Prime numbers

February 4th, 2021

Introduction

Prime numbers play a crucial role in number theory: they are the integers greater than 1 which can't be factorized further while any other positive integer admits a unique expression as a product of prime numbers.

While negative integers are relatively new, prime numbers have been studied for quite a long time (maybe even before human beings developped writing systems).
All the results from today's lecture were already known in *Euclid's Elements* (circa 300BC).

Nonetheless, there are still many conjectures involving prime numbers which are easy to state but are still open (some despite several centuries of attempts), for instance:

- *Goldbach conjecture (1742):* any even natural number greater than 2 may be written as a sum of two prime numbers (e.g. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 5 + 5 = 7 + 3 \ldots$).
- *The twin prime conjecture (1849):* there are infinitely many prime numbers p such that $p + 2$ is also prime (e.g. $(3, 5)$, $(5, 7)$, $(11, 13) \ldots$).
- *Legendre conjecture (1912):* given $n \in \mathbb{N} \setminus \{0\}$, we may always find a prime number between n^2 and $(n + 1)^2$.

Definition

Definition: prime numbers

We say that a natural number p is a *prime number* if it has exactly two distinct positive divisors. A positive natural number with more than 2 positive divisors is said to be a *composite number*.

Remarks

- 0 is not a prime number since any natural number is a divisor of 0.
- 1 is not a prime number because it has only one positive divisor.

Hence $p \in \mathbb{N}$ is a prime number if and only if $p \geq 2$ and the only positive divisors of p are 1 and p.

Examples

The first prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97…

How to check whether a natural number is prime?

Proposition

A composite number a admits a positive divisor b such that $1 < b^2 \leq a$.

Proof. Write $a = b_1 b_2$ for two natural numbers b_1 and b_2 which are not equal to 1 or a. Assume by contradiction that both $b_1^2 > a$ and $b_2^2 > a$. Then

$$a^2 = (b_1 b_2)^2 = b_1^2 b_2^2 > a^2$$

Hence a contradiction. ∎

Example: 97 is a prime number

Since $10^2 = 100 > 97$, it is enough to check that none of 2, 3, 4, 5, 6, 7, 8 and 9 are divisors of 97.

Towards the fundamental theorem of arithmetic

Lemma

A natural number $n \geq 2$ has at least one prime divisor.

Proof.

We are going to prove with a strong induction that every natural number $n \geq 2$ has a prime divisor.

Base case at $n = 2$: 2 admits a prime divisor (itself).

Induction step: assume that the natural numbers $2, \dots, n$ admit a prime divisor for some $n \geq 2$.

- First case: $n + 1$ is a prime number, then it has a prime divisor (itself).
- Second case: $n + 1$ is a composite, then $n + 1 = ab$ where $a, b \in \mathbb{N}$ satisfy $1 < a, b < n + 1$.
  Since $2 \leq a \leq n$, a admits a prime divisor p by the induction hypothesis,
  i.e. $a = pk$ for some $k \in \mathbb{N}$.
  Then $n + 1 = ab = pkb$.
  Thus p is a prime divisor of $n + 1$.

Which proves the induction step. ■

How many prime numbers are there? – A lot!

Euclid's theorem

There are infinitely many prime numbers.

Proof. Assume by contradiction that there exist only finitely many prime numbers, namely:

$$p_1, p_2, \dots, p_n$$

Set $q = p_1 p_2 \cdots p_n + 1$.
Since q has a prime divisor, there exists $i \in \{1, 2, \dots, n\}$ such that $p_i | q$.
Then, since $p_i | p_1 p_2 \dots p_n$ and $p_i | q$, we have that

$$p_i | (q - p_1 p_2 \dots p_n) = 1$$

Therefore $p_i = 1$, which is a contradiction because 1 is not a prime number. ■

Euclid's lemma

Euclid's lemma

Let $a, b \in \mathbb{Z}$ and p be a prime number. If $p|ab$ then $p|a$ or $p|b$ (or both).

