Homework #3. Solutions to selected problems.

1. Let p be a prime. As in class, for a nonzero integer x, denote by $\mathrm{ord}_p(x)$ the largest integer e s.t. p^e divides x (if $p \nmid x$, we set $\mathrm{ord}_p(x) = 0$). We also put $\mathrm{ord}_p(0) = \infty$, 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) $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$

(ii) $\mathrm{ord}_p(x+y) \geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$

(iii) $\mathrm{ord}_p(x+y) = \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$ whenever $\mathrm{ord}_p(x) \neq \mathrm{ord}_p(y)$

Solution: All three statements are clear if $x = 0$ or $y = 0$, so for the rest of the proof we shall assume that both x and y are nonzero. Below we shall use a slightly different definition of ord_p function (which is easily seen to be equivalent to the original definition):

Definition: Let z be a nonzero integer. Then $\mathrm{ord}_p(z)$ is the unique integer $k \in \mathbb{N}$ such that $z = p^k w$ where w is an integer not divisible by p.

Let $m = \mathrm{ord}_p(x)$ and $n = \mathrm{ord}_p(y)$. This means that $x = p^m u$ and $y = p^n v$ where $p \nmid u$ and $p \nmid v$.

(i) We have $xy = p^{n+m}uv$. Since $p \nmid u$ and $p \nmid v$, by (contrapositive of) Euclid's lemma, $p \nmid uv$. Hence the equality $xy = p^{n+m}uv$ implies that $\mathrm{ord}_p(xy) = n + m$.

(ii) WOLOG (without loss of generality) we can assume that $n \geq m$. We can write $x + y = p^m(x + p^{n-m}y)$. Since $n \geq m$, we have $x + p^{n-m}y \in \mathbb{Z}$, and so $\mathrm{ord}_p(x+y) \geq m = \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$.

(iii) As in (ii), we have $x + y = p^m(x + p^{n-m}y)$. This time we know that $n > m$, hence the number $x + p^{n-m}y$ is not divisible by p (being the sum of two integers, one of which is divisible by p and the other not divisible p). Hence $\mathrm{ord}_p(x+y)$ is equal to $m = \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$.

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:

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

(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 $f_1, \ldots, f_k$.

Answer: (i) $m \mid n \iff \text{ord}_p(m) \leq \text{ord}_p(n)$ for every prime p.
(ii) $gcd(m,n) = p_1^{\min\{e_1,f_1\}} \ldots p_k^{\min\{e_k,f_k\}}$ and $LCM(m,n) = p_1^{\max\{e_1,f_1\}} \ldots p_k^{\max\{e_k,f_k\}}$.

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

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

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

Solution: (a) The given system is equivalent to the following system of 7 congruences:

$$x \equiv a \mod p^3, \qquad x \equiv a \mod q, \tag{1}$$

$$x \equiv b \mod p^2, \qquad x \equiv b \mod q^2, \qquad x \equiv b \mod r, \tag{2}$$

$$x \equiv c \mod p \qquad x \equiv c \mod q^3 \tag{3}$$

As discussed in class, this system has a solution $\iff$ the following compatibility conditions hold: $b \equiv a \mod p^2$, $c \equiv a \mod p$, $c \equiv b \mod q^2$ and $c \equiv a \mod q$.

In the presence of the condition $b \equiv a \mod p^2$, the condition $c \equiv a \mod p$ is equivalent to $c \equiv b \mod p$. Similarly, since $c \equiv b \mod q^2$, we can replace $c \equiv a \mod q$ by $b \equiv a \mod q$.

Thus, an equivalent system of conditions is $b \equiv a \mod p^2$, $c \equiv b \mod p$, $c \equiv b \mod q^2$ and $b \equiv a \mod q$. Since any power of p and any power of q are coprime, conditions 1 and 4 combined are equivalent to $b \equiv a \mod p^2 q$ and conditions 2 and 3 are equivalent to $c \equiv b \mod pq^2$.

(b) If compatibility conditions hold, to find the general solution to the system, for each prime we pick a congruence modulo the highest power of that prime in (1)-(3) above, and solve the obtained system using an algorithm from the

proof of CRT. In our situation we end up with the system $x \equiv a \mod p^3$, $x \equiv b \mod r$ and $x \equiv c \mod q^3$.

When $p = 5, q = 2, r = 3$, the general solution is given by $x = -624a + 1000b - 375c + 3000k$ with $k \in \mathbb{Z}$.

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.

Solution: Note that $30 = 2 \cdot 3 \cdot 5$. As shown in class, the congruence $x^2 \equiv x \mod 30$ holds if and only if there exist $a, b, c \in \{0, 1\}$ such that $x \equiv a \mod 2$, $x \equiv b \mod 3$ and $x \equiv c \mod 5$. The general solution to this system is $x \equiv 15a + 10b + 6c \mod 30$ (note that to find this formula we use an algorithm from the proof of CRT, and in the process we need to solve precisely three congruences!) There are eight choices for the triple (a, b, c) which give us eight solutions: $x = 0, 15, 10, 6, 25, 21, 16, 31$. The first seven on this list are already reduced and $31 \equiv 1 \mod 30$. Thus the general solution is $x \equiv 0, 1, 6, 10, 15, 16, 21$ or $25 \mod 30$.

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

Solution: Since $70 = 2 \cdot 5 \cdot 7$ and $2, 5$ and 7 are pairwise coprime, to prove the result it suffices to show that for any $x \in \mathbb{Z}$ we have $x^{13} \equiv x \mod 2$, $x^{13} \equiv x \mod 3$ and $x^{13} \equiv x \mod 5$. The proofs of each of those congruences are analogous, so we will just do the last one.

If $5 \mid x$, then $x^{13} \equiv x \mod 5$ since both sides are divisible by 5. And if $5 \nmid x$, then by Fermat's little theorem $x^4 \equiv 1 \mod 5$. Raising both sides to third power, we get $x^{12} \equiv 1 \mod 5$, and multiplying by x, we get $x^{13} \equiv x \mod 5$.