Instructor: Leo Goldmakher

NAME: _____

Williams College
Department of Mathematics and Statistics

MATH 313 : NUMBER THEORY

Problem Set 3 – due Thursday, October 11th

INSTRUCTIONS:
This assignment should be turned in to me in person (i.e. don't leave them in my mailbox or ask someone else to submit on your behalf) at the beginning of Thursday's class. Late assignments may be left in my mailbox (just inside the entrance to Bascom) by **4pm** on Friday; however, 5% will be deducted for late submission. *Assignments submitted later than 4pm on Friday will not be graded.*

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

PROBLEM	**GRADE**
3.1	
3.2	
3.3	
3.4	
3.5	
Total	

Please read the following statement and sign **before starting this problem set:**

I understand that I am not allowed to use the internet to assist with this assignment. I also understand that I must write down the final version of my assignment in isolation from any other person, and to not copy from any set of written notes created when another person was present. I pledge to abide by the Williams honor code.

SIGNATURE:_____

Problem Set 3

3.1 Use the Doomsday algorithm to calculate the day of the week of the following dates. You don't have to show much work, but do write down all five relevant numbers that come up in the algorithm (the doomsday number, the century day, the year over 12, the remainder, the remainder over 4).

(a) June 6, 1944 (D-day)

(b) November 19, 1863 (Gettysburg address)

(c) January 21, 1793 (Execution of Louis XVI)

3.2 Write down the multiplication table (excluding the 0 row and columns) for arithmetic (mod 12).

3.3 In this problem, you'll explore one way to do division in modular arithmetic.

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

(b) Use part (a) to find $1/5 \pmod{17}$.

(c) Use part (b) to find $3/5 \pmod{17}$.

(d) Determine $3 \div 7 \pmod{53}$.

3.4 Show that for any prime $p \geq 3$, the equation $x^2 \equiv 1 \pmod{p}$ has *exactly* two solutions $\pmod{p}$.

3.5 Suppose a is relatively prime to N, where $N \geq 2$. Prove that the integer $a \pmod{N}$ – i.e. the unique number in $\{0, 1, 2, \ldots, N-1\}$ that's congruent to a – is also relatively prime to N.