Elliptic Curves.
Some exam-style questions.

The following are some exam-style questions, to supplement the actual exams available.

Elliptic Curves. Some Exam-style Questions.

Question 1.

(i) Find an $x \in \mathbb{Z}$ such that $|x^2+3|_7 < 7^{-1}$.

(ii) For what prime p does $-\frac{9}{8}$ have p-adic expansion $1, \overline{2} = 1 + 2p + 2p^2 + 2p^3 + \ldots$?

(iii) Let $p \equiv 1 \pmod 3$ be prime. Show that -3 is a quadratic residue mod p [*Hint: consider separately the cases* $p \equiv 1$ (*mod* 4) *and* $p \equiv 3$ (*mod* 4)]. Use Hensel's Lemma to deduce that -3 is a square in $\mathbb{Q}_p^*$.

(iv) Let $q \equiv 1 \pmod{27}$ be prime. Show that $(X^2+3)(X^3-q) = 0$ has solutions in $\mathbb{R}$ and every $\mathbb{Q}_p$.

Question 2.

(i) Find the torsion group over $\mathbb{Q}$ of the elliptic curve $Y^2 = X^3 + 3$.

(ii) Find the torsion group over $\mathbb{Q}$ of the elliptic curve $Y^2 = X^3 + 4X$.

(iii) Let $n \in \mathbb{Z}$ satisfy $n \neq 0, \pm 1$. Show that $\big(n, \pm n(n+1)\big)$, $\big(-n, \pm n(n-1)\big)$ are points of order 4 on the elliptic curve $Y^2 = X(X+1)(X+n^2)$. Find the torsion group over $\mathbb{Q}$ when $n \equiv 2$ (modulo 5).

(iv) Let $k \in \mathbb{Z}$, $k \neq 0$, let $\mathcal{E}$ be the elliptic curve $Y^2 = X^3 - k^2X + k^3$, and let (x, y) be a point of finite order in $\mathcal{E}(\mathbb{Q})$. Show that $|y| \leqslant 5|k|^3$ and $|x| \leqslant 3|k|^2$.

Question 3. Let $\mathcal{C} : Y^2 = X(X^2 + aX + b)$ and $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1)$, where $a, b \in \mathbb{Z}$ with $b(a^2 - 4b) \neq 0$ and $a_1 = -2a$, $b_1 = a^2 - 4b$. Let the map ϕ [which you may assume to be a homomorphism] be defined as usual by

$$\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto \left(\frac{y^2}{x^2}, y - \frac{by}{x^2}\right).$$

Let q be defined as usual by

$$q : \mathcal{D}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u \text{ when } u \neq 0,$$

$$q : (0,0) \mapsto b_1, \;\; q : \underline{\mathbf{o}} \mapsto 1,$$

where $\underline{\mathbf{o}}$ denotes the point at infinity on $\mathcal{D}$.

(i) Show that the image of q is a subset of the finite set

$$\{r : r \text{ is a square free integer and } r | b_1\}.$$

(ii) Find the rank of the elliptic curve $Y^2 = X(X^2 + 2X + 3)$.

Question 4. 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 $d = 4451$, modulo $N = 10001$. The encoded message reads:

$$6847,\ 2577.$$

You may assume that N is the product of two primes.

(i) Factorise N by applying Pollard's "$p-1$" method, using base 2 and exponent 68.

(ii) Use the factorisation of N to decode the message (which is the name of the animal used as the mascot for the sports teams at the University of California at Santa Cruz).

(iii) Let A be an Abelian group with group operation $+$, and let $h : A \longrightarrow \mathbb{R}$ satisfy:

(1) For any $Q \in A$, there exists $C_1 = C_1(Q)$ such that $h(P+Q) \leqslant 2h(P) + C_1$ for all $P \in A$.

(2) There exists C_2, independent of P, such that $h(2P) \geqslant 4h(P) - C_2$ for all $P \in A$.

(3) For any C_3, the set $\{P \in A : h(P) \leqslant C_3\}$ is finite.

Suppose also that $A/2A$ is finite. Prove that A is finitely generated.

(iv) Let A and h be as in (c). Suppose that P is a torsion element of A [that is: there exists an integer $N > 0$ such that NP is the identity element of A]. Show that $h(P) \leqslant \frac{1}{3}C_2$.