Homework due Wednesday December 1.
Read Chapters 5 and 6 of An Introduction to the Theory of Numbers.

Problems to turn in:
Problem 1. Let C be a non-singular cubic equation given by

$$y^2 = f(x) = x^3 + ax + b.$$

Prove that
$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)}.$$

Using this expression deduce that a point has order dividing three if and only if the point is an inflection point of C. Assuming a and b are real show that the numerator of the above expression has exactly two real roots $c < d$. Show $f(c) < 0$ and $f(d) > 0$. Deduce that the real points of order dividing three on C form a cyclic group of order 3.

Problem 2. Let p be a prime number. Let C be the elliptic curve

$$y^2 = x^3 + px.$$

Determine all the rational points of finite order on C.

Problem 3. For the following elliptic curves determine all the rational points of finite order.

$$a)\ y^2 = x^3 - 2,$$
$$b)\ y^2 = x^3 + 8,$$
$$c)\ y^2 = x^3 + 4x,$$
$$d)\ y^2 = x^3 - 4x$$

page 248 section 5.5 problems: 1, 4, 6
page 260 section 5.6 problems: 2, 4, 5, 9, 14
page 278 section 5.7 problems: 3, 4, 10, 11