Primes

Primes

Definition: Suppose $n \in \mathbb{N}$.

Primes

Definition: Suppose $n \in \mathbb{N}$.

n is prime if $n > 1$ and the only factors of n are 1 and n.

Primes

Definition: Suppose $n \in \mathbb{N}$.

n is prime if $n > 1$ and the only factors of n are 1 and n.

n is composite if $n > 1$ and n is not prime.

Primes

Definition: Suppose $n \in \mathbb{N}$.

n is prime if $n > 1$ and the only factors of n are 1 and n.

n is composite if $n > 1$ and n is not prime.

(1 is neither prime nor composite.)

Primes

Definition: Suppose $n \in \mathbb{N}$.

n is prime if $n > 1$ and the only factors of n are 1 and n.

n is composite if $n > 1$ and n is not prime.

(1 is neither prime nor composite.)

The primes are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Prime factors

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Idea of proof: Use strong induction.

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Idea of proof: Use strong induction.

Inductive step:

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Idea of proof: Use strong induction.

Inductive step:
If n is prime, then n is a prime factor of n.

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Idea of proof: Use strong induction.

Inductive step:
If n is prime, then n is a prime factor of n. ✓

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Idea of proof: Use strong induction.

Inductive step:
If n is prime, then n is a prime factor of n. ✓

If n is not prime, then n has a factor b, where $1 < b < n$.

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Idea of proof: Use strong induction.

Inductive step:
If n is prime, then n is a prime factor of n. $\checkmark$

If n is not prime, then n has a factor b, where $1 < b < n$. By the inductive hypothesis b has a prime factor p.

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Idea of proof: Use strong induction.

Inductive step:
If n is prime, then n is a prime factor of n. ✓

If n is not prime, then n has a factor b, where $1 < b < n$. By the inductive hypothesis b has a prime factor p.

Now $p \mid b$ and $b \mid n$, so $p \mid n$.

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Idea of proof: Use strong induction.

Inductive step:
If n is prime, then n is a prime factor of n. ✓

If n is not prime, then n has a factor b, where $1 < b < n$. By the inductive hypothesis b has a prime factor p.

Now $p \mid b$ and $b \mid n$, so $p \mid n$. So p is a prime factor of n.

Prime factors

Lemma 4.3: If $n > 1$, then n has at least one prime factor.

Idea of proof: Use strong induction.

Inductive step:
If n is prime, then n is a prime factor of n. ✓

If n is not prime, then n has a factor b, where $1 < b < n$. By the inductive hypothesis b has a prime factor p.

Now $p \mid b$ and $b \mid n$, so $p \mid n$. So p is a prime factor of n. ✓

Prime factorisation

Prime factorisation

In fact n can be written as a product of primes. This is called the prime factorisation of n.

Prime factorisation

In fact n can be written as a product of primes. This is called the prime factorisation of n.

$$240 =$$

Prime factorisation

In fact n can be written as a product of primes. This is called the prime factorisation of n.

$$240 = 2$$

Prime factorisation

In fact n can be written as a product of primes. This is called the prime factorisation of n.

$$240 = 2 \times 2$$

Prime factorisation

In fact n can be written as a product of primes. This is called the prime factorisation of n.

$$240 = 2 \times 2 \times 2$$

Prime factorisation

In fact n can be written as a product of primes. This is called the prime factorisation of n.

$$240 = 2 \times 2 \times 2 \times 2$$

Prime factorisation

In fact n can be written as a product of primes. This is called the prime factorisation of n.

$$240 = 2 \times 2 \times 2 \times 2 \times 3$$

Prime factorisation

In fact n can be written as a product of primes. This is called the prime factorisation of n.

$$240 = 2 \times 2 \times 2 \times 2 \times 3 \times 5.$$

Prime factorisation

In fact n can be written as a product of primes. This is called the prime factorisation of n.

$$240 = 2 \times 2 \times 2 \times 2 \times 3 \times 5.$$

Fundamental Theorem of Arithmetic: The prime factorisation is unique up to re-ordering.

A famous proof

A famous proof

Theorem 4.4: There are infinitely many primes.

A famous proof

Theorem 4.4: There are infinitely many primes.

Idea of proof:

A famous proof

Theorem 4.4: There are infinitely many primes.

Idea of proof: by contradiction.

A famous proof

Theorem 4.4: There are infinitely many primes.

