JUNE 6TH MODULAR ARITHMETIC PROBLEM SET #1

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

Well 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 $4 \equiv_3 31$. We also sometimes write things like $5 (\text{mod } 3) = 2$ (here (mod $\bullet$) means take the remainder).

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.

For example, I might roll $6, 10, 9$ and have the operations $+, *$ working modulo 11. I could try using one $*$ and one $+$.

$$6 * 10 + 9 = 69 \equiv_{11} 3$$

which is pretty close to 5, but it would be better to do

$$10 + 6 * 3 = 28 \equiv_{11} 6.$$

If you have extra operations, you don't have to use them all. But you must use all the numbers.

Whoever gets closest wins. Play this a few times as a group, then well 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 you have to worry about 0,1,2,3,...,n-1. Also, any time you are doing a computation modulo n, you can take remainders periodically to make your life easier.

For instance if you want to compute $7 \cdot 14 \cdot 16 \cdot 19 (\text{mod } 5)$, one can first find the remainder of $7, 14, 16$, and 19 modulo 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 $4 \cdot 5 \cdot 7 \cdot 13 \cdot 301 \cdot 1007 (\text{mod } 3)$. 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 throughout the camp.

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 $b = 0, 1, ..., n1$). Have each person in your team choose a different value of n (say $n = 5, 6, 7, 8, 9, 10, 11, \ldots$) and try to answer the following questions

- Find which $a = 0, 1, ..., n-1$ are invertible and which are not.
- How many inverses does each a have?

Then come together and try to find a pattern and explain it here.

4. Given $n = 101$, which $a = 0, 1, ..., 100$ are invertible based on your pattern? What if n = 50?