

Roots, powers, logarithms and modular arithmetic



Outline

Roots, powers, logarithms

Arithmetic n -th roots

Powers with real exponent

Logarithms

Approximations

Modular arithmetic

Roots, powers, logarithms



Introduction: Roots, powers, logarithms

- ▶ As a consequence of property R_4 we can perform, in the real field, operations that are only occasionally possible in the rational field, such as extracting roots or raising to a power.
- ▶ In this section we define **n -th roots**, **powers with real exponent** and **logarithms**, together with their properties
- ▶ Finally we discuss what it means to **approximate** an irrational number

Arithmetic n -th roots

Theorem 1

For every $y \in \mathbb{R}$, $y > 0$ and $n \in \mathbb{N}$, $n \geq 1$, there exists one and only one $x \in \mathbb{R}$, $x > 0$, such that $x^n = y$.

- ▶ This number is called the arithmetic n -th root of y and is denoted by one of the symbols

$$\sqrt[n]{y} \quad \text{or} \quad y^{\frac{1}{n}}.$$

Proof

The proof of this Theorem will be given using the properties of continuous functions. □

- ▶ The arithmetic n -th root is non-negative.

Example

Arithmetic n -th root. For example:

$$\sqrt{4} = 2, \quad \sqrt{9} = 3.$$

Moreover, we have:

$$\sqrt{x^2} = |x|$$

Decimal representation of the n -th root ($1/3$)

- ▶ We look for the decimal expansion of

$$\sqrt{2} \approx 1.41421356237$$

this number, not being rational, will be represented by an infinite (non-periodic) expansion.

- ▶ We proceed as follows: we build a class of rational numbers of the form:

$$\begin{aligned} 0 < a_0 < a_0, a_1 < a_0, a_1 a_2 < a_0, a_1 a_2 a_3 \\ < \dots < a_0, a_1 a_2 a_3 \dots a_n < \dots \end{aligned}$$

Decimal representation of the n -th root (2/3)

The rule is: each of these numbers is the largest among those with the same number of digits after the decimal point whose square is less than 2. The first of these numbers are:

$$\begin{array}{lll} 1 & 1^2 & = 1 \\ 1.4 & (1.4)^2 & = 1.96 \\ 1.41 & (1.41)^2 & = 1.9881 \\ 1.414 & (1.414)^2 & = 1.999396 \\ 1.4142 & (1.4142)^2 & = 1.99996164 \\ \dots & & \end{array}$$

- ▶ This set of numbers, which we call E_- , is bounded above (each one is < 2); by property R_4 it has a supremum, and this is used to define $\sqrt{2}$.
- ▶ The number $\sqrt{2}$ is defined precisely as $\sup E_-$

Decimal representation of the n -th root (3/3)

We could also have built a class of numbers E_+ like the previous one, with the rule that each of them is the smallest among those with the same number of digits after the decimal point whose square is greater than 2; we would have obtained:

$$\begin{array}{lll} 2 & 2^2 & = 4 \\ 1.5 & (1.5)^2 & = 2.25 \\ 1.42 & (1.42)^2 & = 2.0164 \\ 1.415 & (1.415)^2 & = 2.002225 \\ 1.4143 & (1.4143)^2 & = 2.00024449 \\ \dots & & \end{array}$$

This set E_+ is bounded below (every element is > 1), therefore it has an infimum; one proves that:

$$\sqrt{2} = \inf E_+ = \sup E_-$$

The numbers of the class E_- approximate $\sqrt{2}$ from below, those of the class E_+ from above.

Powers with rational exponent

Extracting the n -th root is the inverse operation of raising to an integer power.

Rational exponent

- ▶ The operation of raising to a power can be extended to every rational exponent if the base is positive (using the previous theorem).

$$\text{If } r = \frac{m}{n} \quad \text{and} \quad a > 0 \quad \text{then} \quad a^r = (a^m)^{\frac{1}{n}} = \sqrt[n]{a^m}$$

(we assume $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$ positive)

Powers with real exponent

Real exponent

- ▶ If the exponent is real, $b = b_0, b_1 b_2 b_3 \dots b_n \dots$, the number a^b ($a > 0$) will be determined by the class of numbers

$$a^{b_0} \quad a^{b_0, b_1} \quad a^{b_0, b_1 b_2} \quad \dots$$

in a way similar to the case of the root.

Negative base

If the base a is negative, the operation of raising to a power a^b is defined only in certain cases:

1. if the exponent b is an integer, or
2. if the exponent $b = \frac{n}{m}$ is rational, *in lowest terms*, provided that it is not the case that n is odd and m is even.

