Homework #3. Due on Thursday, September 15th in class

Reading:

1. For this assignment: Online lectures 6-7 and Section 1.3 of the book.
2. For next week's classes: Online lectures 8-9 and Sections 1.4 and 2.2 of the book. Also read Lemma 6.6 and Proposition 7.1 in online notes (which were not discussed in class this week).

Online lectures are currently posted on last semester's webpage

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

Problems:

Problem 1: Let $a, b, c \in \mathbb{Z}$ be such that $a \mid c$, $b \mid c$ and $gcd(a, b) = 1$. Prove that $ab \mid c$. **Note:** There are (at least) two solutions: the first one uses prime factorization and Problem 8 from HW#2, and the second one uses the "coprime lemma" (Lemma 5.1 from online notes).

Problem 2: 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 3: 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 class is not applicable to parts (b) and (c). In (b) and (c) it is probably easiest to get the answer directly from definition of the congruence.

Preface to problem 4: Recall from the previous homework that for $n, k \in \mathbb{Z}$ with $0 \leq k \leq n$, the binomial coefficient $\binom{n}{k}$ is defined by $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (where $0! = 1$). Also recall the binomial theorem: for every $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \ldots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n.$$

Note that $\binom{n}{k}$ is always an integer – this is not obvious from definition, but it is (almost) obvious from the binomial theorem.

Problem 4: Suppose that p is prime and $0 < k < p$. Prove that $p \mid \binom{p}{k}$. **Hint:** First prove the following lemma: Suppose that $n, m \in \mathbb{Z}$, p is prime, $m \mid n$, $p \mid n$ and $p \nmid m$. Then $p \mid \frac{n}{m}$ (this follows from Euclid's lemma).

Problem 5: Now prove the (little) Fermat's theorem: If p is prime, then $n^p \equiv n \mod p$ for any $n \in \mathbb{N}$. **Hint:** Fix p and use induction on n. For the induction step use the result of Problem 4.

Problem 6:

(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.

Problem 7: Find all $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 2 \mod 7 \\ x \equiv 3 \mod 11 \\ x \equiv 4 \mod 13 \end{cases}$$

in two different ways:

(a) using "iterative" method (discussed in class) – first solve the system of the first two congruences, express the answer as a single congruence mod 77 and then solve another system of two congruences to get the final answer (you can change the order of congruences in the original system if you find it convenient)

(b) using "direct" method (see Example 3 in online Lecture 7).

Bonus Problem: Prove that there are infinitely many primes of the form $4k + 3$ with $k \in \mathbb{N}$. **Hint:** This can be done using suitable variation of Euclid's proof that there are infinitely many primes.