Homework #2. Due on Thursday, September 8th in class

Reading:
1. For this assignment: Online lectures 3-5 and Sections 1.1 and 1.2 of the book.
2. For next week’s classes: Online lectures 6-7 and Section 1.3 of the book.

Online lectures are currently posted on last semester’s webpage

[http://people.virginia.edu/~mve2x/3354_Spring2016](http://people.virginia.edu/~mve2x/3354_Spring2016)

Problems:

Problem 1: Given \( n, k \in \mathbb{Z} \) with \( 0 \leq k \leq n \), define the binomial coefficient \(^n\!_k\) by

\[
\binom{n}{k} = \frac{n!}{k!(n-k)!}
\]
(recall that \( 0! = 1 \)).

(a) Prove that \(^n\!_k = (n-1)\!_{k-1} + (n-1)!\) for any \( 1 \leq k < n \) (direct computation).

(b) Now prove the binomial theorem: for every \( a, b \in \mathbb{R} \) and \( n \in \mathbb{N} \),

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

**Hint:** Use induction on \( n \). For the induction step write

\((a + b)^{n+1} = (a + b)^n \cdot (a + b)\) and use part (a).

Problem 2:

(a) Let \( R \) be an ordered ring. Prove that \( x^2 > 0 \) for every nonzero \( x \in R \). **Hint:** Consider two cases.

(b) Use (a) to prove that \( \mathbb{C} \) (complex numbers) is not an ordered ring

(no matter how we try to define the set of positive elements).

Problem 3: Let \( a, b, c \in \mathbb{Z} \) such that \( c \mid a \) and \( c \mid b \). Prove directly from definition of divisibility that \( c \mid (ma + nb) \) for any \( m, n \in \mathbb{Z} \) (do not refer to any divisibility properties proved in class).

Problem 4: Let \( a, b, c \in \mathbb{Z} \) such that \( c \mid ab \). Is it always true that \( c \mid a \) or \( c \mid b \)? If the statement is true for all possible values of \( a, b, c \), prove it; otherwise give a counterexample.

Problem 5: Let \( a = 382 \) and \( b = 26 \). Use Euclidean algorithm to compute \( \gcd(a, b) \) and find \( u, v \in \mathbb{Z} \) such that \( au + bv = \gcd(a, b) \).

Problem 6: Prove the key lemma, justifying the Euclidean algorithm:
Lemma: Let $a, b \in \mathbb{Z}$ with $b > 0$. Divide $a$ by $b$ with remainder: $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

Hint: Show that the pairs $\{a, b\}$ and $\{b, r\}$ have the same set of common divisors, that is,

(i) if $c \mid a$ and $c \mid b$, then $c \mid r$ (and so $c$ divides both $b$ and $r$)
(ii) if $c \mid b$ and $c \mid r$, then $c \mid a$ (and so $c$ divides both $a$ and $b$).

Problem 7: Let $a, b \in \mathbb{Z}$, not both 0, let $d = \gcd(a, b)$, and let $S = \{x \in \mathbb{Z} : x = am + bn \text{ for some } m, n \in \mathbb{Z}\}$.

By GCD Theorem, $d$ is the smallest positive element of $S$, and a natural problem is to describe all elements of $S$.

(a) Prove that if $k$ is any element of $S$, then $d \mid k$. Hint: Problem 1.

(b) Prove that if $k \in \mathbb{Z}$ and $d \mid k$, then $k \in S$. Hint: Use the first of part of GCD Theorem (as stated in class).

(c) Deduce from (a) and (b) that elements of $S$ are precisely integer multiples of $d$.

Problem 8: Let $a, b \in \mathbb{N}$, and let $p_1, \ldots, p_k$ be the set of all primes which divide $a$ or $b$ (or both). By UFT (unique factorization theorem), we can write $a = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ and $b = p_1^{\beta_1}p_2^{\beta_2} \ldots p_k^{\beta_k}$ where each $\alpha_i$ and each $\beta_i$ is a non-negative integer (note: some exponents may be equal to zero since some of the above primes may divide only one of the numbers $a$ and $b$). For instance, if $a = 12$ and $b = 20$, our set of primes is $\{2, 3, 5\}$, and we write $12 = 2^1 \cdot 3^2 \cdot 5^0$ and $20 = 2^2 \cdot 3^0 \cdot 5^1$.

(a) Prove that $a \mid b \iff \alpha_i \leq \beta_i$ for each $i$.

(b) Give a formula for $\gcd(a, b)$ in terms of $p_i$’s, $\alpha_i$’s and $\beta_i$’s and justify it using the definition of GCD.

(c) Give a formula for the least common multiple of $a$ and $b$ in terms of $p_i$’s, $\alpha_i$’s and $\beta_i$’s. No proof is necessary.