If $c < 0$ and m is odd, we define

$$\sqrt[m]{c} = -\sqrt[m]{-c}$$

Example

Negative base. For example:

$$(-2)^{\frac{3}{5}} = \sqrt[5]{(-2)^3} = \sqrt[5]{-8} = -\sqrt[5]{8}$$

$$(-2)^{\frac{2}{5}} = \sqrt[5]{(-2)^2} = \sqrt[5]{4}$$

The “lowest terms” assumption is essential: $\frac{1}{3}$ and $\frac{2}{6}$ are the same rational number, but

$$\sqrt[3]{(-8)^1} = -2 \quad \text{while} \quad \sqrt[6]{(-8)^2} = 2$$

- ▶ When we say “does not exist in $\mathbb{R}$ ” we mean that it is not possible to define this operation in such a way that the usual rules of computation remain valid.

Example

Non-existence of the power with real exponent. For example:

$$(-2)^{\frac{3}{4}}$$

does not exist in the real field!

Properties of powers (1/3)

Let

$$a, b \in \mathbb{R}, \quad a > 0 \quad \text{and} \quad b > 0 \quad (\text{positive reals})$$

and

$$c, d \in \mathbb{R} \quad (\text{arbitrary reals}),$$

the main properties of raising to a power are:

$$a^0 = 1 \quad \forall a \neq 0$$

$$1^c = 1 \quad \forall c$$

$$a^c > 0 \quad \forall c$$

$$a^c > 1 \quad \forall a > 1 \quad \text{and} \quad c > 0$$

$$a^c < 1 \quad \forall a < 1 \quad \text{and} \quad c > 0$$

Properties of powers (2/3)

$$a^{c+d} = a^c \cdot a^d$$

$$(a \cdot b)^c = a^c \cdot b^c$$

$$(a^b)^c = a^{b \cdot c}$$

Properties of powers (3/3)

$$c < d \Rightarrow a^c < a^d \text{ if } a > 1$$

$$c < d \Rightarrow a^c > a^d \text{ if } a < 1$$

$$0 < a \leq b \Rightarrow a^c \leq b^c \quad \forall c > 0$$

Logarithms

- ▶ Consider the equation

$$a^x = y, \quad a > 0$$

with y given and x unknown. First of all, if $a = 1$, it is solvable only if $y = 1$ (and in that case every real number x is a solution). So let $a \neq 1$.

- ▶ If $y \leq 0$ it has no solution, see property $a^c > 0 \forall c$.
- ▶ The following theorem tells us that it has exactly one solution for every $y > 0$.

Theorem 2

Let $a > 0$, $a \neq 1$, $y > 0$. There exists a unique real number x such that $a^x = y$.

- ▶ This number is called the logarithm to base a of y and is denoted by the symbol:

$$\log_a y$$

- ▶ The logarithm is the inverse operation of raising to a power.
- ▶ The logarithm of a number to a given base is the exponent to which the base must be raised to obtain the number itself.

Properties of logarithms (1/2)

Let

$x, y, a \in \mathbb{R}$, $x > 0, y > 0, a > 0$ (positive reals) and $a \neq 1$,

the main properties of logarithms are (they follow from those of exponentials):

$$\log_a(x \cdot y) = \log_a x + \log_a y$$

$$\log_a\left(\frac{x}{y}\right) = \log_a x - \log_a y$$

$$\log_a\left(\frac{1}{y}\right) = -\log_a y$$

Properties of logarithms (2/2)

$$\log_a x^\alpha = \alpha \log_a x \quad (\forall \alpha \in \mathbb{R})$$

$$\log_b x = \frac{\log_a x}{\log_a b} \quad (\forall b > 0, b \neq 1)$$

$$\log_a x = \frac{1}{\log_x a} = -\log_{\frac{1}{a}} x \quad (x \neq 1)$$

Notation

- ▶ $\lg n = \log_2 n \rightarrow$ **binary logarithm**
- ▶ $\ln n = \log_e n \rightarrow$ **natural logarithm** (where $e \approx 2.718$ is **Euler's number** (Napier's constant)) (sometimes the natural logarithm $\ln$ is also denoted by $\log$)
- ▶ $\lg^k n = (\lg n)^k \rightarrow$ **power**
- ▶ $\lg \lg n = \lg(\lg n) \rightarrow$ **composition**

Approximations

- ▶ A rational number can always be expressed with absolute precision, using either the fractional or the decimal notation (possibly with repeating digits).
- ▶ On the other hand, it is of course not possible to write all the decimal digits of an irrational number, since there are infinitely many of them and they follow one another without periodicity.
- ▶ What does it mean, then, to “know” or “specify” an irrational number? It means knowing some algorithm that allows us (at least in theory) to write as many exact decimal digits as we wish.

