**Homework #2. Due Thursday, January 30th, by 4pm**

**Reading:**

1. For this homework assignment: Chapter 3 up to the end of Section 3.3.

2. For the next two classes: the rest of Chapter 3 and the beginning of Chapter 4.

**Problems:**

1. Let $n_1, \ldots, n_k$ and $m$ be positive integers, and let $n = n_1 n_2 \ldots n_k$.
   (a) Assume that $gcd(n_i, m) = 1$ for each $1 \leq i \leq k$. Prove that $gcd(n, m) = 1$.
   (b) Now assume that $n_i \mid m$ for each $1 \leq i \leq k$ and $gcd(n_i, n_j) = 1$ for $i \neq j$. Prove that $n \mid m$.

Note that both (a) and (b) were used in the proof of the Chinese Remainder Theorem (CRT). Also note that part (b) in the case $k = 2$ is simply the assertion of Corollary 1.11(a) from the book.

2. Find the general solution for each of the following congruences:
   (a) $8x \equiv 7 \mod 203$
   (b) $14x \equiv 7 \mod 203$
   (c) $14x \equiv 6 \mod 203$

3.
   (a) Use the proof of CRT given in class to find a solution to the system of congruences
   $$x \equiv a \mod 7, \quad x \equiv b \mod 11, \quad x \equiv c \mod 13,$$
   where $a, b$ and $c$ are fixed (but unspecified) integers. Recall that first one needs to solve the system for the triples $(a, b, c) = (1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$, after which one can write down a solution in the general case.
   (b) Now use your answer in (a) to find the general solution to the system of congruences
   $$x \equiv 3 \mod 7, \quad 2x \equiv 4 \mod 11, \quad 3x \equiv 5 \mod 13.$$

4. Find a solution to the congruence $25x \equiv 31 \mod 84$ using the method of Example 3.16.

5.

(a) Let $n$ be a positive integer. Prove that for any integer $x$ there exists an integer $r$ such that $x \equiv r \mod n$ and $0 \leq r \leq n-1$.

(b) Prove that $x^4 \equiv 0$ or $1 \mod 5$ for any integer $x$. **Hint:** using (a) one can solve the problem by simple case exhaustion.

(c) Prove that there exist no integers $a$ and $b$ such that $a^4 + b^4 = 20000000013$. **Hint:** the number of zeroes on the right hand side is completely irrelevant.

6. Given integers $n$ and $k$ with $0 \leq k \leq n$, the binomial coefficient $\binom{n}{k}$ is defined by $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (where $0! = 1$).

(a) Prove that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for any $1 \leq k \leq n$ (direct computation). Deduce that $\binom{n}{k}$ is always an integer (this is not obvious from definition).

(b) Prove that $\binom{n}{k}$ is the number of ways to choose $k$ objects from a collection of $n$ objects, where the order in which objects are chosen does not matter.

(c) Use (a) or (b) to prove the binomial theorem: for every $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$,

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

7. Let $p$ be a prime.

(a) Let $0 < k < p$ be an integer. 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 $p \mid \frac{n}{m}$.

(b) Now prove that $(a+b)^p \equiv a^p + b^p \mod p$ for any integers $a$ and $b$.

(c) Show by example that the assertions of (a) and (b) may become false without the assumption that $p$ is prime.

**Hint for Problem 1:** For (a) use that $gcd(a, b)$ is the smallest integer representable in the form $au + bv$ with $u, v \in \mathbb{Z}$. Part (b) can be proved by induction using (a) and Corollary 1.11(a).