WRITTEN HOMEWORK #3, DUE APRIL 23, 2010

Unless explicitly noted, you are to justify all of your responses with work and/or proofs.

(1) Exercise 1.11 from the text. Notice that part (d) tells you that it doesn't matter which point you choose as the identity on an elliptic curve, from the standpoint of group theory.
(2) Exercise 1.15 from the text. For part (a), you want to show that the given map has a rational inverse.
(3) Exercise 1.16 from the text. This exercise might explain why elliptic curves got their name, even though they certainly aren't ellipses.
(4) Exercise 1.19 from the text. Part (c) is a repeat of material we will be covering in class, so you can either wait until we cover it and copy it, or read ahead in the book, or figure it out yourself (it's not overly hard).
(5) Exercise 1.20 from the text.
(6) Exercise 2.1 from the text.

Suggested Exercises: Exercise 1.12 will give you experience with calculations for the addition law on a cubic curve not in Weierstrass normal form. Exercise 1.13 elaborates on an example we gave in class, but (b) is probably pretty hard, or at least tedious. Exercise 1.14 is a good problem to do if you want to learn how to convert a cubic curve to Weierstrass normal form, but you will have to work out the details of the sketchy procedure described on pgs. 22 and 23 of the book. Exercise 1.18ab is interesting to work out, c is good if you know how to write simple programs for a calculator or computer, and 1.18d is probably impossible given what we currently know.