

# After Calculus: A Brief History of Groups, Rings, and Fields

Mathematicians have always been interested in solving equations. Over the past 150 years they have studied techniques for solving equations, properties of operations that allow one to develop strategies for solving equations, and, eventually, entire *systems* in which one can calculate, and hence solve, equations.

# Groups



The three main areas that were to give rise to group theory are:

- **Geometry** at the beginning of the 19<sup>th</sup> Century,
- **Number theory** at the end of the 18<sup>th</sup> Century,
- The theory of **algebraic equations** at the end of the 18<sup>th</sup> Century leading to the study of **permutations**.

An algebraic structure is a collection of objects and operations that can be used to calculate and solve equations.

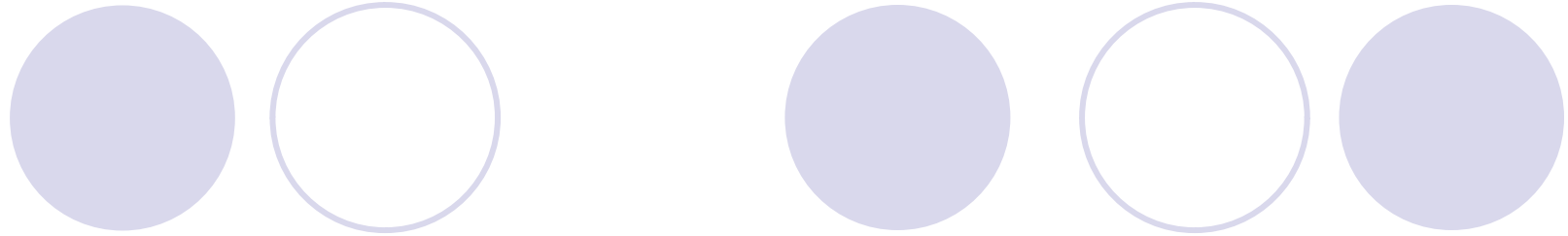
- In 1761 Euler studied modular arithmetic- provided an example of the decomposition of an abelian group into cosets of a subgroup. He also proves a special case of the order of a subgroup being a divisor of the order of the group.
- Gauss in 1801 was to take Euler's work much further and give a considerable amount of work on modular arithmetic comprising most of the basic theory of abelian groups. (Math 151)

# Solvability




- Permutations were first studied by [Lagrange](#) in his 1770 paper on the theory of algebraic equations. [Lagrange](#)'s main object was to find out why **cubic** and **quartic** equations could be solved *algebraically*.

- The solution of an algebraic equation is said to admit an **"algebraic solution"** or a **"solution in radicals"** if the solution can be expressed in terms of the addition, subtraction, multiplication, division, and the extraction of roots.
- The **Abel–Ruffini theorem** (also known as **Abel's impossibility theorem**) states that there is no general solution in radicals to polynomial equations of degree five or higher.



- One of the fundamental theorems of Galois theory states that an equation is solvable in radicals if and only if it has a solvable Galois group, so the proof of the Abel-Ruffini theorem comes down to computing the Galois group of the general polynomial of the fifth degree. (Math 251)

- 
- Algebraic structures come up naturally in mathematical investigations. We will next investigate *Units digit arithmetic*. Our goal here is to look at the underlying structure of this arithmetic, not just the calculations involved in it.

# Units digit Arithmetic

- Suppose, for example, that you are looking at the last digit, or units digit, of whole numbers.

- Find the units digit of:

$$(22 * 43 + 59 * 27) * (47 + 1,432 * 268 * 21,343)$$

Units digit Arithmetic contd.

- Using this line of reasoning, find the units digit of  $2,314 * 426 + 573 * 234$ .
  
- True or false: The units digit of  $2,314 * 426 + 573 * 234$  is the same as that of  $2312 * 422 + 576 * 232$ .

Units digit Arithmetic contd.

