Instructor: Leo Goldmakher

NAME: _____

Williams College
Department of Mathematics and Statistics

MATH 313 : NUMBER THEORY

Problem Set 1 – due Thursday, September 20th

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**
1.1	
1.2	
1.3	
1.4	
1.5	
1.6	
1.7	
1.8	
1.9	
1.10	
1.11	
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 1

1.1 Why don't we consider 1 a prime? (Give a short but compelling argument.)

1.2 Prove that $n^2 - 1$ is prime for exactly one value of $n \in \mathbb{N}$.

1.3 Given an integer a and a positive integer d, we proved in class that there exist integers q and r such $a = qd + r$ and $0 \leq r < d$. Prove (*without using the Euclidean algorithm*) that $\gcd(a, d) = \gcd(d, r)$.

1.4 Prove the following claim, asserted by Miranda in Lecture 1:

Claim (Miranda)**.** *Given $a, b \in \mathbb{Z}$, let $d := \gcd(a, b)$ and set $a' := a/d$ and $b' := b/d$. Then $\gcd(a', b') = 1$.*

1.5 Suppose $a, b, c \in \mathbb{Z}$, and define a' and d as in **1.4** above. Prove that $a \mid bc$ if and only if $a' \mid c$.

1.6 Given $a, b, c \in \mathbb{Z}$, consider the equation

$$(*) \qquad ax + by = c.$$

The goal of this problem is to describe all integer solutions (x, y) to this equation. Suppose that x_0 and y_0 are integers satisfying $ax_0 + by_0 = c$, i.e. that (x_0, y_0) is an integer solution to (*).

(a) Prove that $x = x_0 + b'k, y = y_0 - a'k$ is an integral solution to (*) for every $k \in \mathbb{Z}$. [See problem **1.4** for the definitions of a' and b'.]

(b) Conversely, show that if x, y is an integral solution to (*), then there exists some integer k such that $x = x_0 + b'k$ and $y = y_0 - a'k$. [*Hint: you may find problem **1.5** helpful.*]

1.7 Prove that $\gcd(a, a + k) \mid k$ for all integers a and k.

1.8 Suppose $a \mid n$ and $b \mid n$.

(a) If $\gcd(a, b) = 1$, prove that $ab \mid n$.

(b) Does the same conclusion hold if $\gcd(a, b) \neq 1$? Either prove that it does or find a counterexample.

1.9 Prove that $d \mid n$ if and only if $\nu_p(d) \leq \nu_p(n)$ for every prime p. [*Hint: Look at the proof of Konnor's assertion from the end of Lecture 3.*]

1.10 In Lecture 3, Konnor observed (and then we proved) that $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

(a) Express $\nu_p\big(\gcd(a, b)\big)$ and $\nu_p\big(\mathrm{lcm}(a, b)\big)$ in terms of $\nu_p(a)$ and $\nu_p(b)$. [lcm *denotes the least common multiple.*]

(b) What can you say about $\gcd(a, b) \cdot \mathrm{lcm}(a, b)$? Prove your assertion.

1.11 The goal of this exercise is to prove the following result. (Recall that $\mathbb{Q}$ denotes the set of all fractions, i.e. all numbers of the form a/b with $a, b \in \mathbb{Z}$ and $b \neq 0$.)

Theorem 1. *For any positive integer n, either $\sqrt{n} \in \mathbb{Z}$ or $\sqrt{n} \notin \mathbb{Q}$.*

(a) Prove that $b \mid a$ if and only if $b^2 \mid a^2$.

(b) Use part (a) to prove that if $\sqrt{n} \in \mathbb{Q}$ then $\sqrt{n} \in \mathbb{Z}$. This proves the theorem!