Homework #3. Due Thursday, September 16th, in class

Reading:

1. For this assignment: Sections 2.4 and 2.5, up to Theorem 2.26.

2. Before the class on Tuesday, Sep 14th: the rest of Section 2.5, Section 2.6. Before the class on Thursday, Sep 16th: Section 3.1 (start).

Problems:

Problem 1: 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 2: 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 Theorem 2.14.

Problem 3: Section 2.5, Problem #30. **Hint:** Use induction on m (and basic properties of congruences).

Problem 4: Find all solutions for each of the following congruences:

(a) $8x \equiv 7 \mod 203$

(b) $2x \equiv 4 \mod 6$

(c) $2x \equiv 1 \mod 6$

Warning: Theorem 2.25 is not applicable to parts (b) and (c). In (b) and (c) it is probably easiest to get the answer directly from definition of the congruence.

Preface to problem 5: Recall from the previous homework that for $n, k \in \mathbb{Z}$ with $0 \leq k \leq n$, the binomial coefficient $\binom{n}{k}$ is defined by $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

(where $0! = 1$). Also recall the binomial theorem: for every $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$,

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

Note that $\binom{n}{k}$ is always an integer – this is not obvious from definition, but it is (almost) obvious from the binomial theorem.

Problem 5: Suppose that p is prime and $0 < k < p$. 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 $p \mid \frac{n}{m}$ (this follows from Euclid's lemma).

Problem 6: Now prove the (little) Fermat's theorem: If p is prime, then $n^p \equiv n \mod p$ for any $n \in \mathbb{N}$. **Hint:** Fix p and use induction on n. Do the induction step in the form "$P_n \Rightarrow P_{n+1}$" (to make algebra simpler) and use the result of Problem 5.

Problem 7: (a) Prove that $x^2 \equiv 0, 1$ or $4 \mod 5$ for any $x \in \mathbb{Z}$
(b) Use (a) to show that the equation $3a^2 - 5b^2 = 1$ has no integer solutions.