(1) Suppose $E$ is an elliptic curve $y^2 = x^3 + ax + b$.
   (a) Show that $P$ is a point of order 3 on $E$ if and only if the tangent line to $E$ at $P$ intersects $E$ with multiplicity 3.
   (b) Use (a) to compute the polynomial whose roots are the $x$-coordinates of the points of order 3 on $E$.

(2) Suppose $a \in \mathbb{Q}^\times$ and consider the curve $E : x^3 + y^3 = az^3$ in $\mathbb{P}^2$. Then $E$ has genus 1 (you may assume this), so with the rational point $O := [1, -1, 0]$, $E$ is an elliptic curve.
   (a) Show that three points of $E$ sum to $O$ if and only if they are collinear.
   (b) Show that $-[x, y, z] = [y, x, z]$.
   (c) Find all the points of order 2 in $E(\mathbb{Q})$, $E(\mathbb{C})$.
   (d) Use the method of problem (1) to show that the points of order dividing 3 in $E(\mathbb{C})$ are the ones with $xyz = 0$. Find all the points of order 3 in $E(\mathbb{Q})$.

(3) Let $E$ be the elliptic curve of problem (2).
   (a) At which primes of $\mathbb{Z}$ does $E$ have good reduction?
   (b) Show that if $E$ has good reduction at $p$ and $p \equiv 2 \pmod{3}$, then $|E(\mathbb{F}_p)| = p+1$.
   (c) Determine $E(\mathbb{Q})_{tor}$.

(4) Suppose $E$ is an elliptic curve over a field $K$, $m \in \mathbb{Z}$, $m \geq 3$ and $\text{char}(K) \nmid m$. Prove (without using the classification of possible endomorphism algebras of $E$) that the natural map

$$\text{Aut}(E) \to \text{Aut}(E[m])$$

is injective.

(5) Suppose $K$ is a finite extension of $\mathbb{Q}_p$, $v : K^\times \to \mathbb{Z}$ is the valuation on $K$, and $E$ is an elliptic curve over $K$. Prove that if $j(E) \geq 0$, then the minimal discriminant $\Delta(E)$ satisfies

$$v(\Delta(E)) < 12 + 12v(2) + 6v(3).$$

(6) Suppose $E$ is the elliptic curve $y^2 + y = x^3$ over $\mathbb{Q}$.
   (a) Show that $E$ has good reduction at all primes different from 3.
   (b) Show that $(0,0) \in E(\mathbb{Q})$ has order 3.
   (c) Let $K = \mathbb{Q}(\sqrt{-3})$ and $\zeta = (-1 + \sqrt{-3})/2$. Show that $(-1, \zeta) \in E(K)$ has order 3.
   (d) Show that the rank of $E(K)$ is at most 2 (you may use that the maximal abelian extension of $K$ of exponent 3, unramified outside of the prime above 3, is $K(\sqrt[3]{2}e^{2\pi i/9}, \sqrt[3]{3})$).
   (e) Conclude that the rank of $E(\mathbb{Q})$ is at most 2.
(7) Show that for the curve $E$ of problem (6), $E(Q)_{\text{tors}} = \mathbb{Z}/3\mathbb{Z}$ and $E(K)_{\text{tors}} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(8) Suppose $K$ is a number field, $E$ is an elliptic curve over $K$, and $L/K$ is an infinite Galois extension of number fields. Suppose further that the rank of $E(M)$ is bounded as $M$ ranges over finite extensions of $K$ in $L$.

(a) Prove that $E(L) \otimes \mathbb{Q}$ is a finite-dimensional $\mathbb{Q}$-vector space.

(b) Prove that if $E(L)_{\text{tors}}$ is finite, then $E(L)$ is finitely generated.

(9) Suppose $E$ is an elliptic curve over a number field $K$, $m \in \mathbb{Z}$, $m \geq 2$, and there is a function $h : E(K) \to \mathbb{R}$ satisfying:

(a) For every $Q \in E(K)$ there is a constant $C_Q \in \mathbb{R}$ such that for all $P \in E(K)$,

\[ h(P + Q) \leq 2h(P) + C_Q. \]

(b) There is a constant $D \in \mathbb{R}$ such that for every $m \in E(K)$,

\[ h(mP) \geq m^2 h(P) - D. \]

(c) For every $B \in \mathbb{R}$, \( \{ P \in E(K) : h(P) < B \} \) is finite.

Prove that if $E(K)/mE(K)$ is finite, then $E(K)$ is finitely generated.

(10) Let $\mathfrak{H}$ be the complex upper half plane, $N \in \mathbb{Z}^+$, and

\[ \Gamma_1(N) = \{ \alpha \in \text{SL}_2(\mathbb{Z}) : \alpha \equiv \begin{pmatrix} 1 & \ast \\ 0 & 1 \end{pmatrix} \pmod{N} \} \]

acting on $\mathfrak{H}$ via linear fractional transformations. For every $\tau \in \mathfrak{H}$ let $L_\tau = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ and let $E_\tau$ be the elliptic curve

\[ y^2 = 4x^3 - g_2(\tau)x - g_3(\tau), \]

so that

\[ \xi_\tau = (\varphi(\cdot ; L_\tau), \varphi'(\cdot ; L_\tau)) : \mathbb{C}/L_\tau \cong E_\tau(\mathbb{C}) \]

is an isomorphism.

Suppose $\tau, \tau' \in \mathfrak{H}$.

(a) Prove that $E_\tau$ is isomorphic to $E_{\tau'}$ over $\mathbb{C}$ if and only if there is a $\gamma \in \text{SL}_2(\mathbb{Z})$ such that $\gamma(\tau) = \tau'$.

(b) Let $P = \xi(1/N) \in E_\tau[N]$ and $P' = \xi(1/N) \in E_{\tau'}[N]$ Prove that there is an isomorphism $\phi : E_\tau \to E_{\tau'}$ such that $\phi(P) = P'$ if and only if there is a $\gamma \in \Gamma_1(N)$ such that $\gamma(\tau) = \tau'$. 