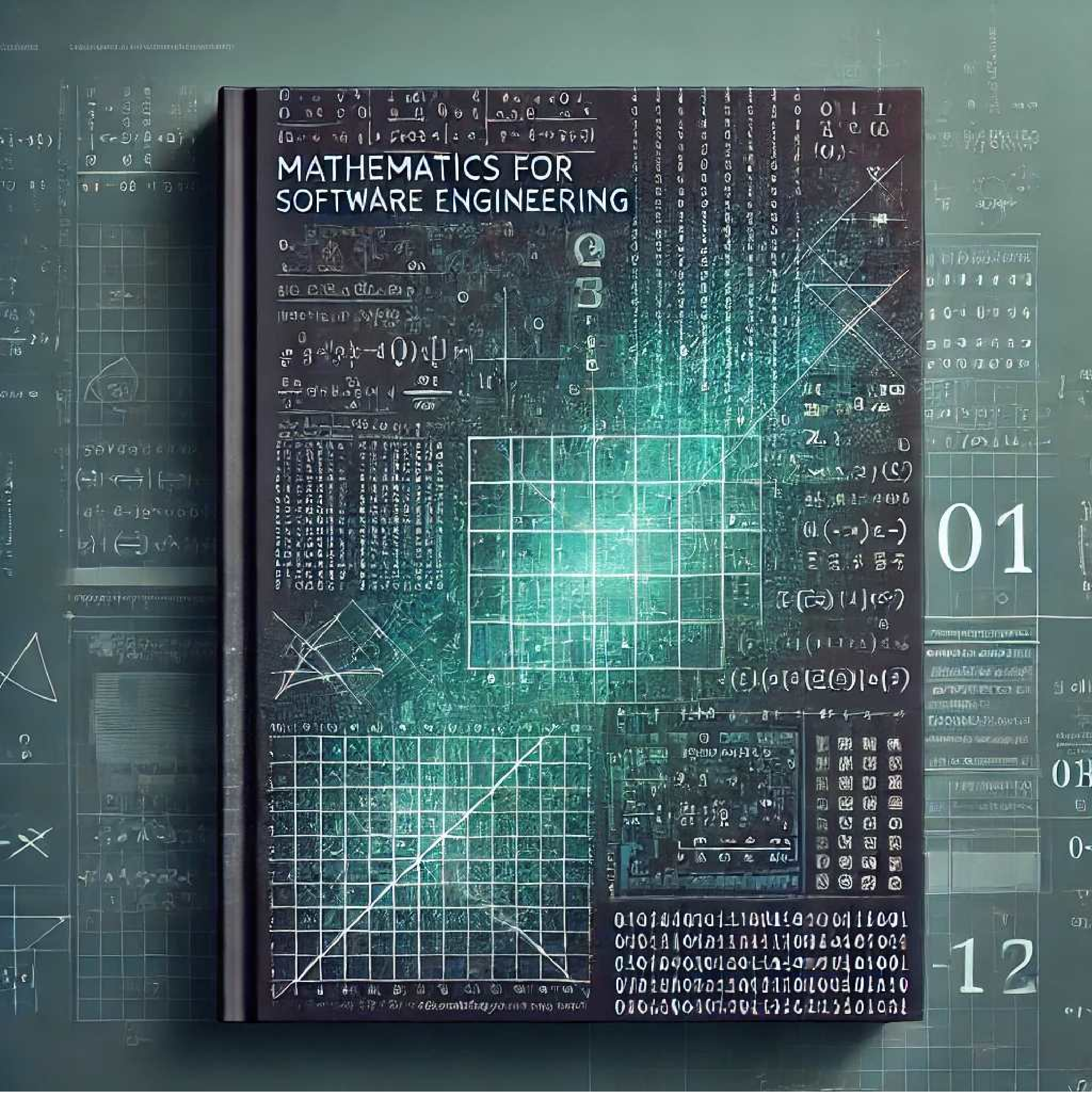


Mathematics for Software Engineering

Author: Richard Brooks

Date: August, 2024

Version: 1.0

Contents

Chapter 1 Basic Arithmetic and Functions

In the study of mathematics, a solid understanding of basic arithmetic operations and the concept of functions forms the foundation for more advanced topics. Arithmetic involves the manipulation of numbers through fundamental operations such as addition, subtraction, multiplication, and division. These operations are not only essential in everyday calculations but also serve as the building blocks for more complex mathematical procedures.

