That Interesting Number 5

*Take attendance
*Collect homework.

A warning. Don't panic. Today we are going to take a close look at the solutions to polynomial equations. The material is very hard. But this is mostly for entertainment. The importing things to learn today are not very hard. So don't panic.

Who can tell me an interesting number?
(Discuss)

Who can tell me an uninteresting number? Is there such a thing?
(Discuss)

I'm going to prove there are no uninteresting numbers. Do you all remember what a proof is?

What's a proof?
(Discuss)

Here's a proof that there are no uninteresting numbers

Proof:
Assume there are uninteresting numbers.

So there must be a an uninteresting number whose absolute value is the smallest.

But that makes it interesting, since it is the smallest uninteresting number.

So it is not an uninteresting numbers.

Which proves all numbers are interesting by contradiction.

OK, but seriously, this is a silly proof.

The number 5

Today we're going to look at a number you might not think is all that interesting.

That number is 5.

This is going to take some work.

Actually I'm not going to show you why 5 is so interesting. That would probably take two more years of math and an whole semester course.

However I'm going to give you a really good hint as to why it is an interesting number.

We're going to start with some basic algebra that you should all know.

Let's start with a simple problem.

$5x + 10 = 0$

How do we solve this?

Well first we subtract 10 from both sides and then divide both sides by 2 and we get $x = 2$. You probably could do that in your head.

Let's do it a little more generally.

What is the solution to $ax + b = 0$?

(Discuss).

So we have a formula for the solution to this equation. $x = -\frac{b}{a}$

Does anyone remember what degree this equation is and why?
(Discuss)

OK, moving forward, how about this equation. How do we solve it?

$3x^2 - 4x + 5 = 0$?
(Discuss)

What is the degree of this equation? How many solutions does it have?

(Discuss)

So here we have the quadratic formula that gives us the solution to the equation $ax^2 + bx + c = 0$ using rational numbers and maybe a root.

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

This formula was known in a different form to the Greeks over 1000 years ago.

Does anyone remember what we call the theorem that a first degree equation has one solution and a second degree equation has two solutions?

THE FUNDAMENTAL THEORM OF ALGEBRA

Wow, that's The fundamental theorem of Algebra. Pretty important.

Let's take this one step further.

What about this equation?

$$ax^3 + bx^2 + cx + d = 0$$

Well sometimes it can be easy, for example if $d = 0$, then we have

$$x\left(ax^2 + bx + c\right) = 0$$

which has zero as a root. The other two roots can be found using the quadratic formula.

But is there a general solution like the quadratic formula?

A history lesson .

A famous mathematician named Niccolò Fontana Lived in the 1500's. He was afflicted with a condition that caused him to stammer and was given the nick name "Tartaglia" which means "the stammerer".

Not very politically correct, but this was the 1500's.

In 1535 He was the first mathematician to find a way to solve this cubic equation. He kept his method secret until he was later convinced by Girolamo Cardan to reveal the details.

One of the roots can be found with the following formula.

$$x = \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) + \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}}$$

$$+ \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) - \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} - \frac{b}{3a}$$

Not quite as easy to remember as the quadratic formula.

If you can find one of the roots p then you could in principle reduce the equation as follow:

$$\frac{ax^3 + bx^2 + cx + d}{(x - p)} = 0$$

This gets you a quadratic equation that you can solve with the quadratic formula.
So the next question is: Is there a similar solution for a quartic or 4th degree equation?

Lodovico Ferrari is a mathematician who is credited with discovering the solution to the quartic in 1540. Mostly he built on the work of Tartaglia and Cardan. I will not repeat it here. Be satisfied with knowing it is similar to and even more complicated than Tartaglia's solution.

So here we come to the first interesting thing about the number 5.

