PROBLEM SET 5: SURVEY, TELESCOPING SUMS, MODULAR ARITHMETIC

CS 198-087: INTRODUCTION TO MATHEMATICAL THINKING
UC BERKELEY EECS
SPRING 2019

This homework is due on Sunday, March 17th, at 11:59 PM on Gradescope (note the two week deadline). As usual, this homework is graded on participation, but it is in your best interest to put full effort into it. This is a good opportunity to learn how to use LaTeX.

---

1. *Feedback Form*

   Fill out the following feedback form: https://goo.gl/forms/VSgyvzyFZXUee6hq2.

   The form is anonymous. Please be as detailed as possible. After finishing, include a screenshot stating that you've filled out the form as your response to Q1.

2. *Proofs of Sums from Lecture*

   a. Derive $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ using a telescoping sum. (Note: This was done in lecture.)

   b. Derive $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$ using a telescoping sum.

3. *Telescoping Sums (Optional)*

   Prove the following. Using telescoping sums might be useful.

   a. $\sum_{i=2}^{2n+1} \frac{2}{i(i+2)} = \frac{5}{6} - \frac{4n+5}{(2n+2)(2n+3)}, n \geq 1$

   b. $\sum_{n=1}^{2019} \frac{1}{n!+(n-1)!} = 1 - \frac{1}{2020!}$

   (Hint: $n!$ is defined as the product $n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$. You might find the following property useful: $n! = n \cdot (n-1)!$. This follows trivially from the definition above.)

4. *GCD and LCM mechanics (skip if you feel comfortable)*

   Determine the greatest common divisor and lowest common multiple for each pair of numbers.

   a. 24, 36

   b. 14, 15

   c. 1200, 2350

   d. 144, 768

e. 24, 152

5. *GCD and LCM proof*

   Prove that $\text{lcm}(a, b) = a \cdot b$ if and only if $\text{gcd}(a, b) = 1$.

6. *Order of Operations – Multiplication*

   In lecture, we showed that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

   Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \cdot c \equiv b \cdot d \pmod{m}$.

7. *Last Digit Trick*

   Consider the task of finding the last digit of 3^{15}. One *could* multiply out and determine 3^{15} and read out the last digit, but there is an easier solution.

   When multiplying 3 by itself, there is a pattern in the last digit. Observe:

$$3^1 = (3), 3^2 = (9), 3^3 = 2(7), 3^4 = 8(1), 3^5 = 24(3), 3^6 = 72(9), ...$$

   We see that the last digits of the first four powers of 3 are 3, 9, 7 and 1. The fifth power of 3 ends in a 3, meaning the pattern will now repeat itself. The key realization is that the last digit of 3^n only depends on the last digit of 3^{n-1}, and nothing else.

   We can generalize this pattern: If we let $L(n)$ represent the last digit of n, we have:

$$L(3^n) = \begin{cases} 3, & n \equiv 1 \pmod{4} \\ 9, & n \equiv 2 \pmod{4} \\ 7, & n \equiv 3 \pmod{4} \\ 1, & n \equiv 0 \pmod{4} \end{cases}$$

   Similar patterns can also be found for all other digits. However, we don't necessarily need to consider powers of digits. We could also use the same properties when looking at powers of 23 — again, all we care about is the last digit. Looking at only the last digit of a number is equivalent to considering all numbers mod 10.

   It should also be noted that $L(a + b) = L(L(a) + L(b))$, for all natural numbers a, b (reason to yourself why this is true).

   a. Write a one-line Python function that takes in n and returns $L(n)$ *(this is just to check your understanding; don't use this function for the rest of the problems!).*

   b. Determine $L(23^{23})$.

   c. Determine $L(7^7 + 8^7 + 9^7)$.

   d. Show that when n is any odd positive integer, $L(1^n + 2^n + 3^n + ... + 9^n) = 5$. *(Hint: Look at the last sentence of the above paragraph.)*

8. *Products of Relative Primes*

   Consider the following statement:

$$\forall x, p, q \in \mathbb{N}, x \equiv 0 \pmod{pq} \implies x \equiv 0 \pmod{p} \wedge x \equiv 0 \pmod{q}$$

   a. Prove this statement.

   b. Is the converse of this statement true in general?

   c. For what p, q is the converse of this statement true? Prove your hypothesis using the results from Problem 5.

9. *Exponentiation – Mechanical*

   Determine each of the following values. You may need to use Fermat's Little Theorem, or other techniques discussed in lecture.

   a. $5^6 \pmod{7}$

   b. $14^{18} \pmod{15}$

   c. $12^{20} \pmod{20}$

   d. $17^{63} \pmod{22}$

   e. $9^{61} \pmod{11}$

10. *Extending Fermat's Little Theorem*

   Recall, Fermat's Little Theorem says $a^{p-1} \equiv 1 \bmod p$ for any prime p and $0 < a < p$.

   In this problem, we will use FLT to prove the following statement for any relatively prime natural numbers p, q:

$$a^{(p-1)(q-1)} \equiv 1 \bmod pq \quad (1)$$

   We will do so by instead proving the following statement:

$$a^{(p-1)(q-1)} - 1 \equiv 0 \bmod pq \quad (2)$$

   This result is very important in proving why the RSA encryption algorithm works.

   a. i. Show that $a^{(p-1)(q-1)} - 1 \equiv 0 \bmod p$.

      ii. Argue why $a^{(p-1)(q-1)} - 1 \equiv 0 \bmod q$. *(Hint: Think about symmetry.)*

   b. Use the result from the last part of Problem 5 to show that part (a) implies that equation (2) is true.

   c. Now, reason as to why equation (1) is true (this should only take a line).

   d. Use this result to evaluate $5^{37} \pmod{26}$.

11. *Finding Inverses – Euclidean Algorithm*

    Find each of the following quantities, or state that they do not exist.

    a. $5^{-1} \pmod{24}$

    b. $x : 5x \equiv 3 \pmod{24}$

    c. $(n-1)^{-1} \pmod{n}$, where $n \geq 2 \in \mathbb{N}$

    d. $5^{-1} \pmod{23}$

    e. $12^{-1} \pmod{42}$

    f. $24^{-1} \pmod{47}$

    g. $17^{-1} \pmod{63}$