Homework #3. Due Thursday, February 6th, by 4pm

Reading:

1. For this homework assignment: Sections 3.5 and parts of Chapter 4.

2. For the next two classes: Sections 4.3, 4.1 and 5.1. Also review the definition of the ring of congruence classes $\mathbb{Z}_n$ (see Chapter 3).

Problems:

1. Let p be a prime. As in class, for a nonzero integer x, denote by $ord_p(x)$ the largest integer e s.t. p^e divides x (if $p \nmid x$, we set $ord_p(x) = 0$). We also put $ord_p(0) = \infty$, so that we get a function $ord : \mathbb{Z} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ Prove the following properties of the ord function:

(i) $ord_p(xy) = ord_p(x) + ord_p(y)$

(ii) $ord_p(x + y) \geq \min\{ord_p(x), ord_p(y)\}$

(iii) $ord_p(x + y) = \min\{ord_p(x), ord_p(y)\}$ whenever $ord_p(x) \neq ord_p(y)$

2. Let m and n be positive integers.

(i) Express the condition $m \mid n$ in terms of ord_p function for different p. Your statement should be of the form:

$$m \mid n \iff \text{some expression involving } ord_p(m) \text{ and } ord_p(n).$$

(ii) Let $p_1, \ldots, p_k$ be the complete set of primes which divide m or n. By the unique factorization theorem we can write $m = p_1^{e_1} \ldots p_k^{e_k}$ and $n = p_1^{f_1} \ldots p_k^{f_k}$ for unique $e_1, \ldots, e_k, f_1, \ldots, f_k \in \mathbb{Z}_{\geq 0}$ (some of these numbers may be equal to 0 since some primes may divide m, but not n, or vice versa). Give and prove formulas for $gcd(m, n)$ and $lcm(m, n)$ in terms of $p_1, \ldots, p_k, e_1, \ldots, e_k$ and $f_1, \ldots, f_k$ (Hint: the formulas should also involve prime factorization).

3. Let p, q and r be distinct primes and let a, b, c be integers. Consider the system of congruences

$$x \equiv a \mod p^3q; \quad x \equiv b \mod p^2q^2r; \quad x \equiv c \mod pq^3.$$

(a) Prove that the system has a solution if and only if $a \equiv b \mod p^2q$ and $b \equiv c \mod pq^2$.

(b) Let $p = 5, q = 2, r = 3$. Assuming hypotheses of (a) hold, find a formula for the general solution to the system (in terms of a, b and c).

4. Find all solutions mod 30 to the congruence $x^2 \equiv x \mod 30$ making as few computations as possible. In particular, **do not solve more than three systems** of linear congruences in the course of your proof.

5. Let p be a prime.

(a) Use Problem 7 from Homework#2 to prove Fermat's little theorem: $x^p \equiv x \mod p$ for any $x \in \mathbb{Z}$.

(b) Deduce from (a) that $x^{p-1} \equiv 1 \mod p$ whenever $gcd(x, p) = 1$.

Note that a completely different proof of these results is given in Section 4.1.

6. Use Problem 5 to prove that $x^{13} \equiv x \mod 70$ for any $x \in \mathbb{Z}$.