M403 Homework 8

Enrique Areyan
October 24, 2012

(1.77) (iii) **False**. Let $a = 2$. Then $a^6 = 64 = 10 \cdot 6 + 4 \Rightarrow 64 \equiv 4 \pmod 6$.

(iv) **False**. Let $a = 2$. Then, $a^4 = 16 = 4 \cdot 4 + 0 \Rightarrow 16 \equiv 0 \pmod 4$.

(vii) **True**. On the one hand, $n \equiv 1 \pmod{100} \iff n = 100p + 1$, where $p \in \mathbb{Z}$.
On the other, $n \equiv 4 \pmod{1001} \iff n = 1001q + 4$, where $q \in \mathbb{Z}$.
Hence, $100p + 1 = 1001q + 4 \iff$

$$\begin{aligned} 3 &= 100p - 1001r \\ &= 100p - (1000 + 1)r \\ &= 100p - 1000r - r \\ &= 100(p - 10r) - r \end{aligned}$$

Hence, a possible solution is:

$$p - 10r = 1 \text{ and } r = 97$$

$$p - 10r = 1 \iff p - 10 \cdot 97 = 1 \iff p = 971$$

Substituting p in our first equation we find that the number n is:

$$n = 100 \cdot p + 1 = 100 \cdot 971 + 1 = 97100 + 1 = 97101$$

Indeed, it is the case that $97101 \equiv 1 \pmod{100}$ and $97101 \equiv 4 \pmod{1001}$

(viii) **False**. Let $p = 5, a = 3, m = 5$ and $n = 0$. Clearly 5 is prime. Also, $m \equiv n \pmod p$ since $5|5 - 0$. But, $a^m = 3^5 = 243 \equiv 0 \pmod 3$ and $3^0 = 1 \equiv 1 \pmod 3$. Hence, $3^5 \not\equiv 3^0 \pmod 3$.

(1.78) (i) $3x \equiv 2 \pmod 5 \iff x = 4 + 5k$ for some $k \in \mathbb{Z} \iff x \equiv 4 \pmod 5$

(ii) $7x \equiv 4 \pmod{10} \iff x = 2 + 10k$ for some $k \in \mathbb{Z} \iff x \equiv 2 \pmod{10}$

(iii) $243x + 17 \equiv 101 \pmod{725} \iff x = 63 + 725k$ for some $k \in \mathbb{Z} \iff x \equiv 63 \pmod{725}$

(iv) $4x + 3 \equiv 4 \pmod 5$. The solution is $x = 4$ since $4x + 3 = 4 \cdot 4 + 3 = 16 + 3 = 19 = 5 \cdot 3 + 4 \equiv 4 \pmod 5$. The general solution is therefore $x = 4 + 5 \cdot k$ for some $k \in \mathbb{Z} \iff x \equiv 4 \pmod 5$.

(v) $6x + 3 \equiv 4 \pmod{10} \iff 6x \equiv 1 \pmod{10}$. But, $gcd(10, 6) = gcd(10 - 6, 6) = gcd(6, 4) = gcd(6 - 4, 4) = gcd(4, 2) = gcd(4 - 2, 2) = gcd(2, 2) = 2 > 1$ and 2 does not divide 1. Hence, this system has no solution.

(vi) $6x + 3 \equiv 1 \pmod{10}$. The solution is $x = 3$ since $6x + 3 = 6 \cdot 3 + 3 = 18 + 3 = 21 \equiv 1 \pmod{10}$. The general solution is therefore $x = 3 + 10 \cdot k$ for some $k \in \mathbb{Z} \iff x \equiv 3 \pmod{10}$

(1.81) Since $100 = 2 \cdot 49 + 2$, $10^{100} = 10^{2 \cdot 49 + 2} = 10^{2 \cdot 49} \cdot 10^2$. Now, by the same fact used before, $10^2 \equiv 2 \pmod 7$. Moreover,

$$\begin{aligned} 10^{2 \cdot 49} &= 10^{2 \cdot 7 \cdot 7} && \text{Exponent rule} \\ &= 10^{7^{2 \cdot 7}} && \text{Exponent rule} \\ &\equiv 10 \pmod 7 && \text{By Fermat's little theorem, since 7 is prime} \\ &\equiv 3 \pmod 7 \end{aligned}$$

Combining this results we obtain: $10^{100} \equiv 3 \cdot 2 = 6 \pmod 7$. Therefore, the remainder after dividing 10^{100} by 7 is 6.

