MATH 6310, Homework 7
Due in class 10/16

Please continue to look over §8 and do

- §7.5, question 3
- §7.6, questions 6, 8, 10, 11
- §8.1, questions 6, 8 (see §7.1 for the definitions)
- §8.2, questions 1, 8

and —

1. Show that a ring R in which $x^3 = x$ for every $x \in R$ is commutative. (*I think this is harder than the $x^2 = x$ version! There's no assumption that R has a 1. Assuming such makes the question easier, so do so if you can't solve the problem in its more general form.*)

2. Here's a basic version of the RSA public key cryptosystem. Bob publishes a number N which is the product of a pair of distinct primes p and q, both of which equal 2 mod 3, and which he keeps secret. Bob finds some $t \in \mathbb{Z}$ such that $3t \equiv 1 \mod (p-1)(q-1)$.

   Alice wishes to send Bob a secret key x, an integer between 0 and $N-1$. (This key will then be used by Alice and Bob to exchange messages via another cryptosystem such as *DES* or *AES*.) Alice sends Bob $x^3 \mod N$. Bob can decode this by calculating $x^{3t} \mod N$ which will equal $x \mod N$.

   The security of this system depends on it being computationally hard to find t from N. This, in turn, depends on (but is not known to be equivalent to) the problem of factorizing N.

   (a) Why does such a t exist and how can Bob find it (efficiently)?

   (b) Why is $x^{3t} \equiv x \mod N$?

   (c) Explain (briefly) why encoding and decoding as described above can be done efficiently.

   (d) Suppose Alice sends the same key to Bob_1, Bob_2, and Bob_3, using their N_1, N_2 and N_3, and that Eve intercepts $x^3 \mod N_i$ for $i = 1, 2, 3$. Explain how Eve can efficiently find x. (*For this reason, and others,* 65537 *is used in place of* 3.)

Read on in §8.3 and §9.