Prime Factorizations
GCD & LCM

Adam Klepáč

January 15, 2024

Contents

Divisibility

Divisibility

We say that a number $n \in \mathbb{N}$ **is divisible** by $m \in \mathbb{N}$ or that m **divides** n

Divisibility

We say that a number $n \in \mathbb{N}$ **is divisible** by $m \in \mathbb{N}$ or that m **divides** n if there exists a number $q \in \mathbb{N}$ (called the **quotient**) such that

$$n = m \cdot q.$$

Divisibility

We say that a number $n \in \mathbb{N}$ **is divisible** by $m \in \mathbb{N}$ or that m **divides** n if there exists a number $q \in \mathbb{N}$ (called the **quotient**) such that

$$n = m \cdot q.$$

We write the fact that m divides n as $m \mid n$.

Divisibility

Even if m doesn't divide n, we can always at least **divide with remainder**.

Divisibility

Even if m doesn't divide n, we can always at least **divide with remainder**.

Formally, for every two numbers $n, m \in \mathbb{N}$, there always exist number $q \in \mathbb{N}$ and $r \leq n$ (called the **remainder**) such that

$$n = m \cdot q + r.$$

Integer Division & Modulus

- The operation which to a pair (n, m) assigns the **quotient** of the division of n by m is called **integer division** and denoted by div.

Integer Division & Modulus

- The operation which to a pair (n, m) assigns the **quotient** of the division of n by m is called **integer division** and denoted by div.
    - For example, $7 \operatorname{div} 2 = 3$ and $5 \operatorname{div} 9 = 0$.

Integer Division & Modulus

- The operation which to a pair (n, m) assigns the **quotient** of the division of n by m is called **integer division** and denoted by div.
    - For example, $7 \operatorname{div} 2 = 3$ and $5 \operatorname{div} 9 = 0$.
- The operation which to a pair (n, m) assigns the **remainder** of the division of n by m is called **modulus** and denoted $\bmod$.

Integer Division & Modulus

- The operation which to a pair (n, m) assigns the **quotient** of the division of n by m is called **integer division** and denoted by div.
  - For example, $7 \operatorname{div} 2 = 3$ and $5 \operatorname{div} 9 = 0$.
- The operation which to a pair (n, m) assigns the **remainder** of the division of n by m is called **modulus** and denoted $\bmod$.
  - For example, $7 \bmod 2 = 1$ and $5 \bmod 9 = 5$.

Integer Division & Modulus

Using integer division and modulus, we can write the operation of division with remainder like this:

$$n = m \cdot (n \operatorname{div} m) + n \bmod m.$$

Chinese Remainder Theorem

Counting Soldiers

The famous Chinese military general, strategist and philosopher 孙子 describes in his book 孙子兵法 an efficient method to count the number of soldiers.

Counting Soldiers

The famous Chinese military general, strategist and philosopher 孙子 describes in his book 孙子兵法 an efficient method to count the number of soldiers.
He instructs the soldiers to arrange into a grid with

- 21 soldiers in each row. He counts the number of soldiers remaining in the last row to be 3.

Counting Soldiers

The famous Chinese military general, strategist and philosopher 孙子 describes in his book 孙子兵法 an efficient method to count the number of soldiers.
He instructs the soldiers to arrange into a grid with

- 21 soldiers in each row. He counts the number of soldiers remaining in the last row to be 3.
- 25 soldiers in each row. He counts the number of soldiers remaining in the last row to be 6.

Counting Soldiers

The famous Chinese military general, strategist and philosopher 孙子 describes in his book 孙子兵法 an efficient method to count the number of soldiers.
He instructs the soldiers to arrange into a grid with

- 21 soldiers in each row. He counts the number of soldiers remaining in the last row to be 3.
- 25 soldiers in each row. He counts the number of soldiers remaining in the last row to be 6.
- 32 soldiers in each row. He counts the number of soldiers remaining in the last row to be 23.

Counting Soldiers

The famous Chinese military general, strategist and philosopher 孙子 describes in his book 孙子兵法 an efficient method to count the number of soldiers.
He instructs the soldiers to arrange into a grid with

- 21 soldiers in each row. He counts the number of soldiers remaining in the last row to be 3.
- 25 soldiers in each row. He counts the number of soldiers remaining in the last row to be 6.
- 32 soldiers in each row. He counts the number of soldiers remaining in the last row to be 23.

孙子 then determines, that there are 1431 soldiers standing before him.