Functions, on the other hand, represent a crucial concept in mathematics, serving as a bridge between arithmetic and higher-level mathematical analysis. A function can be thought of as a special relationship between two sets, where each input (from the domain) is associated with exactly one output (from the co-domain). Understanding functions and their properties allows us to model and solve real-world problems with greater precision and flexibility.

In this section, we will explore the basic arithmetic rules and introduce the concept of functions, including their definitions, notations, and key properties. We will also discuss how these concepts are applied in various contexts, setting the stage for more advanced mathematical discussions.

1.1 Factorisation and the Order of Operations

Recall that when computing a product such as

$$a(b+c) = ab + ac$$

we distribute the factor a across each term inside the parentheses. We call this the **the distributive property**. However, it is often advantageous or necessary to perform the reverse operation, known as factorisation. Factorisation involves expressing the sum $ab + ac$ in its factored form $a(b + c)$.

Mathematically, the expression $a(b+c)$ is considered more simplified or "better" than $ab+ac$. To understand why, we must distinguish between **terms** and **factors**. Terms are separated by addition or subtraction, while factors are separated by multiplication or division. For instance, the expression

$$8 - 5 + 3$$

consists of three terms (8, -5, and 3), whereas the expression

$$2 \times 5 \times 3$$

consists of three factors (2, 5, and 3). Consider the expression

$$5 + 2 + 7 \times 8$$

which consists of three terms (5, 2, and 7×8), and note that one of the terms itself contains two factors (7 and 8). Similarly, the expression

$$5(2 + 4)(-9)$$

consists of three factors (5, $2 + 4$, and -9), with one factor, $2 + 4$, containing two terms.

The advantage of expressing mathematical expressions solely in terms of factors lies in the ability to simplify them more effectively. This concept will be elaborated throughout this chapter, especially when dealing with fractions and equations. Consider the following examples of factorisation:

$$8 - 5 + 3$$

consists of three terms (8, -5 and 3), while the expression

$$2 \times 5 \times 3$$

consists of three factors (2, 5 and 3). The expression

$$5 + 2 + 7 \times 8$$

consists of three terms (5, 2 and 7 × 8) and one of the terms consists of two factors (7 × 8), while the expression

$$5(2 + 4)(-9)$$

consists of three factors (5, (2 + 4), (-9)) and one of the factors consists of two terms ((2 + 4)).

It can be advantageous to express terms solely in factors because this allows us to simplify the expressions. This will become clearer as we progress through the lesson, and it is particularly important when working with fractions and equations. Here are some more examples of factorisation:

Example 1.1 Factorisation

$$\begin{aligned} ab - ac &= a(b - c) \\ -ab - ac &= a(-b - c) \\ -ab - ac &= -a(b + c) \\ ab - ac + aa - aa &= a(b - c + a - a) \\ abc - ab + aba &= ab(c - 1 + a) \\ ab - abc - a &= a(b - bc - 1) = b(1 - c) - 1 \end{aligned}$$

When evaluating mathematical expressions, it is crucial to follow a specific order of operations to ensure accurate results. The correct sequence for performing these operations is as follows:

1. **Brackets (Parentheses)**: First, perform all operations inside brackets or parentheses.
2. **Exponents and Radicals**: Next, evaluate exponents (powers) and radicals (roots).
3. **Multiplication and Division**: Then, perform multiplication and division from left to right as they appear.
4. **Addition and Subtraction**: Finally, execute addition and subtraction from left to right as they appear.

