Instructor: Leo Goldmakher

NAME: _____

Williams College
Department of Mathematics and Statistics

MATH 313 : NUMBER THEORY

Problem Set 4 – due Thursday, October 18th

INSTRUCTIONS:
This assignment should be turned in to me in person (i.e. don't leave them in my mailbox or ask someone else to submit on your behalf) at the beginning of Thursday's class. Late assignments may be left in my mailbox (just inside the entrance to Bascom) by **4pm** on Friday; however, 5% will be deducted for late submission. *Assignments submitted later than 4pm on Friday will not be graded.*

Please print and attach this page as the first page of your submitted problem set.

PROBLEM	**GRADE**
4.1	
4.2	
4.3	
4.4	
4.5	
Total	

Please read the following statement and sign **before starting this problem set:**

I understand that I am not allowed to use the internet to assist with this assignment. I also understand that I must write down the final version of my assignment in isolation from any other person, and to not copy from any set of written notes created when another person was present. I pledge to abide by the Williams honor code.

SIGNATURE:_____

Problem Set 4

4.1 In this problem, you'll explore the structure of $\mathbb{Z}_n^\times$.

(a) Prove that $\mathbb{Z}_n^\times$ is closed under multiplication (mod n), i.e., that given any $x, y \in \mathbb{Z}_n^\times$ we have $xy \pmod{n} \in \mathbb{Z}_n^\times$.

(b) Given $a, b \in \mathbb{Z}_n^\times$, prove that there exists some $x \in \mathbb{Z}_n^\times$ such that $bx \equiv a \pmod{n}$. [*Hint: Start by proving this for the special case $a = 1$. Then generalize!*]

(c) Prove that the choice of x in part (c) is unique. [Combining (b) and (c) proves that division is a well-defined operation in $\mathbb{Z}_n^\times$.]

4.2 For each of the following, compute $\varphi(n)$, as well as the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ for every $a \in \mathbb{Z}_n^\times$. [*To clarify: you should only give a single value of k that works for every single $a \in \mathbb{Z}_n^\times$.*]

(a) $n = 5$

(b) $n = 7$

(c) $n = 11$

4.3 The goal of this problem is to develop a primality test (a way of testing whether or not a given integer is prime without manually checking its divisibility).

(a) Prove that $(p-1)! \equiv -1 \pmod{p}$ for all primes p.

(b) Prove that if $(n-1)! \equiv -1 \pmod{n}$ for some integer $n \geq 3$, then n must be prime.

(c) Combining (a) and (b) gives an algorithm for determining whether a given n is prime: evaluate $(n-1)!$ in $\mathbb{Z}_n^\times$, and check whether it's congruent to $-1 \pmod{n}$. Is this a useful algorithm? Why or why not?

4.4 Prove that $\sum_{d|n} \varphi(d) = n$ for every $n \in \mathbb{N}$. [*Hint: consider the fractions $\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n}$. Reduce each fraction to lowest terms.*]

4.5 In this problem, you will explore some divisibility rules.

(a) Prove that $n \in \mathbb{N}$ is a multiple of 3 if and only if the sum of the digits of n is a multiple of 3. [*Hint: any three digit number can be written in the form $a_0 + 10a_1 + 100a_2$, where $a_i \in \{0, 1, \ldots, 9\}$.*]

In the next two parts you will explore a divisibility rule for 7. Given a k-digit natural number n, form a new number $f_7(n)$ as follows: split off the last (rightmost) digit of n, double it, and subtract it from the number formed by the first $k-1$ digits of n. The resulting number is what we call $f_7(n)$. I claim that $7 \mid n$ iff $7 \mid f_7(n)$. For example, is 3528 a multiple of 7? Split off the last digit (8), double it (16), and subtract it from the number formed by the other digits ($352 - 16 = 336$). So, $f_7(3528) = 336$, and the divisibility rule asserts that 3528 is a multiple of 7 iff 336 is. But now we can repeat the same procedure for 336: split off and double the last digit, and subtract from the other digits to find that ($f_7(336) = 33 - 12 = 21$). Since this is divisible by 7, so is 336; and hence, so is 3528.

(b) Use the above divisibility rule to determine (by hand!) whether or not 285786 is a multiple of 7.

(c) Prove that $7 \mid n$ iff $7 \mid f_7(n)$.

(d) Formulate and prove divisibility rules for 11 and 13.