Solutions to Quiz # 4 for Dr. Z.'s Number Theory Course for Oct. 17, 2013

1. Using the the formula find the unique x between 0 and 44 such that

$$x \equiv 3 \pmod 5 \quad , \quad x \equiv 5 \pmod 9 \quad .$$

Solution to 1.: The formula is: The solution of the system

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

is

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

Here $m_1 = 5$ and $m_2 = 9$. Since $gcd(5, 9) = 1$ we are guaranteed a solution, but let's find both $[9^{-1}]_5$ and $[5^{-1}]_9$. We can do it at the same time by doing the Extended Euclidean algorithm for 5 and 9.

$$\mathbf{9} = 1 \cdot \mathbf{5} + 4 \quad ,$$

Hence

$$4 = \mathbf{9} - 1 \cdot \mathbf{5} \quad .$$

Next

$$\mathbf{5} = 1 \cdot 4 + 1 \quad ,$$

Hence

$$1 = \mathbf{5} - 4 = \mathbf{5} - (\mathbf{9} - 1 \cdot \mathbf{5}) = 2 \cdot \mathbf{5} - 1 \cdot \mathbf{9}$$

So we got

$$1 = 2 \cdot \mathbf{5} - 1 \cdot \mathbf{9} \quad .$$

Taking it mod 5 we get

$$1 \equiv (-1) \cdot \mathbf{9} \pmod 5 \quad ,$$

so $[9^{-1}]_5 = -1$ $(= 4)$. It is easier to keep it as -1. Taking it mod 9, we get

$$1 \equiv 2 \cdot \mathbf{5} \pmod 9 \quad ,$$

so $[5^{-1}]_9 = 2$. Since $a_1 = 3$ and $a_2 = 5$ we have

$$x \equiv 3 \cdot 9 \cdot [9^{-1}]_5 + 5 \cdot 5 \cdot [5^{-1}]_9 \pmod{45}$$

$$\equiv 3 \cdot 9 \cdot (-1) + 5 \cdot 5 \cdot 2 \pmod{45}$$

$$\equiv -27 + 50 \pmod{45} \equiv 23 \pmod{45} \quad .$$

But this is **not** the final answer. The question asked for an **integer** NOT a congruence class! The unique integer between 0 and 44 that satisfies the two conditions of the problem is $x = 23$.

Ans. to 1.: $x = 23$.

Note about partial credit policy: Quite a few people followed the right method and formula, but made careless computational mistakes that lead to the wrong answer. It is OK to make mistakes, but in this problem (and many other problems in this class), it is **very easy** to check your answer.

In this case 23 *modulo* 5 = 3 and 23 *modulo* 9 = 5, so you know that you got the right answer. Suppose that you made a careless error and got $x = 20$, then 20 *modulo* 5 = 0 and you know right away that you made a mistake.

If you would write: "I realize that I made an error, since my answer does not agree with the conditions", you would get more partial credit.