Instructor: Leo Goldmakher

NAME: _____

University of Toronto Scarborough
Department of Computer and Mathematical Sciences

MATC15: NUMBER THEORY

Problem Set 1 (due Thursday, January 31st at the start of lecture)

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

PROBLEM	MARK
1.1	
1.2	
1.3	
1.4	
1.5	
1.6	
1.7	
1.8	
1.9	
1.10	
Total	

Please read the following statement and sign below:

I understand that I am not allowed to use the internet to assist (in any way) with this assignment. I also understand that I must write down the final version of my assignment in isolation from any other person.

SIGNATURE:_____

Problem Set 1

I recommend proceeding in order, as some problems are easier to solve using the results of prior problems.

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

1.2 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 $(a, d) = (d, r)$. [Note that this gives another proof that the Euclidean algorithm outputs the greatest common divisor of the two inputs.]

1.3 Use the Euclidean algorithm to determine (a, b), where:

(i) $a = 37, b = 50$

(ii) $a = 2709, b = 5518$

1.4 Find $x, y \in \mathbb{Z}$ such that $37x + 50y = 1$. [*Hint: use your work from 1.3(i).*]

1.5 Given $a, b \in \mathbb{Z}$, let $d := (a, b)$, and set $a' := a/d$ and $b' := b/d$. Prove that $(a', b') = 1$.

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

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

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

Suppose that $x = x_0, y = y_0$ is an integral solution to (*), i.e. that x_0 and y_0 are integers satisfying $ax_0 + by_0 = c$.

(i) 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 1.5 for the definitions of a' and b'.]

(ii) 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 1.6 helpful.*]

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

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

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

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

1.10 Given positive integers a and b with $a > b$, set $n_1 = b$, and let n_2, n_3, ..., n_{k-1} be the set of all nonzero remainders outputted by the Euclidean algorithm. Recall that the Euclidean algorithm asserts that $n_{k-1} = (a, b)$.

(i) Prove that $n_{j+2} < \frac{1}{2} n_j$ for all $j \geq 1$.

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