Numbers

$3.33333...$

$\sqrt{7}$

-372

$\frac{27}{7}$

$0, 1, 2, 3, 4, 5...$

$e = 2.71828...$

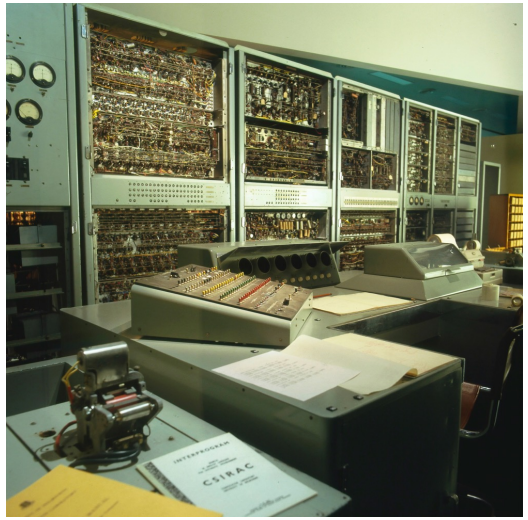
$\sqrt{5 + 3\sqrt{3}}$

$\frac{1}{\sqrt{2 + \sqrt{2}}}$

$e^3 + 72$

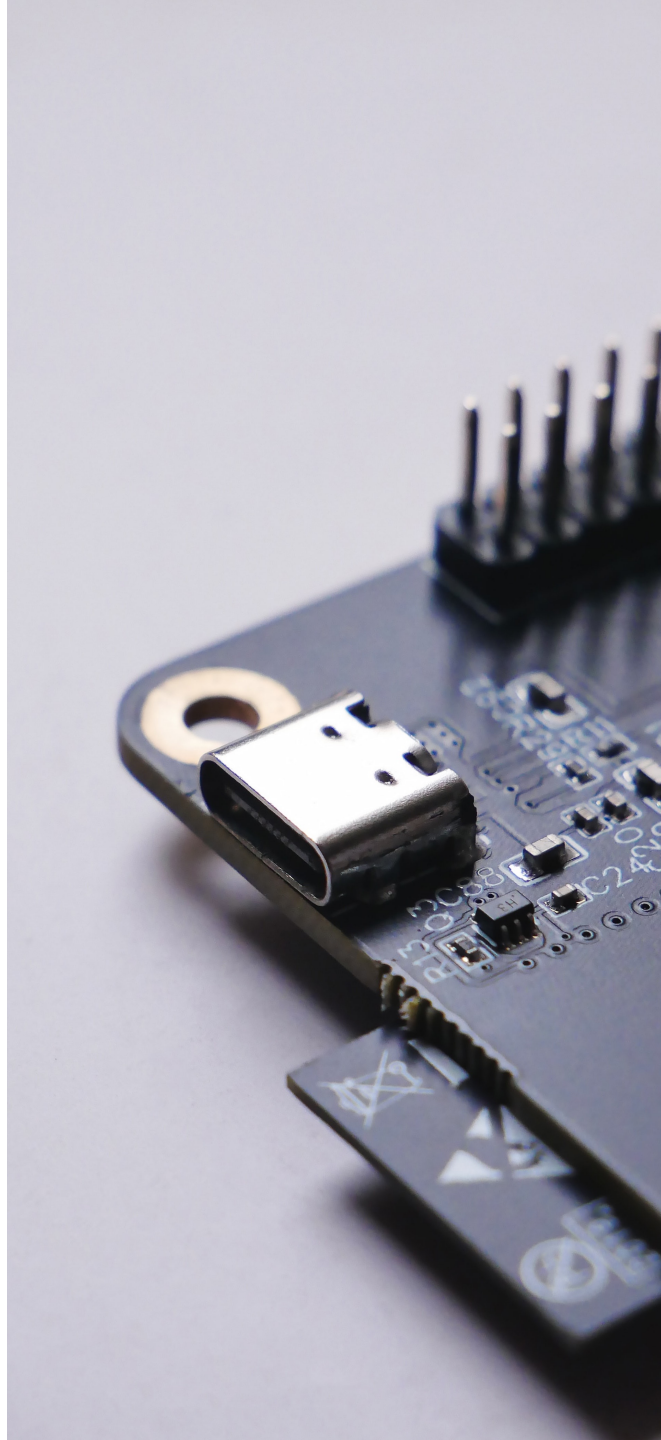
$3 - 2i$

Computational Challenge



Computers, especially early ones, can’t accommodate fractional numbers effectively, leading to precision problems.

DEMO



A New Numbers System - Objectives

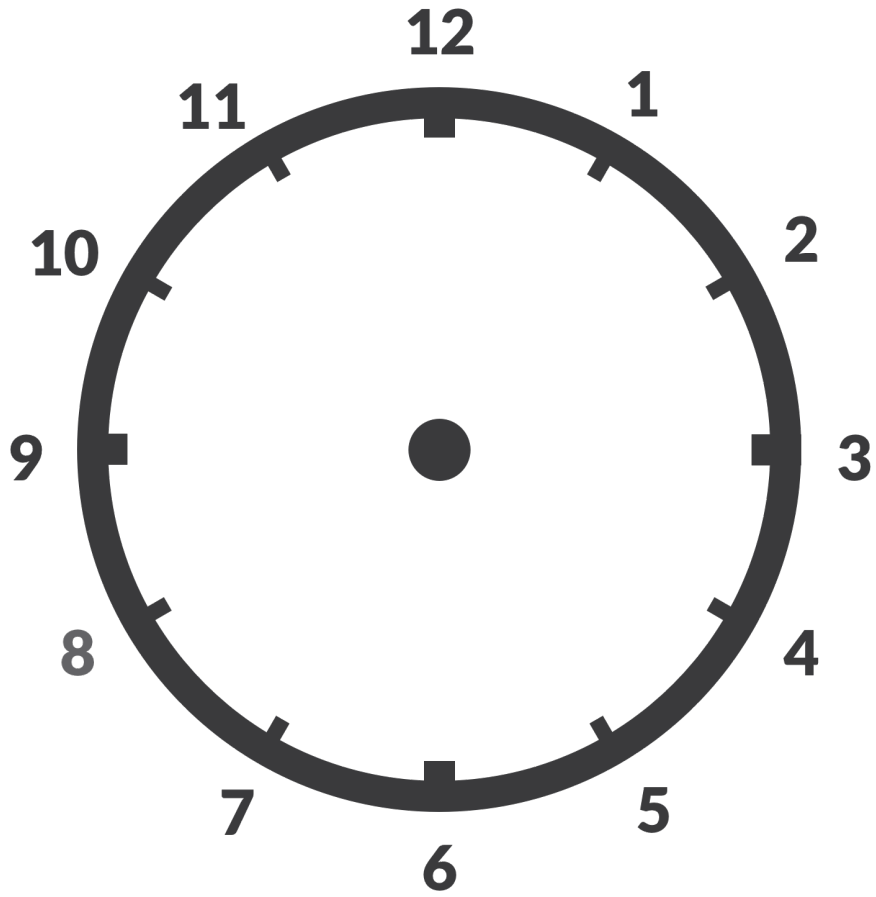
1. It will only use ”whole numbers”. For example, 0, 1, 2, 3, 4, 5 …