1

Prime Factorization

Prime Number

Prime Number

A number $n \in \mathbb{N}$ is **prime** if it has **exactly two divisors** – 1 and itself.
We denote the set of all prime numbers by $\mathbb{P}$.

Decomposition Into Primes

Prime numbers are somewhat of a building blocks of other numbers.

Decomposition Into Primes

Prime numbers are somewhat of a building blocks of other numbers.

Each natural number decomposes **uniquely** into a product of prime numbers.

Decomposition Into Primes

Prime numbers are somewhat of a building blocks of other numbers.

Each natural number decomposes **uniquely** into a product of prime numbers.

Formally,

Prime Factorization

For each number $n \in \mathbb{N}$, there exist prime numbers $p_1, \ldots, p_m \in \mathbb{P}$ and powers $k_1, \ldots k_m \in \mathbb{N}$ such that

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}.$$

Decomposition Into Primes

Prime numbers are somewhat of a building blocks of other numbers.

Each natural number decomposes **uniquely** into a product of prime numbers.

Formally,

Prime Factorization

For each number $n \in \mathbb{N}$, there exist prime numbers $p_1, \ldots, p_m \in \mathbb{P}$ and powers $k_1, \ldots k_m \in \mathbb{N}$ such that

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}.$$

The numbers $p_1, \ldots, p_m$ are called the **prime factors** of n.

Decomposition Into Primes

Currently, there's no known fast algorithm how to decompose a number into its prime factors.

Decomposition Into Primes

Currently, there's no known fast algorithm how to decompose a number into its prime factors.
The best we can do is to try each prime number from 2 up to $\sqrt{n}$.

Decomposition Into Primes

Currently, there's no known fast algorithm how to decompose a number into its prime factors.

The best we can do is to try each prime number from 2 up to $\sqrt{n}$.

We divide the number in question as many times as possible and proceed to find the next prime factor of the resulting quotient.

Decomposition Into Primes – Example

Let's decompose the number 16335 into its prime factors.

Decomposition Into Primes – Example

Let’s decompose the number 16335 into its prime factors.

It’s as easy as keeping a table of all the prime factors we’ve divided the number by.

Decomposition Into Primes – Example

Let's decompose the number 16335 into its prime factors.

It's as easy as keeping a table of all the prime factors we've divided the number by.

Prime Factors	**Quotients**
3	5445

Decomposition Into Primes – Example

Let's decompose the number 16335 into its prime factors.

It's as easy as keeping a table of all the prime factors we've divided the number by.

Prime Factors	Quotients
3	5445
3	1815

Decomposition Into Primes – Example

Let's decompose the number 16335 into its prime factors.

It's as easy as keeping a table of all the prime factors we've divided the number by.

Prime Factors	Quotients
3	5445
3	1815
3	605

Decomposition Into Primes – Example

Let's decompose the number 16335 into its prime factors.

It's as easy as keeping a table of all the prime factors we've divided the number by.

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121

Decomposition Into Primes – Example

Let's decompose the number 16335 into its prime factors.

It's as easy as keeping a table of all the prime factors we've divided the number by.

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121
11	11

Decomposition Into Primes – Example

Let's decompose the number 16335 into its prime factors.

It's as easy as keeping a table of all the prime factors we've divided the number by.

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121
11	11
11	1

Decomposition Into Primes – Example

Let's decompose the number 16335 into its prime factors.

It's as easy as keeping a table of all the prime factors we've divided the number by.

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121
11	11
11	1

This means that $16335 = 3^3 \cdot 5 \cdot 11^2$.

Greatest Common Divisor

Greatest Common Divisor

Given two numbers $n, m \in \mathbb{N}$, their **Greatest Common Divisor** (GCD) or Highest Common Factor (HCF) is the largest natural number $k \in \mathbb{N}$ such that $k \mid n$ and $k \mid m$.

Greatest Common Divisor

The simplest (and most inefficient) way how to compute the GCD is to decompose the two numbers into prime factors and take all those that the two numbers have in common.

Greatest Common Divisor

The simplest (and most inefficient) way how to compute the GCD is to decompose the two numbers into prime factors and take all those that the two numbers have in common. For example, let's take a look at the decompositions of 16335 and 17325.

