Due Monday, December 6 at 11:59pm. Please turn in via email or in my mailbox in Hylan 913. All chapter and exercise numbers refer to Silverman's *A Friendly Introduction to Number Theory*, 4th edition.

(1) Ex. 36.5(a)

(2) Ex. 28.5

(3) Ex. 28.7

(4) Ex. 29.6

Definition. The **order** of a point P of an elliptic curve E is the smallest positive integer k such that $kP = \mathcal{O}$.

(5) Consider the point $P = (3, 8)$ on the cubic curve

$$y^2 = x^3 - 43x + 166.$$

Compute $2P$, $4P$, and $8P$. Determine the order of P.

(6) Let E be an elliptic curve $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$ and $\Delta(E) \neq 0$.

(a) Find a polynomial whose roots are the x-coordinates of all points in $E(\mathbb{C})$ with order 3. (Hint: if $3P = \mathcal{O}$, then $2P = -P$.)

(b) Find an upper bound bound on the number of points in $E(\mathbb{C})$ with order 3.

(c) For the particular curve $y^2 = x^3 + 1$, find all points of order 3.

(d) REMOVED

(7) REMOVED

(8) Consider the elliptic curve $y^2 = x^3 + 2x + 3$. Find all solutions modulo 2, 3, 5, 7, and 11. ~~In each case find a point of maximal order.~~

(9) Consider the elliptic curve $y^2 = x^3 + 33x + 69$. The points $P = (72, 20)$ and $Q = (82, 46)$ are solutions modulo 97.

(a) Compute the following points of E modulo 97.

(i) $2P$

(ii) $5P$

(iii) $7P$

(iv) $10P$

(v) $Q - 10P$

(vi) $Q - 20P$

(vii) $Q - 40P$

(b) Use the coordinates found in part (a) to compute $k \in \mathbb{Z}$ such that $Q \equiv kP \mod 97$. (Hint: Two of the points in part (a) are congruent mod 97. If you did not observe this, check your work.)