Instructor: Leo Goldmakher

NAME: _____

Williams College
Department of Mathematics and Statistics

MATH 313 : NUMBER THEORY

Problem Set 6 – due Thursday, November 1st

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
6.1	
6.2	
6.3	
6.4	
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 6

6.1 In this problem we explore the uniqueness of solutions to power congruences.

(a) Use the method from class to find a solution to $x^{47} \equiv 3 \pmod{77}$.

(b) Prove that $x \notin \mathbb{Z}_{77}^{\times}$ implies $x^{47} \not\equiv 3 \pmod{77}$.

(c) Prove that your solution in part (a) is unique. [*Hint: Suppose x and y are both solutions. Prove that either $x \equiv y \pmod{77}$ or $x \notin \mathbb{Z}_{77}^{\times}$.*]

6.2 The goal of this problem is to explore binary notation.

(a) Write 29 as a sum of distinct powers of 2.

(b) Prove that any positive integer can be written as the sum of distinct powers of 2.
[*Hint: Induction! And split into even / odd cases.*]

(c) Prove that there's a *unique* way to write a given positive integer as the sum of distinct powers of 2.

6.3 Generating large primes.

(a) Assuming the Prime Number Theorem, roughly how many primes would you expect between 10^{100} and 2×10^{100}?

(b) One interpretation of the Prime Number Theorem is that the probability that a randomly selected integer n is prime is approximately $\frac{1}{\log n}$. Assuming this interpretation, how many 100-digit numbers do you expect to have to select before finding a prime? Justify your answer.

6.4 The goal of this exercise is to show that monic polynomials can't have too many roots (mod p). (*Monic* means the coefficient of the highest-degree term is 1.) More precisely:

Theorem 1. *Suppose f is a monic polynomial with integer coefficients, and consider the collection of all the roots of f (mod p):*

$$\mathcal{Z}_f := \{\alpha \in \mathbb{Z}_p : f(\alpha) = 0\}.$$

Then $|\mathcal{Z}_f| \leq \deg f$.

(a) Given f as in the theorem and any $\alpha \in \mathbb{Z}$, prove that $(x - \alpha) \mid \big(f(x) - f(\alpha)\big)$.

(b) Suppose $\alpha \in \mathcal{Z}_f$. Prove that $f(x) = (x-\alpha)g(x)$ for some monic polynomial g with integer coefficients, and that $\mathcal{Z}_f \subseteq \mathcal{Z}_g \cup \{\alpha\}$.

(c) Prove the theorem.

(d) Does the theorem hold if we replace p by an arbitrary integer n? Justify your answer.