Instructor: Leo Goldmakher

NAME: ______________________________

University of Toronto Mississauga
Department of Mathematical and Computational Sciences

MAT 302: CRYPTOGRAPHY

Problem Set 4 (due March 15th, 2011 at the start of lecture)

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

PROBLEM	MARK
4.1	
4.2	
4.3	
4.4	
4.5	
Total	

Problem Set 4

4.1 Find the inverse of $e \pmod m$ in each of the following.

(a) $e = 5$, $m = 69$

(b) $e = 5$, $m = 31$

(c) $e = 5$, $m = 44$

4.2 Find all values of $x \in \mathbb{Z}_{77}^{\times}$ satisfying $x^{13} = 3$.

4.3 Problem 7.11 in Paar-Pelzl.

4.4 In class I discussed the Prime Number Theorem, which asserts that

$$\#\{p \leq x\} \sim \int_2^x \frac{dt}{\log t}$$

where log is the natural logarithm.

(a) Prove that

$$\int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$$

[*Hint: Integrate by parts, or use L'Hôpital's rule: If* $f(x)$ *and* $g(x)$ *both tend to* ∞ *or both tend towards 0, then* $\lim_{x\to\infty} f(x)/g(x) = \lim_{x\to\infty} f'(x)/g'(x)$.]

(b) Assuming the validity of the Prime Number Theorem, prove that for *every* sufficiently large value of x, there is a prime between x and $2x$. This statement is known as Chebyshev's Theorem. [*Hint: It may be helpful to rewrite* $f(x) \sim g(x)$ *in the form* $f(x) = \Big(1 + o(1)\Big)g(x)$. *Of course, if you use this, you should be able to prove it!*]

(c) Again assuming the validity of the Prime Number Theorem, roughly how many primes would you expect between 1,000,000 and 2,000,000? How many primes would you expect between 10^{100} and 2×10^{100}?

(d) One way to loosely interpret the Prime Number Theorem is that the probability that a large randomly selected integer n is prime, is roughly $\frac{1}{\log n}$. If you wished to determine a 100-digit prime, how many numbers would you expect to test before finding a prime?

4.5 In this problem you will prove that $\sum_p \frac{1}{p}$, running over all primes p, diverges. You may *not* assume the Prime Number Theorem in this question. However, you *may* use the following helpful fact: if $-1 < x < 1$, then

(*)
$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

(a) Let $F(x) = \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1}$, where the product runs over all primes $p \leq x$. Prove that $F(x) \geq \sum_{n \leq x} \frac{1}{n}$, where n runs over all positive integers up to x. [*Hint: Use (*).*]

(b) Prove that $-\log(1-x) = x + O(x^2)$ whenever $x \leq \frac{1}{2}$.

(c) Prove that $\log F(x) = \sum_{p \leq x} \frac{1}{p} + O\left(\sum_{p \leq x} \frac{1}{p^2} \right)$, where $F(x)$ is defined in part (a). [*Hint: Use part (b)!*]

(d) Prove that $\sum_{p \leq x} \frac{1}{p^2} = O(1)$.

(e) Prove that $\sum_{p} \frac{1}{p}$ diverges.