Math 502 Daily Assignment

due Thursday, April 24, 2008

Exercises from the text

262: 6, 7, 12 – 14, 16, 17, 20, 21, 24, 25

Further Exercises

1. Find a point A of largest possible order on the cubic curve $y^2 + y = x^3 - x$ over the finite field $\mathbf{Z}/59\mathbf{Z}$; then express the affine point $(0, 0)$ as a multiple of A.

2. It is agreed between George and Karla to construct jointly a private value using the Diffie-Hellman algorithm with powers of the primitive root 6 modulo 761. Karla randomly picks the power 221 and, accordingly, sends George the number 481. George sends Karla the number 22. What private value have they jointly constructed?

3. George and Karla decide to use the Diffie-Hellman algorithm with powers (i.e., additive multiples) of the point $(0, 0)$ in the arithmetic of points on the cubic curve E with equation $y^2 + y = x^3 - x$ over the finite field $\mathbf{Z}/761\mathbf{Z}$.

   (a) How many points does E contain in the finite field $\mathbf{Z}/761\mathbf{Z}$.

   (b) What is the order of $(0, 0)$ in the arithmetic of points on E over this field?

   (c) If Karla sends George the 221st power of the point $(0, 0)$ and George sends Karla the point $(265, 321)$, what private point have they jointly constructed on the curve E?