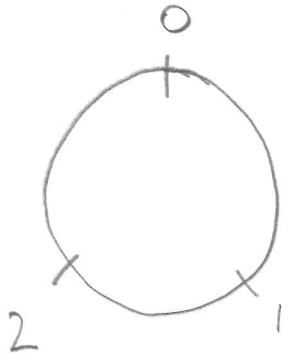
Multiplication & Powers

Multiplication in $\mathbb{Z}/3\mathbb{Z}$



	0	1	2
0	0	0	0
1		1	2
2			

Note: We call "0, 1, 2" the least non-negative residues because they are the smallest non-negative number in each congruence class, e.g.

$\cdots \equiv 22 \equiv 19 \equiv 16 \equiv 13 \equiv 10 \equiv 7 \equiv 4 \equiv 1 \equiv -2 \equiv \cdots \pmod 3$

$\cdots \equiv 21 \equiv 18 \equiv 15 \equiv 12 \equiv 9 \equiv 6 \equiv 3 \equiv 0 \equiv -3 \equiv \cdots \pmod 3$

$\cdots \equiv 23 \equiv 20 \equiv 17 \equiv 14 \equiv 11 \equiv 8 \equiv 5 \equiv 2 \equiv -1 \equiv \cdots \pmod 3$

Any integer is in one of these congruence classes! Why?

Division algorithm! The "least non-negative residue" is the...

① $18 = 6 \cdot (3) + \boxed{0}$

② $19 = 6 \cdot (3) + \boxed{1}$

③ $24 = 7 \cdot (3) + \boxed{2}$

... remainder!

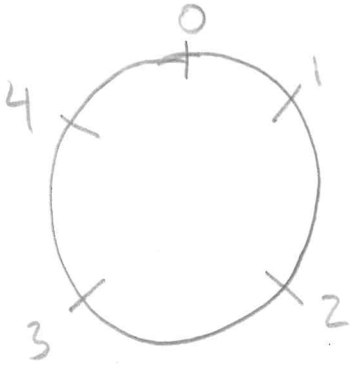
Find inverses:

① $2 \cdot x \equiv 1 \pmod 3$ $\longrightarrow$ $x =$ _____ .

② $1 \cdot x \equiv 1 \pmod 3$ $\longrightarrow$ $x =$ _____ .

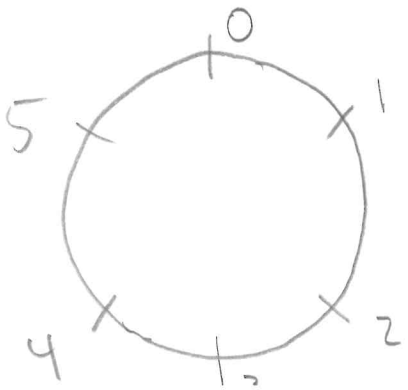
Why are they inverses? In ①, we can think of "x" as playing the role of "$\frac{1}{2}$" ... it's just that "$\frac{1}{2}$" isn't a number on the clock associated to $\mathbb{Z}/3\mathbb{Z}$!

Try: $\mathbb{Z}/5\mathbb{Z}$



	0	1	2	3	4
0					
1					
2					
3					
4					
5					

$\mathbb{Z}/6\mathbb{Z}$



	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Solve:

① $4x \equiv 2 \pmod 5$

② $2x \equiv 1 \pmod 5$

③ $4x + 2 \equiv 4 \pmod 5$

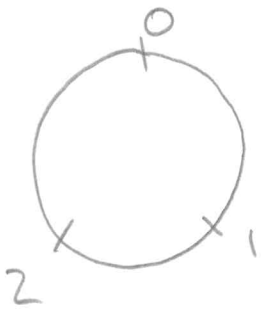
④ $2x + 3 \equiv 1 \pmod 6$

Remember: to find x, we need to "undo the changes made to x".

eg. If we multiply x by 2, then add 3,
to reverse this process, we need to
first subtract 3 and then divide by 2.
Here, we can't divide, but we can find
numbers that behave like "$\frac{1}{2}$", ie. dividing
by 2 since that is the same as multiplying by $\frac{1}{2}$.