2. Only a limited number of whole numbers. Not going to accommodate arbitrarily large integers.

3. All arithmetic operations you can do with real numbers should be defined with this new numbers system.

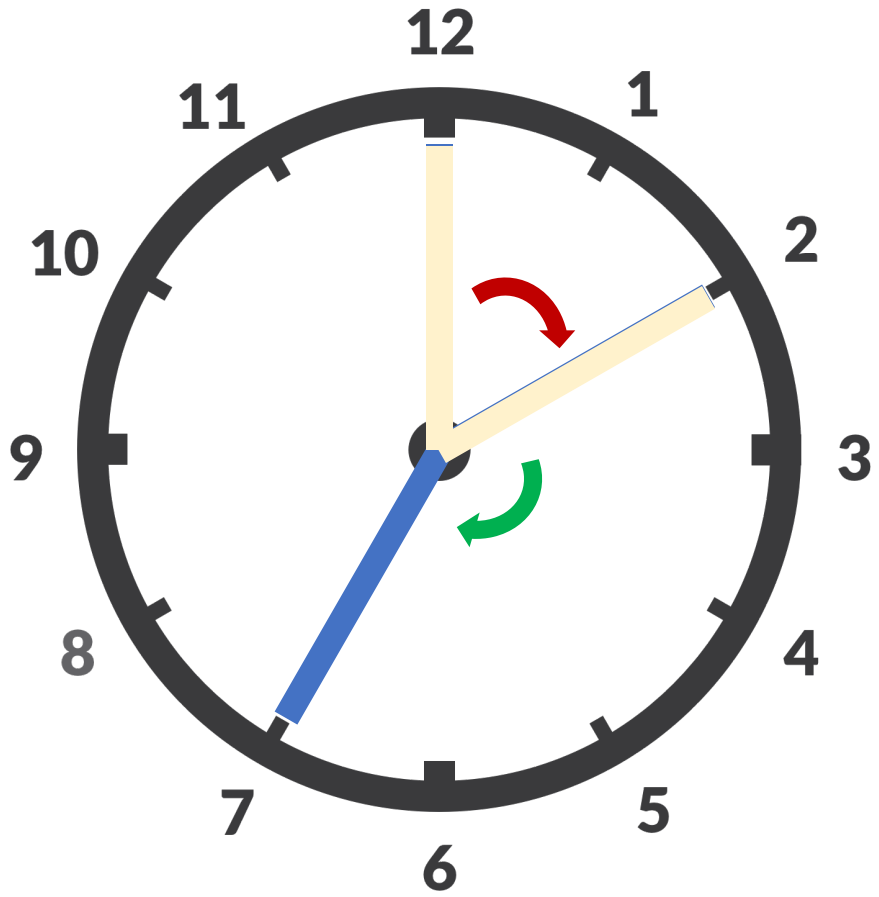
A Very Basic Idea

1. Integer Set: {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}
2. Finite Number of Elements
3. Addition and subtraction



