Instructor: Leo Goldmakher

NAME: _____

Williams College
Department of Mathematics and Statistics

MATH 313 : NUMBER THEORY

Problem Set 5 – due Thursday, October 25th

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**
5.1	
5.2	
5.3	
5.4	
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 5

5.1 Find $\varphi(1600)$.

5.2 For each of the following, find $x \in \mathbb{Z}_{mn}^{\times}$ such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

(a) $m = 3$, $n = 5$, $a = 2$, $b = 4$.

(b) $m = 3371$, $n = 2459$, $a = 313$, $b = 350$.

5.3 It is a major open problem to find an algorithm that quickly computes $\varphi(n)$. (We shall see the importance of this problem when we discuss cryptography soon.) Note that if one knows the prime factorization of n, we can find $\varphi(n)$ with relative ease (e.g. see question **5.1**). But without knowing the prime factorization of n, it's not clear how to compute $\varphi(n)$ other than by brute force (i.e. counting the number of elements in $\mathbb{Z}_n^{\times}$). When n is huge, this is clearly going to take a long time.

The purpose of this exercise is consider a special case of this open problem: the case that n is the product of two distinct prime factors.

(a) Suppose I told you that $n = 1,008,050,083$ is the product of two distinct primes, and that

$$\varphi(n) = 1,007,979,048.$$

Determine the prime factorization of n.

(b) Suppose n is a product of two enormous distinct primes. Prove that there exists a quick way to compute $\varphi(n)$ if and only if there exists a quick way to compute the prime factorization of n.

5.4 Let $\mathcal{F}$ be the set of all multiplicative functions $f : \mathbb{Z}_{>0} \to \mathbb{C}$ satisfying $f(1) = 1$. (Here $\mathbb{Z}_{>0}$ denotes the positive integers.) For example, $\mathcal{F}$ contains the functions $I(n) := n$, $\mathbb{1}(n) := 1$, and the Euler totient function φ. Further, given any f and g in $\mathcal{F}$, define the function $f \star g$ by

$$(f \star g)(n) = \sum_{d|n} f(d) g\big(\frac{n}{d}\big)$$

where the sum runs over all divisors d of n. For example, problem **4.4** asserts $\varphi \star \mathbb{1} = I$.

(a) Find a function $e \in \mathcal{F}$ such that

$$e \star f = f$$

for every $f \in \mathcal{F}$. (The function e is called the *identity* of $\mathcal{F}$.)

(b) Suppose $\mu \in \mathcal{F}$ is a function satisfying $\mu \star \mathbb{1} = e$, where e is the identity function from part (c) and $\mathbb{1}$ denotes the constant function that outputs 1 for every input. Find $\mu(15)$ and $\mu(18)$.

(c) Prove that $\star$ is commutative, i.e. that for any $f, g \in \mathcal{F}$ we have $f \star g = g \star f$.

(d) Prove that $\star$ is associative, i.e. that for any $f, g, h \in \mathcal{F}$ we have $(f \star g) \star h = f \star (g \star h)$. [*Thus, the function $f \star g \star h$ has an unambiguous meaning.*]

(e) Deduce from all the above that $\varphi = I \star \mu$.

(f) Deduce that

$$\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

(g) Give a probabilistic interpretation of the formula in part (f).