Name: _____

Entry number: _____

There are 4 questions for a total of 15 points.

---

1. Use ideas developed in the class to calculate the following. Show all calculations demonstrating how you arrived at the solution in the space provided. *Please note that there are no points for just writing the answer.*

   (a) (3 points) Find the smallest positive integer n such that $3^n \equiv 1 \ (mod\ 319)$.
   (*Your answer should be an integer between* 1 *and* 319.)

   (a) **140**

   Solution: Note that $319 = 11*29$ and both 11 and 29 are prime numbers. Consider the groups $\mathbb{Z}_{11}^*$ and $\mathbb{Z}_{29}^*$. We have $|\mathbb{Z}_{11}^*| = 5*2$ and $|\mathbb{Z}_{29}^*| = 28 = 7*2^2$. We know that $3 \in \mathbb{Z}_{11}^*$ and $3 \in \mathbb{Z}_{29}^*$. Using the result that the order of the element divides the group size we quickly find that the smallest integers p, q such that $3^p \equiv 1 \ (mod\ 11)$ and $3^q \equiv 1 \ (mod\ 29)$ are $p = 5$ and $q = 28$. So, the smallest x such that $3^x \equiv 1 \ (mod\ 319)$ is the LCM of 5 and 28 which is 140.

   (b) (1 point) Find the value of $5^{58} \ (mod\ 61)$.

   (b) **22**

   Solution: Since 61 is a prime number, we have that $5^{60} \equiv 1 \ (mod\ 61)$. So we have $5^2 \cdot 5^{58} \equiv 1 \ (mod\ 61)$. So, $5^{58} \ (mod\ 61)$ will just be the inverse of 25 modulo 61. This can be found using the Extended GCD algorithm and comes out to be 22.

   (c) (3 points) Find a solution of $x^3 - x + 1 \equiv 0 \ (mod\ 385)$.
   (*Your answer should be an integer between* 1 *and* 385.)

   (c) **93**

   Solution: Note that $385 = 5 * 7 * 11$. Note that the following holds:

   1. A solution of $[x^3 - x + 1 \equiv 0 \ (mod\ 5)]$ is $x \equiv 3 \ (mod\ 5)$.
   2. A solution of $[x^3 - x + 1 \equiv 0 \ (mod\ 7)]$ is $x \equiv 2 \ (mod\ 7)$.
   3. A solution of $[x^3 - x + 1 \equiv 0 \ (mod\ 11)]$ is $x \equiv 5 \ (mod\ 11)$.

   To find a solution of the given congruence, we need to find a number x that satisfies $x \equiv 3 \ (mod\ 5)$, $x \equiv 2 \ (mod\ 7)$, $x \equiv 5 \ (mod\ 11)$. This can be done using the Chinese Remaindering Theorem.

   $$\begin{aligned} x &= \left[3 \cdot 77 \cdot (77^{-1} \ (mod\ 5)) + 2 \cdot 55 \cdot (55^{-1} \ (mod\ 7)) + 3 \cdot 35 \cdot (35^{-1} \ (mod\ 11))\right] \ (mod\ 385) \\ &= [3 \cdot 77 \cdot (-2) + 2 \cdot 55 \cdot (-1) + 3 \cdot 35 \cdot (-5)] \ (mod\ 385) \\ &= 93 \end{aligned}$$

2. (2 points) State true or false with reasons: Consider functions $f(n) = 10n2^n + 5^n$ and $g(n) = n5^n$. Then $f(n)$ is $\Omega(g(n))$.

2. **False**

Solution: $f(n)$ is $\Omega(g(n))$ iff there exists constants $c > 0, n_0 \geq 0$ such that for all $n \geq n_0$ $f(n) \geq c \cdot g(n)$. So, $f(n)$ is not $\Omega(g(n))$ iff for all constants $c > 0, n_0 \geq 0$, there exists $n \geq n_0$ such that $f(n) < c \cdot g(n)$. Note that $(c/2)n5^n > 5^n$ when $n > 2/c$ for any constant c. Moreover, note that $(c/2)n5^n > 10n2^n \Leftrightarrow (5/2)^n > 20/c \Leftrightarrow n > \log_{5/2}(20/c)$.