Simple Addition

$$2 + 5 = 7$$

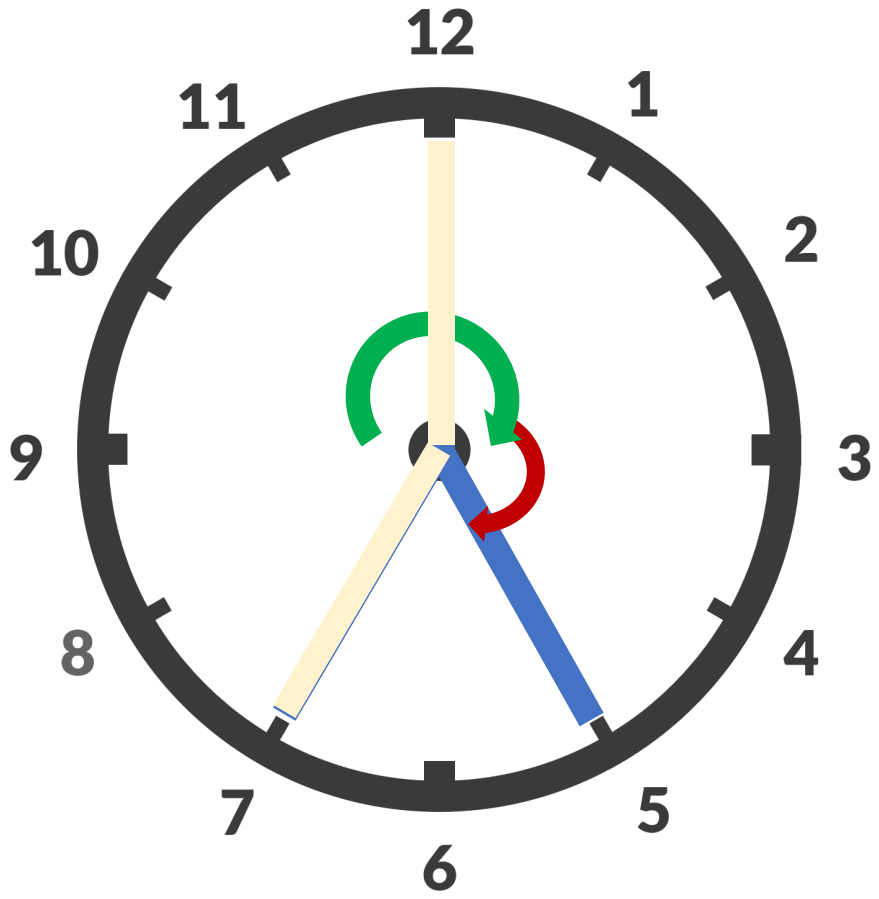


Around the Clock

$$7 + 10 = 5$$

5 mod 12

By modulo operation

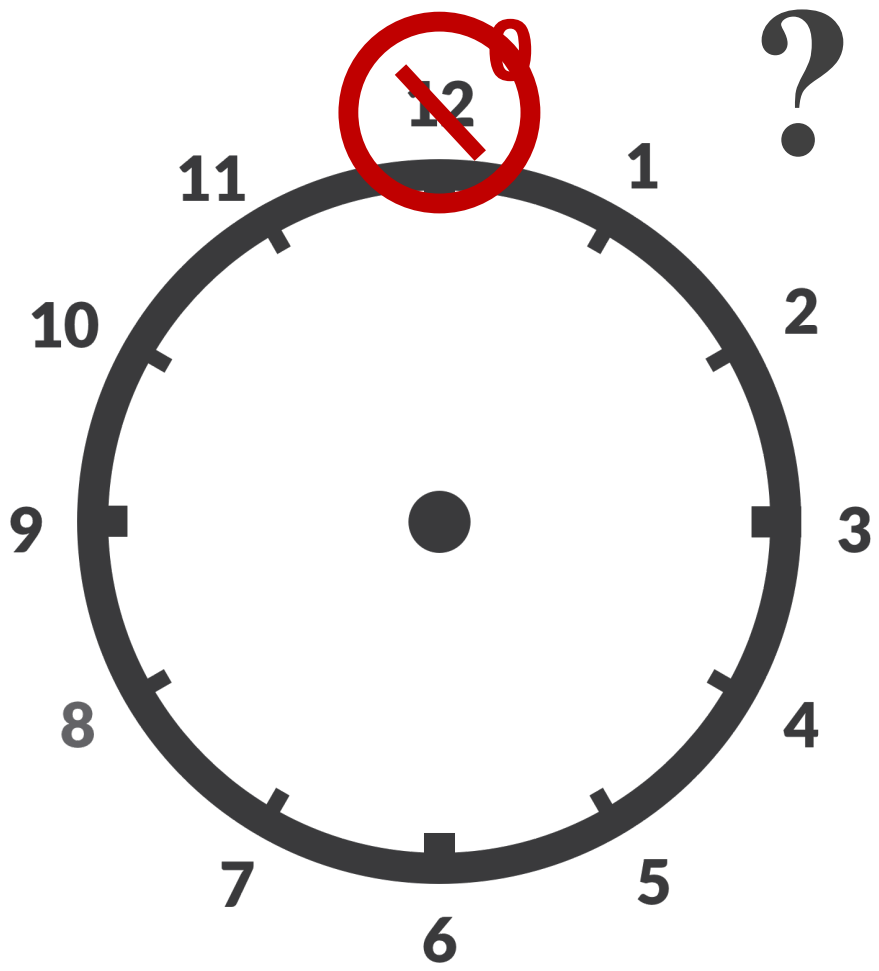


Where is Zero

Observe the behavior of 0 (in real numbers):

1) 1 + 0 = 1
2) 7384985 + 0 = 7384985
3) -3 + 0 = -3
…
…
In the end:
n + 0 = n

12 is the additive identity (zero element).

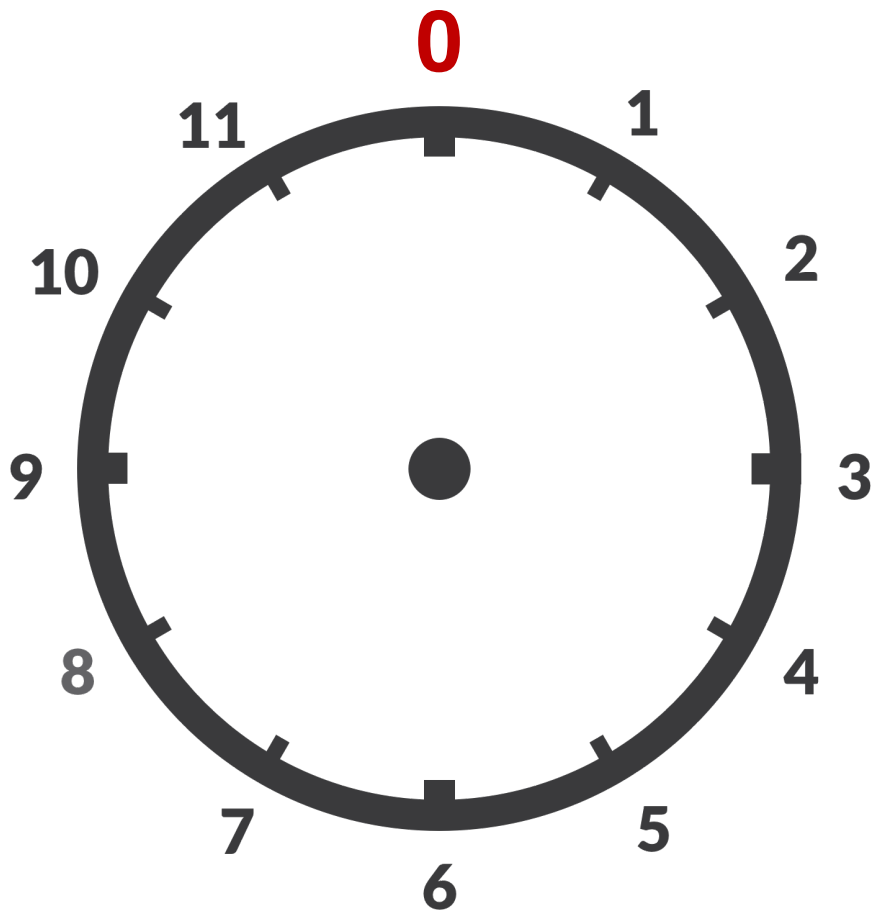


The Negatives?

