Number Theory: Prime Numbers

Ian Ludden

Learning Objectives

By the end of this lesson, you will be able to:

Learning Objectives

By the end of this lesson, you will be able to:

- Compute the prime factorization of (small) positive integers.

Learning Objectives

By the end of this lesson, you will be able to:

- Compute the prime factorization of (small) positive integers.
- State the Fundamental Theorem of Arithmetic.

Learning Objectives

By the end of this lesson, you will be able to:

- Compute the prime factorization of (small) positive integers.
- State the Fundamental Theorem of Arithmetic.
- Remember that there are infinitely many prime numbers.

Why study prime numbers?

Why study prime numbers?

Quote

"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate." – Euler

Why study prime numbers?

Quote

"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate." – Euler

Aside: https://projecteuler.net/

Why study prime numbers?

Quote

"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate." – Euler

Aside: https://projecteuler.net/

Prime numbers are:

- Fascinating

Why study prime numbers?

Quote

"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate." – Euler

Aside: https://projecteuler.net/

Prime numbers are:

- Fascinating
- Essential in cryptography

Why study prime numbers?

Quote

"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate." – Euler

Aside: https://projecteuler.net/

Prime numbers are:

- Fascinating
- Essential in cryptography
- Give us handy prime factorizations (short way of representing large integers)

Definition

Definition

Definition

An integer $q \geq 2$ is called *prime* if the only positive factors of q are q and 1.
An integer $q \geq 2$ is called *composite* if it is not prime.

Definition

Definition

An integer $q \geq 2$ is called *prime* if the only positive factors of q are q and 1.
An integer $q \geq 2$ is called *composite* if it is not prime.

Exercise

Rewrite the definition of prime in logical notation.
Let P denote the set of prime numbers.

biconditional "if and only if"

$$q \in P \leftrightarrow q \in \mathbb{Z} \wedge q \geq 2 \wedge (\forall y \in \mathbb{Z}, (y \geq 2 \wedge y \neq q) \to y \nmid q)$$

Special Cases

What about 0 and 1?

Special Cases

What about 0 and 1?
Neither prime nor composite

Special Cases

What about 0 and 1?
Neither prime nor composite

What about negative integers?

Special Cases

What about 0 and 1?
Neither prime nor composite

What about negative integers?
Neither prime nor composite

Prime Factorization

Prime Factorization

Definition

The *prime factorization* of an integer $q \geq 2$ is the expression of q as the product of one or more prime factors.

Prime Factorization

Definition

The *prime factorization* of an integer $q \geq 2$ is the expression of q as the product of one or more prime factors.

Examples

- $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$ ← canonical form

Prime Factorization

Definition

The *prime factorization* of an integer $q \geq 2$ is the expression of q as the product of one or more prime factors.

Examples

- $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$
- $210 = 2 \cdot 3 \cdot 5 \cdot 7$ $= 3 \cdot 2 \cdot 7 \cdot 5$

Prime Factorization

Definition

The *prime factorization* of an integer $q \geq 2$ is the expression of q as the product of one or more prime factors.

Examples

- $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$
- $210 = 2 \cdot 3 \cdot 5 \cdot 7$
- $91 = 7 \cdot 13$ = 13 · 7

Prime Factorization

Definition

The *prime factorization* of an integer $q \geq 2$ is the expression of q as the product of one or more prime factors.

Examples

- $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$
- $210 = 2 \cdot 3 \cdot 5 \cdot 7$
- $91 = 7 \cdot 13$
- $173 = 173$

Fundamental Theorem of Arithmetic

Theorem (Euclid)

Every integer greater than one has a ***unique*** ∗ *prime factorization.*

∗ Ignoring the order in which we write the factors

Infinitely Many Primes

Infinitely Many Primes

Theorem

There are infinitely many prime numbers.

Infinitely Many Primes

Theorem

There are infinitely many prime numbers.

Proof sketch

Suppose not. Let $p_1, p_2, p_3, \ldots, p_n$.

Let $p = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$.

$p_1 \nmid p, p_2 \nmid p, \ldots, p_n \nmid p \Rightarrow p$ is prime.

$\square$

Theorem

There are infinitely many prime numbers.

Proof sketch

Not a formula for generating primes...

Infinitely Many Primes

Theorem

There are infinitely many prime numbers.

Proof sketch

Not a formula for generating primes...

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510,511 = 19 \cdot 97 \cdot 277$

Recap: Learning Objectives

By the end of this lesson, you will be able to:

- Compute the prime factorization of (small) positive integers.
- State the Fundamental Theorem of Arithmetic.
- Remember that there are infinitely many prime numbers.