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121
11	11
11	1

Prime Factors	Quotients
3	5775
3	1925
5	385
5	77
7	11
11	1

Greatest Common Divisor

If we highlight the prime factors the two numbers share

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121
11	11
11	1

Prime Factors	Quotients
3	5775
3	1925
5	385
5	77
7	11
11	1

Greatest Common Divisor

If we highlight the prime factors the two numbers share

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121
11	11
11	1

Prime Factors	Quotients
3	5775
3	1925
5	385
5	77
7	11
11	1

we deduce that the GCD of 16335 and 17325 is

$$3^2 \cdot 5 \cdot 11 = 495.$$

Greatest Common Divisor

If we highlight the prime factors the two numbers share

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121
11	11
11	1

Prime Factors	Quotients
3	5775
3	1925
5	385
5	77
7	11
11	1

we deduce that the GCD of 16335 and 17325 is

$$3^2 \cdot 5 \cdot 11 = 495.$$

We'll denote the GCD of n and m as $\gcd(n, m)$ or simply as (n, m).

Least Common Multiple

Least Common Multiple

Given $n, m \in \mathbb{N}$ their **Least Common Multiple** (LCM) is the **smallest** number $k \in \mathbb{N}$ such that $n \mid k$ and $m \mid k$.

Least Common Multiple

Least Common Multiple

Given $n, m \in \mathbb{N}$ their **Least Common Multiple** (LCM) is the **smallest** number $k \in \mathbb{N}$ such that $n \mid k$ and $m \mid k$. It is given by the formula

$$\operatorname{lcm}(n, m) = \frac{n \cdot m}{\gcd(n, m)}.$$

Least Common Multiple

The other option how to calculate the least common multiple of two numbers is to take their prime factors elevated on the highest power that appears in at least one of the numbers.

Least Common Multiple

Explicitly, from the prime decompositions of 16335 and 17325

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121
11	11
11	1

Prime Factors	Quotients
3	5775
3	1925
5	385
5	77
7	11
11	1

Least Common Multiple

Explicitly, from the prime decompositions of 16335 and 17325

Prime Factors	Quotients
3	5445
3	1815
3	605
5	121
11	11
11	1

Prime Factors	Quotients
3	5775
3	1925
5	385
5	77
7	11
11	1

we see that their LCM is

$$3^3 \cdot 5^2 \cdot 7 \cdot 11^2 = 571725.$$

2

Congruence

Congruence

Congruence

Congruence is a relation between two natural numbers $n, m \in \mathbb{N}$ that says they have the same remainder when divided by some third number $k \in \mathbb{N}$.

Congruence

Congruence

Congruence is a relation between two natural numbers $n, m \in \mathbb{N}$ that says they have the same remainder when divided by some third number $k \in \mathbb{N}$.

Formally, we write that

$$n \equiv m \pmod{k}$$

and read it as 'n is congruent to m modulo k' if

$$n \bmod k = m \bmod k.$$

Congruence – Examples

For example,

- $14 \equiv 9 \pmod{5}$ because $9 \bmod 5 = 14 \bmod 5$;

Congruence – Examples

For example,

- $14 \equiv 9 \pmod{5}$ because $9 \bmod 5 = 14 \bmod 5$;
- $x \equiv 3 \pmod{6}$ is the same as saying $x \bmod 6 = 3$;

Congruence – Examples

For example,

- $14 \equiv 9 \pmod 5$ because $9 \bmod 5 = 14 \bmod 5$;
- $x \equiv 3 \pmod 6$ is the same as saying $x \bmod 6 = 3$;
- if $x \equiv 1 \pmod 3$, then the remainder of x after division by 3 is 1. This also means that $x = 3k + 1$ for some number $k \in \mathbb{N}$.

Systems Of Linear Congruences

- If we require that a number x satisfies more than one congruence, we call the resulting set of congruences a **system of linear congruences**.

Systems Of Linear Congruences

System Of Linear Congruences

If $k_1, \ldots, k_n, l_1, \ldots, l_n \in \mathbb{N}$, then the set of congruences

$$\begin{aligned} x &\equiv k_1 \pmod{l_1} \\ x &\equiv k_2 \pmod{l_2} \\ &\vdots \\ x &\equiv k_n \pmod{l_n} \end{aligned}$$

where $x \in \mathbb{N}$ is called a **system of linear congruences**.

3

Euclid's Algorithm

An Efficient Way to Calculate GCD

We can calculate the GCD of two numbers by using prime decompositions but that is too slow and cumbersome.

An Efficient Way to Calculate GCD

We can calculate the GCD of two numbers by using prime decompositions but that is too slow and cumbersome.

There's a method known as **Euclid's Algorithm** which is based on repeatedly taking the remainder after the division of the larger number by the smaller.

An Efficient Way to Calculate GCD

We can calculate the GCD of two numbers by using prime decompositions but that is too slow and cumbersome.