Combining the previous two statements, we get that for any constant $c > 0$, $cn5^n > (10n2^n + 5^n)$ when $n > \max(2/c, \log_{5/2}(20/c))$. This further implies that for any constants $c > 0, n_0 \geq 0$, $cn'5^{n'} > (10n'2^{n'} + 5^{n'})$ for $n' = \max(2/c, \log_{5/2}(20/c), n_0) + 1$. Note that $n' \geq n_0$. So, for any constants $c > 0, n_0 \geq 0$, there is a number $n \geq n_0$ (n' above is such a number) such that $cn5^n > (10n2^n + 5^n)$. This implies that $f(n)$ is not $\Omega(g(n))$.

3. (1 point) Consider the following recursive function:

```
F(n)
  - If (n > 1)
      - F(⌊n/3⌋); F(⌊n/3⌋)
  - Print("Hello World")
```

Let $R(n)$ denote the number of times this function prints "Hello World" given the positive integer n as input. Which of the following are true? Circle the correct choices. *You do not need to give any reasons for this question.*

A. $R(n) = O(n)$

B. $R(n) = \Omega(\log_2 n)$

C. $R(n) = 2 \cdot \lceil \log_3 n \rceil + 1$

D. $R(n) = 2 \cdot 2^{\lceil \log_3 n \rceil} - 1$

Solution: (A) and (B) are true.

This is for explanation. You were not expected to write this.
When $n = 3^i$ for $i \geq 1$, then the number of times "Hello World" is printed is $2^{i+1} - 1$.

For any arbitrary $n \geq 1$, let i be an integer such that $3^i \leq n < 3^{i+1}$. Then the number of times t that "Hello World" is printed is $2^{i+1} - 1 \leq t < 2^{i+2} - 1$. Now we observe the following:

$$\begin{aligned} 2^{i+1} - 1 \leq &\quad t &< 2^{i+2} - 1 \\ \Rightarrow i \leq &\quad t &< 3^{i+2} \\ \Rightarrow \log_3 n \leq &\quad t &< 3n \end{aligned}$$

(A) and (B) follow from the above. The fact that (C) and (D) do not hold can be shown using examples such as $R(5), R(17)$.

4. (5 points) n couples attended a party organised by the host and hostess (wife of the host). After several rounds of handshaking, the host asked the guests as well as the hostess to indicate the number of hands each one of them had shaken. He got $2n+1$ different answers. Given that no one shook hands with his or her own spouse, how many hands had the hostess shaken? Note that you have to prove the correctness of your answer.
(*Hint: Try small values of n and then generalize using induction.*)

Solution: Trying with small values of n, we see that the number of handshakes by the hostess is n. We will prove this by induction. We will work with the propositional function:
$P(n)$: The number of handshakes by the Hostess when there are n couples is n.

Basis step: $P(0)$ holds trivially.

Inductive step: Assume that $P(0), P(1), ..., P(i-1)$ holds for an arbitrary $i \geq 1$. We will argue that $P(i)$ holds. Consider the party with i couples (apart from the host and hostess). We show that the following claim hold:

Claim 1: There is a couple other than the host-hostess who do 0 and $2i$ handshakes.

Proof. First, we argue that there is couple who do 0 and $2i$ handshakes. There are two people p and q who shake hands with 0 and $2i$ people respectively. This is because there are $2i+1$ distinct handshakes. Person q is necessarily the spouse of p since otherwise q cannot do $2i$ handshakes (since he/she cannot handshake with p).

Now the host-hostess cannot be a couple with 0 and $2i$ handshakes. This is because if the hostess does 0 handshakes, then there cannot be a person that the host queries that does $2i$ handshakes. Also, if the hostess does $2i$ handshakes, then there cannot be a person that the host queries that does 0 handshakes. This completes the proof of the claim. □

Consider removing this couple that do 0 and $2i$ handshakes. If we consider the handshakes between the remaining couples, we see that the property that the host gets distinct answers still holds. From induction hypothesis, we conclude that the hostess shakes $i-1$ hands excluding the couple (p, q). So, when this couple is included, she shakes i hands.