Math 261 — Fall 2022
Number Theory
`https://sites.aub.edu.lb/kmakdisi/`
Problem set 3, due Friday, September 23 at the beginning of class

Exercise 3.1: Find all solutions to the following systems of linear equations for $(\overline{x}, \overline{y}) \in (\mathbf{Z}/25\mathbf{Z})^2$. Hint: try to eliminate variables, but make sure that you always maintain an **equivalent** system of equations.

$$\begin{cases} 2x - y \equiv 1 & \pmod{25} \\ x + 4y \equiv 8 & \pmod{25} \end{cases}, \begin{cases} 2x - y \equiv 0 & \pmod{25} \\ x + 2y \equiv 0 & \pmod{25} \end{cases}, \begin{cases} 2x - y \equiv 1 & \pmod{25} \\ x + 2y \equiv 8 & \pmod{25} \end{cases}.$$

Also give a specific choice for a, b for which the system $\begin{cases} 2x - y \equiv a & \pmod{25} \\ x + 2y \equiv b & \pmod{25} \end{cases}$ has NO solution. (Prove that your choice of a, b works.)

Exercise 3.2: a) Find the remainder of 2^{110236} divided by 11.

b) Find the remainder of 10^{110236} divided by 13.

Hints: show first that $2^{10} \equiv 1 \pmod{11}$, and $10^6 \equiv 1 \pmod{13}$.

Exercise 3.3: a) Show that if p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ has no zero divisors. (In other words, $\overline{a}\overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.)

b) Show that if p is a prime other than 2, then the equation $x^2 \equiv 4 \pmod{p}$ has exactly two solutions. However, give an example where $x^2 \equiv 3 \pmod{p}$ has no solutions.

c) Find all solutions to $x^2 \equiv 4 \pmod{15}$. (You may need to use trial and error.)

d) Find all solutions to $x^2 + 10x + 6 \equiv 0 \pmod{15}$. Hint: complete the square and use c).

Exercise 3.4: Assume that $\overline{a} \in (\mathbf{Z}/m\mathbf{Z})^*$ has multiplicative order k. Let $\ell \in \mathbf{Z}$, and take $\overline{b} = \overline{a}^\ell$. Suppose that $\gcd(k, \ell) = 1$.

a) Show that $\overline{b}$ also has order k.

b) Show that $\overline{a}$ can be writen as a power of $\overline{b}$ (i.e., $\overline{a} = \overline{b}^n$ for some n).

Exercise 3.5: a) Suppose given numbers a and m, such that

$$a^{360} \equiv 1 \pmod{m}, \quad a^{180} \not\equiv 1 \pmod{m}, \quad a^{120} \not\equiv 1 \pmod{m}, \quad a^{72} \not\equiv 1 \pmod{m}.$$

Show that the order of a mod m is exactly 360. (Hint: $360 = 2^3 3^2 5$, $180 = 360/2$, $120 = 360/3$, and $72 = 360/5$.)

b) Formulate and prove a general theorem giving a criterion for a to have order k mod m, under conditions similar to those in part a).

Exercise 3.6: If p is a prime other than 2 or 5, show that p divides infinitely many numbers of the form

$$11, 111, 1111, 11111, 111111, 1111111, \ldots$$

Suggestion: this is easy if $p = 3$. Otherwise, consider the multiplicative order of 10 $(\mathrm{mod}\, p)$.