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) (½ point) Is there a way to make sure that one of the jugs has exactly 12 litres of water? (*Answer yes or no*)

   (a) _____

   (b) (½ point) Is there a way to make sure that one of the jugs has exactly 10 litres of water? (*Answer yes or no*)

   (b) _____

   (c) (1 ½ 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.

   (d) (½ 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) _____

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) _____

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

(b) _____

(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) _____

3. (4 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 $\mathbb{Z}_N \setminus \mathbb{Z}_N^*$.)

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) (½ point) Is there a way to make sure that one of the jugs has exactly 12 litres of water? (*Answer yes or no*)

   (a) _____

   (b) (½ point) Is there a way to make sure that one of the jugs has exactly 10 litres of water? (*Answer yes or no*)

   (b) _____

   (c) (1 ½ 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.

   (d) (½ 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) _____

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) _____

(b) (1 point) Give the value of 7^{323} (*mod* 33).
(*Note that your answer should be an integer between* 0 *and* 34.)

(b) _____

(c) (1 point) Find an integer x that simultaneously satisfies the following three linear congruences $x \equiv 2$ (*mod* 5), $x \equiv 4$ (*mod* 7), and $x \equiv 5$ (*mod* 9).
(*Your answer should be an integer between* 0 *and* 314.)

(c) _____

3. (4 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 $\mathbb{Z}_N \setminus \mathbb{Z}_N^*$.)

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) (½ point) Is there a way to make sure that one of the jugs has exactly 10 litres of water? (*Answer yes or no*)

   (a) _____

   (b) (½ point) Is there a way to make sure that one of the jugs has exactly 12 litres of water? (*Answer yes or no*)

   (b) _____

   (c) (1 ½ 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.

   (d) (½ 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) _____

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^{443} (*mod* 41).
   (*Note that your answer should be an integer between* 0 *and* 40.)

   (a) _____

(b) (1 point) Give the value of 7^{323} (*mod* 33).
(*Note that your answer should be an integer between* 0 *and* 34.)

(b) _____

(c) (1 point) Find an integer x that simultaneously satisfies the following three linear congruences $x \equiv 2$ (*mod* 5), $x \equiv 4$ (*mod* 7), and $x \equiv 5$ (*mod* 9).
(*Your answer should be an integer between* 0 *and* 314.)

(c) _____

3. (4 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 $\mathbb{Z}_N \setminus \mathbb{Z}_N^*$.)

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) (½ point) Is there a way to make sure that one of the jugs has exactly 10 litres of water? (*Answer yes or no*)

   (a) _____

   (b) (½ point) Is there a way to make sure that one of the jugs has exactly 12 litres of water? (*Answer yes or no*)

   (b) _____

   (c) (1 ½ 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.

   (d) (½ 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) _____

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^{443} (*mod* 41).
   (*Note that your answer should be an integer between* 0 *and* 40.)

   (a) _____

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

(b) _____

(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) _____

3. (4 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 $\mathbb{Z}_N \setminus \mathbb{Z}_N^*$.)