QUIZ #5 – MATH 2200
SPRING 2018

MARCH 30TH, 2018

1. Find all solutions, or explain why there are none, for the following system of congruences: (10 points)

$$\begin{aligned} x &\equiv_5 2 \\ x &\equiv_2 1 \\ 2x &\equiv_3 1 \end{aligned}$$

(Recall that $a \equiv_m b$ is the same as writing $a \equiv b (\mathrm{mod} m)$.)

Hint: For the congruence $2x \equiv_3 1$, first transform it into $x \equiv_3 ???$.

Solution: We begin by transforming the congruence mentioned in the hint. The easiest way to do this is to multiply both sides by 2 (which happens to be the inverse of 2 modulo 3). Then $4x \equiv_3 2$, but $4 \equiv_3 1$ and so $x \equiv_3 1$.

At this point we have three congruences:

$$\begin{aligned} x &\equiv_5 2 \\ x &\equiv_2 1 \\ x &\equiv_3 2. \end{aligned}$$

The book outlines several different ways to solve this system. Using the method from the proof of the Chinese remainder theorem, we write

$$a_1 = 2, a_2 = 1, a_3 = 2, m_1 = 5, m_2 = 2, m_3 = 3 \text{ and } M_1 = 6, M_2 = 15, M_3 = 10.$$

Then we need to find y_k, the inverse of M_k modulo m_k.

- $M_1 = 6$, and $m_1 = 5$, thus M_1 mod m_1 is 1, and so 1 works as y_1.
- $M_2 = 15$ and $m_2 = 2$, thus M_2 mod m_2 is 1, and so 1 works for y_2.
- $M_3 = 10$ and $m_3 = 3$, thus M_3 mod m_3 is 1, and so 1 works for y_3.

Now using the formula from the book,

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = (2 \cdot 6 \cdot 1) + (1 \cdot 15 \cdot 1) + (2 \cdot 10 \cdot 1) = 47$$

is a solution. Let's verify this. Mod 5 we get 2, so the first equation is satisfied. Mod 2 we get 1, and so the second equation is satisfied. Finally we compute $2 \cdot 47 = 94$ modulo 3, which is 1, and so that also works. Thus we have found one solution. However, the set of solutions is equal to the numbers x such that

$$x \equiv_{30} 47 \text{ which can also be written as } x \equiv_{30} 17$$

(note $30 = 5 \cdot 2 \cdot 3$).

2. Explain carefully all the steps in a binary search for the number 7 inside the sorted list

$$\{-5, -1, 0, 3, 5, 7, 7.5, 8, 12, 16, 101, 102, 103\}.$$

Use complete sentences, and carefully identify what part of the list you are searching at each step. (10 points).

Solution: We number our list as follows to make the argument easier to follow.

1	2	3	4	5	6	7	8	9	10	11	12	13
-5	-1	0	3	5	7	7.5	8	12	16	101	102	103

At the start, our `start = 1` and `end = 13`, and so `current`, is the average, which is `7`. We check if the value at `7` (which is 7.5) is equal to 7. It is not, and it is bigger than 7, so we set `start = 1` and `end = 6`, and we are really considering the following list.

1	2	3	4	5	6
-5	-1	0	3	5	7

Next our `current` value becomes the average of the `start` and `end` (rounded down, although if you choose to round up consistently, that's ok too), which is `3`. Thus we check if the value of our list in entry `3`, we see it is 0, which is less than 7, and so we set `start = 4` and `end = 6`, and so we are really considering the following list.

4	5	6
3	5	7

The average of `start` and `end` is `5`, and so we check our value at `current = 5`, which is 5, and still less than 7. So we set `start = 6` and `end = 6`. Our effective list is very small at this point.

6
7

Thus `current = 6` too, and we happily verify that the value of our list at `6` is indeed 7. Thus we have found 7 in our list in entry #`6`.