**Homework 6**

*Due Tuesday Nov 7th*

**1) (a)** Verify that the point P(0, 16) is on the elliptic curve y2 = x3 + 256, defined over the field of rational numbers Q.

**y2 = x3 + 256**

**P(0, 16)**

**x = 0**

**y = 16**

**162 = 03 + 256**

**256 = 256**

**P(0,16) is on the curve y2 = x3 + 256**

**(b)** Find 2P and 3P.

**1P = (0,16)**

**2P = (0,-16)**

**P = -2P**

**3P = O**

**(c)** Find the order of P (the smallest integer n such that nP = O).

**1P = (0,16)**

**2P = (0,-16)**

**P = -2P**

**3P = O**

**Order of P is 3**

**2)** Find the order of P(½, ½) over Q on the curve y2 = x3 + ¼x.