Example

Irrational numbers.

- ▶ In the (already considered) example of the irrational number:

$$0.101001000100001\dots$$

built according to the rule: write one digit 1, one digit 0, one digit 1, two digits 0, one digit 1, three digits 0, and so on) it is clear that we could write as many digits as we wish.

- ▶ In other cases, such as

$$\sqrt{2} \text{ or } \log_2 3,$$

things are more laborious and require iterative computations to determine each successive decimal digit; nevertheless, these computations can actually be carried out.

Numbers specified in a non-constructive way

- ▶ At other times, in Mathematical Analysis, a number is specified in a non-constructive way, by denoting it as the unique number that solves a given problem (once it has been proved that such a solution exists and is unique).
- ▶ This is a less satisfactory approach from an operational point of view, but theoretically flawless.

Practical aspects of computing irrational numbers

- ▶ Whenever we perform computations with a **pocket calculator**, it will only display numbers with a fixed number of decimal digits after the decimal point (typically 9). This means that we are working only with rational numbers, indeed with a finite subset of the set $\mathbb{Q}$.
- ▶ Working with a **computer** things improve somewhat, but we still remain within finite subsets of $\mathbb{Q}$. Of course, one needs to be aware of this.
- ▶ Besides the approximation produced by computing tools, sometimes we ourselves are not interested in too many decimal digits; we then deliberately introduce approximations, writing for example

$$\sqrt{2} \approx 1.414$$

Rounding rule

Rounding rule: the last digit written is rounded down (up) if the first digit discarded is from 0 to 4 (respectively, from 5 to 9).

Example

Rounding. For example:

$$2.4138 \approx 2.41$$

$$2.4152 \approx 2.42$$

Summary (1/2)

Roots:

- ▶ For $y > 0$, $n \geq 1$ there exists a unique $x > 0$ with $x^n = y$:
 $x = \sqrt[n]{y}$; moreover $\sqrt{x^2} = |x|$
- ▶ $\sqrt{2} = \sup E_- = \inf E_+$ (approximations from below and from above)

Powers:

- ▶ $a^{m/n} = \sqrt[n]{a^m}$ for $a > 0$; real exponent through decimal approximations
- ▶ Negative base: only integer exponents or rational $\frac{n}{m}$ in lowest terms, not with n odd and m even
- ▶ Properties: $a^{c+d} = a^c a^d$, $(ab)^c = a^c b^c$, $(a^b)^c = a^{bc}$,
monotonicity

Summary (2/2)

Logarithms:

- ▶ $\log_a y$ is the unique x with $a^x = y$ ($a > 0$, $a \neq 1$, $y > 0$)
- ▶ $\log_a(xy) = \log_a x + \log_a y$, $\log_a x^\alpha = \alpha \log_a x$, change of base
- ▶ Notation: $\lg$, $\ln$, $\lg^k n$, $\lg \lg n$

Approximations:

- ▶ An irrational number is “known” through an algorithm producing its digits
- ▶ Calculators and computers work on finite subsets of $\mathbb{Q}$; rounding rule

Modular arithmetic

Introduction: Modular arithmetic

- ▶ In this section we introduce the **integer part** (floor), the **fractional part** and the **upper integer part** (ceil)
- ▶ We will see some of their properties that are useful in computations
- ▶ We will define divisors, multiples, the **modulo** operation and **equivalence modulo n**
- ▶ These are fundamental tools in discrete mathematics and computer science

Definition 1: of integer part

Given a real number $a \in \mathbb{R}$, we denote by $[a]$ or $\lfloor a \rfloor$ the **integer part** (or “**floor**”) of a :

$$[a] = \text{integer } n \text{ such that } n \leq a < n + 1$$

- ▶ Equivalently, $[a]$ is the **largest** integer less than or equal to a :

$$[a] = \max \{ n \in \mathbb{Z} : n \leq a \}$$

- ▶ While for positive numbers the integer part is obtained simply by “throwing away the digits after the decimal point”, for negative numbers one must take the largest integer $\leq a$, which is different from what is obtained by throwing away the digits after the decimal point (except when a is already an integer)

Example

Integer part.

$$[2.38] = 2; \quad [3] = 3; \quad [-1.8] = -2.$$

Definition 2: of fractional part

Given a real number $a \in \mathbb{R}$, we denote by (a) the **fractional part** (or decimal part, in Italian “mantissa”) of a :

$$(a) = a - [a]$$

- ▶ The fractional part is therefore not an integer but a real number, lying in $[0, 1)$.
- ▶ For positive numbers, it is obtained simply by “throwing away the digits before the decimal point”; for negative numbers the fractional part is the **one's complement** of the number obtained by throwing away the digits before the decimal point.