For 200 years after Ferrari, mathematicians searched for a similar solution for the 5th degree or quintic equation

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

It's easy to see that there are some solvable quintic's

How about

$$x^5 + 2x^4 + x^3 = 0$$
$$x^3\left(x^2 + 2x + 1\right) = 0$$

The roots are 0 and -1.

But there was no general solution found like the quadratic, cubic and quartic equation.

5 ----- Why is that? To get a hint why, I will have to take a major digression to see why there is no quintic formula.

Group Theory

I want to start with a question. Does anyone remember some properties of real numbers when we add them?

(Discuss)

1) Closure
2) Associate property
*) Commutative property (True, but I'm not interested right now
3) Identity property
4) Inverse property *a*--> -*a* and *a* + -*a* = 0 (the identity)

Mathematicians are interested in sets and operations on those sets that have these properties.

Can anyone tell me any other sets that have these properties on addition?
(Rationals, Integers, Irrationals of the form $a+\sqrt{b}$)

This is such an important idea that we give it a name, a **group**.

That is a set with an operation on it that has these four properties is called a group.

Let's start with integers.

$\{\ldots-2,-1,0,1,2,\ldots\}$

The integers have all 4 of these properties.

What about the even integers?

$\{\ldots-4,-2,0,2,4,\ldots\}$

They also have all 4 properties.

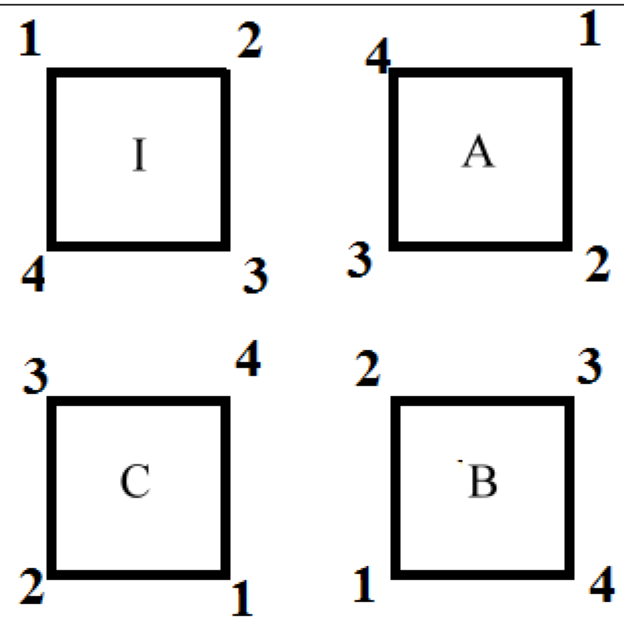
Interestingly, the even integers is a subset the integers, so we give a new definition.

A **subgroup** H of a group G is a group whose set is a subset of G's set and is by itself a group.

So the even integers are a subgroup of the integers with respect to addition.

Here's a set and a group you might not have thought of.

Take a square and label its corners 1-4. Let's take a look at all the possible configurations of that square if I just rotate it.



You can think of each of these objects as a rotation of the squares.

I + I =I
I + A = A
I + B = B
I + C = C
A + A = B
A + B = C
A + C = I
B + B = I
B + C = A
C + C = B

Let's write down the whole table

+	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

Now let's look at the properties I just mentioned.

1) Every move gets to another element of the set so we have closure

2) It appears to be associative
Example:

(A+B)+C = C+C = B
A + (B+C) = A + A = B

3) I appears to be the identity element I+X = I

4) Every element appears to have an inverse, eg.
I + I = I
A + C = I
B + B = I (Note: B is its own inverse, just like I)
C + A = I

Notice anything else?
(The elements are commutative. The matrix is symmetric along the diagonal)

Other Groups

Groups are found all over mathematics.

Examples

Matrices with respect to addition and multiplication.

Rotations of geometric objects.

The ways you change a Rubix cube form a group.

There are many more examples.

It's a good idea to remember that to be a group the operation does not need to be commutative.

