JUNE 7TH MODULAR ARITHMETIC PROBLEM SET

In mathematics, you dont understand things. You just get used to them. – Johann von Neumann

1. How many solutions are there to the congruence $6x + 1 \equiv 4 \bmod 15$?

2. Work in your group to fill out the following multiplication tables for taking things modulo 5, 8, 10, and 11. Contrast the ones for 5 and 11 with those for 8 and 10. Explain why nonzero numbers multiply together to give zero in the tables for 8 and 9 but not in those for 5 and 11.

	0	1	2	3	4
0					
1					
2					
3					
4					

	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

	0	1	2	3	4	5	6	7	8	9
0										
1										
2										
3										
4										
5										
6										
7										
8										
9										

	0	1	2	3	4	5	6	7	8	9	10
0											
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

3. Based on the tables you made on the previous page, how many inverses can a number have? In other words, how many ways are there to solve $1 \equiv_n ax$ for x?

4. Have each person in your group choose a different two digit prime number p. This will be your modulus. All your operations will be performed with this modulus. For every integer x between 1 and $p-1$, some power of x, at least modulo p, will be equivalent to 1. Find the smallest such power and fill in the table below.

Example For instance, if $p = 31$ and $x = 5$ then then $x^3 = 125 \equiv_{31} 1$ (since 125/31 has remainder 1), so the power is 3.

x	smallest power
2	
3	
4	
5	
6	

x	smallest power
7	
8	
9	
10	
11	

5. How do the powers you constructed compare with the number $p-1$? Compare across what everyone in you group did and make a prediction.