Instructor: Leo Goldmakher

NAME: ____________________________

University of Toronto Scarborough
Department of Computer and Mathematical Sciences

MATC15: NUMBER THEORY

Problem Set 3 – due Wednesday, March 27th, in the C15 drop box by 12pm sharp

(The drop box is on the 4th floor of the IC building, near the main offices of the CMS department.)

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

PROBLEM	MARK
3.1	
3.2	
3.3	
3.4	
3.5	
3.6	
3.7	
3.8	
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 3

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

3.1 In this problem, you'll explore an algorithm for finding inverses of elements in $\mathbb{Z}_n^\times$.

(a) Use the Euclidean algorithm to determine integers x and y such that $5x + 17y = 1$.

(b) Use the above to find 5^{-1} in $\mathbb{Z}_{17}$.

3.2 In class we sketched a proof that $\varphi(p^k) = p^{k-1}(p-1)$ for any prime p and any $k \in \mathbb{N}$. Give an alternative proof of this by using induction on k. (You may assume the relation $\varphi(p) = p - 1$.)

3.3 Showing all relevant work / proofs, compute the following (no calculators allowed!):

(a) 7^{-1} in $\mathbb{Z}_{53}^\times$

(b) 7^{-1} in $\mathbb{Z}_{54}^\times$

(c) 2^{-1} in $\mathbb{Z}_p^\times$, where p is an odd prime.

(d) $\varphi(1600)$

(e) $3 \div 7$ in $\mathbb{Z}_{53}^\times$

(f) $5 \div 4$ in $\mathbb{Z}_{54}$

(g) The order of 5 in $\mathbb{Z}_{16}^\times$

(h) The order of 10 in $\mathbb{Z}_{13}^\times$

3.4 In this problem, you'll prove a primality test (a way of testing whether or not a given integer is prime).

(a) Show that for any prime $p \geq 3$, the equation $x^2 = 1$ has *exactly* two solutions in $\mathbb{Z}_p^\times$.

(b) Prove that $(p-1)! \equiv -1 \pmod{p}$ for all primes p. [*Hint: what does part (a) say about inverses in* $\mathbb{Z}_p^\times$*?*]

(c) Prove that if $(n-1)! \equiv -1 \pmod{n}$ for some integer $n \geq 3$, then n must be prime.

(d) Combining (c) and (d) gives an algorithm for determining whether a given n is prime: evaluate $(n-1)!$ in $\mathbb{Z}_n^\times$, and check whether it's congruent to $-1 \pmod{n}$. Is this a good algorithm? Why or why not?

3.5 For any prime $p \geq 29$, prove that $182 \mid p^{12} - 1$. [*Hint:* $182 = 2 \times 7 \times 13$.]

3.6 In this problem, you will explore some divisibility rules.

(a) Prove that $n \in \mathbb{N}$ is a multiple of 3 if and only if the sum of the digits of n is a multiple of 3. [*Hint: any three digit number can be written in the form* $a_0 + 10a_1 + 100a_2$*, where* $a_i \in \{0, 1, \dots, 9\}$.]

In the next two parts you will explore a divisibility rule for 7. Given a k-digit natural number n, form a new number $f_7(n)$ as follows: split off the last (rightmost) digit of n, double it, and subtract it from the number formed by the first $k-1$ digits of n. The resulting number is what we call $f_7(n)$. I claim that $7 \mid n$ iff $7 \mid f_7(n)$. For example, is 3528 a multiple of 7? Split off the last digit (8), double it (16), and subtract it from the number formed by the other digits ($352 - 16 = 336$). So, $f_7(3528) = 336$, and the divisibility rule asserts that 3528 is a multiple of 7 iff 336 is. But now we can repeat the same procedure for 336: split off and double the last digit, and subtract from the other digits to find that ($f_7(336) = 33 - 12 = 21$). Since this is divisible by 7, so is 336; and hence, so is 3528.

(b) Use the above divisibility rule to determine (by hand!) whether or not 285786 is a multiple of 7.

(c) Prove that $7 \mid n$ iff $7 \mid f_7(n)$.

(d) Formulate and prove divisibility rules for 11 and 13.

3.7 Prove that $\sum_{d \mid n} \varphi(d) = n$ for every $n \in \mathbb{N}$. [*Hint: consider the fractions* $\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n}$. *Reduce each fraction to lowest terms.*]

3.8 Suppose $(a, N) = 1$. Prove that the integer $a \pmod{N}$ – i.e. the unique element of $\mathbb{Z}_N$ congruent to a – is also relatively prime to N, i.e. $a \pmod{N} \in \mathbb{Z}_N^\times$.