Name ________________________________

Modular Arithmetic

Multiplication

Modular numbers can be multiplied. Determine the product of the two numbers then reduce the result by multiples of the modulus until you get number between 0 and the (modulus -1) NOTE: the modulus is always replaced by zero. 5 ≡ 0 (mod 5)

Examples:

Mod 5

2 * 3 = 6 ≡ 1 (mod 5)

5 * 4 = 20 ≡ 0 (mod 5) 20÷ 5 can be evenly divided. Starting at 0, count 20 spaces in a clockwise direction and you arrive at 0 again.

4 * 3 = 12 ≡ 2 (mod 5) 12 ÷ 5 can not be divided evenly, 5 goes into 12 two times with 2 left over. Start at 0, move 12 spaces, pass 0 twice and end up at 2.

0 & 1 behave as usual under standard multiplication.

Mod 5 Multiplication	0	1	2	3	4
0					
1					
2					
3					
4					

Mod 11

4 * 4 = 16 ≡ 5 (mod 11) 16 can be divided by 11 only once, with 5 left over. Start at 0, count 16 spaces.

9 * 5 = 45 ≡ 1 (mod 11) Since 11 * 4 = 44; one past 0 is 1

16 * 17 = 272 ≡ 8 (mod 11) Since 11 * 24 = 264

Multiplicative Inverse

When two numbers multiply together to equal 1, the numbers are multiplicative inverses of each other.

An example in standard arithmetic:

$$4 \times \frac{1}{4} = 1$$

4 is the multiplicative inverse of 1/4 and 1/4 is the multiplicative inverse of 4

Multiplicative Inverses are sometimes written as A^{-1}.

The multiplicative inverse of 4 can be written as 4^{-1} or as $\frac{1}{4}$.

Mod 7

Changing the Modulus, changes the inverses.

BEWARE: *Unless the modulus is prime, not all nonzero values will have a multiplicative inverse!*

The multiplicative inverse occurs when the answer is 1 (mod 7).

Think about when that occurs:

After one time around 8 ≡ 1 (mod 7)
After two times around 15 ≡ 1 (mod 7);

List 3 more times when this occurs: ____________, ___________, ___________,

Find two numbers that produce the answer of 1 (mod 7):

Example: 2 * 4 = 8 8 ≡ 1 (mod 7)

Therefore 2 is the multiplicative inverse of 4 in modulus 7

and

4 is the multiplicative inverse of 2 in modulus 7

Also, since 3 * 5 = 15, 3 is the multiplicative inverse of 5 and vice versa in modulus 7.

Find other multiplicative inverses in mod 7 to correspond to the numbers listed in the table below.

Number	Multiplicative Inverse	Explanation
0	No inverse	Nothing can be multiplied by 0 to get 1
1	1	1 * 1 = 1
2	4	2 * 4 = 8 ≡ 1 (mod 7)
3		
4		
5		
6		

Describe how you would find the multiplicative inverse of a number in a different modulus:

<u>Mod 29</u>

Find all the multiplicative inverses for Mod 29 and fill in the table below:

Number	Inverse	Number	Inverse	Number	Inverse
1		11		21	
2		12		22	
3		13		23	
4		14		24	
5		15		25	
6		16		26	
7		17		27	
8		18		28	
9		19			
10		20			

Mod 9

Find all the multiplicative inverses for Mod 9 and fill in the table below (note that you won't be able to find an inverse for every number):

Number	Inverse	Number	Inverse
1		5	
2		6	
3		7	
4		8	

Mod 10

Find all the multiplicative inverses for Mod 10 and fill in the table below (note that you won't be able to find an inverse for every number):

Number	Inverse	Number	Inverse
1		5	
2		6	
3		7	
4		8	
		9	

What's your theory on determining which numbers will have multiplicative inverses?