Instructor: Leo Goldmakher

NAME: ______________________________

Williams College
Department of Mathematics and Statistics

MATH 313 : NUMBER THEORY

Problem Set 2 – due Thursday, September 27th

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
2.1	
2.2	
2.3	
2.4	
2.5	
2.6	
2.7	
2.8	
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 2

2.1 Is the fraction $\frac{110257}{110385}$ reduced? Justify your answer (without using calculators, computers, etc.).

2.2 'Real-world applications of number theory'

(a) Use the Euclidean algorithm to determine $\gcd(50, 37)$.

(b) Find $x, y \in \mathbb{Z}$ such that $37x + 50y = 1$.

(c) A farmer buys a bunch of cows and pigs (at least one of each). Cows cost \$50 each, and pigs cost \$37 each. If he spends \$3000 altogether, how many of each did he buy? You may use a calculator for basic arithmetic, but do not write any programs or draw any graphs. [*Hint: see problem **1.6**.*]

2.3 Use the Euclidean algorithm to determine $\gcd(2709, 5518)$.

2.4 Given positive integers a and b with $a > b$, set $r_0 = b$, and let r_1, r_2, ..., r_k be the set of all nonzero remainders outputted by the Euclidean algorithm. Recall that the Euclidean algorithm asserts that $r_k = \gcd(a, b)$.

(a) Prove that $r_{j+2} < \frac{1}{2} r_j$ for all $j \geq 0$.

(b) Conclude that the Euclidean algorithm terminates after at most $2 \log_2 b$ steps, where $\log_2$ denotes the logarithm base 2.

2.5 In class we discussed Euclid's proof that there are infinitely many primes. The purpose of this problem is to give a different proof, which was apparently discovered only a few years ago by F. Saidak.

(a) Let $n > 1$ be an integer. Show that n and $n + 1$ are coprime.

(b) Show that $n(n + 1) + 1$ is relatively prime to each of n and $n + 1$.

(c) Construct a number that is relatively prime to n, $n + 1$, and $n(n + 1) + 1$.

(d) Use the above to prove that there are infinitely many prime numbers.

2.6 In this problem, you will prove the infinitude of primes in yet another way. Consider the sets

$$A_n = \{1 + k(n!) : 1 \leq k \leq n\},$$

where the parameter k is assumed to be an integer.

(a) Show that any two distinct elements of A_n are relatively prime. [*Hint: two numbers are* not *relatively prime iff they have a common prime divisor.*]

(b) Use this to give another proof that there are infinitely many primes.

2.7 In class we gave four proofs that $\sqrt{2}$ is irrational. Recall that $S := \{n \geq 1 : n\sqrt{2} \in \mathbb{Z}\}$.

(a) Prove that if $b \in S$ then $b(\sqrt{2} - 1) \in S$. (Recall that this was at the heart of Proof 2 from class.)

(b) Adapt the method from Proof 4 to prove that for any integer $n \geq 1$ we either have $\sqrt{n} \in \mathbb{Z}$ or $\sqrt{n} \notin \mathbb{Q}$.

(c) Suppose $a, b \in \mathbb{Z}$, and let α be a solution to the equation $x^2 + ax + b = 0$. Adapt the method from Proof 3 to prove that α must be either an integer or irrational.

2.8 Suppose $n \geq 1$ is a positive integer. Prove that $\log x \leq x^{1/n}$ for all $x \geq n^{2n}$.