## Homework #4. Due Thursday, September 23rd, in class

## Reading:

For this homework assignment: Sections 1.7, 2.6 and the end of 2.5.
For next week's classes: Sections 3.1 and 3.2

## To hand in:

**Problem 1:** Let $A$ be a set and $\sim$ an equivalence relation on $A$. Recall that for $a \in A$ we denote by $[a]$ its equivalence class. Prove that for any $a, b \in A$ either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

**Extended hint:** The problem can be reformulated as follows: if $a, b \in A$ are such that $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$ (make sure you understand why this is indeed a reformulation). If $[a] \cap [b] \neq \emptyset$, there exists $c \in A$ such that $c \in [a]$ and $c \in [b]$. Use the definitions of equivalence relation and equivalence class to show that $[a] \subseteq [b]$, that is, every element of $[a]$ is also an element of $[b]$. Then by a similar argument show that $[b] \subseteq [a]$ and finally conclude that $[a] = [b]$.

**Problem 2:** Define the relation $\sim$ on $\mathbb{Z}$ as follows: $x \sim y$ if and only if $x^2 + y^2$ is even.

(a) Prove that $\sim$ is an equivalence relation (check 3 conditions)

(b) Describe the equivalence classes with respect to $\sim$. State the number of equivalence classes, and describe all elements in each class.

**Problem 3:**

(a) Find $x \in \mathbb{Z}$ such that $x \equiv 247 \mod 5$ and $x \equiv 251 \mod 23$.

(b) Now find $x \in \mathbb{Z}$ such that $x \equiv 247 \mod 5$, $x \equiv 251 \mod 23$ and $x \equiv 75 \mod 114$.

**Hint:** The algorithm for solving such problems is implictly contained in the proof of the Chinese Remainder Theorem given in class. DO NOT use calculators.

**Problem 4:** Compute muplitplication tables for the rings $\mathbb{Z}_5$ and $\mathbb{Z}_6$. How can you see directly from these tables that $\mathbb{Z}_5$ is a field, while $\mathbb{Z}_6$ is not? Describe any other patterns you observe (optional).

**Problem 5:** Section 2.6: 6(d) and 7(d). In 6(d) compute the inverse for each element you found. Compare your answers in 6(d) and 7(d).

**Problem 6:** Section 2.6: 16.

**Problem 7:** Let $R$ be a commutative ring. 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).

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

(b) Let $n \geq 2$ be an integer. Prove that $\mathbb{Z}_n$ has zero divisors if and only if $n$ is non-prime. **Hint:** The forward direction ($\Rightarrow$) (which is best proved by contrapositive) follows directly from part (a) and Corollary 8.4. For the backward direction ($\Leftarrow$) you may want to start with $n = 6$ (in which case zero divisors are exhibited in the above computation) and then generalize to arbitrary non-prime $n$.

(c) (bonus) Again let $n \geq 2$ be an integer. Prove that if $a \in \mathbb{Z}$ is any integer such that $gcd(a, n) > 1$, then there exists $b \in \mathbb{Z}$ such that $[b] \neq [0]$ in $\mathbb{Z}_n$, but $[a][b] = [0]$ in $\mathbb{Z}_n$. **Note:** Combined with Theorem 8.3, this result shows that any nonzero element of $\mathbb{Z}_n$ is either invertible or a zero divisor.

**Problem 8:** (a) Let $p$ be a prime number, and let $[x]$ be an element of $\mathbb{Z}_p$. Prove that

$$[x]^{-1} = [x] \text{ if and only if } [x] = [1] \text{ or } [x] = [p-1].$$

**Hint:** The backward direction is not hard. To prove the statement in the forward direction, think of how you would start solving the equation $z^{-1} = z$ over the real numbers. Keep in mind, however, that not all properties of reals hold in arbitrary commutative rings, so you should clearly justify every step.

(b) Give an example of a non-prime number $n$ and an element $[x] \in \mathbb{Z}_n$ such that $[x]^{-1} = [x]$, but $[x] \neq [1]$ and $[x] \neq [n-1]$.

**Problem 9 (practice):** This problem illustrates the concept of a "not well defined map". In class we used the symbol $[a]$ for $a \in \mathbb{Z}$ to denote the congruence class of $a$ modulo a fixed integer $n$. Sometimes one needs to work with congruence classes modulo different integers, in which case more precise notation is needed: the congruence class of $a$ modulo $n$ will be denoted by $[a]_n$ (so $[a]_n$ is an element of $\mathbb{Z}_n$).
Let us try to define the following two maps $f$ and $g$:
(i) $f : \mathbb{Z}_{10} \to \mathbb{Z}_5$ given by the formula $f([x]_{10}) = [x]_5$
(ii) $g : \mathbb{Z}_5 \to \mathbb{Z}_{10}$ given by the formula $g([x]_5) = [x]_{10}$.
One of these two is really a map, while the other is NOT a map (that is, not a function) since it is not well defined. Decide which is which and explain why.