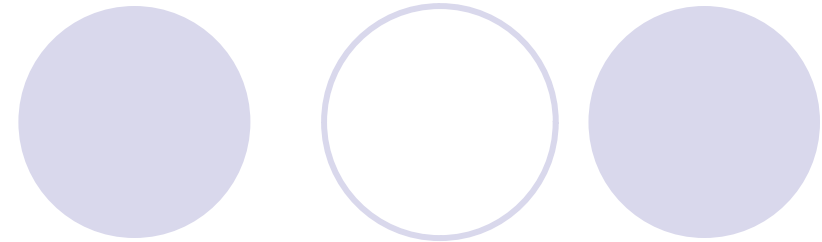
- Find the units digit of  $(312 * 423 + 57 * 57) * (28 + 1,045 * 68 * 68 * 68)$

## Units digit Arithmetic contd.

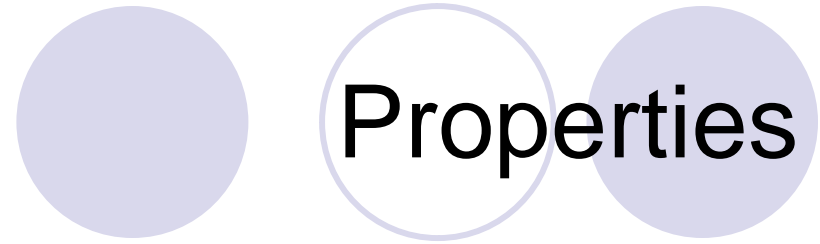
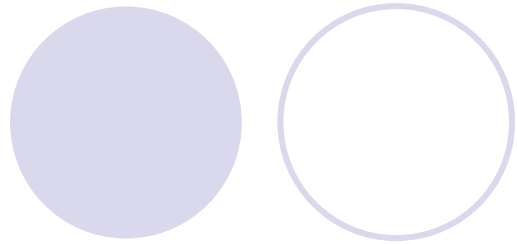
- Some people say that "the units digit of the sum is the units digit of the sum of the units digits" and "the units digit of the product is the units digit of the product of the units digits." Is what they say correct? Why or why not?
- Explain why "taking the units digit" is the same as "divide by 10 and take the remainder."

# Algebraic Structures

## Units digit Arithmetic



<b>+</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>		<b>*</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>		
<b>0</b>	0	1	2	3	4	5	6	7	8	9		<b>0</b>	0	0	0	0	0	0	0	0	0	0	0	0
<b>1</b>	1	2	3	4	5	6	7	8	9	0		<b>1</b>	0	1	2	3	4	5	6	7	8	9		
<b>2</b>	2	3	4	5	6	7	8	9	0	1		<b>2</b>	0	2	4	6	8	0	2	4	6	8		
<b>3</b>	3	4	5	6	7	8	9	0	1	2		<b>3</b>	0	3	6	9	2	5	8	1	4	7		
<b>4</b>	4	5	6	7	8	9	0	1	2	3		<b>4</b>	0	4	8	2	6	0	4	8	2	6		
<b>5</b>	5	6	7	8	9	0	1	2	3	4		<b>5</b>	0	5	0	5	0	5	0	5	0	5		
<b>6</b>	6	7	8	9	0	1	2	3	4	5		<b>6</b>	0	6	2	8	4	0	6	2	8	4		
<b>7</b>	7	8	9	0	1	2	3	4	5	6		<b>7</b>	0	7	4	1	8	5	2	9	6	3		
<b>8</b>	8	9	0	1	2	3	4	5	6	7		<b>8</b>	0	8	6	4	2	0	8	6	4	2		
<b>9</b>	9	0	1	2	3	4	5	6	7	8		<b>9</b>	0	9	8	7	6	5	4	3	2	1		



● Is this structure

○ Commutative

$$a+b=b+a \quad ?$$

○ Associative

$$(2+3)+5=2+(3+5) \quad ?$$

○ Distributive

$$2(3+5)=2(3)+2(5) \quad ?$$

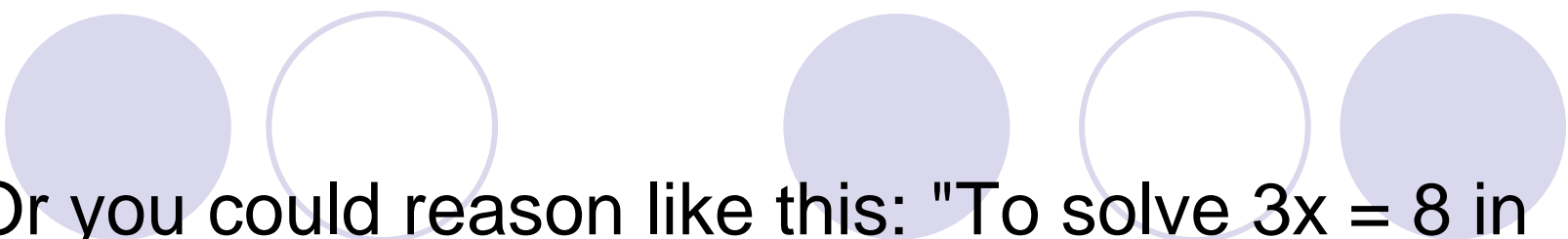
As far as you can tell; with some examples?

