Homework #4. Due on Thursday, September 26th, 11:59pm on Canvas

Reading:

1. For this assignment: Online lectures 6, 8 and parts of 7, 9 (note: there are some relevant examples we have not discussed in class). From Hungerford: 2.1 and 2.2.

2. For next week's classes: Online lecture 9. From Hungerford: 2.3 and parts of 4.1-4.3, 5.1.

Online lectures are currently posted on the Spring 2016 webpage

`https://m-ershov.github.io/3354_Spring2016/`

Problems:

Problem 1: Suppose that $x \equiv y \mod n$. Prove that $x^m \equiv y^m \mod n$ for all $m \in \mathbb{N}$ using induction on m.

Problem 2: Find all solutions for each of the following congruences:

(a) $8x \equiv 7 \mod 203$
(b) $2x \equiv 4 \mod 6$
(c) $2x \equiv 1 \mod 6$

Warning: Theorem 6.5 from online notes is not applicable to (b) and (c).

Problem 3:

(a) Prove that $x^2 \equiv 0, 1$ or $4 \mod 5$ for any $x \in \mathbb{Z}$.
(b) Use (a) to show that the equation $3a^2 - 5b^2 = 1$ has no integer solutions.

Note: There is a similar example in the online notes (see the end of Lecture 6 and the beginning of Lecture 7).

Problem 4: Compute $[38]^{-1}$ in $\mathbb{Z}_{83}$. **Hint:** The proof of Theorem 9.1 from online notes (also proved at the end of class on Wed, Sep 18) shows how to reduce this problem to another computational problem that was explicitly discussed in class.

The following definitions will be used in some of the remaining problems:
Let R be a commutative ring with 1. An element $a \in R$ is called

(a) *invertible* if there exists $b \in R$ such that $ab = 1$;
(b) *zero divisor* if $a \neq 0$ and there exists NONZERO $b \in R$ such that $ab = 0$;
(c) *idempotent* if $a^2 = a$.

Problem 5: Let R be a commutative ring with 1. 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 6: 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 $\mathbb{Z}_n$. How are your answers in (b) and (c) related to each other?
(e) Use the multiplication table to find all idempotents of $\mathbb{Z}_n$.

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 $[x]^2 = [0]$.