Instructor: Leo Goldmakher

Name (Last, Nickname): ____________________

Section # (10am = 1, 11am = 2): ____________

Williams College
Department of Mathematics and Statistics

MATH 200 : DISCRETE MATH

Problem Set 10 – due Thursday, May 2nd

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

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

PROBLEM	**GRADE**
10.1	
10.2	
10.3	
10.4	
10.5	
10.6	
10.7	
Total	

Please read the following statement and sign **before writing the final version of this problem set:**

I understand that I am not allowed to use the internet to assist with this assignment, apart from accessing the course website or looking up definitions. 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 10

10.1 Use Fermat's Little Theorem to prove that 341 is composite. Do not use a calculator or computer to assist with any calculations. [*Hint: you may find it helpful to compute* 2^{10} *and* $7^3 \pmod{341}$.]

10.2 In class we noticed that every diagonal in the multiplication table $\pmod{p}$ is a palindrome. State this formally and then prove it.

10.3 Suppose $n \mid ab$, where a, b, n are positive integers and $\gcd(a, n) = 1$. Prove that $n \mid b$.

10.4 Given an integer a such that $31 \nmid a(a^{10} - 1)$, prove that $31 \mid a^{20} + a^{10} + 1$.

10.5 In class we used Fermat's Little Theorem to test whether or not a given integer is prime without manually looking for factors; this is an example of a *primality test.* The goal of this problem is to develop a different primality test.

(a) Prove that for any $a \in \{1, 2, \ldots, p-1\}$ there exists a unique $b \in \{1, 2, \ldots, p-1\}$ such that $ab \equiv 1 \pmod{p}$. (This b is called the inverse of $a \pmod{p}$.)

(b) Given a prime p, find all $x \in \{1, 2, \ldots, p-1\}$ such that $x^2 \equiv 1 \pmod{p}$, and prove that you've found all such x.

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

(d) Prove that if $(n-1)! \equiv -1 \pmod{n}$ for some integer $n \geq 3$, then n must be prime. [*Hint: suppose* n *is a composite number larger than 5. What can you say about* $(n-1)! \pmod{n}$*? Consider separately two cases:* n *is the square of a prime, or it isn't.*]

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

10.6 The purpose of this problem is to refine Fermat's Little Theorem. Given a prime p and an integer $a \not\equiv 0 \pmod{p}$, set

$$\operatorname{ord}_p(a) := \min\{k \in \mathbb{Z}_{>0} : a^k \equiv 1 \pmod{p}\}$$

(read 'order of $a \pmod{p}$'). For example, $\operatorname{ord}_7(1) = 1$, $\operatorname{ord}_7(-1) = 2$, and $\operatorname{ord}_7(2) = 3$.

(a) Work out (by hand, of course) the value of $\operatorname{ord}_{11}(a)$ for each $a \in \{1, 2, \ldots, 10\}$.

(b) Note that for any prime $p \geq 3$ and any $a \equiv -1 \pmod{p}$ we have $\operatorname{ord}_p(-1) = 2$. Does there exist a prime p and an $a \in \{2, 3, \ldots, p-2\}$ such that $\operatorname{ord}_p(a) = 2$? If so, give an example. If not, prove it.

(c) Work out (by hand, of course) the value of $\operatorname{ord}_p(10)$ for all primes p between 7 and 19 (including both 7 and 19).

(d) Work out (by hand, of course) the decimal expansion of $\frac{1}{p}$ for all primes p between 7 and 19 (including both 7 and 19). Describe all the connections to (c) you observe. (You don't have to prove anything.)

10.7 The purpose of this problem is to explore the Diffie-Hellman Key Exchange a bit more.

(a) What makes $p = 577$ and $g = 24$ a particularly terrible choice for Alice and Bob to make if they wanted to use DHKE?

(b) In practice for DHKE, Alice and Bob select g and p so that $\operatorname{ord}_p(g) = p - 1$; when this is the case, g is called a *primitive root* $\pmod{p}$. For example, both 2 and 3 are primitive roots (mod 5), but neither 1 nor 4 is. Work out (by hand, of course) the smallest positive primitive root $\pmod{p}$ for all primes between 7 and 23 (including both 7 and 23). [*Comment: a remarkable theorem due to Gauss, which we won't prove in this course, is that there exists a primitive root* $\pmod{p}$ *for every prime* p.]

(c) Given a prime p and two positive integers a and b, it takes your computer on the order of 10^{-6} seconds to compute $ab \pmod{p}$. Suppose n is a positive integer that's 100 digits long. Roughly how many years would it take to compute $2^n \pmod{p}$ if you multiply each $2 \pmod{p}$ one at a time? Roughly how many seconds would it take to compute $2^n \pmod{p}$ if you use the successive squaring technique we discussed in class? (You may assume that no additional computation is necessary to figure out how to express n in binary. Also, you may use a calculator for this problem.)

(d) Suppose Alice and Bob use DHKE to establish a key, with $g = 2$ and p a 100-digit prime such that 2 is a primitive root $\pmod{p}$. Eve intercepts Alice's transmission of $2^a \pmod{p}$. Assuming Eve is using a computer like the one described in (c), roughly how long would it take Eve to determine the value of a? You may use a calculator for this problem. [*A famous unproved assertion, called Artin's Conjecture, asserts that* 2 *is a primitive root* $\pmod{p}$ *roughly* 37% *of the time. In fact, it's not even known whether* 2 *is a primitive root for infinitely many primes!*]