**Homework #2. Due Thursday, September 9th, in class**

**Reading:**

1. For this assignment: Sections 2.3 and 2.4 (up to Definition 2.13).

2. Before the class on Tuesday, Sep 7th: the rest of Section 2.4. Before the class on Thursday, Sep 9th: Section 2.5.

**Problems:**

**Problem 1:** 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 $m, n \in \mathbb{Z}$.

**Problem 2 (practice):** (a) Prove that $2 \mid n(n+1)$ for any $n \in \mathbb{Z}$.
(b) Prove that $3 \mid n(n+1)(n+2)$ for any $n \in \mathbb{Z}$.
(c) Formulate and prove suitable generalization of (a) and (b).
**Hint:** For part (a): consider 2 cases; for part (b) consider 3 cases.

**Problem 3:** 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 4:** (a) Fix $b \in \mathbb{Z}$, and let $f : \mathbb{Z}^+ \to \mathbb{Z}$ be a function such that
(i) $b \mid f(1)$
(ii) $b \mid (f(n) - f(n-1))$ for any integer $n \geq 2$.
Prove by induction that

$$b \mid f(n) \text{ for any } n \in \mathbb{Z}^+.$$

**Note:** You may use properties of divisibility proved in the book, in class or earlier in this homework.

(b) Prove that $8 \mid (9^n - 1)$ for any $n \in \mathbb{Z}^+$ by applying part (a) to a suitable $b \in \mathbb{Z}$ and suitable function $f$ (we did this problem in class in a different way).

**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 following 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 the 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 GCD Theorem.

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

**Problem 8:** Let $n > 1$ be a non-prime integer.

(a) Prove that $n = kl$ for some integers $k, l > 1$ (this follows very easily from the definition of a prime number).

(b) Prove that $n$ has a divisor $d$ such that $1 < d \leq \sqrt{n}$. **Hint:** Prove this by contradiction using (a).

**Binomial theorem (bonus, strongly recommended).** Given $n, k \in \mathbb{Z}$ with $0 \leq k \leq n$, define the binomial coefficient $\binom{n}{k}$ by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

(recall that $0! = 1$).

(a) Prove that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for any $1 \leq k \leq n$ (direct computation).

(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 induction step write $(a+b)^n = (a+b)^{n-1} \cdot (a+b)$ and use part (a).