Observe the behavior of negatives (real numbers):

1) 1 + (-1) = 0
2) (1/2) + (-1/2) = 0
3) 6494585 + (- 6494585) = 0
…
…
In the end:
n + (-n) = 0

The complement number on the clock is the inverse (negative)

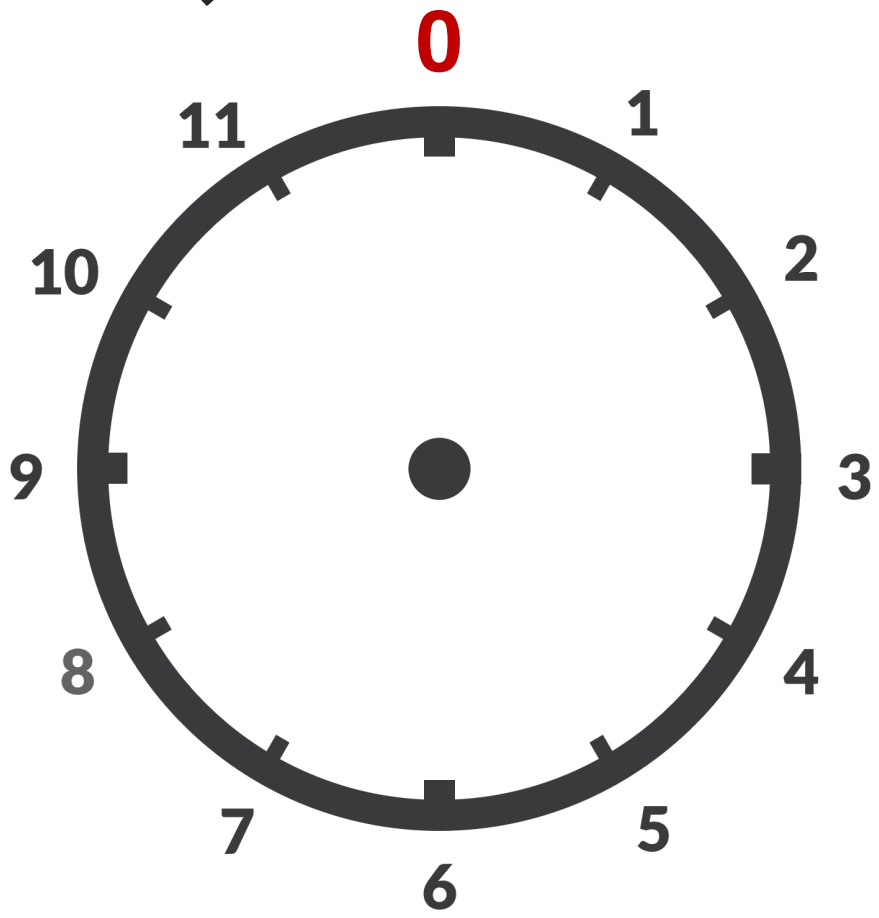


The Additive Inverse (Negatives)

n	Inverse n
1	11
2	10
3	9
4	8
5	7
6	6

n	Inverse n
11	1
10	2
9	3
8	4
7	5
6	6

Example: 3 - 11 = 3 + (-11) = 3 + 1 = 4



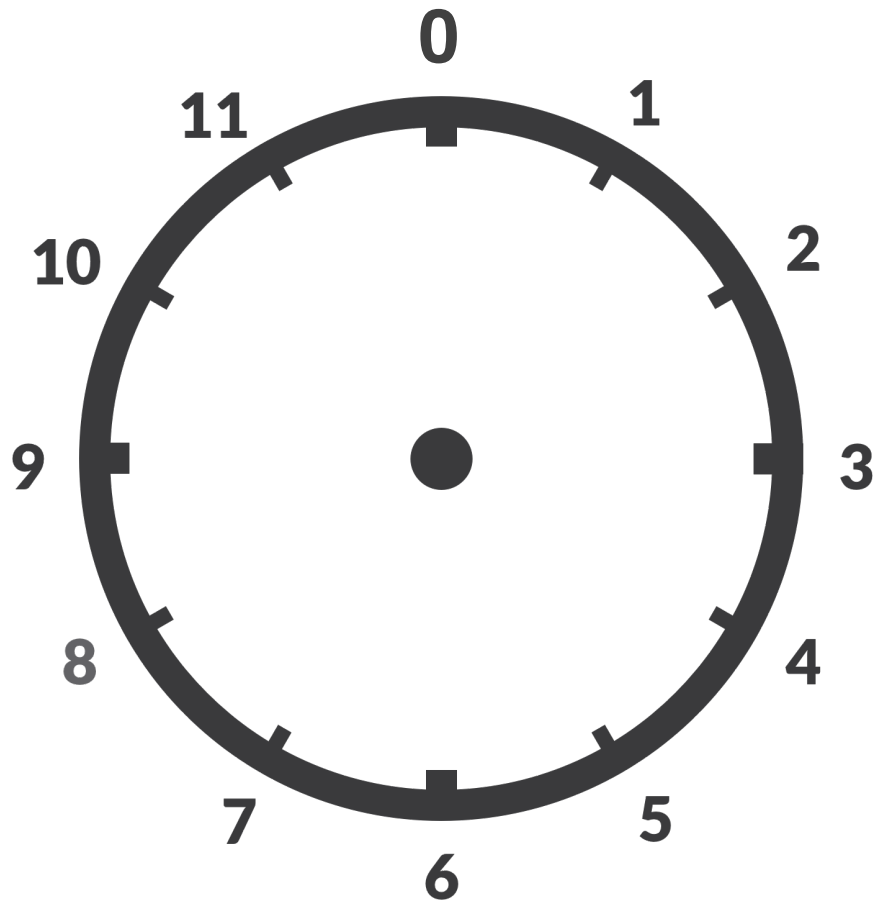
Progress: A New Numbers System

1) Finite set { 0, 1, 2, 3, 4, 5 …, 11 }
2) Addition using modular arithmetic
3) The additive identity (zero element)
4) The additive inverse (replacing negatives)

Multiplication!

A Good Start?

Expression	Product	Rewrite	Result
7x2	14	12x2 + 2	2
5x6	30	12x2 + 6	6
9x9	81	12x6 + 9	9
10x12	120	12*10 + 0	0



