MAT 301 Problem Set 5

[Posted: March 25, 2013. Due: noon on April 3 (**Wednesday**), 2013. Worth: 100 points]

1. **Elliptic Curves (50 points)**

   (a) Let E be the elliptic curve over the rationals $\mathbb{Q}$ defined by the equation $Y^2 = X^3 - 2X + 4$ and let $P = (0, 2)$ and $Q = (3, -5)$. (Check that P and Q are actually on the curve). Compute $P \oplus Q$, $2P$ and $2Q$.

   (b) Let p be a prime satisfying $p = 2 \pmod 3$. Let E be the elliptic curve over $\mathbb{F}_p$ defined by $y^2 = x^3 + 1 \pmod p$. How many points does E have, and why?

2. **Secret Sharing (50 points)** Suppose that the teaching staff of a course consists of three professors and two TAs. The solutions to problem sets in the course are encrypted with a key K that is shared between the five staff members. Your goal is to come up with a method of secret-sharing the key so that

   (a) all the three professors together, or

   (b) both the TAs together, or

   (c) any TA together with any professor

   should be able to access the solutions. No other combination of staff members should be able to lay their hands on it (for example, if two professors come together, they should have no idea what the key K is, and therefore, they will not be able to decrypt and figure out the solutions).

   Assume that the key is a number in $\mathbb{Z}_q$ for some prime number q.