Let's consider examples for each operation to illustrate the order of operations:

Example 1.2 Brackets

Evaluate the expression: $(2+3)\times 4$

$$(2+3)\times 4 = 5\times 4 = 20$$

Example 1.3 Exponents and Radicals
Evaluate the expression: $3^2+\sqrt{16}$

$$3^2+\sqrt{16} = 9+4 = 13$$

Example 1.4 Multiplication and Division
Evaluate the expression: $6\div 2\times 3$. According to the standard order of operations, we perform division and multiplication from left to right:

$$6\div 2\times 3 = (6\div 2)\times 3 = 3\times 3 = 9$$

Example 1.5 Addition and Subtraction
Evaluate the expression: $8-3+2$

$$8-3+2 = 5+2 = 7$$

1.2 Fractions

By definition, a fraction always consists of (at least) two factors. The first factor we will call the **numerator** and is the "top part" of the fraction. The bottom part we will call the **denominator**. Perhaps the most important rule when working with fractions is that two fractions can only be added or subtracted if they have identical denominators. Also, the denominator must never be equal to 0.

Example 1.6

$$\frac{1}{x^2-2}$$

Here we must make sure that $x^2-2\neq 0$ which means that we may only use values different from $\pm\sqrt{2}$.

Definition 1.1 (Rules for Calculations Involving Fractions)

$\frac{a}{b}\times m = \frac{am}{b}$ where $b\neq 0$

$\frac{a}{b}\div m = \frac{a}{bm}$ where $b\neq 0$ and $m\neq 0$

$m\div\frac{a}{b} = m\times\frac{b}{a} = \frac{mb}{a}$ where $b\neq 0$ and $a\neq 0$

$\frac{a}{b}\times\frac{c}{a} = \frac{ac}{ba}$ where $b\neq 0$ and $a\neq 0$

$\frac{a}{b}\div\frac{c}{a} = \frac{a}{b}\times\frac{a}{c}$ where $b\neq 0$ and $a\neq 0$

$\frac{a}{b} = \frac{ac}{bc}$ where $b\neq 0$ and $c\neq 0$

$\frac{a}{b}+\frac{c}{a} = \frac{aa}{ba}+\frac{cb}{ba} = \frac{aa+cb}{ba}$ where $b\neq 0$ and $a\neq 0$

♣

To extend or reduce a fraction, we must multiply or divide by the same numbers in the denominator and numerator:

Example 1.7 Extending or reducing fractions

$$\frac{72}{144} = \frac{72 \div 12}{144 \div 12} = \frac{6}{12} = \frac{6 \div 6}{12 \div 6} = \frac{1}{2}$$

$$\frac{2}{3} = \frac{2 \times 6}{3 \times 6} = \frac{12}{18}$$

$$\frac{2x}{2xx} = \frac{2}{2x}$$

$$\frac{3a}{6a+3b} = \frac{3a}{3(2a+b)} = \frac{a}{2a+b}$$

To factorise an expression, all terms must be divided or multiplied uniformly. This implies that it is not possible to simplify the following expression any further, even though it might be tempting:

$$\frac{a}{2a+b} \neq \frac{1}{2+b}$$

For proper factorisation of $\frac{a}{2a+b}$, you must divide a into all terms in the denominator:

$$\frac{a}{2a+b} = \frac{1}{2+\frac{b}{a}}$$

As illustrated above, the multiplication of fractions is straightforward: you multiply the numerators and denominators with each other, respectively.

Example 1.8 Multiplication of fractions

Consider the fractions $\frac{a}{b}$ and $\frac{c}{d}$. Their product is:

$$\frac{a}{b} \times \frac{c}{d} = \frac{a \times c}{b \times d}$$

For instance, if $a = 2$, $b = 3$, $c = 4$, and $d = 5$, then:

$$\frac{2}{3} \times \frac{4}{5} = \frac{2 \times 4}{3 \times 5} = \frac{8}{15}$$