Idea of proof: by contradiction. Suppose there are finitely many primes

$$p_1, p_2, \ldots, p_m$$

A famous proof

Theorem 4.4: There are infinitely many primes.

Idea of proof: by contradiction. Suppose there are finitely many primes

$$p_1, p_2, \ldots, p_m$$

and let $n = p_1 p_2 \ldots p_m + 1$.

A famous proof

Theorem 4.4: There are infinitely many primes.

Idea of proof: by contradiction. Suppose there are finitely many primes

$$p_1, p_2, \ldots, p_m$$

and let $n = p_1 p_2 \ldots p_m + 1$. Then n has a prime factor, which must be p_k for some k.

A famous proof

Theorem 4.4: There are infinitely many primes.

Idea of proof: by contradiction. Suppose there are finitely many primes

$$p_1, p_2, \ldots, p_m$$

and let $n = p_1 p_2 \ldots p_m + 1$. Then n has a prime factor, which must be p_k for some k.
But now $p_k \mid n$ and $p_k \mid n - 1$, which is a contradiction.

Greatest common divisors

Greatest common divisors

Take $a, b \in \mathbb{N}$.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.

a and b are coprime if $\gcd(a, b) = 1$.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) =$

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) =$

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) = 5$.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) = 5$.
- $\gcd(100, 1005) =$

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) = 5$.
- $\gcd(100, 1005) = 5$.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) = 5$.
- $\gcd(100, 1005) = 5$.
- $\gcd(9457, 9458) =$

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) = 5$.
- $\gcd(100, 1005) = 5$.
- $\gcd(9457, 9458) = 1$.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) = 5$.
- $\gcd(100, 1005) = 5$.
- $\gcd(9457, 9458) = 1$.
- If a and b are primes and $a \neq b$, then $\gcd(a, b) = 1$.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) = 5$.
- $\gcd(100, 1005) = 5$.
- $\gcd(9457, 9458) = 1$.
- If a and b are primes and $a \neq b$, then $\gcd(a, b) = 1$.
- $\gcd(a, 1) = 1$ for any a.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) = 5$.
- $\gcd(100, 1005) = 5$.
- $\gcd(9457, 9458) = 1$.
- If a and b are primes and $a \neq b$, then $\gcd(a, b) = 1$.
- $\gcd(a, 1) = 1$ for any a.
- $\gcd(a, a) = a$ for any a.

Greatest common divisors

Take $a, b \in \mathbb{N}$. The greatest common divisor of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. Write this as $\gcd(a, b)$.
a and b are coprime if $\gcd(a, b) = 1$.

Examples

- $\gcd(9, 15) = 3$.
- $\gcd(55, 65) = 5$.
- $\gcd(100, 1005) = 5$.
- $\gcd(9457, 9458) = 1$.
- If a and b are primes and $a \neq b$, then $\gcd(a, b) = 1$.
- $\gcd(a, 1) = 1$ for any a.
- $\gcd(a, a) = a$ for any a.
- If $b \mid a$, then $\gcd(a, b) = b$.

Finding gcd (a, b)

Finding gcd (a, b) – slow method

Finding gcd (a, b) – slow method

Write down all the divisors of a and b, and find the highest number in both lists.

Finding gcd (a, b) – slow method

Write down all the divisors of a and b, and find the highest number in both lists.

$a = 72$, $b = 27$.

Finding gcd (a, b) – slow method

Write down all the divisors of a and b, and find the highest number in both lists.

$a = 72$, $b = 27$.
Divisors of 72:

$$1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72.$$

Finding gcd (a, b) – slow method

Write down all the divisors of a and b, and find the highest number in both lists.

$a = 72$, $b = 27$.
Divisors of 72:

$$1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72.$$

Divisors of 27:

$$1, 3, 9, 27.$$

Finding gcd (a, b) – slow method

Write down all the divisors of a and b, and find the highest number in both lists.

$a = 72$, $b = 27$.
Divisors of 72:

$$1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72.$$

Divisors of 27:

$$1, 3, 9, 27.$$

The highest number in both lists is 9.

Finding gcd (a, b) – slow method

Write down all the divisors of a and b, and find the highest number in both lists.

$a = 72$, $b = 27$.
Divisors of 72:

$$1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72.$$

Divisors of 27:

$$1, 3, 9, 27.$$

The highest number in both lists is 9.
So $\gcd(72, 27) = 9$.

