GROUP WORK, MONDAY AFTERNOON

SPY GAMES CAMP – PSU, 2014

The Theory of Numbers has always been regarded as one of the most obviously useless branches of Pure Mathematics.–G. H. Hardy

We'll learn more about modular arithmetic. Given two integers[1] a and b, and another integer $n > 0$, we write $a \equiv_n b$ if a and b have the same remainder after dividing by n. In this case we say that a equals b modulo n. For example, $5 \equiv_{10} 15$ and $4 \equiv_3 31$.

1. Play the following game within your team. Given the numbers and operations, try to write them in a way that equals 5 modulo n. Roll 2 dice, three times. Whoever gets closest wins. Play this a few times as a group, then we'll play it with each group as a team.

Numbers	Operations	n = Modulus	Your expression
	+, +, -	10	
	+, *	7	
	*, *	11	
	-, *	12	
	+, *, -	19	

[1]Whole positive or negative numbers

The nice thing about working modulo n is that there are only n different numbers $0, 1, 2, 3, \ldots, n-1$. Also, any time you are doing a computation modulo n, you can take remainders to make your life easier.

For instance if you want to compute $7 \cdot 14 \cdot 16 \cdot 19 \pmod 5$, one can first find the remainder of 7, 14, 16, and 19 mod 5 (which is 2, 4, 1 and 4) and then multiply those numbers together before taking remainders. One should get remainder 2 regardless of how you do it.

2. Within each team, have a race to compute $4 \cdot 5 \cdot 7 \cdot 13 \cdot 301 \cdot 1007 \pmod 3$. Use the principal above to make this computation easier. See who is fastest. Discuss strategies, being able to do this in your head quickly will be important.

3. We say that a is *invertible* modulo n if there is an integer b such that $ab \equiv_n 1$ (one only needs to check $b = 0, 1, \ldots, n-1$. How many different b work?). Have each person in your team choose a different value of n and try to find which $a = 0, 1, \ldots, n-1$ are invertible and which are not. Then come together and try to find a pattern. Given $n = 101$, which $a = 0, 1, \ldots, 100$ are invertible? What if $n = 50$?