Prime numbers
Lecture 3b: 2022-01-26

MAT A02 – Winter 2022 – UTSC

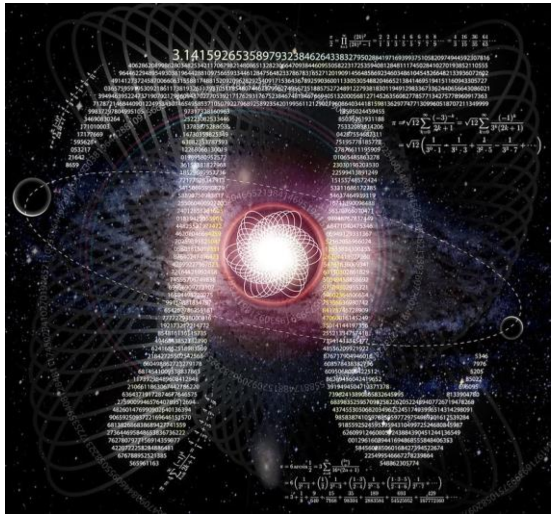
Prof. Yun William Yu

What is math?

A: Math is invented by humans

Mike Peters's _Mother Goose and Grimm_ for the 23rd of June, 2014

B: Math exists and we just discover it

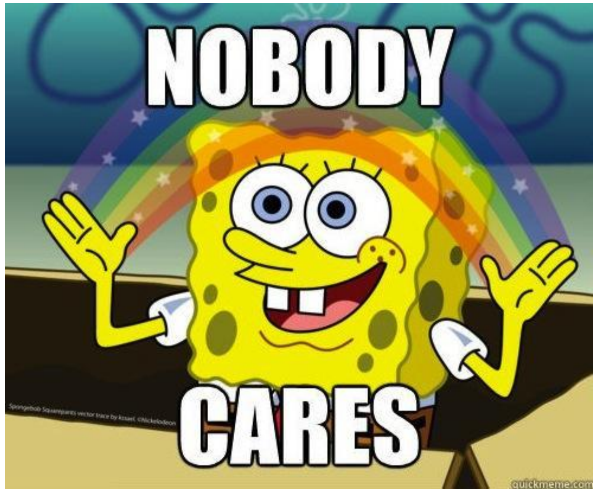


Tom Blackwell:
https://www.flickr.com/photos/tjblackwell/6849008278

C: Math is both invented and discovered

Old El Paso advertisement; Mia Agraviador pictured

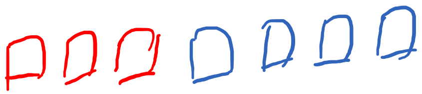
D: Who cares so long as it works?



Invention of addition and multiplication

- Addition = repeated counting

$3 + 4 = 7$



- Multiplication = repeated addition

3×4

$3 + 3 + 3 + 3 = 12$

- Commutative property

$$x + y = y + x$$
$$x \times y = y \times x$$

- Associative property

$$x + (y + z) = (x + y) + z$$
$$x \times (y \times z) = (x \times y) \times z$$

- Identity property

$$x + 0 = x$$
$$x \times 1 = x$$

Building the natural numbers

- We can get every whole number by repeatedly adding 1---i.e. using 1 as a building block under addition.

$1+1=2$

$1+1+1=3$ $(2+1)=3$ $1, 2, 3, 4, 5, 6, 7, 8, \dots$

$1+1+1+1=4$ $(3+1)=4$

- What about for multiplication?

$1, 1, 1, 1, \dots$

$2, 4, 8, 16, \dots$

$3, 9, 27, 81, \dots$

Let's invent a new number α that works as a multiplicative building block

✗

$$\begin{array}{cccc} \alpha, & \alpha^2, & \alpha^3, & \alpha^4, \dots \\ \shortparallel & \shortparallel & \shortparallel & \shortparallel \\ 1 & 2 & 3 & 4 \end{array}$$

$\rightarrow \alpha = 1$

$\rightarrow \alpha = 2$

simimultaneously

Multiplicative building blocks

$2 \times 2 = 4$
$2 = 2$

- Let's just try to build just numbers from 1 to 100.
- Would the following work as multiplicative building blocks? If no, give an example of a number that fails?
  - Numbers from 1 to 100: {1,2,3,…,100}

    Yes, by construction.

