Math 322 Exam 1 Solutions

Instructor: Jay Daigle

Problem 1. (a) 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,,

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

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

Solution:

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

Thus $(322, 504) = 14$.

Problem 2. (a) 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

$$\begin{aligned} x &\equiv 1 \cdot 315 \cdot 3 + 2 \cdot 252 \cdot 3 + 3 \cdot 180 \cdot 3 + 4 \cdot 140 \cdot 2 \\ &\equiv 0 + 5197 \equiv 157 \mod 1260. \end{aligned}$$

(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

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

Problem 3. Find all solutions to the equation $x^3 + x + 2 \equiv 0 \mod 200$.

Solution: $200 = 2^3 \cdot 5^2$ so we first solve the equation mod 2 and mod 5. We note that $f'(x) = 3x^2 + 1$.

Mod 2, we see that both 0 and 1 work. $f'(0) = 1 \not\equiv 0 \mod 2$, so there is a unique lift to mod 4. We solve

$$t = -(f'(0))^{-1}(f(0)/2) = -1(2/2) = -1 \equiv 1 \mod 2$$

so the lift is given by $0 + 2 \cdot 2 \equiv 2 \mod 4$. We can lift this one more level, with the formula

$$t = -(f'(0))^{-1}(f(0)/2) = -1 \equiv 1 \mod 2$$

so the lift is $2 + 2 \cdot 4 \equiv 6 \mod 8$. Thus 6 is the unique lift of 0 to a solution mod 8.

Now we lift 1. $f'(1) = 4 \equiv 0 \mod 2$, so either both lifts work or neither lift works. We have $f(1) = 1 + 1 + 2 = 4 \equiv 0 \mod 4$, so both 1 and 3 are solutions mod 4.

$f'(1) \equiv f'(3) \equiv 0 \mod 2$, so each is all or nothing. We see that $f(1) = 4 \not\equiv 0 \mod 8$, so neither 1 nor 5 is a solution mod 8. We see that $f(3) = 32 \equiv 0 \mod 8$, so both 3 and 7 are solutions mod 8. Thus the solutions mod 8 are $3, 6, 7$.

Now we work mod 5. We see that 4 is the only solution mod 5. $f'(4) = 49 \equiv -1 \mod 5$, so there is a unique lift to a solution mod 25. We calculate

$$t = -(-1)^{-1}(f(4)/5) = -(-1) \cdot 70/5 = 14 \equiv 4 \mod 5$$

so the lift is $4 + 4 \cdot 5 = 24$. Thus the unique solution mod 25 is 24.

We finally use the Chinese Remainder Theorem to patch these together. We have $m_1 = 8, m_2 = 25$, so $M_1 = 25$ and $y_1 = 25^{-1} \equiv 1^{-1} \equiv 1 \mod 8$; and $M_2 = 8$ so $M_2^{-1} = 8^{-1} = -3 = 22 \mod 25$. Then:

If $x \equiv 3 \mod 8, x \equiv 24 \mod 25$, then by the Chinese Remainder Theorem we get $x \equiv 3 \cdot 25 \cdot 1 + 24 \cdot 8 \cdot 22 = 4299 \equiv 99 \mod 200$.

If $x \equiv 6 \mod 8, x \equiv 24 \mod 25$, then by the Chinese Remainder Theorem we get $x \equiv 6 \cdot 25 \cdot 1 + 24 \cdot 8 \cdot 22 = 4374 \equiv 174 \mod 200$.

If $x \equiv 7 \mod 8, x \equiv 24 \mod 25$, then by the Chinese Remainder Theorem we get $x \equiv 7 \cdot 25 \cdot 1 + 24 \cdot 8 \cdot 22 = 4394 \equiv 199 \mod 200$.