Instructor: Leo Goldmakher

NAME: _____

University of Toronto Scarborough
Department of Computer and Mathematical Sciences

MATC15: NUMBER THEORY

Problem Set 4 – due Thursday, April 4th, during the first 5 minutes of lecture

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

PROBLEM	MARK
4.1	
4.2	
4.3	
4.4	
4.5	
4.6	
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 4

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

4.1 (a) Let g be a primitive root $\pmod p$. Prove that

$$(p-1)! \equiv g \cdot g^2 \cdot g^3 \cdots g^{p-1} \pmod p$$

(b) Use part (a) to prove that $(p-1)! \equiv -1 \pmod p$.

4.2 Given $k \in \mathbb{N}$. Prove that $k \mid \varphi(a^k - 1)$ for all integers $a \geq 2$. [*Hint: what is the order of a in $\mathbb{Z}^\times_{a^k-1}$?*]

4.3 (a) Prove that for every integer $k \geq 0$, $5^{2^k} \equiv 1 \pmod{2^{k+2}}$ and $5^{2^k} \not\equiv 1 \pmod{2^{k+3}}$. [*Hint: induction!*]

(b) Prove that for any $a \geq 2$, the order of 5 in $\mathbb{Z}^\times_{2^a}$ is 2^{a-2}.

(c) Prove that for every $n \in \mathbb{Z}^\times_{2^a}$, there exists an integer $k \geq 0$ such that $n = \pm 5^k$ in $\mathbb{Z}^\times_{2^a}$.

4.4 For any $k \in \mathbb{N}$ and p prime, prove that

$$\sum_{n=1}^{p-1} n^k \equiv \begin{cases} -1 \pmod p & \text{if } (p-1) \mid k \\ 0 \pmod p & \text{if } (p-1) \nmid k. \end{cases}$$

[*Hint: use primitive roots. Also, the following identity might be helpful:*

$$(x + x^2 + x^3 + \cdots + x^{m-1})(1 - x) = x - x^m.]$$

4.5 Suppose p is prime. Prove that the sequence n^n is periodic in $\mathbb{Z}_p$. What is its (smallest) period? [*Hint: by experimenting, make a conjecture about the period, then try to prove it.*]

4.6 Consider the decimal expansion of $1/p$, where $p \geq 7$ is prime. For example,

$$1/7 = 0.\overline{142857}$$

Here, the overline indicates that the pattern of digits underneath repeats indefinitely:

$$0.\overline{142857} = 0.142857142857142857\ldots$$

(a) Suppose $p \geq 7$ is prime. Prove that the decimal expansion of $1/p$ is periodic (and hence, that the decimal doesn't terminate). What is the period? [*I strongly urge you to build up intuition by calculating (by hand!) the decimal expansion of $1/p$ for a few primes. Using a calculator won't help you in this exercise, since you're trying to understand the output (as opposed to simply obtaining it).*]

(b) Suppose that the period is even, say, $1/p = 0.\overline{a_1 a_2 \cdots a_{2k}}$. Prove that $a_i + a_{k+i} = 9$ for all i. [*Hint: prove that $10^k \equiv -1 \pmod p$.*]