    $17 = 17 \cdot 1$
    $1 = 1 \cdot 1$
    $1 = 1$
    $100 = 100$
    $100 = 20 \cdot 5$
  - Numbers from 1 to 10: {1,2,3,4,5,6,7,8,9,10}

    No. Cannot build 11, 13, 17, 22
  - All odd numbers: {1,3,5,7,9,11,…,99}

    No. Can't build even numbers like 2, 40, etc.
  - All odd numbers and the number 2: {1,2,3,5,7,9,11,…,99}

    Yes. If even, divide by 2 until get odd number. $42 = 2 \times 21$
  - All numbers from 1 to 50, and all even numbers after 50: {1,2,3,4,5,…,50,52,54,56,58,…,100}

    No. 53, 59 fail

A: Yes
B: No
E: ???

Discovering the prime numbers

- Let's find the smallest possible set of building blocks for numbers from 1 to 20. We'll start with all numbers in 1 to 20 and remove ones we don't need.

special: only used to make 1

①	$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	$\boxed{7}$	~~8~~	~~9~~	~~10~~
			2×2		2×3		2×4 = 2×2	3×3	= 2×5

$\boxed{11}$	~~12~~	$\boxed{13}$	~~14~~	~~15~~	~~16~~	$\boxed{17}$	~~18~~	$\boxed{19}$	~~20~~
	2×6 = 2×2×3		2×7	3×5	= 2×8 = 2×2×4 = 2×2×2×2		= 2×9 = 2×3×3		= 2×10 = 2×2×5

Smallest multiplicative building blocks

- 1 is a special case because it’s not useful for building any number except itself; let’s ignore it for now.
- In any set of integers from 2 to N, the smallest set of multiplicative building blocks seems to be only numbers that cannot be written as a product of two smaller numbers.
- Let’s call a number composite if it is the product of two strictly smaller whole numbers.
- Let’s call a number prime if it is not. Equivalently, a number is prime if it is divisible only by 1 and itself.
- By convention, we do NOT consider 1 prime, because it is a special case that’s not useful as a building block.

Proof that the primes suffice

- We saw a pattern that suggested prime numbers are the smallest set of multiplicative building blocks. Let's prove it!
- Clearly, prime numbers have to be included our list of multiplicative building blocks, since you cannot build them.
- Notice that any number x not in our list must be built from smaller numbers in our list.
- Let c be the smallest composite number in our list. Then $c = ab$, where $a, b < c$.
- But a, b are either prime or are not in our list. If they are not in our list, then they must be built from smaller numbers in our list, which are all prime.
- Thus, c can be built from primes, so we can remove c.
- Repeating, we remove all composites from our list of blocks.

$2, 3, 5, 7, \cancel{8}$

$6 = 2 \times 3$

$8 = 2 \times 4$

2 is prime

4 is not in list

$\Rightarrow 4 = \underbrace{2 \times 2}_{\text{both prime}}$

$8 = 2 \times 2 \times 2$

Prime factorization

- Every composite number can be written as a product of two smaller numbers.
- We can repeat this process until we write the composite number as a product of prime numbers.

Ex. $120 = 2 \times 60 = 2 \times 2 \times 30 = 2 \times 2 \times 2 \times 15$

$= 2 \times 2 \times 2 \times 3 \times 5$

$= 2^3 \cdot 3 \cdot 5$

Notice: $120 = 10 \times 12 = 2 \times 5 \times 3 \times 4 = 2 \times 5 \times 3 \times 2 \times 2$

$= 2 \times 2 \times 2 \times 3 \times 5$

$= 2^3 \cdot 3 \cdot 5$

- Prime factorizations are unique. (proof later)