Example

Fractional part.

$$(2.38) = 0.38; \quad (3) = 0; \quad (-1.8) = 0.2.$$

Definition 3: of upper integer part

Given a real number $a \in \mathbb{R}$, we denote by $\lceil a \rceil$ the **upper integer part** (or “*ceil*”) of a :

$$\lceil a \rceil = \text{integer } n \text{ such that } n - 1 < a \leq n$$

- Equivalently, $\lceil a \rceil$ is the **smallest** integer greater than or equal to a :

$$\lceil a \rceil = \min \{ n \in \mathbb{Z} : n \geq a \}$$

Example

Ceil.

$$\lceil 2.38 \rceil = 3; \quad \lceil 3 \rceil = 3; \quad \lceil -1.8 \rceil = -1.$$

Some properties (1/2)

Given a real number $a \in \mathbb{R}$, we have

$$a - 1 < \lfloor a \rfloor \leq a \leq \lceil a \rceil < a + 1$$

This follows at once from the two definitions: from $\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1$ and from $\lceil a \rceil - 1 < a \leq \lceil a \rceil$.

- ▶ We now look at how the integer part and the upper integer part behave with respect to the change of sign and with respect to integers
- ▶ These are the properties we will use to study the integer part functions

Change of sign and integers

Observation 1

For every real number $a \in \mathbb{R}$ we have

$$-\lfloor a \rfloor = \lceil -a \rceil \quad \text{and} \quad -\lceil a \rceil = \lfloor -a \rfloor$$

and moreover

$$\lfloor a \rfloor = a \iff a \in \mathbb{Z} \iff \lceil a \rceil = a$$

Proof

Set $n = \lfloor a \rfloor$, that is, $n \leq a < n + 1$. Multiplying by -1 :

$$n \leq a < n + 1 \implies (-n) - 1 < -a \leq -n$$

$$\implies \lceil -a \rceil = -n = -\lfloor a \rfloor$$

The second identity is obtained by applying the first one to the number $-a$.

If $\lfloor a \rfloor = a$ then $a \in \mathbb{Z}$, because $\lfloor a \rfloor$ is an integer; conversely, if $a \in \mathbb{Z}$ then $a \leq a < a + 1$, that is, $\lfloor a \rfloor = a$. The same holds for $\lceil a \rceil$. □

Characterizations (1/2)

Observation 2

For every $a \in \mathbb{R}$ and every $n \in \mathbb{Z}$ we have:

$$\lfloor a \rfloor = n \iff n \leq a < n + 1$$

$$\lfloor a \rfloor = n \iff a - 1 < n \leq a$$

$$\lceil a \rceil = n \iff n - 1 < a \leq n$$

$$\lceil a \rceil = n \iff a \leq n < a + 1$$

Characterizations (2/2)

Observation 3

For every $a \in \mathbb{R}$ and every $n \in \mathbb{Z}$ we also have:

$$a < n \iff \lfloor a \rfloor < n$$

$$n \leq a \iff n \leq \lfloor a \rfloor$$

$$a \leq n \iff \lceil a \rceil \leq n$$

$$n < a \iff n < \lceil a \rceil$$

and

$$\lfloor a + n \rfloor = \lfloor a \rfloor + n \quad \text{and} \quad \lceil a + n \rceil = \lceil a \rceil + n$$

Proof

The first four equivalences are the two definitions and their rewritings.

For $a < n \Leftrightarrow \lfloor a \rfloor < n$: if $a < n$ then $\lfloor a \rfloor \leq a < n$; conversely, if $\lfloor a \rfloor < n$, both being integers, $\lfloor a \rfloor \leq n - 1$ and hence $a < \lfloor a \rfloor + 1 \leq n$.

For $a \leq n \Leftrightarrow \lceil a \rceil \leq n$: if $a \leq n$, then n belongs to $\{k \in \mathbb{Z} : k \geq a\}$, whose minimum is $\lceil a \rceil$; conversely $a \leq \lceil a \rceil \leq n$.

