JUNE 14TH MATH PROBLEM SET

A mathematician is a blind man in a dark room looking for a black cat which isn't there. – Charles Darwin

Today we are going to formalize some of the things we touched on last week.

1. Consider the number $p = 11$. For each number $a = 1, 2, 3, \ldots, 10$ write down all of its powers.

Let me do a couple for you. If $a = 1$, then $a^2 = 1, a^3 = 1$, and higher powers also equal 1. So the sequence is $\{1, 1, 1, 1, \ldots\}$. That was easy :-). Ok, let me do another one for you. Take $a = 3$, then $a^2 = 9$, $a^3 = 27 \bmod 11 = 6$, $a^4 = 81 \bmod 11 = 4$, $a^5 = 243 \bmod 11 = 1$, $a^6 = 3$, $a^7 = 9$ (and the mattern repeats). The sequence is $\{3, 9, 6, 4, 1, 3, 9, 6, 4, 1, 3, 9, 6, 4, 1, \ldots\}$. You do the rest

Hint: You have a team, break up the workload!

2. Do the same thing for $p = 13$.

What observations can you make about the patterns you found.

You should have noticed that for some choices of a, every number between 1 and 10 is a power of a when $p = 11$. Likewise when $p = 13$. **Definition**. Fix an integer n to use as a modulus. We say that x is *a generator*[1] *modulo* n if every integer y with $\gcd(y, n) = 1$ is a power of x. When n is prime, this just means that every number $1, \ldots, n-1$ is a power of x.

The security of one of the main modern cryptographic protocols is based on the following problem. Solving the equation

$$x^{?} \equiv_p b$$

for ? is HARD. It takes a long time because all you can do is guess and check. We will explore using the computer to see how hard it is later. To use these cryptographic protocols however, first you need a generator x for working modulo a prime p.

3. Suppose x is a generator mod p where p is prime. Show that $x^{p-1} \equiv_p 1$. Does this work with the examples you computed on the previous page?

Hint: Make two observations. First, if $x^i \equiv_p 1$ then the powers of x start repeating after the ith power. Second, recall that if $x^j = x^k$ with $j > k$, then $x^{j-k} \equiv_p 1$. Use this to conclude that if x is a generator, it must hit every number in the range $1, \ldots, p-1$ until it hits 1.

[1]Sometimes also called a *primitive root*.

Here is an algorithm for checking if x is a generator modulo p (for p a prime). For each factor i of $p-1$ (with $i \neq p-1$) compute

$$x^i (\text{mod } p).$$

- If ever you got 1, then x is *not* a generator.
- If you never got 1 then x *is* a generator.

For example, if $p = 11$, then $p - 1 = 10$, and the factors of 10 are $i = 2, 5$. To show that $x = 2$ is a generator modulo $p = 11$, you just have to check that

$$\begin{aligned} 2^2 (\text{mod } 11) &\neq 1 \\ 2^5 (\text{mod } 11) &\neq 1. \end{aligned}$$

This is a lot easier than checking all the powers. We will learn why this works later.

4. For each prime p in the table below, find a generator x.

p	x
7	
17	
19	
23	
29	
37	

5. Solve the equations for e (this type of equation is called a discrete logarithm).

(a) $3^e \equiv_{17} 5$

(b) $3^e \equiv_{17} 14$.