Units digit Arithmetic contd.

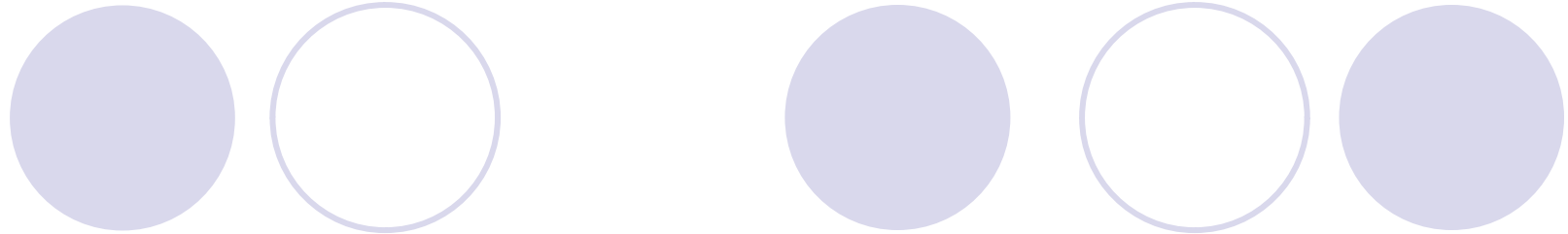
- How might you solve equations in this new system?
- Let's start with the equation  $3x = 8$ .

Can you find the solution in the table?

Is it the only solution?

- 
- Or you could reason like this: "To solve  $3x = 8$  in our regular system, I would divide both sides by 3. That's the same as multiplying by the reciprocal of 3. In this system,  $3 * 7 = 1$ , so 7 is the reciprocal of 3."

- $3x = 8$   
 $7(3x) = 7 * 8$   
 $(7 * 3)x = 6$  (Note that in the table,  $7 * 8 = 6$ )  
 $x = 6$



- What if you needed to solve the equation  $x + 4 = 2$  , how could you do it in this different number system?

## Recall Units digit Arithmetic

+	0	1	2	3	4	5	6	7	8	9	*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9	0	0	0	0	0	0	0	0	0	0	0
1	1	2	3	4	5	6	7	8	9	0	1	0	1	2	3	4	5	6	7	8	9
2	2	3	4	5	6	7	8	9	0	1	2	0	2	4	6	8	0	2	4	6	8
3	3	4	5	6	7	8	9	0	1	2	3	0	3	6	9	2	5	8	1	4	7
4	4	5	6	7	8	9	0	1	2	3	4	0	4	8	2	6	0	4	8	2	6
5	5	6	7	8	9	0	1	2	3	4	5	0	5	0	5	0	5	0	5	0	5
6	6	7	8	9	0	1	2	3	4	5	6	0	6	2	8	4	0	6	2	8	4
7	7	8	9	0	1	2	3	4	5	6	7	0	7	4	1	8	5	2	9	6	3
8	8	9	0	1	2	3	4	5	6	7	8	0	8	6	4	2	0	8	6	4	2
9	9	0	1	2	3	4	5	6	7	8	9	0	9	8	7	6	5	4	3	2	1

- Notice  $6 \cdot 2 = 12$  which divided by 10, gives remainder 2; the unit digit answer.
- Likewise  $7 \cdot 8 = 56$  which divided by 10 gives remainder 6; the unit digit answer.

Another name for the Unit digit system is:  
**Mod10.**

- Mod10 simply means to take the remainder when dividing by 10.
  - Congruence Modulo M is defined as:  
 $A \equiv B \pmod{m}$  means that  $A - B$  is divisible by  $m$ .
- Ex.  $56 \equiv 6 \pmod{10}$  because  $56 - 6 = 50$  and 10 divides 50 5 times with 0 remainder.