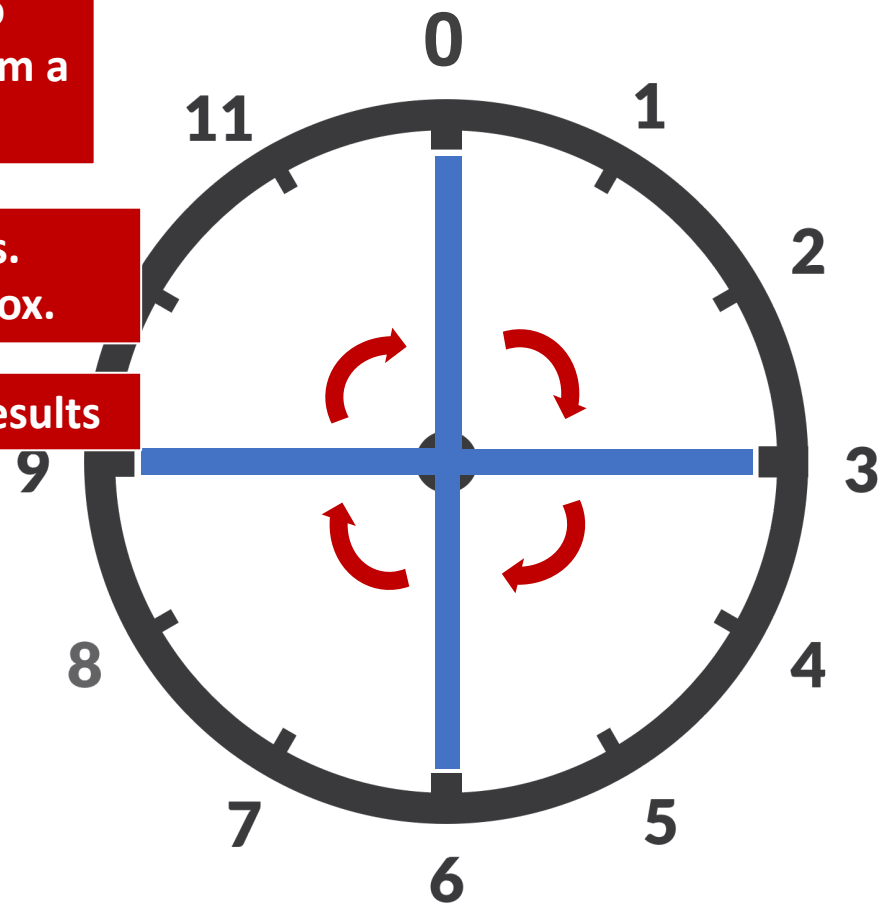
The Case of 3

Expression	Result	Expression	Resu
3x1	**3**	3x7	**9**
3x2	**6**	3x8	**0**
3x3	**9**	3x9	**3**
3x4	**0**	3x10	**6**
3x5	**3**	[illegible]	**9**
3x6	**6**	3x12	**0**

