CSL202: Discrete Mathematical Structures (Semester-I-2018-19) Quiz-08

Name: ____________________________

Entry number: ________________________

There are 3 questions for a total of 10 points.

1. Consider the two jugs problem as in the homework and previous quiz. You are given two jugs with integer capacities. Let us call these jugs X and Y. Jug X has capacity 21 litres and jug Y has capacity 39 litres. You also have an unlimited source of water. Answer the following questions:

   (a) (1 point) Is there a way to make sure that one of the jugs has exactly 12 litres of water? (*Answer yes or no*)

   (a) **Yes**

   (b) (1 point) Is there a way to make sure that one of the jugs has exactly 10 litres of water? (*Answer yes or no*)

   (b) **No**

   (c) (2 points) If your answer to part (a) or part (b) was "yes", describe the steps that will lead to one of the jugs having the amount of water specified in the problem. Do any one in case your answer to both (a) and (b) was "yes". In case your answer to both part (a) and (b) was "no", just write "Not applicable" below.

   Solution: We can make 12 litres using the following procedure:

   > Fill the 21 litres jug 8 times emptying it into the 39 litres jug and whenever the 39 litres jug gets full, its water in it is thrown away.

   (d) (1 point) Does your answer to part (b) change if the jugs were of capacities 21 and 34 instead of 21 and 39? (*Answer yes or no*)

   (d) **Yes**

2. Use ideas developed in the class to calculate the following. Show calculations in the space provided.

   (a) (1 point) Give the value of 15^{442} $(mod\ 41)$.
   (*Note that your answer should be an integer between* 0 *and* 40.)

   (a) **20**

   Solution: We know that for any prime number p and any $1 \leq a < p$, we have $a^{p-1} \equiv 1\ (mod\ p)$. We can apply this theorem in the current context since 41 is a prime number. So, we have $15^{442}\ (mod\ 41) = (15^{11 \cdot 40} \cdot 15^2)\ (mod\ 41) = 20$. So, the answer is 20.

   (b) (1 point) Give the value of 7^{324} $(mod\ 33)$.
   (*Note that your answer should be an integer between* 0 *and* 34.)

   (b) **25**

Solution: $33 = 3 \cdot 11$. Note that 3 and 11 are relatively prime. Also note that $7 \in \mathbb{Z}_{33}^{\star}$. Also note that $|\mathbb{Z}_{33}^{\star}| = (3-1)\cdot(11-1) = 20$. For this problem, we use the theorem that for any element g of the group $g^m = 1$ when m equals the size of the group. We have $7^{324} \ (mod\ 33) = 7^{16*20+4} \ (mod\ 33) = 256 \ (mod\ 33) = 25$. So, the answer is 25.

(c) (1 point) Find an integer x that simultaneously satisfies the following three linear congruences $x \equiv 2 \ (mod\ 5)$, $x \equiv 2 \ (mod\ 7)$, and $x \equiv 5 \ (mod\ 9)$.
(*Your answer should be an integer between* 0 *and* 314.)

(c) **212**

Solution: *This is just for explanation. You need not have written this.*
We use the Chinese Remaindering Theorem(CRT) since $5, 7$, and 9 are pairwise relatively prime. We use the construction given in the proof of CRT.

$$\begin{aligned} x &= 2\cdot(7\cdot 9)\cdot((7\cdot 9)^{-1} \ (mod\ 5)) + 2\cdot(5\cdot 9)\cdot((5\cdot 9)^{-1} \ (mod\ 7)) + 5\cdot(5\cdot 7)\cdot((5\cdot 7)^{-1} \ (mod\ 9)) \\ &= 2\cdot 63\cdot 2 + 2\cdot 45\cdot 5 + 5\cdot 35\cdot 8 \\ &= 2102 \end{aligned}$$

Since $2102 \equiv 212 \ (mod\ 315)$. So, $x = 212$ is a solution to the above three linear congruences.

3. (2 points) Let $p, q > 1$ be prime numbers, $N = p\cdot q$, $M = (p-1)\cdot(q-1)$, and e, d be such that $ed \equiv 1 \ (mod\ M)$. Show that for *every* $x \in \mathbb{Z}_N$, $x^{ed} \equiv x \ (mod\ N)$.
(*Note that in the class, we have already showed that for every* $x \in \mathbb{Z}_N^*, x^{ed} \equiv 1 \ (mod\ N)$. So, you only need to argue for numbers in the set $\mathbb{Z}_N \setminus \mathbb{Z}_N^*$.)

Solution: Consider any $x \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$. WLOG we assume that p divides x and q does not. So, $a = x \ (mod\ p) = 0$. Let $b = x \ (mod\ q)$. Note that b is relatively prime to q and hence $b^{q-1} \equiv 1 \ (mod\ q)$. Since $ed \equiv 1 \ (mod\ M)$, let $ed = k\cdot(p-1)(q-1)+1$. So, we have:

$$x^{ed} \ (mod\ p) = a^{ed} \ (mod\ p) = 0 = x \ (mod\ p) \quad , \text{and}$$

$$\begin{aligned} x^{ed} \ (mod\ q) = \quad b^{ed} \ (mod\ q) &= b^{k(p-1)(q-1)+1} \ (mod\ q) \\ &= (b\cdot(b^{(q-1)})^{k(p-1)}) \ (mod\ q) \\ &= b \\ &= x \ (mod\ q) \end{aligned}$$

Since $x^{ed} \equiv x \ (mod\ p)$ and $x^{ed} \equiv x \ (mod\ q)$, from the Chinese Remaindering Theorem, we get that $x^{ed} \equiv x \ (mod\ N)$.