(1.84) The solutions depend on whether m is odd or even.

<u>If m is odd</u>, then the solutions are $r \equiv 0$ (mod m), Since $m|r \iff r = m \cdot k$ for some $k \in \mathbb{Z}$ and then $2r = 2(m \cdot k) \equiv 0 \pmod m$. Note that in the case when m is odd these are the only solutions. Indeed, if anther solution $r = m \cdot k + m'$, where $m' \in \mathbb{Z}$ exists, then $2r = 2(m \cdot k + m') = 2 \cdot m \cdot k + 2 \cdot m' \equiv 0 + 2 \cdot m' \pmod m$, which is never congruent to 0 since m is odd and does not divive $2 \cdot m'$ (an even number).

<u>If m is even</u>, then the solutions are $r \equiv \frac{m}{2} \pmod m$, since $m|r - \frac{m}{2} \iff r = m \cdot k + \frac{m}{2}$. Indeed, $2r = 2(m \cdot k + \frac{m}{2}) = 2 \cdot m \cdot k + m \equiv 0 \pmod m$. These are all the solutions (you can just vary k freely).

(1.89) Since $gcd(a.m) = d > 1$ then $d|a \iff a = da'$ and $d|m \iff m = dm'$.
By definition, $ax \equiv b \pmod b \iff ax = b + mk$ for some $k \in \mathbb{Z}$. Rearranging the equation: $ax - mk = b$. Since d is the $gcd(a, m)$, then $da'x - dm'k = b \iff d(a'x - m'k) = b \iff d|b$, so if d does not divide b there is no solution.

(1.90) $x^2 \equiv 1 \pmod{21} \iff x^2 \equiv 1 \pmod 7$ AND $x^2 \equiv 1 \pmod 3$. The following table summarizes the possibilities for x:

$x =$	0	1	2
$x^2 =$	0	1	4
$x^2 \equiv \pmod 3$	0	1	1

$x =$	0	1	2	3	4	5	6
$x^2 =$	0	1	4	9	16	25	36
$x^2 \equiv \pmod 7$	0	1	4	2	2	4	1

$x = 1$ OR $x = 2$ $\qquad\qquad$ $x = 1$ OR $x = 6$

Therefore, all the solutions are given by solving four different systems:

$$\begin{cases} x \equiv 1 & \pmod 3 \\ x \equiv 1 & \pmod 7 \end{cases} \Rightarrow \boxed{x \equiv 1 \pmod{21}} \text{ by the Chinese Remainder Theorem.}$$

$$\begin{cases} x \equiv 1 & \pmod 3 \Rightarrow x = 3k+1 \\ x \equiv 6 & \pmod 7 \Rightarrow 3k+1 \equiv 6 \pmod 7 \iff 3k \equiv 5 (\mathrm{mod}\ 7) \iff k = 4 + 7k' \text{ for some } k' \in \mathbb{Z} \end{cases}$$

Hence, the solutions are: $x = 3(4+7k') + 1 = 12 + 21k' + 1 = 21k' + 13 \iff \boxed{x \equiv 13 \pmod{21}}$

$$\begin{cases} x \equiv 2 & \pmod 3 \Rightarrow x = 3k+2 \\ x \equiv 1 & \pmod 7 \Rightarrow 3k+2 \equiv 1 \pmod 7 \iff 3k \equiv -1 (\mathrm{mod}\ 7) \iff k = 2 + 7k' \text{ for some } k' \in \mathbb{Z} \end{cases}$$

Hence, the solutions are: $x = 3(2+7k') + 2 = 6 + 21k' + 2 = 21k' + 8 \iff \boxed{x \equiv 8 \pmod{21}}$

$$\begin{cases} x \equiv 2 & \pmod 3 \Rightarrow x = 3k+2 \\ x \equiv 6 & \pmod 7 \Rightarrow 3k+2 \equiv 6 \pmod 7 \iff 3k \equiv 4 \pmod 7 \iff k = 6 + 7k' \text{ for some } k' \in \mathbb{Z} \end{cases}$$

Hence, the solutions are: $x = 3(6+7k') + 2 = 18 + 21k' + 2 = 21k' + 20 \iff \boxed{x \equiv 20 \pmod{21}}$

(1.91) (i) Since $gcd(5,1) = gcd(8,3) = 1$; both of the following equations have a solution by their own.