1. You can't get to every number from a multiple of 3

2. Cyclic Results. Duplicity Paradox.

3. Ridiculous Results



The Good Case of 5

Expression	Result
5x1	**5**
5x2	**10**
5x3	**3**
5x4	**8**
5x5	**1**
5x6	**6**

Expression	Resu
5x7	**11**
5x8	**4**
5x9	**9**
5x10	**2**
5x11	**7**
5x12	**0**

1. You can get to every number from a multiple of 5

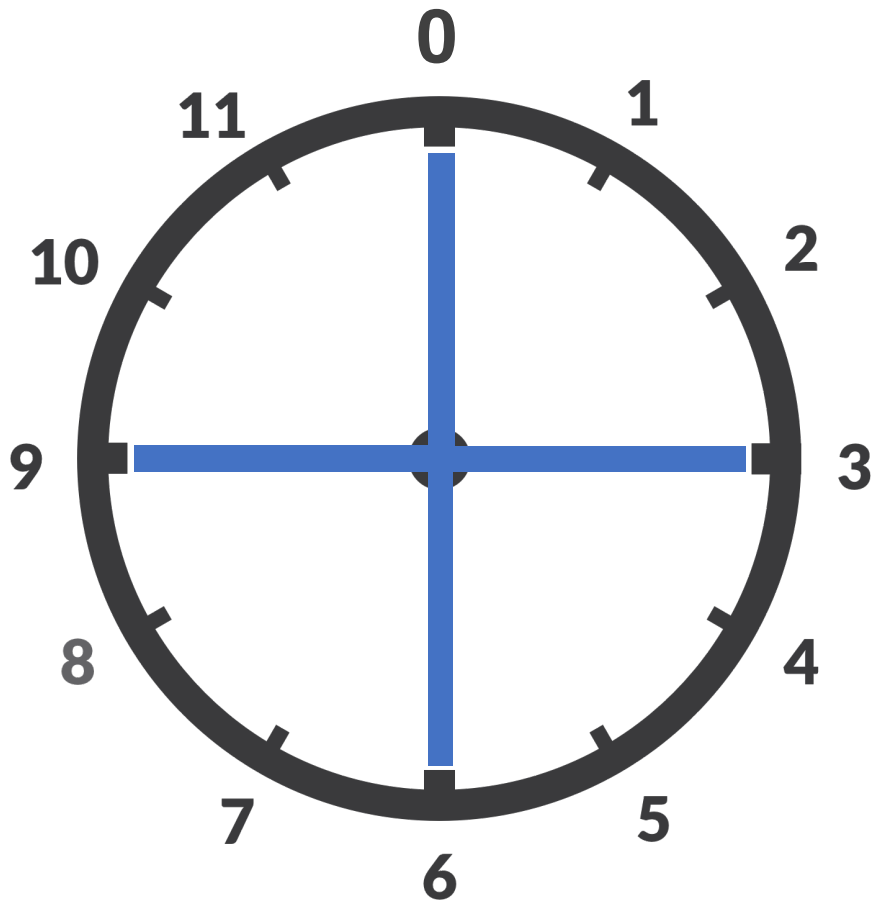
2. No cyclic results

3. Logical results

The Case of 3

Expression	Result
3x1	**3**
3x2	**6**
3x3	**9**
3x4	**0**
3x5	**3**
3x6	**6**

Expression	Result
3x7	**9**
3x8	**0**
3x9	**3**
3x10	**6**
3x11	**9**
3x12	**0**



The Good Case of 5

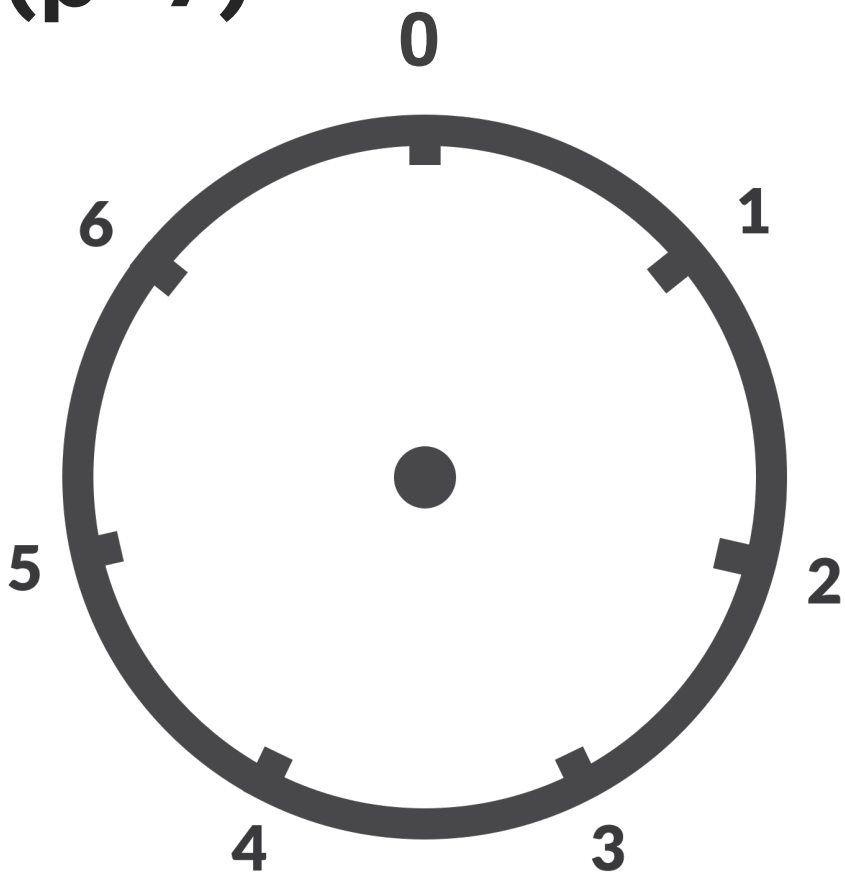
Expression	Result
5x1	**5**
5x2	**10**
5x3	**3**
5x4	**8**
5x5	**1**
5x6	**6**

Expression	Result
5x7	**11**
5x8	**4**
5x9	**9**
5x10	**2**
5x11	**7**
5x12	**0**

Pick a prime number to be on top of the clock. Then every member element will behave logically under multiplication!

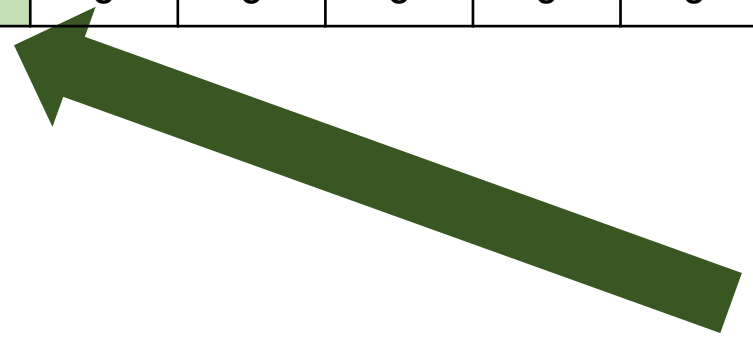
Multiplication in Prime Field (p=7)

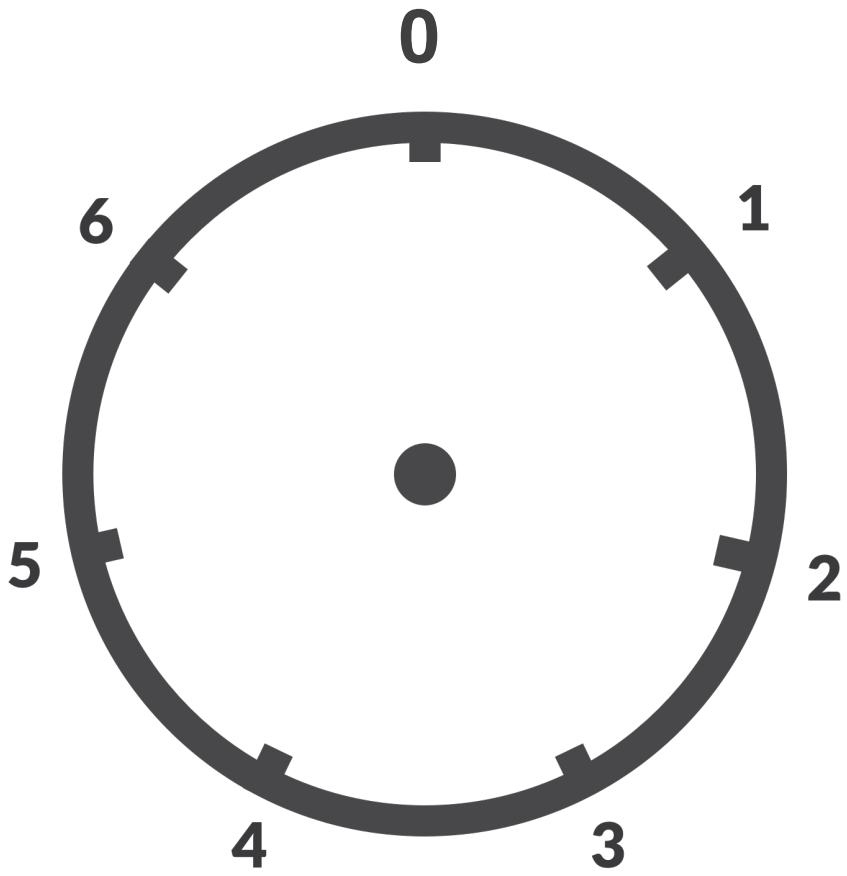
Mul	1	2	3	4	5	6	7/0
1	1	2	3	4	5	6	0
2	2	4	6	1	3	5	0
3	3	6	2	5	1	4	0
4	4	1	5	2	6	3	0
5	5	3	1	6	4	2	0
6	6	5	4	3	2	1	0
7/0	0	0	0	0	0	0	0



Multiplicative Identity

Mul	1	2	3	4	5	6	7/0
1	1	2	3	4	5	6	0
2	2	4	6	1	3	5	0
3	3	6	2	5	1	4	0
4	4	1	5	2	6	3	0
5	5	3	1	6	4	2	0
6	6	5	4	3	2	1	0
7/0	0	0	0	0	0	0	0

