Math 100a Fall 2009 Homework 3

Due 10/16/09 in class or by 4pm in the HW box on the 6th floor of AP&M

Reading

All references are to Beachy and Blair, 3rd edition.

Reading: 3.1, 3.2, 2.3. (After we cover 3.2, I have decided to cover 2.3 next, which is not what the online calendar originally said.)

Warmup problems

These are easier/extra problems which would be a good idea to take a look at first to brush up on definitions, etc. Do not hand these in.

Section 3.1: 1, 4, 5, 6, 7, 11

Section 3.2: 1, 5, 6, 7, 15, 19(a)(b)

Assigned Problems

Write up neat solutions to these problems:

Section 3.1: 2(b)(c)(d), 13, 14, 15, 23, 24 (Hint: same hint as for 23, notice that $x^2 = e$ is the same thing as $x = x^{-1}$; so you are being asked to find a non-identity element which is its own inverse.)

Section 3.2: 8, 20, 21(a)(b).

Problems not from the text (also to be handed in):

1. Is $(\mathbb{Z}_{14}^{\times}, \cdot)$ cyclic? is $(\mathbb{Z}_{12}^{\times}, \cdot)$ cyclic? Prove your answers.

2. Find all cyclic subgroups of $(\mathbb{Z}_{10}, +)$. Do this just by computation: take the cyclic subgroup generated by each element in turn. You should find only 4 *distinct* cyclic subgroups, including the trivial subgroup and the whole group. Use this example as a guide for intuition as you do the next problem.

3. Fix some $n \geq 2$. In this problem, you will find *all* subgroups of the group $G = (\mathbb{Z}_n, +)$. As a consequence, you will prove that *every subgroup of* $\mathbb{Z}_n$ *is cyclic, equal to* $\langle [d]_n \rangle$ *for some positive divisor* d *of* n. (Check that this statement matches your answer to problem 2!) All congruence classes are mod n in this problem.

(a). Show that if $d \geq 1$ and $d|n$, then $\langle [d] \rangle$, in other words the cyclic subgroup of $G = \mathbb{Z}_n$ generated by $[d]$, has exactly n/d elements. Describe these elements.

(b). Let H be any subgroup whatsoever of $G = \mathbb{Z}_n$ (don't assume H is cyclic.) Show that there must be a *positive* integer m such that $[m] \in H$. Thus it makes sense to let d be the smallest positive integer such that $[d] \in H$, using the well-ordering principle. Prove that $d|n$. (Hint: use the division algorithm to write $n = qd + r$. Show that $[r] \in H$, so...)

(c). Again let H be any subgroup of G and let d be defined as in part (b). Prove that H is equal to the cyclic subgroup $\langle [d] \rangle$ of G. (Hint: suppose that $[c] \in H$. Use the division algorithm to write $c = qd + r$. Show that $[r] \in H$, and so...)