NUS National University of Singapore

School of Computing

# Algorithm Design
## (Some Old Algorithms)
## Video 6.3c


Hon Wai Leong

Department of Computer Science

National University of Singapore

Email, FB: leonghw@comp.nus.edu.sg


*Algorithm is Cool. Learn Algorithms.*

# Outline

## Overview:

- ❑ Definition of Algorithm
- ❑ Algorithms in Everyday Life
- ❑ Some Old Algorithms
- ❑ Some Simple Algorithms
- ❑ Abstraction & Decomposition

**What is the oldest algorithm you know?**

# Do you know what's prime?

Yes, those numbers like

2, 3, 5, 7, 11, 13, and so on….

**What's so special about them…**

they cannot be divided by any smaller number (except for 1)

And yes, there are other ways to define…

**Task:** *Given a number n,*

*find all the prime numbers between 2 and n.*

# Prime Number Joke…

# Theorem: All odd numbers are prime

# Theorem: All odd numbers are prime

*Input:*

- a Mathematician,
- a Physicist,
- an Engineer,
- a computer scientist…

## Theorem: All odd numbers are prime

**Mathematician: (*pen-and-paper person*)**

- **1 is prime, 3 is prime,**
- **5 is prime, 7 is prime,**
- **9….**

  **Counter-example** (yes, disconfirmation!)

**Therefore, Theorem is false…**

## Theorem: All odd numbers are prime

**Physicist: *(…does some experiments)***

- **1 is prime, 3 is prime,**
- **5 is prime, 7 is prime,**
- **9…. Hmmm… *experimental error***
- **11 is prime, 13 is prime,**

**Therefore, All odd numbers are prime +**

*+ subject to tolerable experimental error*


LeongHW, CS, NUS

# Theorem: All odd numbers are prime

Engineer: (...*quick and dirty solution*)

- 1 is prime, 3 is prime,
- 5 is prime, 7 is prime,
- *9 is prime*, 11 is prime, 13 is prime

Therefore, All odd numbers are prime

# Theorem: All odd numbers are prime

*Computer Scientist:*

- ***take course on  Analysis of Algorithm,***
- ***write algorithm in pseudo-code,***
- ***program in Fortran/Pascal/C/C++/Java/python***
- ***Debug,***
- ***Debug some more,***
- ***Lots of debugging later,***
- **Program compiles!!!**        ***Eureka*!!!**

# Theorem: All odd numbers are prime

**Computer Scientist:** *(runs the program...)*

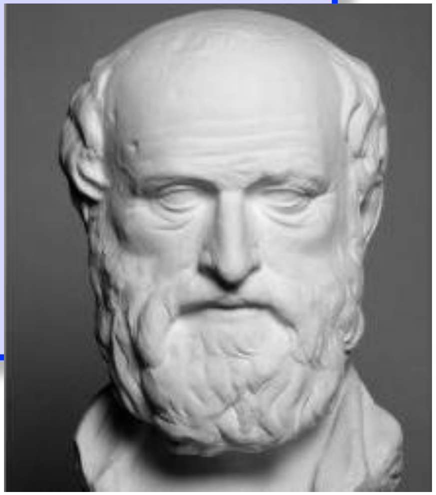
- 1 is prime,
- 3 is prime,
- 5 is prime,
- 7 is prime,
- *7 is prime,*
- *7 is prime,*
- *7 is prime,*
- *7 is prime,*

Back

# Seive of Eratosthenes (200 BC)

**A *cool* algorithm for finding all prime numbers between 2 and *n*.**

by literally by sieving away all the non-primes (multiples of smaller primes)



https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes

# Seive of Eratosthenes

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 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 |
| 101 | 102 | 103 | 104 | 105 | 106 | 107 | 108 | 109 | 110 |
| 111 | 112 | 113 | 114 | 115 | 116 | 117 | 118 | 119 | 120 |

Prime numbers

https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes

# Early Algorithms: Sieve

**To find all the prime numbers ≤ a given integer $n$:**
**(using Eratosthenes' method)**

1. Create a list of consecutive integers from 2 through $n$:
   (2, 3, 4, ..., $n$).
2. Initially, let $p$ equal 2, the smallest prime number.
3. Enumerate the multiples of $p$ by counting to $n$ from $2p$ in increments of $p$, and mark them in the list
   (these will be $2p$, $3p$, $4p$, ...; the $p$ itself should not be marked).
4. Find the first number greater than $p$ in the list that is not marked. If there was no such number, stop. Otherwise, let $p$ now equal this new number (which is the next prime), and repeat from step 3.
5. When the algorithm terminates, the numbers remaining not marked in the list are all the primes below $n$.

# Sieve of Eratosthenes

**"Correctness Proof of the Algorithm:"**

The main idea here is that every value assigned to *p* will be prime, because if it were *composite* it would be marked (and thrown away) as a multiple of some other, smaller prime.

Note that some of the numbers may be marked more than once (e.g., 15 will be marked both for 3 and 5).

Next, we go
100 years
further back?

# Euclid's algorithm, 300 BC (1)

**Euclid gave an algorithm for GCD of 2 numbers**

**GCD** = Greatest Common Divisor

**Used Cool decomposition idea**
(based on simple math equation)

# Euclid's algorithm, 300 BC (2)

**Euclid gave an algorithm for GCD of 2 numbers**

**GCD** = Greatest Common Divisor

If GCD($P$, $Q$) = $x$
then $x$ divides $P$, and $x$ divides $Q$,
and $x$ is the greatest number with this property

**Example:** What is GCD(24, 60)?
D: divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24
D: divisors of 60: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60
CD: common divisors: 1, 2, 3, 4, 6, 12
GCD: greatest common divisor = **12**

# Euclid's decomposition method (1)

**Euclid's idea (extended):**

Assume $P \le Q$,

then $\text{GCD}(P, Q) = \text{GCD}(P, Q-P)$

Example: How to compute GCD(24, 60)?

$$\begin{aligned}\text{GCD}(24, 60) &= \text{GCD}(24, 36) && [36 = 60-24]\\ &= \text{GCD}(24, 12) && [12 = 36-24]\\ &= \text{GCD}(12, 12) && [12 = 24-12]\\ &= 12\end{aligned}$$

Can you "see" the decomposition?



Hon Wai Leong, SoC, NUS

# Exercise:

Can you turn the decomposition idea of Euclid into an algorithm?

Write out Euclid's method as an algorithm.

# Euclid's decomposition method (2)

**Euclid's idea (extended):**

Assume $P \le Q$,

then $\mathrm{GCD}(P, Q) = \mathrm{GCD}(P, (Q \bmod P))$

(A **mod** B) = "remainder when A is divided by B"

Example: How to compute GCD(24, 60)?

| | | |
|---|---|---|
| GCD(24, 60) | = GCD(24, 12) | 12=(60 mod 24) |
| | = GCD( 0, 12) | 0=(24 mod 12) |
| | = 12 | |

# References:

**One the Sieve of Eratosthenes (200 BC):**

https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes
http://www.geeksforgeeks.org/sieve-of-eratosthenes/
http://primes.utm.edu/glossary/xpage/sieveoferatosthenes.html

**Euclid's Algorithm (300 BC)**

https://en.wikipedia.org/wiki/Euclidean_algorithm
http://mathworld.wolfram.com/EuclideanAlgorithm.html
http://www.cut-the-knot.org/blue/Euclid.shtml

# *(End of video 6.3c)*

**If you want to contact me,**

**Email: leonghw@comp.nus.edu.sg**

NUS
National University of Singapore

School of Computing