There's a method known as **Euclid's Algorithm** which is based on repeatedly taking the remainder after the division of the larger number by the smaller.

Concretely, let's say we want to calculate (x, y) and $x > y$. Then,

$$(x, y) = (x \bmod y, y).$$

An Efficient Way to Calculate GCD

Concretely, let's say we want to calculate (x, y) and $x > y$. Then,

$$(x, y) = (x \bmod y, y).$$

But why?

An Efficient Way to Calculate GCD

Concretely, let's say we want to calculate (x, y) and $x > y$. Then,

$$(x, y) = (x \bmod y, y).$$

But why?

Let's denote $g = (x, y)$ and $r = x \bmod y$. We need to make sure that $g \mid r$ and g is the largest number that divides both r and y.

An Efficient Way to Calculate GCD

Concretely, let's say we want to calculate (x, y) and $x > y$. Then,

$$(x, y) = (x \bmod y, y).$$

But why?

Let's denote $g = (x, y)$ and $r = x \bmod y$. We need to make sure that $g \mid r$ and g is the largest number that divides both r and y.

When we divide x by y, we get $x = q \cdot y + r$ for some $q \in \mathbb{N}$. We know that $g \mid x$ and so I can divide the whole equation by g and get natural numbers:

$$\frac{x}{g} = \frac{q \cdot y + r}{g}.$$

An Efficient Way to Calculate GCD

When we divide x by y, we get $x = q \cdot y + r$ for some $q \in \mathbb{N}$. We know that $g \mid x$ and so I can divide the whole equation by g and get natural numbers:

$$\frac{x}{g} = \frac{q \cdot y + r}{g}.$$

We also know that $g \mid y$ and so $q \cdot y/g \in \mathbb{N}$. We can write the right fraction like this:

$$\frac{q \cdot y + r}{g} = \frac{q \cdot y}{g} + \frac{r}{g}.$$

Because the left side is a natural number, so is the right. This means that $r/g \in \mathbb{N}$ and thus $g \mid r$.

An Efficient Way to Calculate GCD

When we divide x by y, we get $x = q \cdot y + r$ for some $q \in \mathbb{N}$. We know that $g \mid x$ and so I can divide the whole equation by g and get natural numbers:

$$\frac{x}{g} = \frac{q \cdot y + r}{g}.$$

We also know that $g \mid y$ and so $q \cdot y/g \in \mathbb{N}$. We can write the right fraction like this:

$$\frac{q \cdot y + r}{g} = \frac{q \cdot y}{g} + \frac{r}{g}.$$

Because the left side is a natural number, so is the right. This means that $r/g \in \mathbb{N}$ and thus $g \mid r$.

The fact that g is the **largest** common divisor of r and y is clear because if there was a larger number $g' > g$ that divided both y and r, then it would also divide $q \cdot y + r = x$.

Euclid's Algorithm

Euclid's Algorithm is a way to compute (x, y) for two natural numbers $x, y \in \mathbb{N}$.

Euclid's Algorithm

Euclid's Algorithm is a way to compute (x, y) for two natural numbers $x, y \in \mathbb{N}$. It goes like this:

1. If $x \geq y$, substitute $x := x \bmod y$. Otherwise, substitute $y := y \bmod x$.

Euclid's Algorithm

Euclid's Algorithm is a way to compute (x, y) for two natural numbers $x, y \in \mathbb{N}$.
It goes like this:

1. If $x \geq y$, substitute $x := x \bmod y$. Otherwise, substitute $y := y \bmod x$.
2. If $x = 0$, the answer is y. If $y = 0$, the answer is x. If $x, y \neq 0$, repeat step 1.

4

Chinese Remainder Theorem

Coprime Numbers

Coprime Numbers

We say that two numbers $n, m \in \mathbb{N}$ are **coprime** if $(n, m) = 1$, that is, if n and n have no common divisor besides 1.

Chinese Remainder Theorem

Chinese Remainder Theorem

If $l_1, \ldots, l_n \in \mathbb{N}$ are **mutually coprime** numbers and $k_1, \ldots, k_n \in \mathbb{N}$ are any natural numbers, then every system

$$\begin{aligned} x &\equiv k_1 \pmod{l_1} \\ x &\equiv k_2 \pmod{l_2} \\ &\vdots \\ x &\equiv k_n \pmod{l_n} \end{aligned}$$

of linear congruences has **exactly one solution** between 0 and $l_1 \cdot l_2 \cdot \ldots \cdot l_n$.