Number Theory:
Primes

Adila A. Krisnadhi

Fakultas Ilmu Komputer, Universitas Indonesia

Version date: 2022-02-16 05:00:20+07:00
Reference: Rosen, Ed.8, Ch.4

Primes

Definition

An integer $p > 1$ is a **prime** iff p has exactly two positive factors, namely 1 and p.

An integer $n > 1$ that is not a prime is called a **composite**. So, n is a composite iff there exists an integer a with $1 < a < n$ such that $a \mid n$.

- The integer 1 is not a prime since it only has one positive factor.

Fundamental theorem of arithmetics

Why are primes important?

Fundamental theorem of arithmetics

Why are primes important?

Theorem (Fundamental theorem of arithmetics)

Every integer $n > 1$ can be written **uniquely** *as:*

- *a (single) prime; or*
- *a product of two or more primes (with duplicates allowed) such that those prime factors are written in an increasing order.*

The above theorem yields **prime factorization** of integers:

- $200 =$
- $641 =$
- $741 =$
- $899 =$
- $1024 =$

Determining if n is prime

Theorem

If n is a composite, then n has a prime factor that is less than or equal to $\sqrt{n}$.

Proof?

Determining if n is prime

Theorem

If n is a composite, then n has a prime factor that is less than or equal to $\sqrt{n}$.

Proof?

- To determine if n is prime, it suffices to divide n with all primes less than or equal to $\sqrt{n}$.
- If any of those primes divides n, then n is composite. Otherwise, n is prime.
- Example: Is 101 prime?

Sieve of Eratosthenes

Finding **all** primes that are less than or equal to a given positive integer n.

- List all integers from 2 to n.
- Cross out all multiples of 2 that is greater than 2.
- From the remaining numbers, the smallest and not crossed out is 3. So, cross out all multiples of 3 that is greater than 3.
- From the rest, the smallest and not crossed out is 5. So, cross out all multiples of 5 that is greater than 5.
- From the rest, the smallest and not crossed out is 7. So, cross out all multiples of 7 that is greater than 7.
- From the rest, the smallest and not crossed out is 11. So, cross out all multiples of 11 that is greater than 11.
- and so forth ..

Find all primes not exceeding 100.

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 many primes are there?

How many primes are there?

Theorem (from Euclid)

There are infinitely many primes.

Proof: