Solutions to Attendance Quiz # 11 for Dr. Z.'s Number Theory Course for Oct. 10, 2013

1. Using the first way, find the unique $x \in \{0, 1, 2, \ldots, 20\}$such that

$$x \equiv 2 \pmod 3 \quad , \quad x \equiv 4 \pmod 7 \quad .$$

Sol. to 1: Define $f(x) := (x \; mod \; 3, x \; mod \; 7)$.

$$f(0) = (0,0) \quad , \quad f(1) = (1,1), \quad f(2) = (2,2), \quad f(3) = (0,3)$$

$$f(4) = (1,4) \quad , \quad f(5) = (2,5), \quad f(6) = (0,6), \quad f(7) = (1,0)$$

$$f(8) = (2,1) \quad , \quad f(9) = (0,2), \quad f(10) = (1,3), \quad f(11) = (2,4)$$

we could go on, but since we found our target $(2,4)$, we are done!

Ans. to 1: $x = 11 \pmod{21}$.

2. Using the second way (the formula) find the unique x between 0 and 62 such that

$$x \equiv 4 \pmod 7 \quad , \quad x \equiv 2 \pmod 9 \quad .$$

Ans. to 2: The beautiful formula (in the wikipedia notation) is If m_1, m_2 are relatively prime, then The solution of

$$x \equiv a_1 \pmod{m_1} \quad , \quad x \equiv a_2 \pmod{m_2} \quad ,$$

is given by

$$a_1 m_2 [m_2^{-1}]_{m_1} + a_2 m_1 [m_1^{-1}]_{m_2} \pmod{m_1 m_2} \quad .$$

In this problem, $a_1 = 4, m_1 = 7$, $a_2 = 2, m_2 = 9$. In remains to find

$[m_2^{-1}]_{m_1}$ and $[m_1^{-1}]_{m_2}$. We do these **together**, by applying the Extended Euclidean algorithm to 7 and 9.

$$\mathbf{9} = 1 \cdot \mathbf{7} + 2 \quad ,$$

so

$$2 = \mathbf{9} - 1 \cdot \mathbf{7} \quad .$$

$$\mathbf{7} = 3 \cdot 2 + 1 \quad ,$$

so

$$1 = \mathbf{7} - 3 \cdot 2 = \mathbf{7} - 3 \cdot (\mathbf{9} - 1 \cdot \mathbf{7}) = \mathbf{7} - 3 \cdot \mathbf{9} + 3 \cdot \mathbf{7} = 4 \cdot \mathbf{7} - 3 \cdot \mathbf{9} \quad .$$

So

$$1 = 4 \cdot \mathbf{7} - 3 \cdot \mathbf{9} \quad .$$

Now we take this identity modulo 7 getting

$$1 \equiv (-3) \cdot \mathbf{9} \pmod{7} \quad .$$

So

$$[9^{-1}]_7 = -3 = 4 \quad .$$

Now we take this identity modulo 9 getting

$$1 = 4 \cdot \mathbf{7} \pmod{9} \quad .$$

So

$$[7^{-1}]_9 = 4 \quad .$$

Finally, putting

$$a_1 = 4 \quad , \quad m_1 = 7 \quad , \quad a_2 = 2 \quad , \quad m_2 = 9,$$

$$[m_2^{-1}]_{m_1} = 4 \quad , \quad [m_1^{-1}]_{m_2} = 4 \quad ,$$

we get

$$x = a_1 m_2 [m_2^{-1}]_{m_1} + a_2 m_1 [m_1^{-1}]_{m_2} \pmod{m_1 m_2} \quad .$$

$$\equiv 4 \cdot 9 \cdot 4 + 2 \cdot 7 \cdot 4 \pmod{7 \cdot 9}$$

$$\equiv 144 + 56 \pmod{63} \equiv 200 \pmod{63} \equiv 11 \pmod{63} \quad .$$

Ans. to 2: $x \equiv 11 \pmod{63}$. The unique x between 0 and 62 satisfying the two congruences is $x = 11$.

Comment: The above is the official way. If you are in a rush, you can find $[9^{-1}]_7$ and $[7^{-1}]_9$ by 'trial and error'.

First, since $9 \equiv 2 \pmod{7}$,we have $[9^{-1}]_7 = [2^{-1}]_7$. Now by trial and error, $2 \cdot 4 \equiv 1 \pmod{7}$. For $[7^{-1}]_9$ there is no such shortcut, but again by trying out $7, 14, 21, 28$ and taking it modulo 9 we soon get that it is 4.