

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.

(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 $N = 10481 = 47 \cdot 223$.

(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.