OK back to that number 5

We're going to do something interesting.   We're going to look at groups with a small number of elements. Let's start with 1

Let the set be $\{e\}$ where *e* is an identity element.

So we can descript the group with this table:

*	*e*
e	*e*

This is not a very interesting group.
You have one element and when you operate on it, you get that element.
So it has an identity.
The inverse of the element is itself.
It's obviously associative and closed.

You could think of this as being a set with 0 on addition, or a set with 1 using multiplication.

Let's try 2 elements.

*	*e*	A
e	*e*	A
A	A	*e*

So there are two elements, an identity element and an element whose inverse is itself.
Again, not very interesting.

One thing to note is that if you draw a diagonal line from the to left to the bottom right, the elements are the same on each side of that line.

This group is also commutative.

Also note that the group with 1 element is a subgroup of the group with two elements.

In fact every group will have the group with 1 element as a subgroup.

Next Comes 3

*	*e*	A	B
e	*e*	A	B
A	A		
B	B		

At this point we have to think a bit.

A * A ≠ A because A * *e* = A
If A * A = A then A = *e* which is not possible because *e* ≠ A

If A * A = *e* then A * B = B, but again that would mean A = *e*

So we conclude that A * A = B
Similarly B *B = A
A * B = *e* and B * A = *e*

*	*e*	A	B
e	*e*	A	B
A	A	B	*e*
B	B	*e*	A

So A and B are inverses of each other.

This is the only way to fill in this table, so like 1 and 2, there is only one group with 3 elements.

Note that like the group with 2 elements, the group with 1 element is a sub-group.

As before, note that this group is commutative

With 4 elements things get interesting.
There are two ways to fill in the table:

*	*e*	A	B	C
e	*e*	A	B	C
A	A	B	C	*e*
B	B	C	*e*	A
C	C	*e*	A	B

You could think of this as modular arithmetic base 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

It has two subgroups, the one element subgroup of course but also

*	*e*		B	
e	*e*		B	
B	B		*e*	

This is the same as the group with 2 elements.

So this is the first group with more than 1 subgroup!

Finally notice that this group is commutative

But wait, there is another way to fill in the table

*	*e*	A	B	C
e	*e*	A	B	C
A	A	*e*	C	B
B	B	C	*e*	A
C	C	B	A	*e*

This unusual group is given a special name.

The other four groups we looked at were called cyclic.

This is the first non-cyclic group.   It is called the Klein group or Vierergruppe.

If you check the diagonal, you will see that like all the previous groups it is commutative. It has the same two subgroups as the cyclic group.

Finally a groups with 5 elements

Here's the Cyclic group

*	*e*	A	B	C	D
e	*e*	A	B	C	D
A	A	B	C	D	*e*
B	B	C	D	*e*	A
C	C	D	*e*	A	B
D	D	*e*	A	B	C

It's a commutative group with just the one subgroup that has one element.

But Wait, there's one more way to fill out the table.

*	*e*	A	B	C	D
e	*e*	A	B	C	D
A	A	*e*	C	D	B
B	B	D	*e*	A	C
C	C	B	E	*e*	A
D	D	C	A	B	*e*

Hmmmm! Just one subgroup, check.

There's something different about this table. Can anyone see what it is?

A * B = D
B * A = C

This table is not commutative.

A group with 5 elements is the first group that doesn't have to be commutative.

At this point I have to cheat a bit.

I'm going to tell you that the there is just a bit more about this group, but I'm not going to tell you what that is, only that there's one more difference between this group and all the others.

But those two differences, not being commutative and this one more item explain why there's no general solution to the equation

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

In order to fully understand why, you would need to take a few more years of math, and you would have to study a topic in "Modern Algebra" called Galois theory.

Évariste Galois was a mathematician who lived as sadly short life dying at the age of 21 in 1832 from a duel. However he solved this mystery that had stood for 350 years.

So now you know something unique and interesting about the number 5!