Math 322 Exam 1 Solutions

Instructor: Jay Daigle

Problem 1. Using the principle of induction, prove that if m, n_i, a_i are integers for $1 \leq i \leq k$, and $m|a_i$ for each i, then $m| \sum_{i=1}^k n_i a_i$. (Hint: we proved in class that if $m|a, m|b$, then $m|n_1 a + n_2 b$).

Solution: Base case: Suppose $k = 2$. Then if $m|a_1, a_2$, we know that $m|n_1 a_1 + n_2 a_2$ by the lemma on linear combinations.

Inductive step: suppose this result holds for k terms. Then suppose $m|a_1, a_2, \ldots, a_{n+1}$. By our inductive hypothesis, we know that

$$m| \sum_{i=1}^{k} n_i a_i.$$

But

$$\sum_{i=1}^{k+1} n_i a_i = \sum_{i=1}^{k} n_i a_i + n_{k+1} a_{k+1}$$

is a linear combination of a_{k+1} and the k-fold sum, and m divides both of these, so by the lemma on linear combinations,,

$$m| \sum_{i=1}^{k+!} n_i a_i.$$

Problem 2. Let p be a prime and r, n be natural numbers. If $p|r^n$ then prove that $p^n|r^n$.

Solution: Since $p|r^n = \prod_{i=1}^n r$, then by the corollary to Euclid's Lemma we know that $p|r$. Thus there is an integer $m \in \mathbb{Z}$ such that $mp = r$, and thus $r^n = (mp)^n = m^n p^n$. Thus $p^n|r^n$ by definition of division.

Problem 3. Using the Chinese Remainder Theorem, find all x such that

$$x \equiv 1 \mod 4 \qquad x \equiv 2 \mod 5$$
$$x \equiv 3 \mod 7 \qquad x \equiv 4 \mod 9.$$

Solution: We have $M = 4 \cdot 5 \cdot 7 \cdot 9 = 1260$. Then we compute

$$M_1 = 5 \cdot 7 \cdot 9 = 315 \equiv 3 \mod 4 \qquad y_1 = 3 \mod 4$$
$$M_2 = 4 \cdot 7 \cdot 9 = 252 \equiv 2 \mod 5 \qquad y_2 = 3 \mod 5$$
$$M_3 = 4 \cdot 5 \cdot 9 = 180 \equiv 5 \mod 7 \qquad y_3 = 3 \mod 7$$
$$M_4 = 4 \cdot 5 \cdot 7 = 140 \equiv 5 \mod 9 \qquad y_4 = 2 \mod 9$$

So the solution is

$$x \equiv 1 \cdot 315 \cdot 3 + 2 \cdot 252 \cdot 3 + 3 \cdot 180 \cdot 3 + 4 \cdot 140 \cdot 2$$
$$\equiv 0 + 5197 \equiv 157 \mod 1260.$$

Problem 4.

(a) Compute $(322, 504)$.

Solution:

$$(504, 322) = (322, 182) = (182, 140) = (140, 42) = (42, 14) = (14, 0).$$

Thus $(322, 504) = 14$.

(b) Find all solutions to the following system of linear congruences:

$$3x + 2y \equiv 4 \mod 12$$
$$4x + 3y \equiv 7 \mod 12$$

Solution: We have $\Delta = 9 - 8 = 1 \equiv 1 \mod 12$, and indeed $(1, 12) = 1$. Then we compute $\Delta^{-1} \equiv 1 \mod 12$. Thus by formula

$$x \equiv -1(2 \cdot 7 - 3 \cdot 4) \equiv -1(2) \equiv -2 \equiv 10 \mod 12$$
$$y \equiv -1(3 \cdot 7 - 4 \cdot 4) \equiv -1(7) \equiv 5 \mod 12.$$