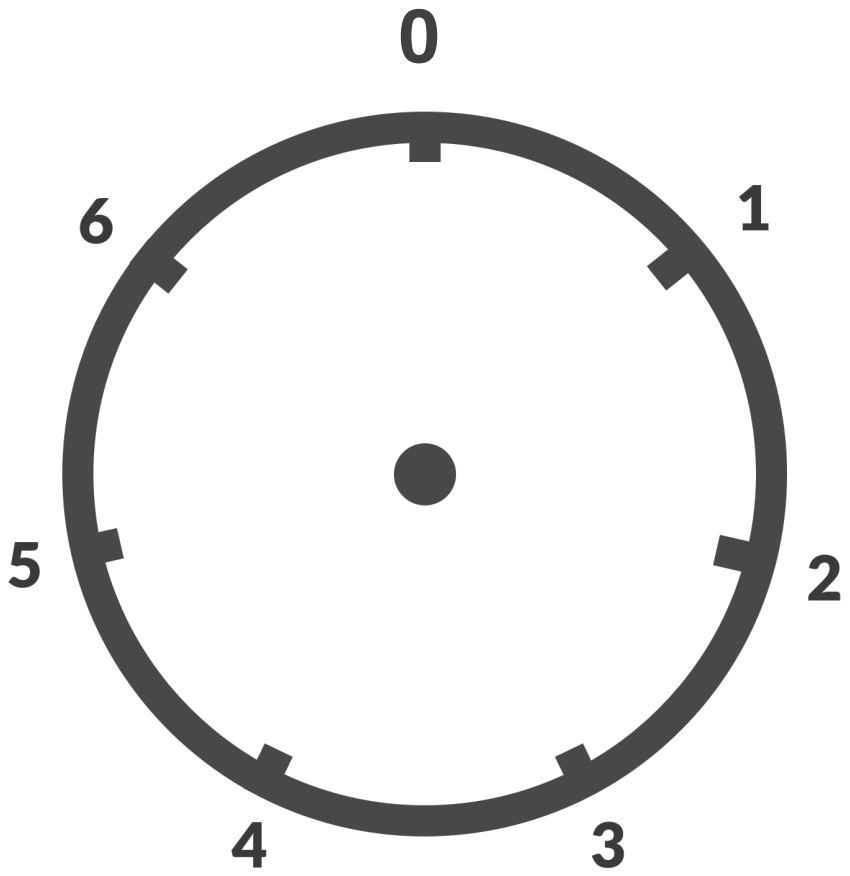




Multiplicative Inverses

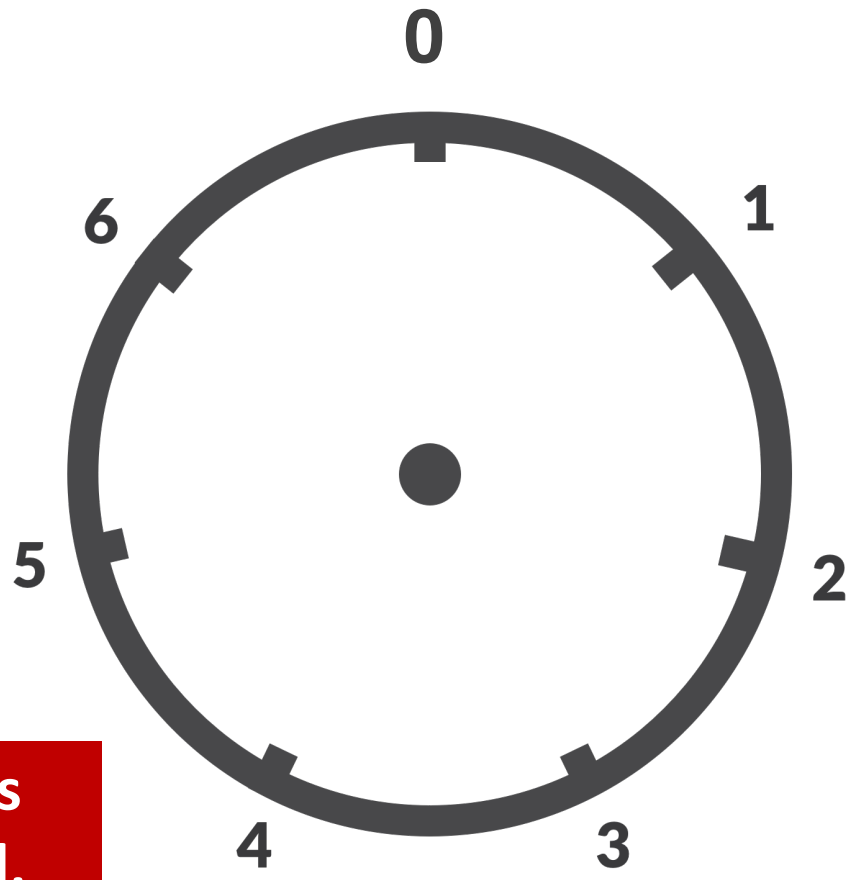
Mul	1	2	3	4	5	6	7/0
1	1	2	3	4	5	6	0
2	2	4	6	1	3	5	0
3	3	6	2	5	1	4	0
4	4	1	5	2	6	3	0
5	5	3	1	6	4	2	0
6	6	5	4	3	2	1	0
7/0	0	0	0	0	0	0	0

Example: $2/3 = 2 \times (3^{-1}) = 2 \times 5 = 3$



Division by 0

Mul	1	2	3	4	5	6	7/0
1	1	2	3	4	5	6	0
2	2	4	6	1	3	5	0
3	3	6	2	5	1	4	0
4	4	1	5	2	6	3	0
5	5	3	1	6	4	2	0
6	6	5	4	3	2	1	0
7/0	0	0	0	0	0	0	0



Division by 0 is still undefined.

