Instructor: Leo Goldmakher

NAME: _____

University of Toronto Scarborough
Department of Computer and Mathematical Sciences

MATC15: NUMBER THEORY

Midterm exam (due Tuesday, March 12th, during the first five minutes of the lecture)

INSTRUCTIONS: Please print and attach this page as the first page of your submitted midterm. You may freely refer to the textbook (Silverman) or to your lecture notes. You may NOT refer to any other books. You are also NOT allowed to use the internet in any way (even to look up definitions), nor to consult with any human (other than me) regarding the problems. If you are unsure whether something is allowed, please check with me first.

PROBLEM	MARK
M.1	
M.2	
M.3	
M.4	
M.5	
M.6	
Total	

Please read the following statement and sign below:

I understand that I am only not allowed to use the internet, books other than Silverman, or any human to assist (in any way) with this exam.

SIGNATURE:_____

Midterm

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

M.1 Let p_n denote the n-th prime, listed in increasing order (e.g. $p_1 = 2$, $p_2 = 3$, etc). Prove that there exist positive constants a and b such that

$$an \log n < p_n < bn \log n$$

for all natural numbers $n \geq 2$. [*Note: you do NOT have to explicitly determine the constants!*]

M.2 Recall that for any $x \in \mathbb{R}$, the floor of x (denote $[x]$) is the largest integer which does not exceed x. In symbols: $[x] := \max\{n \in \mathbb{Z} : n \leq x\}$. Prove that for every $x \in \mathbb{R}$,

$$[2x] - 2[x] = 0 \text{ or } 1.$$

M.3 Recall that $\mathrm{ord_p(n)}$ is the largest integer k such that $p^k \mid n$.

(a) Find $\mathrm{ord_2(13!)}$ and $\mathrm{ord_3(13!)}$.

(b) Prove that for any prime p and any $n \in \mathbb{N}$,

$$\mathrm{ord_p(n!)} = \sum_{\mathrm{k=1}}^{\mathrm{n}} \left[\frac{\mathrm{n}}{\mathrm{p^k}} \right].$$

(Here $[\cdot]$ denotes the floor function; see M.2 for definition.)

(c) Prove that for every prime p and every $n \in \mathbb{N}$, $\mathrm{ord_p}\binom{2n}{n} \leq \frac{\log n}{\log p} + 2$. (By exploring this further, it's possible to sharpen the constants in our proof of Chebyshev's theorem. You do not need to do so for this problem, however.)

M.4 Suppose $p \geq 5$ is prime. Prove that $24 \mid p^2 - 1$.

M.5 Determine all natural numbers n such that $n^4 + n^2 + 1$ is prime. You must prove that your list is complete!

M.6 Given positive integers A, B, and C, such that $(A, B) = 1$.

(a) Prove that there exist integers x, y such that $Ax + By = C$.

(b) Prove that if $C \geq A + B + AB$, then there exist *positive* integers x, y such that $Ax + By = C$.