Intro + Lecture 1.1

About me: Andrew Kobin

ajkobin@emory.edu

Post-Doctoral Fellow

Office: MSC E425

Office Hours

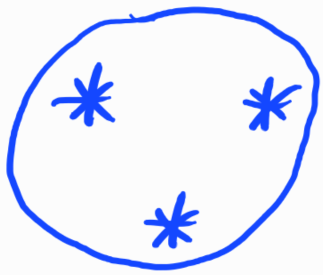
Agenda:
- introductions
- syllabus
- quick tour of Canvas
- intro to number theory

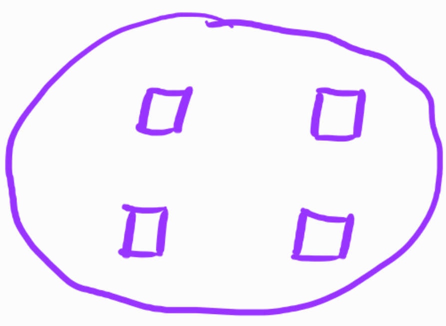
Introduction

What is a number?

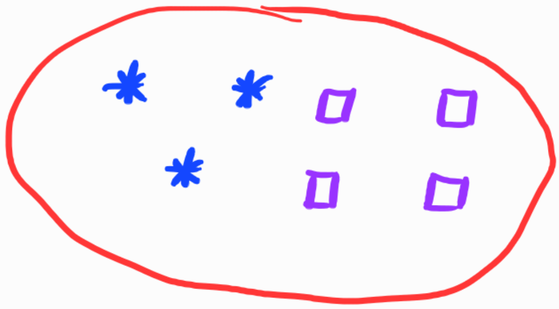
- Definitions, examples, uses?

As we start studying different properties of numbers, I want you to keep in mind what these symbols represent:

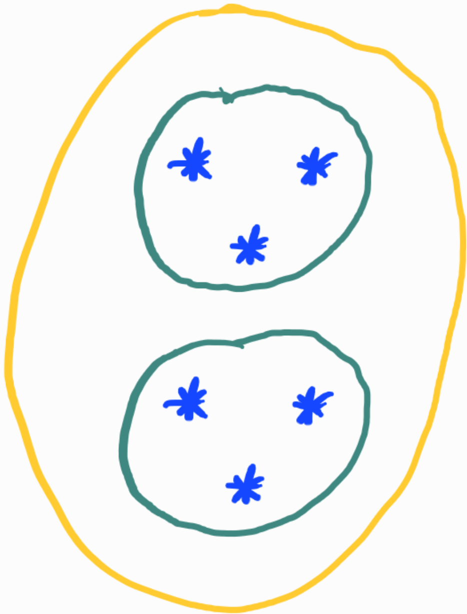
3 

4 

$3 + 4 = 7$

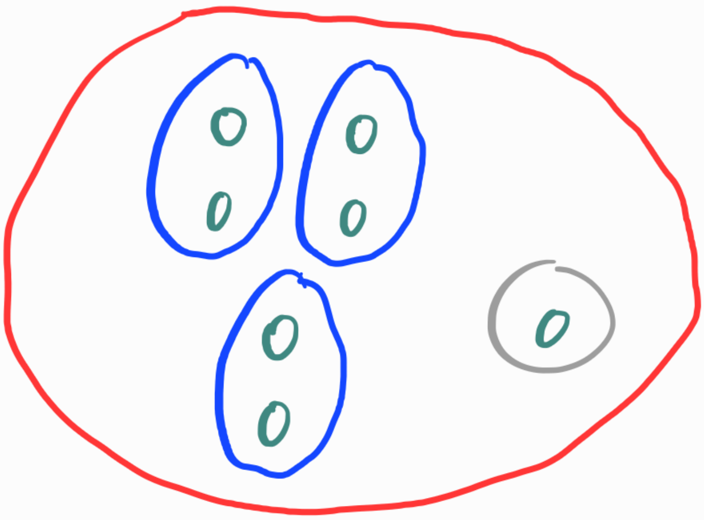


$2 \times 3 = 6$



$7 \div 3 = 2$

with remainder 1



Philosophical questions:

- Are numbers an invention or

a naturally occurring phenomenon?

- What does the symbol = mean?

An important application we will study is to cryptography, which at its heart relies on the fact that it's <u>much</u> easier to multiply two numbers than to factor one.

Ex It's easy to factor

1202909

if I tell you one of its factors is 63311:

$$\frac{1202909}{63311} = 19 \Rightarrow 1202909 = 63311 \times 19.$$

But without this information, it would be difficult to come up with the factorization on your own.

Related: can you factor 1202909 any further?

One way to study numbers a little more systematically is to look for patterns, for example:

- 1, 2, 3, 4, 5, ... are all **natural numbers**, denoted $\mathbb{N}$.

- 2, 4, 6, 8, 10, ... are the even numbers — what does this really mean?

- 1, 3, 5, 7, 9, ... are the odd numbers, or what's left after writing out all the even numbers.

