# Number Theory

The study of integers $\mathbb{Z}$, the oldest branch of mathematics.

Long considered to be the “purest” (most theoretical) form of mathematics.

Many simply stated problems that remain unsolved after hundreds of years!

Interesting popular books:

A Mathematician’s Apology, by G.H. Hardy
The man who knew infinity, by Robert Kanigel
Fermat’s Enigma, by Simon Singh

“I have never done anything "useful". No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world.” G.H. Hardy

Galois died at twenty, Abel at twenty-seven, Ramanujan at thirty-three, Riemann at forty.

# An unsolved problem

Goldbach's conjecture (1742):

Is every even number greater than 2 expressible as the sum of two primes?

$12 = 5 + 7$

$72 = 31 + 41$

$148 = 41 + 107$

# An unsolved problem

Goldbach's conjecture (1742):

Is every even number greater than 2 expressible as the sum of two primes?

1930: Every number is expressible as the sum of at most 800,000 primes.

1937: The fraction of even numbers for which the conjecture holds tends to 1.

1995: Every number is expressible as the sum of at most 6 primes.

2012: Computer verification of the conjecture for numbers up to $4\times10^{18}$

2013: Proof of the "Weak" Goldbach conjecture.

Every odd number greater than 7 is expressible as the sum of 3 odd primes.

This implies that every even number greater than 2 is expressible as the sum of 4 primes.

After 276 years so close and yet …..

# A little history

Ancient China, Greece, India, Egypt, Mesopotamia, South America (< 1000 BCE)

Very sophisticated mathematics developed.

The concept of “zero” as a number and decimal notation (600 CE)

While in Europe in the 12th century CE:

MMDCCLVII + MCCCDLXIII = ???
MMDCCLVII X MCCCDLXIII = ???

# A little history

Ancient China, Greece, India, Egypt, Mesopotamia, South America (< 1000 BCE)
The concept of “zero” as a number and decimal notation (600 CE)

Collected and Expanded by Arabs, Persians (Al Khwarizmi’s “Al Jabr”, 773 CE)

Leonardo Pisano Bigollo aka “Fibonacci” (1200 CE) learns the decimal system as a child in North Africa from the Arabs and brings it to Europe; European renaissance begins in the 1300s, fueled by knowledge brought by the Arab Moors to Spain

Set Theory (1873)

Giuseppe Peano’s Axioms of Arithmetic (1889)

# What ***is*** a Natural Number Anyway?

Peano's Axioms for Arithmetic : Defining $\mathbb{N}$, the set of natural numbers by its properties.

1. 0 is a natural number.
2. The relation $=$ is reflexive, symmetric, and transitive
3. Natural numbers are closed under $=$

   If $a$ is a natural number and $a = b$, then $b$ is a natural number.
4. For every natural number $n$ there is a successor natural number $S(n)$.
5. For all natural numbers $m, n$: $m = n \ \ if \ and \ only \ if \ S(m) = S(n)$. ($S$ is injective.)
6. For every natural number $n$, the statement $S(n) = 0$ is False.
7. Induction Axiom: $\Big(\phi(0) \wedge \forall k \ \Big(\phi(k) \Rightarrow \phi\big(S(k)\big)\Big)\Big) \Longrightarrow \forall n \ \phi(n)$

Using 0 and $S(\cdot)$ as primitives, we can implement ***all*** arithmetic operations in Scheme!

***0 is the only natural number!!!***

# Defining Addition and Multiplication

$$+: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$+(a, 0) = a$$
$$+\big(a, S(b)\big) = S\big(+(a, b)\big)$$

$$*: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$*(a, 0) = 0$$
$$*\big(a, S(b)\big) = +\big(a, *(a, b)\big)$$

Using 0 and $S(\cdot)$ as primitives, we can implement all arithmetic operations in Scheme!

# Division

$a \mid b$ is read as "$a$ divides $b$"

Given two numbers $a, b \in \mathbb{Z}, a \neq 0$,

$$a \mid b \stackrel{\text{def}}{=} \exists c \in \mathbb{Z}: \quad ac = b$$

Division by 0 is undefined.

Every non-zero integer divides 0.

