Name: _____

ID number: _____

There are 3 questions for a total of 10 points.

---

1. Recall the `Extended-Euclid-GCD` algorithm discussed in class for finding the gcd of positive integers $a \geq b > 0$ and integers $x, y$ such that $ax + by = gcd(a, b)$. The algorithm makes a sequence of recursive calls until the second input becomes 0. For example, the sequence of recursive calls along with the function-call returns for inputs $(2, 1)$ are:

$$\overset{(1,0,1)}{\leftarrow} \texttt{Extended-Euclid-GCD}(2,1) \overset{(1,1,0)}{\leftarrow} \texttt{Extended-Euclid-GCD}(1,0)$$

   (a) (1 ½ points) Write down the sequence of recursive calls along with function-call returns that are made when the algorithms is executed with inputs $(991, 53)$.

   **Solution:** $\overset{(1,-10,187)}{\leftarrow}$ `Extended-Euclid-GCD`$(991,53)$ $\overset{(1,7,-10)}{\leftarrow}$ `Extended-Euclid-GCD`$(53,37)$ $\overset{(1,-3,7)}{\leftarrow}$ `Extended-Euclid-GCD`$(37,16)$ $\overset{(1,1,-3)}{\leftarrow}$ `Extended-Euclid-GCD`$(16,5)$ $\overset{(1,0,1)}{\leftarrow}$ `Extended-Euclid-GCD`$(5,1)$ $\overset{(1,1,0)}{\leftarrow}$ `Extended-Euclid-GCD`$(1,0)$

   (b) (½ point) What is the inverse of 53 modulo 991? That is, give a positive integer $x$ such that $53 \cdot x \equiv 1$ $(mod\ 991)$.

   (b) **187**

2. Use ideas developed in the class to calculate the following:

   (a) (1 point) Give the value of $7^{442}$ $(mod\ 41)$.
   (*Note that your answer should be an integer between* 0 *and* 40.)

   (a) **8**

   *This is just for explanation. You need not have written this.*
   Fermat's little theorem says 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 $7^{442}$ $(mod\ 41) \equiv (7^{11 \cdot 40} \cdot 7^2)$ $(mod\ 41) \equiv 49$ $(mod\ 41) \equiv 8$ $(mod\ 41)$. So, the answer is 8.

   (b) (1 point) Give the value of $9^{313}$ $(mod\ 35)$.
   (*Note that your answer should be an integer between* 0 *and* 34.)

   (b) **9**

   *This is just for explanation. You need not have written this.*
   $35 = 5 \cdot 7$. Note that 5 and 7 are relatively prime. Also note that $9 \in \mathbb{Z}^{\star}_{35}$. Also note that $|\mathbb{Z}^{\star}_{35}| = (5-1) \cdot (7-1) = 24$. 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 $9^{313}$ $(mod\ 35) \equiv$

$9^{24*13+1} \pmod{35} \equiv 9 \pmod{35}$. So, the answer is 9.

(c) (1 point) Find an integer $x$ that simultaneously satisfies the following three linear congruences $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$, and $x \equiv 5 \pmod 9$.
(*Your answer should be an integer between* 0 *and* 314.)

*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.

$$\begin{aligned} x &= 3 \cdot (7 \cdot 9) \cdot ((7 \cdot 9)^{-1} \pmod 5) + 2 \cdot (5 \cdot 9) \cdot ((5 \cdot 9)^{-1} \pmod 7) + 5 \cdot (5 \cdot 7) \cdot ((5 \cdot 7)^{-1} \pmod 9) \\ &= 3 \cdot 63 \cdot 2 + 2 \cdot 45 \cdot 5 + 5 \cdot 35 \cdot 8 \\ &= 2228 \end{aligned}$$

Since $2228 \equiv 23 \pmod{315}$. So, $x = 23$ is a solution to the above three linear congruences.

3. Consider one of the problems in the tutorial sheet. You are given two jugs with integer capacities. Let us call these jugs $X$ and $Y$. Jug $X$ has capacity 26 litres and jug $Y$ has capacity 46 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 10 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 11 litres of water? (*Answer yes or no*)

(b) **No**

*This is just for explanation. You need not have written this.*
Note that the amount of water in each of the jugs at any stage is a linear combination of the capacities of the jugs and hence should be divisible by the gcd of the capacities. Since 11 is not divisible by the gcd of 23 and 46, we get that 11 litres cannot be made using these jugs.

(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 10 litres using the following procedure:
Repeat 20 times:
- Fill the 46 litres jug and empty it into the 26 litres jug and whenever the 26 litres jug gets full, the water in it is thrown away.

(d) (1 point) Does your answer to part (a) change if the jugs were of capacities 15 and 21 instead of 26 and 46? (*Answer yes or no*)

(d) **Yes**

*This is just for explanation. You need not have written this.*
Note that the amount of water in each of the jugs at any stage is a linear combination of the capacities of the jugs and hence should be divisible by the gcd of the capacities. Since 10 is not divisible by the gcd of 15 and 21 (which is 3), we get that 10 litres cannot be made using these jugs.