Homework #4. Due on Thursday, September 22nd in class

Reading:

1. For this assignment: Online lectures 8-9 and Section 1.4 and 2.2 of the book.

2. For next week's classes: Online lectures 9-10 and Sections 1.4 and 3.1 of the book.

Online lectures are currently posted on last semester's webpage

`http://people.virginia.edu/~mve2x/3354_Spring2016`

Problems:

Problem 1: Let $X = \mathbb{R}^2$ (the set of ordered pairs of real numbers) and define a relation $\sim$ on X by

$$(x_1, y_1) \sim (x_2, y_2) \iff x_1 + y_1 = x_2 + y_2.$$

(a) Prove that $\sim$ is an equivalence relation.

(b) Describe equivalence classes with respect to $\sim$. **Hint:** there is a very easy geometric description if you think of elements of X as points on the Euclidean plane.

Problem 2: Define a relation $\sim$ on $\mathbb{Z}$ by

$$x \sim y \iff x^3 \equiv y^3 \mod 4.$$

(a) Prove that $\sim$ is an equivalence relation.

(b) Find the number of equivalence classes with respect to $\sim$ and describe (explicitly) each class.

Hint for (b): The equivalence classes with respect to $\sim$ are closely related to congruence classes mod 4. Once you figure out the relationship (and why it holds), it is fairly easy to finish the problem.

Problem 3: Let R be a commutative ring with 1.

(a) Recall that an element $a \in R$ is called *invertible* if there exists $b \in R$ such that $ab = 1$

(b) An element $a \in R$ is called a *zero divisor* if $a \neq 0$ and there exists NONZERO $b \in R$ such that $ab = 0$. For instance, $[2]$ is a zero divisor in $\mathbb{Z}_6$ since $[2] \neq [0]$ and $[3] \neq [0]$ but $[2] \cdot [3] = [6] = [0]$ (this calculation shows that $[3]$ is also a zero divisor).

Prove that no element of R can be both invertible and a zero divisor. **Hint:** This is very similar to Problem 2 in Homework#1.

Problem 4: Do each of the following for $n = 8$ AND $n = 10$.

(a) Compute the multiplication table in $\mathbb{Z}_n$

(b) Use the multiplication table to find all invertible elements of $\mathbb{Z}_n$.

(c) Use the multiplication table to find all zero divisors of $\mathbb{Z}_n$

(d) Verify that your answers in (b) and (c) are consistent with Proposition 1.4.5 in the book.

Problem 5: Compute $[38]^{-1}$ in $\mathbb{Z}_{83}$. **Hint:** The proof of Proposition 1.4.5(a) (equivalently, Theorem 9.1 from online notes) shows how to reduce this problem to another computational problem that was explicitly discussed in class.

Let R be a ring. An element $x \in R$ is called *idempotent* if $x^2 = x$. Note that 0 and 1 (if 1 exists in R) are always idempotent elements.

Problem 6: Use direct computation to find all idempotent elements in $\mathbb{Z}_5, \mathbb{Z}_8$ and $\mathbb{Z}_{10}$.

Problem 7: Let p be a prime. Prove that $\mathbb{Z}_p$ has no idempotents apart from [0] and [1].

Bonus Problem: Let $n \geq 2$ be an integer. Prove that the following are equivalent:

(a) $n = p_1 \dots p_k$ where $p_1, \dots, p_k$ are distinct primes (possibly $k = 1$), that is, in the prime factorization of n all the exponents are equal to 1.

(b) if $[x] \in \mathbb{Z}_n$ is any nonzero element, then $[x]^2 \neq [0]$.

Hint: It is probably easiest to prove the implication (b)"$\Rightarrow$"(a) by contrapositive. Assume that n is not a product of distinct primes. Then one can write $n = p^2 m$ for some prime p and $m \in \mathbb{N}$. Find x (which can be explicitly expressed in terms of p and m) such that $[x] \neq [0]$ in $\mathbb{Z}_n$, but $[x]^2 = [0]$.