# Lets look at mod2 arithmetic:

- $2/2$  with 0 remainder, so 2 is equivalent to  $0 \pmod{2}$ .  $3=1 \pmod{2}$  since  $3-1=2$ .
- $4=0 \pmod{2}$  since  $(4-0)/2=2$  with 0 remainder.
- What is any odd number equivalent to in  $\pmod{2}$ ?
- What is any even number equivalent to in  $\pmod{2}$ ?

Lets make an addition table for a mod2 system:

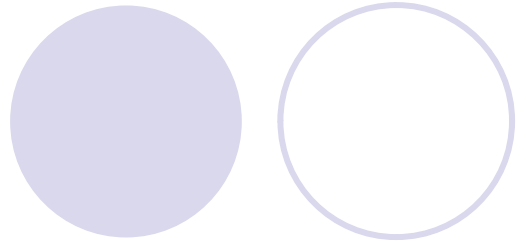
+	0	1
0		
1		

Lets make an addition table for a mod2 system:

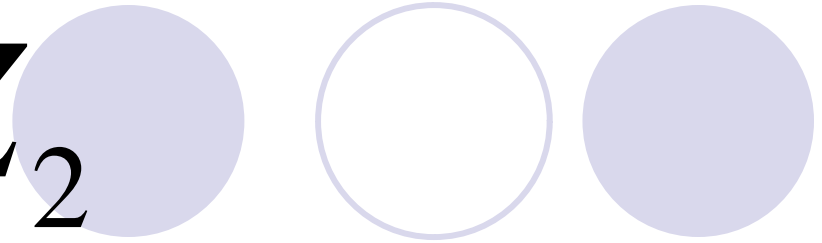
+	0	1
0	0	1
1	1	0

Now lets make a multiplication  
Table for a mod2 system

*	0	1
0		
1		



$\mathbb{Z}_2$



+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

+	0	1
0	0	1
1	1	0

$\mathbb{Z}_2$

*	0	1
0	0	0
1	0	1

● Solve the following equations:

$x-1=0$

$x+1=0$

$x-1=1$

$x+1=1$

+	0	1	2	3	4	5	6	7	8	9
0	0	1	0	1	0	1	0	1	0	1
1	1	0	1	0	1	0	1	0	1	0
2	0	1	0	1	0	1	0	1	0	1
3	1	0	1	0	1	0	1	0	1	0
4	0	1	0	1	0	1	0	1	0	1
5	1	0	1	0	1	0	1	0	1	0
6	0	1	0	1	0	1	0	1	0	1
7	1	0	1	0	1	0	1	0	1	0
8	0	1	0	1	0	1	0	1	0	1
9	1	0	1	0	1	0	1	0	1	0

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0	1	0	1
2	0	0	0	0	0	0	0	0	0	0
3	0	1	0	1	0	1	0	1	0	1
4	0	0	0	0	0	0	0	0	0	0
5	0	1	0	1	0	1	0	1	0	1
6	0	0	0	0	0	0	0	0	0	0
7	0	1	0	1	0	1	0	1	0	1
8	0	0	0	0	0	0	0	0	0	0
9	0	1	0	1	0	1	0	1	0	1



# Modular Arithmetic warm-up

$$1342 \stackrel{?}{\equiv} 1244 \pmod{3}$$



Modular Arithmetic: remember

$$a \equiv b \pmod{m}$$

When  $a - b$  is  
divisible by  $m$ .



# Modular Arithmetic warm-up:

$$1342 \stackrel{?}{\equiv} 1244 \pmod{3}$$

What are these numbers equivalent  
to in

$$\mathbb{Z}_3$$

0, 1, ... or 2 ?

Why does this definition work?

$$a \equiv b \pmod{m}$$

Let's look at a few cases in  $\mathbb{Z}_3$ :

1. 17 and 29.       $17=(15+2)$     and  $29=(27+2)$ .
2. 7 and 10.       $7=(6+1)$     and  $10=(9+1)$ .
3. 6 and 30.       $6=(6+0)$     and  $30=(30+0)$ .

Activity: First working alone, find two fairly large numbers in some  $Z_m$ , with  $m$  larger than 3, and work out if they are equivalent, and what they are equivalent to. Then show your partner the problem and ask them to work it out.

(One more thing, I want you to use **equation editor** at your computer and show your problem to your partner on your monitor!)

