Homework #3. Due on Thursday, September 19th, 11:59pm on Canvas

Reading:

1. For this assignment: Online lectures 4 and 5. From Hungerford: 1.2 and 1.3
2. For next week's classes: Online lectures 6 and 8. From Hungerford: 2.1, 2.2 and the beginning of 2.3. Note: I am planning to skip the majority of the content of the online lecture 7, including the Chinese Remainder Theorem, but I still recommend reading this material before you start working on the following homework (HW#4).

Online lectures are currently posted on the Spring 2016 webpage

`https://m-ershov.github.io/3354_Spring2016/`

Problems:

Problem 1:

(a) Prove that $9 \mid (10^k - 1)$ for all $k \in \mathbb{N}$.

(b) Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9. **Hint:** Given an integer n, let $a_k a_{k-1} \dots a_0$ be its decimal expansion (so that $a_k, \dots, a_0$ are the digits of n). Start with the formula for n in terms of $a_k, \dots, a_0$ and then use (a) and basic divisibility properties to prove (b).

Problem 2: Let $a = 382$ and $b = 26$. Use the Euclidean algorithm to compute $gcd(a, b)$ and find $u, v \in \mathbb{Z}$ such that $au + bv = gcd(a, b)$.

Problem 3: 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 4: 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 Bezout identity (part (a) of GCD Theorem as stated in online notes), 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 $d \mid k$.
(b) Prove that if $k \in \mathbb{Z}$ and $d \mid k$, then $k \in S$.

Note that by combining parts of (a) and (b), we deduce that

$$S = d\,\mathbb{Z} = \{x \in \mathbb{Z} : x = dm \text{ for some } m \in \mathbb{Z}\}.$$

Problem 5: 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. **Hint:** The backwards direction ("$\Leftarrow$") can be proved directly from the definition of divisibility. One way to prove the forward direction ("$\Rightarrow$") is to imitate the proof of the unique factorization theorem, as presented in class.
(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 6: 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 the second one uses the Coprime lemma (Lemma 5.1 in online notes; in class we proved it at the end of Lecture 4).

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 a suitable variation of Euclid's proof that there are infinitely many primes. Note that the analogous statement about primes of the form $4k+1$ is also true, but cannot be proved using the same method. It may be convenient to use congruences in your argument, although this is by no means necessary.