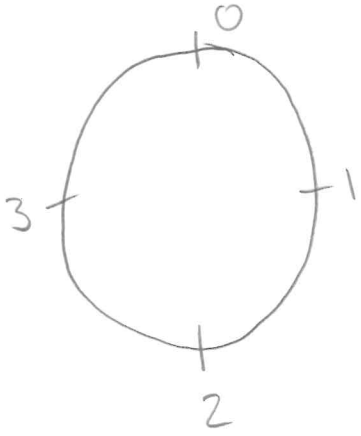
Since multiplication is defined ... we can also take powers.

In $\mathbb{Z}/3\mathbb{Z}$:



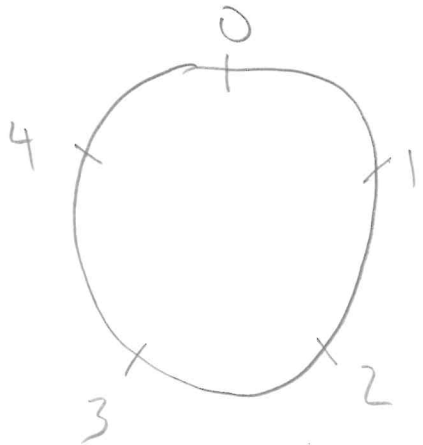
$n =$	1	2	3	4	5
$0^n \pmod 3$					
$1^n \pmod 3$					
$2^n \pmod 3$					

In $\mathbb{Z}/4\mathbb{Z}$



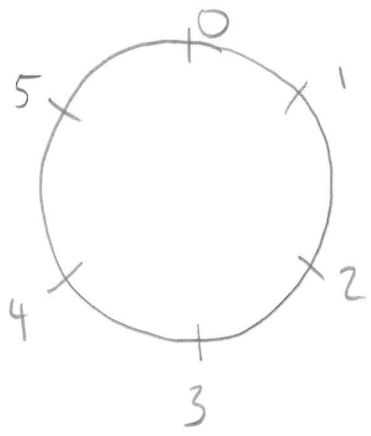
$n =$	1	2	3	4	5	6
$0^n \pmod 4$						
$1^n \pmod 4$						
$2^n \pmod 4$						
$3^n \pmod 4$						

In $\mathbb{Z}/5\mathbb{Z}$



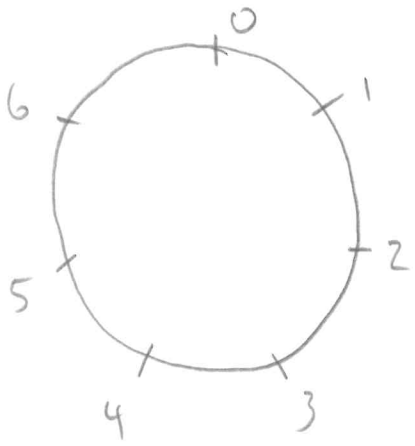
$n =$	1	2	3	4	5	6
$0^n \pmod 5$						
$1^n \pmod 5$						
$2^n \pmod 5$						
$3^n \pmod 5$						
$4^n \pmod 5$						

In $\mathbb{Z}/6\mathbb{Z}$:



$n=$	1	2	3	4	5	6	7
$0^n \pmod 6$							
$1^n \pmod 6$							
$2^n \pmod 6$							
$3^n \pmod 6$							
$4^n \pmod 6$							
$5^n \pmod 6$							

In $\mathbb{Z}/7\mathbb{Z}$:



$n=$	1	2	3	4	5	6	7
$0^n \pmod 7$							
$1^n \pmod 7$							
$2^n \pmod 7$							
$3^n \pmod 7$							
$4^n \pmod 7$							
$5^n \pmod 7$							
$6^n \pmod 7$							

Question: What do you notice about the tables? Any patterns?

Theorem Let p be a prime number. If $a \not\equiv 0 \pmod{p}$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(Same as: $a^p \equiv a \pmod{p}$.)

This is called Fermat's Little Theorem!

Question: What if we are looking at $\mathbb{Z}/n\mathbb{Z}$ where n is not prime?