$$\begin{cases} x \equiv 2 & \pmod 5 \Rightarrow x = 5k+2 \\ 3x \equiv 1 & \pmod 8 \Rightarrow 3(5k+2) \equiv 1 \pmod 8 \iff 15k \equiv -5 (\mathrm{mod}\ 8) \iff k = -3 + 8k' \text{ for some } k' \in \mathbb{Z} \end{cases}$$

Hence, the solutions are: $x = 5(-3+8k') + 2 = -15 + 40k' + 2 = 35k' - 13 \iff \boxed{x \equiv -13 \pmod{40}}$

(ii) Since $gcd(5,3) = gcd(2,3) = 1$; both of the following equations have a solution by their own.

$$\begin{cases} 3x \equiv 2 & \pmod 5 \Rightarrow x = 5k+4 \\ 2x \equiv 1 & \pmod 3 \Rightarrow 2(5k+4) \equiv 1 \pmod 3 \iff 10k \equiv -7 (\mathrm{mod}\ 3) \iff k = 2 + 3k' \text{ for some } k' \in \mathbb{Z} \end{cases}$$

Hence, the solutions are: $x = 5(2+3k') + 4 = 10 + 15k' + 4 = 15k' + 14 \iff \boxed{x \equiv 14 \pmod{15}}$

(1.92) We want to find the smallest positive integer x such that:

$$\begin{cases} x \equiv 4 & \pmod 5 \iff x = 5k+4 \\ x \equiv 3 & (\mathrm{mod}\ 7) \Rightarrow 5k+4 \equiv 3 \ (\mathrm{mod})7 \iff 5k \equiv -1 \ (\mathrm{mod})7 \iff k = 4 + 7k' \text{ for some } k' \in \mathbb{Z} \\ x \equiv 1 & \pmod 9 \end{cases}$$

The solutions for the <u>first two</u> equations are: $x = 5(4+7k') + 4 = 20 + 35k' + 4 = 35k' + 24 \iff x \equiv 24 \ (\mathrm{mod})\ 35$

Now we can solve the simpler system:

$$\begin{cases} x \equiv 24 & \pmod{35} \Rightarrow x = 35k+24 \\ x \equiv 1 & \pmod 9 \Rightarrow 35k+24 \equiv 1 \pmod 9 \iff 35k \equiv -23 (\mathrm{mod}\ 9) \iff k = 2 + 3k' \text{ for some } k' \in \mathbb{Z} \end{cases}$$

But, $-23 \equiv 4 \pmod 9$, since $-23 - 4 = -27 = 9 \cdot (-3)$. Also, $35k = 27k + 8k \equiv 8k \pmod 9$.
We can restate the equation $35k \equiv -23 (\mathrm{mod}\ 9)$ as $8k \equiv 4 \pmod 9$. The solutions as $k = 5 + 9k'$.
Hence, the solutions are: $x = 35(5+9k') + 24 = 175 + 315k' + 24 = 315k' + 199 \iff \boxed{x \equiv 199 \pmod{315}}$

(1.95)

$$\begin{cases} x \equiv 12 & \pmod{25} \Rightarrow x = 25k + 12 \\ x \equiv 2 & \pmod{30} \Rightarrow 25k + 12 \equiv 2 \pmod{30} \iff 25k \equiv -10 \pmod{30} \end{cases}$$

But $-10 \equiv 20 \pmod{30}$, since it is true that $30 | -10 - 20$. Hence, we can rewrite the last equation as

$$25k \equiv 20 \pmod{30} \iff k = 2 + 30k'$$

Hence, the solutions are: $x = 25(2 + 30k') + 12 = 50 + 750k' + 12 = 750k' + 62 \iff \boxed{x \equiv 62 \pmod{750}}$

(1.96) Let x and y be two solutions. Then both satisfy the following systems of equations:

$$\begin{cases} x \equiv b & \pmod{m} \\ x \equiv b' & \pmod{m'} \end{cases} \quad \begin{cases} b \equiv y & \pmod{m} \\ b' \equiv y & \pmod{m'} \end{cases} \Rightarrow \text{Transitivity of mod} \quad \begin{cases} x \equiv y & \pmod{m} \\ x \equiv y & \pmod{m'} \end{cases}$$

In particular, the last equations mean that $m|x - y$ and $m'|x - y$. Since any integer that is divisible by m and m' is also divisible by $l = lcm(m, m')$, then $l|x - y \iff x \equiv y \pmod{l}$