4400-001 - SPRING 2022 - WEEK 3 (1/25, 1/27)
MODULAR ARITHMETIC (CHAPTER 2, §2,3, AND 5)

Most of these exercises can be found in Savin - Chapter 2, but have been reorganized below.

Exercise 1. Mod n times tables

(1) Write down the times table for $\mathbb{Z}/n\mathbb{Z}$ for each positive integer $n \leq 13$.
(2) An integer a has a multiplicative inverse modulo n if there is an integer b such that $ab = 1 \bmod n$. Can you guess a simple condition on a and n that describes when a has a multiplicative inverse modulo n? Can you justify it?

Exercise 2. Euler's ϕ function. For $n \in \mathbb{N}$, $\phi(n)$ is defined to be the number of natural numbers less than or equal to n that are coprime to n (two integers a and b are said to be coprime if they share no common divisor except 1, i.e. if $\gcd(a, b) = 1$).

(1) Compute $\phi(n)$ for $n \leq 13$.
(2) For p a prime and k a positive integer, find a simple formula for $\phi(p^k)$.
(3) Can you guess a formula for $\phi(n)$ in general? Can you justify it?
(4) Compute $\sum_{d|1000} \phi(d)$. Give a simple explanation for your answer.

Exercise 3. ISBN numbers.

(1) The number 3-520-97285-9 is obtained from a valid ISBN-10 number by switching two consecutive digits. Find the ISBN-10 number
(2) The number 0-31-030369-0 is obtained from a valid ISBN-10 number by switching two consecutive digits. Find the ISBN-10 number.
(3) ISBN-13 is an update to the ISBN system that came into usage in 2007. An ISBN-13 code consists of 13 digits, $x_1, \ldots, x_{13}$ (unlike ISBN-10, where the last digit can be "X", all digits in ISBN-13 are between 0 and 9). The first 12 digits encode useful infomration, and the 13th digit is chosen so that

$$x_1 + 3x_2 + x_3 + 3x_4 + \ldots + 3x_{12} + x_{13} \equiv 0 \mod 10.$$

Can ISBN-13 detect when two neighboring digits are transposed?

Exercise 4 (Required). Divisibility conditions. Recall from the Tuesday video that a positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3. In this exercise you will establish analogs for divisibility by 9 and 11. In the following, we let

$$n = a_m a_{m-1} \ldots a_0 = \sum_{i=0}^{m} a_i 10^i.$$

(1) Show $9|n$ if and only if $9|\sum_{i=0}^{m} a_i$.
(2) Show $11|n$ if and only if $11|\sum_{i=0}^{m}(-1)^i a_i$.
(3) Is 2121212121212121212121 divisible by 9? By 11?
(4) (Not required) Can you give a similar condition for divisibility by 37?

Exercise 5 (Required). Solving some equations in modular arithmetic.

(1) Use the Euclidean algorithm to compute the multiplicative inverse of 131 modulo 1979.
(2) Solve $131x \equiv 11 \mod 1979$.
(3) Use the Euclidean algorithm to compute the multiplicative inverse of 127 modulo 1091.
(4) Solve $127x \equiv 11 \mod 1091$.
(5) Solve the following system of congruences

$$x \equiv 4 \mod 55$$
$$x \equiv 11 \mod 69$$

(6) Solve the following system of congruences

$$x \equiv 5 \mod 11$$
$$x \equiv 7 \mod 13$$

(7) Solve the following system of congruences

$$x \equiv 11 \mod 16$$
$$x \equiv 16 \mod 27$$