MCS 150 Exam 2 Solutions

Nov 10, 2017

1. (10 pts) Let p be a prime number and $x \in \mathbb{Z}$ such that $p \nmid x$. Show that $x, 2x, \ldots, (p-1)x$ are all distinct modulo p, i.e. no two of them are congruent modulo p. Conclude that

$$\{x, 2x, \ldots, (p-1)x\} \equiv \{1, 2, \ldots, p-1\} \pmod{p},$$

that is to say these two sets contain the same elements modulo p.

Suppose $j, k \in \{1, 2, \ldots, p-1\}$ such that $jx \equiv kx \pmod{p}$. Since $p \nmid x$, x is relatively prime to p. So x is invertible. Hence we can cancel x from the above congruence by multiplying both sides by x^{-1}:

$$\begin{aligned} jx &\equiv kx \pmod{p} \\ (jx)x^{-1} &\equiv (kx)x^{-1} \pmod{p} \\ j(xx^{-1}) &\equiv k(xx^{-1}) \pmod{p} \\ j &\equiv k \pmod{p}. \end{aligned}$$

This means $p|(j-k)$, which is only possible if $j = k$. We have just shown that $x, 2x, \ldots, (p-1)x$ must all be distinct. Notice that modulo p each $x, 2x, \ldots, (p-1)x$ is congruent to some element in $\{1, 2, \ldots, p-1\}$. Since $x, 2x, \ldots, (p-1)x$ are distinct modulo p and there are $p-1$ of them, for each element in $\{1, 2, \ldots, p-1\}$, there must be one in $\{x, 2x, \ldots, (p-1)x\}$ that is congruent to it. Hence

$$\{x, 2x, \ldots, (p-1)x\} \equiv \{1, 2, \ldots, p-1\} \pmod{p}.$$

2. (10 pts) Let $n \in \mathbb{Z}^+$. We remarked in class that if n is equal to a prime p, then every integer that is not congruent to 0 modulo n is a unit. That is among the canonical representatives $0, 1, \ldots, p-1$, all but one is a unit. Suppose $n = p^k$ where p is a prime number and $k \in \mathbb{Z}^+$. What can you say now about the number of units among the canonical representatives $0, 1, \ldots, n-1$?

There are p^k canonical representatives modulo p^k. Among these, the ones that are relatively prime to p^k are the units. Notice that an integer x is not relatively prime to p^k if and only if it is divisible by p. Among the numbers $0, 1, \ldots, p^k - 1$, every p-th is divisible by p, so there are $p^k/p = p^{k-1}$ such numbers. The rest are the units. Hence there are $p^k - p^{k-1} = p^{k-1}(p-1)$ units among the canonical representatives modulo p^k.

3. (10 pts) Let $n \in \mathbb{Z}^+$ and $x \in \mathbb{Z}$. Prove that x is invertible modulo n if and only if x and n are relatively prime.

Suppose that x is relatively prime to n. Then $1 = lx + zn$ for some $l, z \in \mathbb{Z}$. So $lx = 1 - zn$, which shows $lx \equiv 1 \pmod{n}$. Hence x is invertible modulo n.

Conversely, if x is invertible, then there is some $l \in \mathbb{Z}$ such that $lx \equiv 1 \pmod{n}$. That is $1 - lx = zn$ for some $z \in \mathbb{Z}$. So $lx + zn = 1$, and we showed (on HW 3) that this implies x and n are relatively prime.

4. (a) (4 pts) State the Chinese Remainder Theorem.

Let $m, n \in \mathbb{Z}^+$ such that m and n are relatively prime. For any $a, b \in \mathbb{Z}$, the system of congruence equations

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a solution. Any two solutions are congruent modulo mn.

(b) (6 pts) Let x be an integer between 0 and 461 and $a, b, c \in \mathbb{Z}$. Use the Chinese Remainder Theorem or some other suitable method to find x if

$$\begin{aligned} x &\equiv a \pmod{6} \\ x &\equiv b \pmod{7} \\ x &\equiv c \pmod{11}. \end{aligned}$$

Be sure to justify your solution.

Notice that

$$\begin{aligned} 77 &\equiv -1 \pmod{6} \\ 77 &\equiv 0 \pmod{7} \\ 77 &\equiv 0 \pmod{11}. \end{aligned}$$

Also

$$\begin{aligned} 66 &\equiv 3 \pmod{7} \\ 66 &\equiv 0 \pmod{6} \\ 66 &\equiv 0 \pmod{11} \end{aligned}$$

and multiplying these by 2 gives

$$\begin{aligned} 132 &\equiv 6 \equiv -1 \pmod{7} \\ 132 &\equiv 0 \pmod{6} \\ 132 &\equiv 0 \pmod{11}. \end{aligned}$$

Similarly,

$$\begin{aligned} 42 &\equiv -2 \pmod{11} \\ 42 &\equiv 0 \pmod{6} \\ 42 &\equiv 0 \pmod{7} \end{aligned}$$

so multiplying these by 5 gives

$$\begin{aligned} 210 &\equiv -10 \equiv 1 \pmod{11} \\ 210 &\equiv 0 \pmod{6} \\ 210 &\equiv 0 \pmod{7}. \end{aligned}$$

Combining these results yields

$$\begin{aligned} -77a - 132b + 210c &\equiv -77a \equiv a \pmod{6} \\ -77a - 132b + 210c &\equiv -132b \equiv b \pmod{7} \\ -77a - 132b + 210c &\equiv 210c \equiv c \pmod{11} \end{aligned}$$

So to find x, calculate $-77a - 132b + 210c$ and then add or subtract and appropriate multiple of $462 = 6 \cdot 7 \cdot 11$ so that the result falls between 0 and 461.

5. (10 pts) **Extra credit problem.** An integer x such that $x^2 \equiv x \pmod{n}$ is called an *idempotent* modulo n. Let $k, m \in \mathbb{Z}^+$. Suppose that $x \in \mathbb{Z}$ is such that

$$x \equiv 1 \pmod{k}$$
$$x \equiv 0 \pmod{m}.$$

Prove that x is an idempotent modulo km, that is $x^2 \equiv x \pmod{km}$. (Hint: start by showing that k and m must be relatively prime.)

Since $x \equiv 1 \pmod{k}$, $x - 1 = sk$ for some $s \in \mathbb{Z}$. Similarly, $x \equiv 0 \pmod{m}$ means $x = tm$. Hence $tm - 1 = sk$, and so $1 = tm - sk$. This shows that 1 is an integer linear combination of k and m. It follows (by problem 3 on HW 3) that k and m are relatively prime.

Notice that $x^2 \equiv 1 \pmod{k}$ and $x^2 \equiv 0 \pmod{m}$. So x^2 also satisfies the system of congruence equations above. By the Chinese Remainder Theorem, x and x^2 must be congruent modulo km.

There is also a more direct argument. As we noted above, $x - 1 = sk$ and $x = tm$ for some $s, t \in \mathbb{Z}$. Multiply these together to get $(x-1)x = (sk)(tm) = (st)(km)$. Hence $(km)|(x^2 - x)$, which shows that $x^2 \equiv x \pmod{km}$.