Elliptic Curves. HT 2020/21. Sheet 4.

1. Find the torsion group over $\mathbb{Q}$ for each of:
(a). $Y^2 = X^3 + 1$. **(b).** $Y^2 = X(X-1)(X-2)$. **(c).** $Y^2 = X^3 + 1/3^6$.

2. Let, as usual, $\mathcal{C} : Y^2 = X(X^2 + aX + b)$ and $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1)$, where $a, b \in \mathbb{Z}$, $a_1 = -2a, b_1 = a^2 - 4b$ and $b(a^2-4b) \neq 0$. Let $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ denote the set of torsion elements of $\mathcal{C}(\mathbb{Q})$ which have odd order, and let $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ denote the set of torsion elements of $\mathcal{D}(\mathbb{Q})$ which have odd order. Show that $\mathcal{C}_{\text{oddtors}}(\mathbb{Q})$ and $\mathcal{D}_{\text{oddtors}}(\mathbb{Q})$ are isomorphic.

3. Let $\mathcal{C}$ and $\mathcal{D}$ be as in question 2. Let the homomorphisms $\phi, \hat{\phi}$ be defined as usual by

$$\phi : \mathcal{C} \to \mathcal{D} : (x, y) \mapsto \left(\left(\tfrac{y}{x}\right)^2, y - \tfrac{by}{x^2}\right), \quad \hat{\phi} : \mathcal{D} \to \mathcal{C} : (u, v) \mapsto \left(\tfrac{1}{4}\left(\tfrac{v}{u}\right)^2, \tfrac{1}{8}\left(v - \tfrac{b_1 v}{u^2}\right)\right).$$

What are the preimages of $(0,0)$ under $\hat{\phi}$? Show that $(0,0) \in 2\mathcal{C}(\mathbb{Q})$ if and only if there exist $m, n \in \mathbb{Z}$ such that $b = m^2$ and $a + 2m = n^2$.

4. Find the ranks of the following elliptic curves.
(a). $Y^2 = X(X^2 + 2X + 3)$.
(b). $Y^2 = X(X^2 + 14X + 1)$.

5. Let $A, +$ be an Abelian group. Let $h : A \to \mathbb{R}_{\geqslant 0}$ satisfy:
(I) There exists a constant C, independent of P, Q, such that
$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| \leqslant C$, for all $P, Q \in A$,
(II) For any $B \in \mathbb{R}$, the set $\{P \in A : h(P) \leqslant B\}$ is finite.
Show that h is a height function on A. Show also that there exists a constant C_3, independent of P, such that $|h(3P) - 9h(P)| \leqslant C_3$, for all $P \in A$.
[$\mathbb{R}_{\geqslant 0}$ denotes $\{x \in \mathbb{R} : x \geqslant 0\}$].

6. A four-letter word $L_1L_2L_3L_4$ has been divided into two pairs: L_1L_2 and L_3L_4. Each of these pairs has been converted into an integer (of at most 4 digits) via the standard map: $A \mapsto 01, B \mapsto 02, \ldots, Z \mapsto 26$. These integers have been encoded by taking each to the power of $d = 4085$, modulo $N = 10481$. The encoded message reads: **6012**, **3236**. You may assume that N is the product of two primes. You should show, in your calculations, how you are only using numbers of length at most 9 digits.
(a) Find a proper factor of N (that is, a factor d of N satisfying $1 < d < N$) by applying Pollard's "$p-1$" method, using base 2 and exponent 46.
(b) Factorise N by applying the Elliptic Curve Method, using the curve $\mathcal{E} : Y^2 = X^3 - X + 1$ and $3P$, where $P = (5, 11)$.
(c) Use the factorisation of N to decode the message (which is the name of the town famous for being the country music capital of New Zealand).