) - 2h(2P) - h(P)| + |2h(2P) + 2h(e) - 8h(P)| + 2|h(e)| \leq C_3,$$

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

6. 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 be squaring the previous one, and reducing modulo N). Now, we write 46 in base 2: $46 = 2+4+8+32$ and so $2^{46} \equiv 2^2 2^4 2^8 2^{32} \equiv 4 \cdot 16 \cdot 256 \cdot 230 \equiv 64 \cdot 6475 \equiv 5641$ modulo N, so that $2^{46} - 1 \equiv 5640$ modulo N.

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

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

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