# Divisibility Lemma

Divisibility Lemma. The following statements are true:

a. $a|b \implies \forall c: a|bc$

b. $a|b \wedge b|c \implies a|c$

c. $a|b \wedge a|c \implies \forall s,t \in \mathbb{Z}: a|(sb+tc)$

d. $\forall c \neq 0: a|b \iff ca|cb$

$$\begin{aligned} a|b &\Rightarrow b = ax \\ a|c &\Rightarrow c = ay \\ &\Rightarrow sb + tc = sax + tay \\ &\qquad\quad = a(sx + ty) \\ &\Rightarrow a|sb + tc \end{aligned}$$

$$\begin{aligned} a|b &\Rightarrow b = ax \\ &\Rightarrow bc = a(xc) \\ &\Rightarrow a|bc \end{aligned}$$

$$\begin{aligned} a|b &\Rightarrow b = ax \\ b|c &\Rightarrow c = by \\ &\Rightarrow c = a(xy) \\ &\Rightarrow a|c \end{aligned}$$

# The Division Theorem

Division Theorem. $\forall n, d \in \mathbb{Z}$ where $d > 0$ $\exists$ a unique pair $q, r \in \mathbb{Z}$ such that

$$n = qd + r, \qquad 0 \leq r < d.$$

We need to prove the existence of $q, r$ and prove uniqueness.

Proof of existence: Consider the set $\mathrm{R} = \{n - xd : x \in \mathbb{Z} \wedge n - xd \geq 0\}$

Example: $n = 21,\ d = 5$

$$\mathrm{R} = \{21 - 5x : x \in \mathbb{Z} \wedge 21 - 5x \geq 0\}$$

$$= \{21 - 5 \cdot 4,\ 21 - 5 \cdot 3,\ 21 - 5 \cdot 2,\ 21 - 5 \cdot 1,\ 21 - 5 \cdot 0,\ 21 - 5 \cdot -1, \ldots\}$$

$$= \{1,\ 6,\ 11,\ 16,\ 21,\ 26,\ 31,\ 36,\ 41, \ldots\}$$

# The Division Theorem

Division Theorem. $\forall n, d \in \mathbb{Z}$ where $d > 0$ $\exists$ a unique pair $q, r \in \mathbb{Z}$ such that

$$n = qd + r, \qquad 0 \leq r < d.$$

We need to prove the existence of $q, r$ and prove uniqueness.

Proof of existence: Consider the set $\mathrm{R} = \{n - xd : x \in \mathbb{Z} \wedge n - xd \geq 0\}$

This is an infinite set because $x$ can be chosen to be positive/negative depending on $n$.

By the well-ordering principle, it has a least element. Call that element $r$ and let $q$ be the corresponding value of $x$. So, $n - qd = r$, or alternatively, $n = qd + r$.

Now, $r < d$ because otherwise $n - (q + 1)d \geq 0$ is a smaller element of $R$.

# The Division Theorem

Division Theorem. $\forall n, d \in \mathbb{Z}$ where $d > 0$ $\exists$ a unique pair $q, r \in \mathbb{Z}$ such that

$$n = qd + r, \qquad 0 \leq r < d.$$

Proof of uniqueness: Let $q, r$ and $q', r'$ be two pairs such that

$$n = qd + r = q'd + r', \qquad \text{and } 0 \leq r, r' < d$$

Then $(q - q')d = r' - r$

Therefore $d \mid r' - r$

But $-d < r' - r < d$, and the only number divisible by $d$ in this range is 0

So $r' - r = 0$, which implies that $r' = r$. In turn, this implies $q' = q$.

# Introducing Lem E. Hackett

aka  Alfred E. Neuman, the  MAD-hematician

# Lem started to add up all natural numbers

What is $1 + 2 + 3 + \cdots ?$

What is $1 - 1 + 1 - 1 + \cdots \ ?$

Let $S = 1 - 1 + 1 - 1 + 1 - 1 + \cdots$

$S = 0 + 1 - 1 + 1 - 1 + 1 - \cdots$

Add these rows to get:

$$2S = 1 + 0 + 0 + 0 + \cdots = 1$$

Therefore, $S = 1/2$ !!!

# Lem gets more ambitious!

$1 - 1 + 1 - 1 + \cdots = 1/2$ done!

What about the sum $1 - 2 + 3 - 4 + 5 - \cdots$ ?

Again, let $X = 1 - 2 + 3 - 4 + 5 - \cdots$

$X = 0 + 1 - 2 + 3 - 4 + \cdots$

Add these rows to get:

$2X = 1 - 1 + 1 - 1 + 1 - \cdots$

$2X = 1/2$

$X = 1/4$ !!!

# Lem has done it again!

$$1 - 2 + 3 - 4 + 5 - \cdots = 1/4$$ done!

$$\text{Let } Z = 1 + 2 + 3 + 4 + 5 - \cdots$$

$$X = 1 - 2 + 3 - 4 + 5 + \cdots$$

Subtract the second row from the first:

$$Z - X = 0 + 4 + 0 + 8 + 0 + 12 + 0 + 16 + \cdots$$

$$Z - X = 4(1 + 2 + 3 + \cdots)$$

$$Z - X = 4Z$$

$$3Z = -X = -1/4$$

$$Z = -1/12$$

The sum of all natural numbers is $-1/12$ !!!