Finding gcd (a, b) – slow method

Write down all the divisors of a and b, and find the highest number in both lists.

$a = 72$, $b = 27$.
Divisors of 72:

$$1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72.$$

Divisors of 27:

$$1, 3, 9, 27.$$

The highest number in both lists is 9.
So $\gcd(72, 27) = 9$.

This method is very slow.

Finding gcd (a, b)

Finding gcd (a, b) – better method

Finding gcd (a, b) – better method

If we write the prime factorisation of n, then every divisor arises by taking the product of some of the primes appearing.

Finding gcd (a, b) – better method

If we write the prime factorisation of n, then every divisor arises by taking the product of some of the primes appearing.

$$100 = 2 \times 2 \times 5 \times 5.$$

Finding gcd (a, b) – better method

If we write the prime factorisation of n, then every divisor arises by taking the product of some of the primes appearing.

$$100 = 2 \times 2 \times 5 \times 5.$$

Factors are

$$1,\ 2,\ 5,\ 2 \times 2,\ 2 \times 5,\ 5 \times 5,\ 2 \times 2 \times 5,\ 2 \times 5 \times 5,\ 2 \times 2 \times 5 \times 5.$$

Finding gcd (a, b) – better method

If we write the prime factorisation of n, then every divisor arises by taking the product of some of the primes appearing.

$$100 = 2 \times 2 \times 5 \times 5.$$

Factors are

$$1,\ 2,\ 5,\ 2 \times 2,\ 2 \times 5,\ 5 \times 5,\ 2 \times 2 \times 5,\ 2 \times 5 \times 5,\ 2 \times 2 \times 5 \times 5.$$

empty product $= 1$

Finding gcd (a, b) – better method

If we write the prime factorisation of n, then every divisor arises by taking the product of some of the primes appearing.

$$100 = 2 \times 2 \times 5 \times 5.$$

Factors are

$$1,\ 2,\ 5,\ 2 \times 2,\ 2 \times 5,\ 5 \times 5,\ 2 \times 2 \times 5,\ 2 \times 5 \times 5,\ 2 \times 2 \times 5 \times 5.$$

So to find gcd (a, b), write down the prime factorisations of a and b, and take the product of the primes appearing in both products.

Finding gcd (a, b) – better method

If we write the prime factorisation of n, then every divisor arises by taking the product of some of the primes appearing.

$$100 = 2 \times 2 \times 5 \times 5.$$

Factors are

$$1,\ 2,\ 5,\ 2 \times 2,\ 2 \times 5,\ 5 \times 5,\ 2 \times 2 \times 5,\ 2 \times 5 \times 5,\ 2 \times 2 \times 5 \times 5.$$

So to find gcd (a, b), write down the prime factorisations of a and b, and take the product of the primes appearing in both products.

$$120 = 2 \times 2 \times 2 \times 3 \times 5$$

Finding gcd (a, b) – better method

If we write the prime factorisation of n, then every divisor arises by taking the product of some of the primes appearing.

$$100 = 2 \times 2 \times 5 \times 5.$$

Factors are

$$1,\ 2,\ 5,\ 2 \times 2,\ 2 \times 5,\ 5 \times 5,\ 2 \times 2 \times 5,\ 2 \times 5 \times 5,\ 2 \times 2 \times 5 \times 5.$$

So to find gcd (a, b), write down the prime factorisations of a and b, and take the product of the primes appearing in both products.

$$120 = 2 \times 2 \times 2 \times 3 \times 5$$

So

$$\gcd(100, 120) = 2 \times 2 \times 5 = 20.$$

Finding gcd (a, b)

Finding gcd (a, b) – fast method

Finding gcd (a, b) – fast method

Lemma 4.5 ("dividing with remainder"): If $a, b \in \mathbb{N}$, then there are integers q, r such that $0 \leqslant r < b$ and $a = qb + r$.

Finding gcd (a, b) – fast method

Lemma 4.5 ("dividing with remainder"): If $a, b \in \mathbb{N}$, then there are integers q, r such that $0 \leqslant r < b$ and $a = qb + r$.

Proposition 4.6: If $a, b \in \mathbb{N}$ and $q, r \in \mathbb{Z}$ with $0 < r < b$ and $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.