# What do you notice about these two multiplication tables?

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

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

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$Z_4$

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

$Z_6$



- Can they solve equations like:

$$2x + 3 = 0 ?$$

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$$2x + 3 = 0$$

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

$$3x + 1 = 2$$

# What do you notice about these two multiplication tables?

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	2	5	1	6	3
5	0	5	3	1	3	4	2
6	0	6	5	4	3	2	1

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	2	5	1	6	3
5	0	5	3	1	3	4	2
6	0	6	5	4	3	2	1

$$2x+3=1$$

$$3x+2=3$$

$$4x+1=2$$

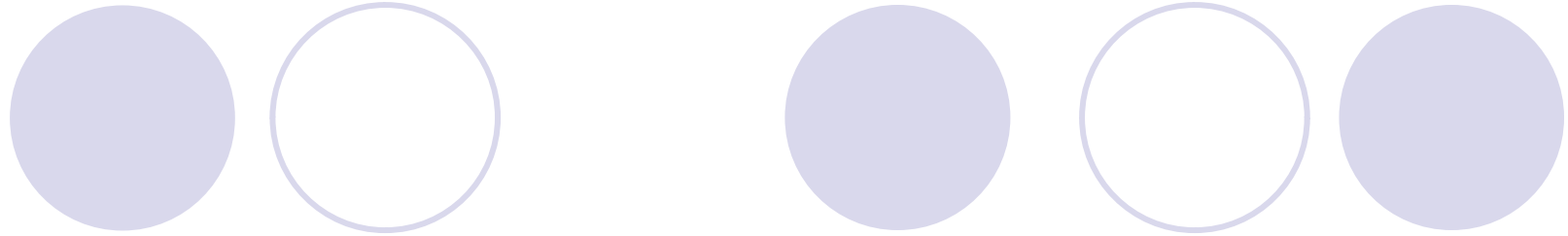


What is going on here? What statement can we predict about the solvability of equations in  $\mathbb{Z}_m$ ?

Maybe it is an issue of Odd or Even  $m$ ?

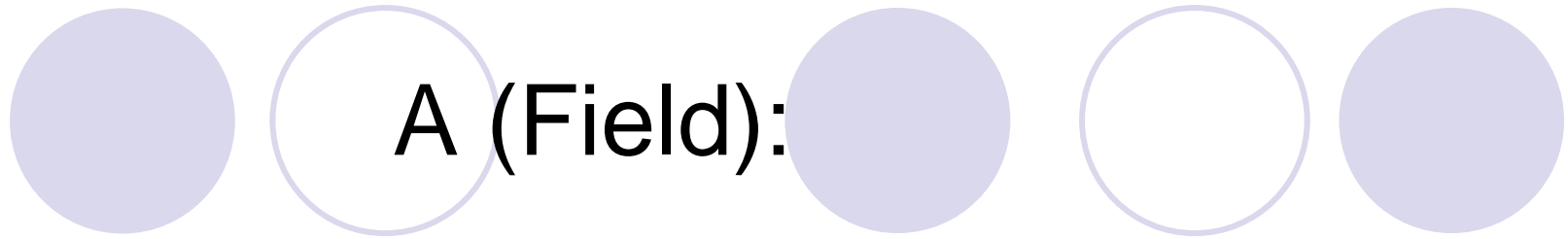
# Let's see with $Z_9$

*	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4							
5	0	5							
6	0	6	3	0	6	3	0	6	3
7	0	7							
8	0	8							



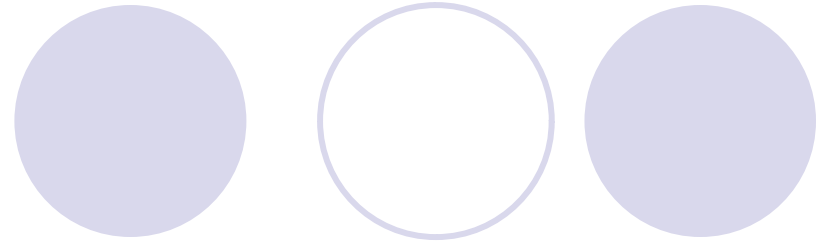
- We have discovered the simplest type of **FIELDS** in Algebra.

Something you have been working in for many years, but maybe never knew it!



- Is an algebraic system or (ring) where every number (except zero) has an inverse.
- That is why we really really needed the **RATIONAL** numbers!
- (we had to add the inverses to the integers)

To summarize:



- We have discovered that  $\mathbb{Z}_p$  is a field only when  $p$  is prime!