Homework #3. Due on Thursday, February 11th, in class

Reading:

1. For this assignment: Online lectures 4 and 5, [Gilbert, §2.3, 2.4] and [Pinter, §22].
2. For next week's classes: Online lectures 6 and 7, [Gilbert, §2.5] and [Pinter, §23]

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 $m, n \in \mathbb{Z}$ (do not refer to any divisibility properties proved in class).

Problem 2: 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 3: 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 4: 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 5: 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 6: Let $a, b \in \mathbb{Z}$, 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 α_i and each β_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, α_i's and β_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, α_i's and β_i's. No proof is necessary.

Problem 7: 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 1, and the second one uses the "coprime lemma" (Lemma 5.1 from class).

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.