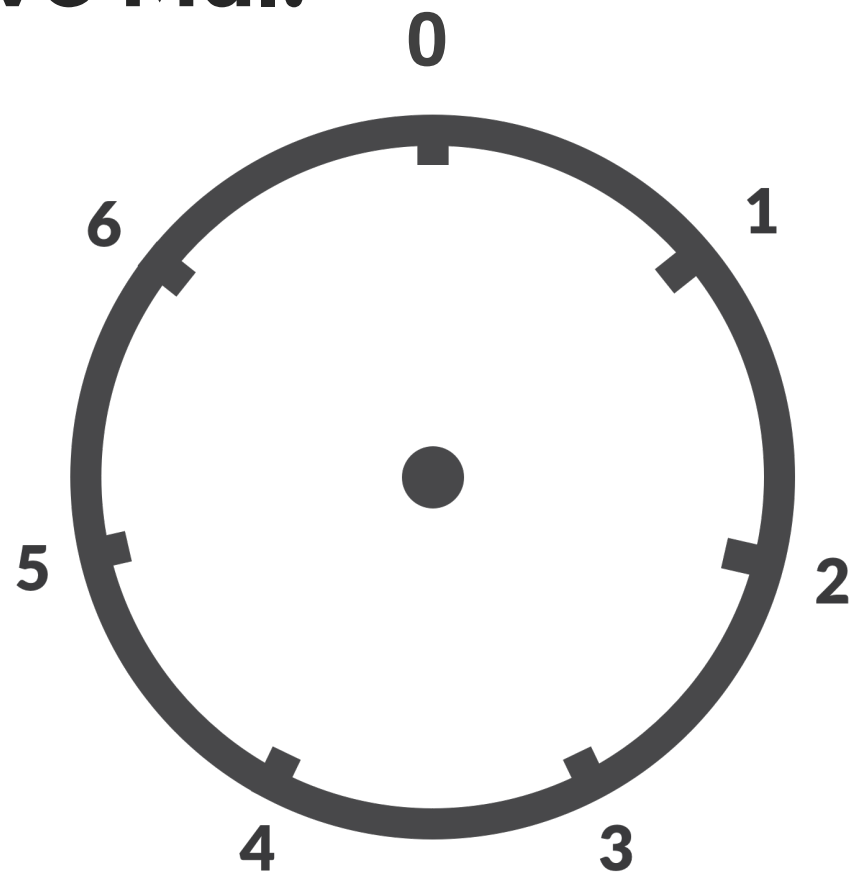
Progress: The Prime Field

Topic	Features
Elements	1) Finite set { 0, 1, 2, 3, 4, 5 …, p-1 }
Addition	2) Addition with modular arithmetic 3) The additive identity (zero element) 4) The additive inverse (replacing negatives)
Multiplication	5) Multiplication with modular arithmetic 6) The multiplicative identity (the number 1) 7) The multiplicative inverse (replacing division)

Exponentiation and Logarithm!

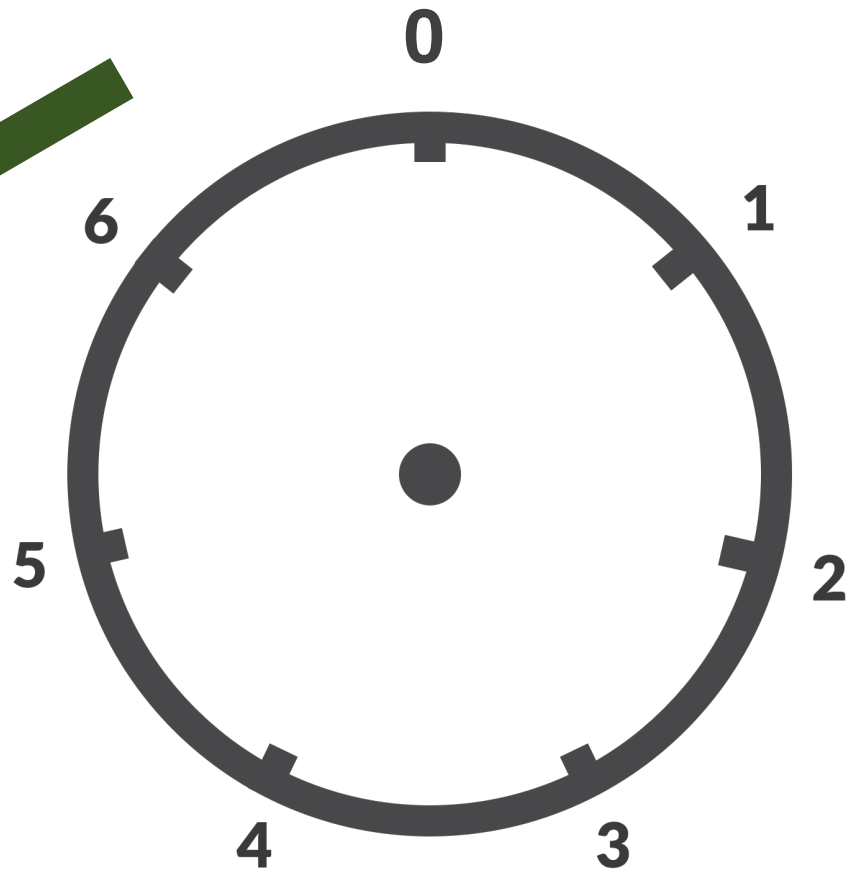
Exponentiation is Consecutive Mul.

Pow.	Equivalent	Pro.	Modular	Result
3^1	3	3	7x0 + 3	**3**
3^2	3x3	9	7x1+ 2	**2**
3^3	3x3x3	27	7x3 + 6	**6**
3^4	3x3x3x3	81	7x11 + 4	**4**
3^5	3x3x3x3x3	243	7x34 + 5	**5**
3^6	3x3x3x3x3x3	729	7x104 + 1	**1**



Field Generator

Pow.	Equivalent	Pro.	Modular	Result
3^1	3	3	7x0 + 3	**3**
3^2	3x3	9	7x1+ 2	**2**
3^3	3x3x3	27	7x3 + 6	**6**
3^4	3x3x3x3	81	7x11 + 4	**4**
3^5	3x3x3x3x3	243	7x34 + 5	**5**
3^6	3x3x3x3x3x3	729	7x104 + 1	**1**



1) A member element whose power can reach every element in a finite field is called a **generator (or primitive element).**

2) Generator raised to the (p-1) power yields 1. **g^(p-1) = 1**

Prime Field

Topic	Features
Elements	1) Finite set { 0, 1, 2, 3, 4, 5 …, p-1 }
Addition	2) Addition with modular arithmetic 3) The additive identity (zero element) 4) The additive inverse (replacing negatives)
Multiplication	5) Multiplication with modular arithmetic 6) The multiplicative identity (the number 1) 7) The multiplicative inverse (replacing division)
Power Operations	8) Exponentiation is consecutive multiplication and is well-defined in a prime field (a finite field with a prime number on top of the clock) 9) Define generators

A New Number System. Objective Complete!

Numbers for Cryptologists

$$\sqrt{5+3\sqrt{3}} \qquad \frac{1}{\sqrt{2+\sqrt{2}}}$$

$$e^3+72$$

$$\frac{27}{7} \qquad 3-2i \qquad \sqrt{7}$$

$$e = 2.71828\ldots$$

$$-372 \qquad 3.33333\ldots$$

$$0, 1, 2, 3, 4, 5\ldots$$

Modulo Identities

Law	Expression	Equivalent
Additive Distribution	$(a + b + c) \bmod m$	$(a \bmod m) + (b \bmod m) + (c \bmod m)$
Multiplicative Distribution	$(a \cdot b) \bmod m$	$[(a \bmod m) \cdot (b \bmod m)] \bmod m$