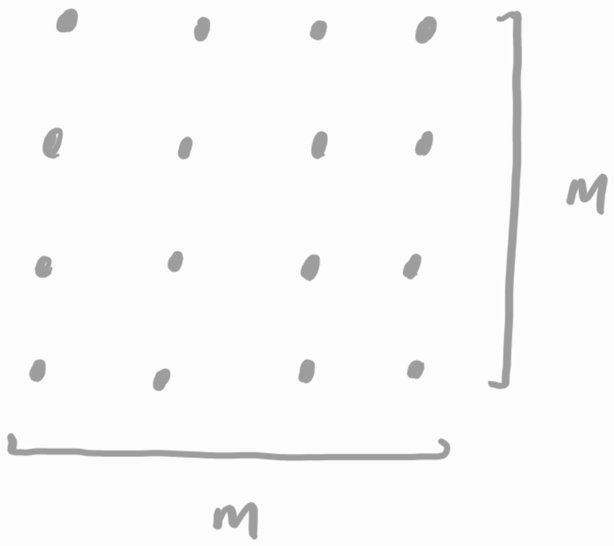
- 1, 4, 9, 16, 25, ... are the squares. Do you see any patterns? How could we prove your assertions?

- 2, 3, 5, 7, 11, ... are the **prime** numbers, those that are only divisible by 1 and itself. They are notoriously difficult to study and will play a prominent role in this course, namely their distribution among all natural numbers.

$\boxed{\text{Squares}}$

A number n is a square if it is of the form $n = m^2$ for some other number m.

n dots arranged in an $m \times m$ square



Warning: it's important to specify what number system we're using when talking about squares.

For example:

- 2 is not the square of an integer (in fact, it's prime), but $2 = x^2$ for the real number $x = \sqrt{2} = 1.414\ldots$

- -1 is not the square of any integer, or even any real number, since real number squares all satisfy $x^2 \geq 0$. However, $-1 = x^2$ for the imaginary number $x = i$.

From now on, we will use "square" to mean a natural number square.

The first few squares are

$$1, 4, 9, 16, 25, 36, 49, \ldots$$

You might have spotted this pattern earlier: the gaps between squares are just the odd numbers in order.

$$1, \underbrace{\;4,}_{3} \underbrace{\;9,}_{5} \underbrace{\;16,}_{7} \underbrace{\;25,}_{9} \underbrace{\;36,}_{11} \underbrace{\;49,}_{13} \ldots$$

Let's show this is always the case.

Proposition The gaps between subsequent squares are the odd numbers in order.

Proof: The nth square is n^2.

By the pattern observed above, we should add the odd number $2n+1$ to this to get the next square:

$$n^2 + 2n + 1 = (n+1)^2.$$

This can be verified easily by FOILing the right side. $\square$

Q: When do two squares add up to another square?

That is, which natural numbers

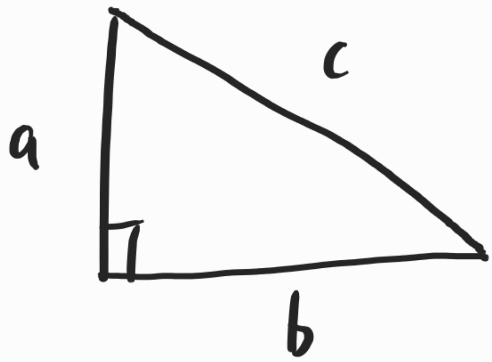
$a, b \in \mathbb{N}$ satisfy the equation

"elements of"

$$a^2 + b^2 = c^2$$

for some $c \in \mathbb{N}$?

$\boxed{\text{Pythagorean Theorem}}$ For a right triangle with legs of lengths a and b and hypotenuse of length c, $a^2 + b^2 = c^2$.



Twitter, 2022

$\boxed{\text{Ex}}$ Here are some Pythagorean triples (a,b,c):

$(3,4,5)$ $(5,12,13)$

$(8, 15, 17)$ $(28, 45, 53)$

Do you notice any patterns?

Do you think there are infinitely many of these triples?

The answer to the second question is yes, and it's easy to prove.

Prop There are infinitely many

Pythagorean triples $a, b, c \in \mathbb{N}$ satisfying $a^2 + b^2 = c^2$.

Pf: For any known Pythagorean triple (a, b, c) and any natural number $d > 1$, (da, db, dc) is also a Pythagorean triple:

$$(da)^2 + (db)^2 = d^2a^2 + d^2b^2$$
$$= d^2(a^2 + b^2)$$
$$= d^2c^2 = (dc)^2. \quad \square$$

Starting with $(3,4,5)$, this allows us to generate infinitely many triples: $(6,8,10)$, $(9,12,15)$, ...

However, $(5,12,13)$ is not of this form.

Definition A Pythagorean triple (a,b,c) is *primitive* if a,b and c do not share any common factors other than 1.

If we can find all the primitive Pythagorean triples, then all Pythagorean triples can be generated from them by multiplication.

Next time: finding primitive Pythagorean triples.