Try it out

- Find a prime factorization of the following:
- 720

$= 10 \cdot 72 = 2 \cdot 5 \cdot 2 \cdot 36$

$= 2^2 \cdot 5 \cdot 6^2$

$= 2^2 \cdot 5 \cdot (2 \cdot 3)^2 = 2^4 \cdot 3^2 \cdot 5$

- 722

$= 2 \cdot 361 = 2 \cdot 19^2$

$$\begin{array}{r} 19 \\ \times\ 19 \\ \hline 171 \\ 19\ \ \\ \hline 361 \end{array}$$

FOIL

$19 \times 19 = (20-1)(20-1) = 400-20-20+1$

$= 361$

A: $2^2 \cdot 6^2 \cdot 5$
B: $2 \cdot 361$
C: $2^3 \cdot 3^3 \cdot 5$
D: $2^4 \cdot 3^2 \cdot 5$
E: None of the above

How do we know if a number is prime?

Ideas in chat, please.

- Test if it is divisible by every number smaller than it.

361 ÷ 2 = 180 r 1

361 ÷ 3 = 120 r 1

361 ÷ 4 = 90 r 1

361 ÷ 5 = 72 r 1

361 ÷ 6 = 60 r 1

361 ÷ 7 = 51 r 4

361 ÷ 8 = 45 r 1

361 ÷ 9 = 40 r 1

361 ÷ 10 = 36 r 1

361 ÷ 11 = 32 r 9

361 ÷ 12 = 30 r 1

361 ÷ 13 = 27 r 10

361 ÷ 14 = 25 r 11

361 ÷ 15 = 24 r 1

361 ÷ 17 = 21 r 4

361 ÷ 18 = 20 r 1

361 ÷ 19 = 19

Any other ideas?

- Make a list of primes, and test only those numbers.

2, 3, 5, 7, 11, 13, 17, 19, 23, ...

$361 \div 2 = 180 \text{ r } 1$

$361 \div 3 = 120 \text{ r } 1$

⋮

$361 \div 19 = 19$

Sieve of Eratosthenes

- Method for computing list of primes by filtering out all multiples of a number.
- Repeatedly filter out all multiples of the smallest remaining number in a list.
- Start with filter out multiples of 2.
- Then multiples of 3.
- Then multiples of 5, because 4 is filtered, etc.

Eratosthenes of Cyrene
276 BCE – 194 BCE

Sieve of Eratosthenes in action

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

- How quickly do we get all the primes between 1 and 100?

Why is the sieve so fast?

2 → 4

3 → 9

5 → 25

7 → 49

- For each prime, what is the first number that is filtered out?

Answers in chat, please.

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Properties of the sieve

- When any number is filtered out, obviously all of its multiples are also filtered out.

4 is filtered out for the prime 2

But then 4n are also filtered because $4n = 2 \cdot (2n)$

- The first multiple of a prime p to be filtered out is always p^2 because any smaller multiple $p \cdot n$ (where $n < p$) would have been filtered out when [illegible] was filtered out.

n

Ex.	11	~~22~~	~~33~~	~~44~~	~~55~~	~~66~~	~~77~~	~~88~~	~~99~~	121
		2	3	4	5	6	7	8	9	

- Therefore, to figure out if a number n is prime, you only have to run the Sieve of Eratosthenes up to a prime $p \leq \sqrt{n}$.
- If n is not prime, then it must be divisible by a prime $p \leq \sqrt{n}$.

$n = ab$, so either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Sieve of Eratosthenes on a restricted set

- What are the primes between 210 and 220?

Primes: 2, 3, 5, 7, 11, 13, [illegible]

17
× 17
119
17
289

prime

~~210~~ 211 ~~212~~ ~~213~~ ~~214~~

~~215~~ ~~216~~ ~~217~~ ~~218~~ ~~219~~ ~~220~~

Try it out

A: Prime
B: Composite
C: Both
D: Neither
E: ???

- Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, …
- Classify the following numbers:
- 1 neither
- 87 $87 \div 3 = 29$ ← composite ~~87[illegible]÷3~~
- 97 prime
- 359 prime. 2, 3, 5, 7, 11, 13, 17. ← check each of these
- 401 prime check through 19
- 623 $$\begin{array}{r}89\\7\overline{)623}\end{array}$$ Composite