TAKE HOME FINAL

TOPICS IN ALGEBRAIC GEOMETRY: ELLIPTIC CURVES

(1) Let $p \equiv 3 \bmod 8$ be a prime. Use descent via 2-isogenies to show that the elliptic curves $y^2 = x(x^2 - p)$ have rank 0.

(2) Let $p \equiv 9 \bmod 16$ be a prime, and consider the elliptic curve $E : y^2 = x(x^2 + p^2)$.
   (a) Show that the torsor $\mathcal{T}(p) : N^2 = pM^4 + pe^4$ has local solutions in every completion $\mathbb{Q}_\ell$.
   Hints: this is taken care of by a theorem for $\ell \nmid 2p$. For $\ell = p$, show that $\mathbb{Z}_p$ contains an element ζ with $\zeta^4 = -1$. For $\ell = 2$, show that $\mathbb{Z}_2$ contains $\sqrt{p}$.
   (b) Show that $\mathcal{T}(p)$ does not have a nontrivial solution in integers.
   Hints: Show that $N = pn$ and cancel. For primes $q \mid n$, show that $x^4 \equiv -1 \bmod q$ is solvable; this implies $q \equiv 1 \bmod 8$. Show that $pn^2 \equiv 9 \bmod 16$, and check out the possibilities of $M^4 + e^4 \bmod 16$.
   This means that $\mathcal{T}(p)$ represents an element of order 2 in the Tate-Shafarevich group of $\overline{E}$.

(3) Consider the elliptic curve
$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$
with coefficients $a_i \in \mathbb{Z}$. We know that a point $P = (x, y)$ on E has order 3 if and only if x is a root of the quartic polynomial
$$T_3(x) = 3x^4 + 4a_2x^3 + 6a_4x^2 + 12a_6x + 4a_2a_6 - a_4^2 = 0.$$
   (a) Compute all nine points in $E[3] = \{P \in E(\overline{\mathbb{Q}}) : 3P = \mathcal{O}\}$ in the special case $a_2 = a_4 = 0$.
   (b) Put $K = \mathbb{Q}(E[3])$ and determine $(K : \mathbb{Q})$ and $\mathrm{Gal}\,(K/\mathbb{Q})$.
   (c) Consider the special case $a_6 = 2k^3$; for which values of k does E have rational points of order 3?
   (d) A subgroup $H \subseteq E[n]$ is called rational if $P \in H$ implies $P^\sigma \in H$ for all automorphisms $\sigma \in G_\mathbb{Q}$. Show that, if $a_6 = 2k^3$, the group $E[3]$ can be written as the direct sum of two rational subgroups.
   Remark: In the language of representation theory, this means that the representation $\rho_3 : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ given by the action of $G_\mathbb{Q}$ on $E[3]$ is reducible.
   (e) In the case $a_6 = 2k^3$, pick generators P and Q of the two rational subgroups; these two points form a basis for $E[3]$. Compute the matrices $\rho_3(P)$ and $\rho_3(Q)$.