Math 322 Fall 2019
Number Theory HW 4
Due Friday, September 27

You may *not* discuss the starred problem with classmates, though you should of course feel free to discuss it with me as much as you like. Linguistic precision is important for this problem.

($\star$) **Starred Problem:** Show that multiplicative inverses $\mod m$ are unique up to congruence. That is, if a, b, c are integers, and m is a positive integer, and $ab \equiv 1 \mod m$ and $ac \equiv 1 \mod m$, then $b \equiv c \mod m$.

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. Prove that an integer is divisible by eleven if and only if the sum of its even-placed base 10 digits minus the sum of its odd-placed digits is divisible by eleven. That is, if $n = n_0 + n_1 \cdot 10 + n_2 \cdot 10^2 + \cdots + n_k 10^k$, then $11|n$ if and only if

$$11| \sum_{i \text{ even}} n_i - \sum_{i \text{ odd}} n_i = n_0 - n_1 + n_2 - n_3 + \dots$$

2. Fix an integer $m > 0$, and suppose that m has the following property: if a is an integer and $m \not| a$, then a has a multiplicative inverse $\mod m$. That is, suppose m is an integer such that every integer is either divisible by m, or has a multiplicative inverse $\mod m$. Then prove that m is prime.

3. Find a solution to each system of congruences:

   (a)

$$5x \equiv 3 \mod 23$$

   (b)

$$\begin{aligned} x &\equiv 0 \mod 2 \\ x &\equiv 1 \mod 5 \end{aligned} \qquad \begin{aligned} x &\equiv 0 \mod 3 \\ x &\equiv 6 \mod 7 \end{aligned}$$

(c)

$$\begin{aligned} x &\equiv 2 \mod 11 & \qquad x &\equiv 3 \mod 12 \\ x &\equiv 4 \mod 13 & \qquad x &\equiv 5 \mod 17 \\ x &\equiv 6 \mod 19 \end{aligned}$$

4. Find (all) the solutions of

$$\begin{aligned} 2x + 3y &\equiv 5 \mod 7 \\ x + 5y &\equiv 6 \mod 7. \end{aligned}$$

5. Find (all) the solutions of

$$\begin{aligned} 4x + y &\equiv 5 \mod 7 \\ x + 2y &\equiv 4 \mod 7. \end{aligned}$$

6. Find (all) the solutions of

$$\begin{aligned} x + y &\equiv 2 \mod 7 \\ 3x + 2y &\equiv 3 \mod 7. \end{aligned}$$