GROUP WORK B, TUESDAY MORNING

SPY GAMES CAMP – PSU, 2013

In mathematics, you don't understand things. You just get used to them. – Johann von Neumann

Choose a two digit prime number p that is at least 26. This will be your modulus. All your operations will be performed with this modulus.

1. For every other integer between 1 and p, some power of x will be equivalent to 1 modulo p. Find the smallest such power and fill in the table below.

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. You can use the ScienceCamp program, File→Modular Arithmetic to make this process much faster.

x	smallest power
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	

x	smallest power
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	

2. Look at the powers that showed up, and especially as to how they factor (and how do they compare with $p-1$). What predictions can you make? Write them here.

3. Check your predictions with another p filling in the following table.

x	smallest power	x	smallest power
2		11	
3		12	
4		13	
5		14	
6		15	
7		16	
8		17	
9		18	
10		19	

4. It is a fact that there is always some x whose smallest power is equal to exactly $p-1$. This x is called a *generator*.

Work on cracking the substitution code from yesterday if you haven't already done it.