The two equivalences on the right are obtained by negating both sides of the previous ones. □

Sum of floor and ceil

Given an integer $n \in \mathbb{Z}$, we have

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = n$$

Proof

We distinguish the two cases.

If $n = 2m$ is **even**, with $m \in \mathbb{Z}$:

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = \lfloor m \rfloor + \lceil m \rceil = m + m = 2m = n$$

If $n = 2m + 1$ is **odd**, with $m \in \mathbb{Z}$:

$$\begin{aligned} \left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil &= \left\lfloor m + \frac{1}{2} \right\rfloor + \left\lceil m + \frac{1}{2} \right\rceil \\ &= m + (m + 1) = 2m + 1 = n \end{aligned}$$



Some properties (2/2)

Given two positive integers $r, s \in \mathbb{Z}$, $r, s > 0$, we have

$$\left\lceil \frac{r}{s} \right\rceil \leq \frac{r + (s - 1)}{s}$$

$$\left\lfloor \frac{r}{s} \right\rfloor \geq \frac{r - (s - 1)}{s}$$

Given, in addition, a non-negative real number $p \in \mathbb{R}$, $p \geq 0$, we have

$$\left\lceil \frac{\left\lceil \frac{p}{r} \right\rceil}{s} \right\rceil = \left\lceil \frac{p}{rs} \right\rceil$$

$$\left\lfloor \frac{\left\lfloor \frac{p}{r} \right\rfloor}{s} \right\rfloor = \left\lfloor \frac{p}{rs} \right\rfloor$$

Definition 4: Divisor

A **divisor** of an integer $n \in \mathbb{Z}$, also called a **factor** of n , is an integer $m \in \mathbb{Z}$ that can be multiplied by some integer $q \in \mathbb{Z}$ to obtain n , i.e., if $n = q \cdot m$.

- ▶ If m is a divisor of n , n is a **multiple** of m .
- ▶ An integer n is **divisible** by another integer m if m is a *divisor* of n .
- ▶ For an integer $a \in \mathbb{Z}$ and a positive integer $n \in \mathbb{Z}$, $n > 0$, the value $a \bmod n$ is the remainder of the division $\frac{a}{n}$.

Definition 5: of modulo (remainder)

Given $a \in \mathbb{Z}$ and $n \in \mathbb{Z}, n > 0$,

$$a \bmod n = a - n \left\lfloor \frac{a}{n} \right\rfloor$$

► It follows that $0 \leq a \bmod n < n$

Equivalence modulo n

If $(a \bmod n) = (b \bmod n)$, we write

$$a \equiv b \pmod{n}$$

and we say that a is **equivalent** to b , modulo n .

- ▶ Equivalently, $a \equiv b \pmod{n}$ if a and b have the same remainder when divided by n .
- ▶ Equivalently, $a \equiv b \pmod{n}$ if and only if n is a divisor of $|b - a|$.

Example

For example, 23 and 13 are equivalent modulo 5 and we write

$$23 \equiv 13 \pmod{5}$$

Summary

- ▶ **Integer part** $\lfloor a \rfloor$: the integer n with $n \leq a < n + 1$ (pay attention to negative numbers)
- ▶ **Fractional part** $\{a\} = a - \lfloor a \rfloor \in [0, 1)$
- ▶ **Upper integer part** $\lceil a \rceil$: the integer n with $n - 1 < a \leq n$
- ▶ $a - 1 < \lfloor a \rfloor \leq a \leq \lceil a \rceil < a + 1$
- ▶ $-\lfloor a \rfloor = \lceil -a \rceil$ and $\lfloor a \rfloor = a \Leftrightarrow a \in \mathbb{Z} \Leftrightarrow \lceil a \rceil = a$
- ▶ $\lfloor a + n \rfloor = \lfloor a \rfloor + n$ and $\lceil a + n \rceil = \lceil a \rceil + n$ for $n \in \mathbb{Z}$
- ▶ $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$ for $n \in \mathbb{Z}$
- ▶ $a \bmod n = a - n\lfloor a/n \rfloor \in [0, n)$
- ▶ $a \equiv b \pmod{n}$ if and only if n divides $|b - a|$

Summary

- ▶ Thanks to property R_4 , in $\mathbb{R}$ the arithmetic n -th roots of positive numbers exist
- ▶ Powers extend to rational and real exponents (positive base), with algebraic and monotonicity properties
- ▶ The logarithm is the inverse operation of the power and turns products into sums
- ▶ Irrational numbers are specified through algorithms or in a non-constructive way; in practice they are approximated
- ▶ Integer part, fractional part, ceil and modulo are the tools of modular arithmetic