Proof. Let $a, b \in \mathbb{Z}$ and p be a prime number such that $p|ab$.
Assume that $p \nmid a$ then $\gcd(a, p) = 1$ since the only positive divisors of p are 1 and itself.
Hence, by Gauss' lemma, $p|b$. ■

The fundamental theorem of arithmetic – 1

The fundamental theorem of arithmetic

Any integer greater than 1 can be written as a product of primes, moreover this expression as a product of primes is unique up to the order of the prime factors.

Proof. **Existence.**
We are going to prove with a strong induction that $n \geq 2$ admits a prime factorization.
Base case for $n = 2$***:*** 2 is a prime number.
Induction step: assume that all the integers $2, 3, \ldots, n$ have a prime factorization for some $n \geq 2$.
We want to prove that $n + 1$ admits a prime factorization.
Since $n + 1$ admits a prime factor, there exist p prime and $k \in \mathbb{N} \setminus \{0\}$ such that $n + 1 = pk$.
If $k = 1$, then $n + 1 = p$. So we may assume that $k \geq 2$.
Since $1 < p$, we also have that $k < pk = n + 1$, i.e. $2 \leq k \leq n$.
Thus, by the induction hypothesis, k admits a prime factorization $k = p_1 p_2 \ldots p_l$.
Finally $n + 1 = p p_1 p_2 \ldots p_l$.

The fundamental theorem of arithmetic – 2

The fundamental theorem of arithmetic

Any integer greater than 1 can be written as a product of primes, moreover this expression as a product of primes is unique up to the order of the prime factors.

Proof. **Uniqueness.**
Assume by contradiction there exists an integer greater than 1 with two prime factorizations.
Denote by n the least such integer (which exists by the well-ordering principle).
Let $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ be two distinct prime factorizations of n.
By Euclid's lemma p_1 divides one of the q_j, WLOG assume that $p_1 | q_1$.
Since q_1 is a prime number, either $p_1 = 1$ or $p_1 = q_1$.
Thus $p_1 = q_1$ since p_1 is a prime number.
Therefore, by cancellation, $m = p_2 \dots p_r = q_2 \dots q_s$ has two distinct prime factorizations.
Note that $m > 1$ since otherwise $n = p_1 = q_1$.
But since $1 < p_1$ we get $m = p_2 \dots p_r < p_1 p_2 \dots p_r = n$.
Which is impossible since n is the least integer greater than 1 with two prime factorizations. ∎

The fundamental theorem of arithmetic – 3

Corollary

Any natural number $n \in \mathbb{N} \setminus \{0\}$ admits a unique expression

$$n = \prod_{p \text{ prime}} p^{\alpha_p}$$

where $\alpha_p \in \mathbb{N}$ (i.e. the α_p are uniquely determined).

Remarks

- The above product is finite since all but finitely many exponents are equal to 0.
- 1 is the special case when $\alpha_p = 0$ for all prime numbers p.

Example

$60798375 = 3^2 \times 5^3 \times 11 \times 17^3$

The fundamental theorem of arithmetic – 4

Corollary

Write $a = \prod_{p \text{ prime}} p^{\alpha_p}$ and $b = \prod_{p \text{ prime}} p^{\beta_p}$ with $\alpha_p, \beta_p \in \mathbb{N}$ all but finitely many equal to 0. Then

- $a|b$ if and only if for every prime number p, $\alpha_p \leq \beta_p$.
- $\gcd(a, b) = \prod_{p \text{ prime}} p^{\min(\alpha_p, \beta_p)}$.

Example

$\gcd(3^2 \times 5^3 \times 11 \times 17^3, 3 \times 5^5 \times 17^2 \times 23) = 3 \times 5^3 \times 17^2$

The fundamental theorem of arithmetic – 5

Corollary

Write $n = \prod_{p \text{ prime}} p^{\alpha_p}$ with $\alpha_p \in \mathbb{N}$ all but finitely many equal to 0.

Then the positive divisors of n are exactly the numbers of the form $n = \prod_{p \text{ prime}} p^{\gamma_p}$ with $0 \leq \gamma_p \leq \alpha_p$.

Particularly, n has $\prod_{p \text{ prime}} (\alpha_p + 1)$ positive divisors.