Example 1.9 Dividing fractions

$$\frac{6}{7} \div \frac{4}{21} = \frac{6}{7} \times \frac{21}{4} = \frac{126}{28} = \frac{63}{14} = \frac{9}{2}$$

$$\frac{1}{2} \div 3 = \frac{1}{2} \div \frac{3}{1} = \frac{1}{2} \times \frac{1}{3} = \frac{1}{6}$$

$$\frac{2}{3} \div \frac{8}{9} = \frac{2}{3} \times \frac{9}{8} = \frac{18}{24} = \frac{3}{4}$$

$$\frac{8}{9} \div 16 = \frac{8}{9} \times \frac{1}{16} = \frac{8}{144} = \frac{4}{72} = \frac{1}{18}$$

Adding and subtracting fractions seems to cause more problems than multiplication and division. The key is to find a common denominator between the fractions and then remember the above-mentioned rule about extending fractions.

Example 1.10 Adding and subtracting fractions

$$\frac{1}{5} + \frac{2}{5} = \frac{1+2}{5} = \frac{3}{5}$$

$$\frac{1}{4}+\frac{2}{3}=\frac{1\times 3}{4\times 3}+\frac{2\times 4}{3\times 4}=\frac{3}{12}+\frac{8}{12}=\frac{3+8}{12}=\frac{11}{12}$$

$$\frac{7}{12}-\frac{5}{8}=\frac{7\times 8}{12\times 8}-\frac{5\times 12}{8\times 12}=\frac{56}{96}-\frac{60}{96}=\frac{56-60}{96}=\frac{-4}{96}=\frac{-1}{24}$$

Note: Never do

$$\frac{a}{b}+\frac{c}{d}=\frac{a+b}{b+d}$$

Example 1.11

$$\frac{x}{x-1}\times\frac{2}{x(x+4)}=\frac{2x}{(x-1)x(x+4)}=\frac{2}{(x-1)(x+4)}$$

$$\frac{2}{x-1}\div\frac{x}{x-1}=\frac{2}{x-1}\times\frac{x-1}{x}=\frac{2(x-1)}{(x-1)x}=\frac{2}{x}$$

$$\frac{x+1}{x^2+2}+\frac{x-6}{x^2+2}=\frac{x+1+x-6}{x^2+2}=\frac{2x-5}{x^2+2}$$

Remember, when a fraction is preceded by a minus sign, all signs in the numerator must be changed accordingly. This is similar to how you would change all signs within parentheses when they are preceded by a minus sign.

Consider the expression:

$$-\frac{a-b}{c}$$

To correctly handle the negative sign, change all the signs in the numerator:

$$-\frac{a-b}{c}=\frac{-a+b}{c}$$

For example, if $a=5$ and $b=3$, then:

$$-\frac{5-3}{c}=\frac{-5+3}{c}=\frac{-2}{c}$$

Example 1.12

$$\frac{x+1}{x^2+2}-\frac{x-6}{x^2+2}=\frac{x+1-x+6}{x^2+2}=\frac{7}{x^2+2}$$

1.3 Exponents, Radicals and Surds

An **exponent** is a shortcut for repeated multiplication of the same number:

Example 1.13 Exponentiation

$$4\times 4\times 4\times 4\times 4=4^5$$

$$x\times x\times x\times x\times x=x^5$$

Radicals, or **roots**, represent the inverse operation of applying exponents. A radical is any number expressed with the radical symbol $\sqrt{}$. Specifically, applying a radical can reverse the effect of an exponent, and vice versa. For instance, squaring 2 yields 4, and taking the square root of 4 returns 2. Similarly, squaring 3 results in 9, and the square root of 9 brings us back to 3.

Example 1.14 Taking the root

$$\sqrt{a} \times \sqrt{a} = (\sqrt{a})^2 = a$$

$$\sqrt{a} = b \implies (\sqrt{a})^2 = b^2 \iff a = b^2$$

A **surd** is a type of radical that is both real and irrational, examples include $\sqrt{2}, \sqrt{3}, \sqrt{5}$, and $\sqrt{6}$.

Numbers can be raised to powers other than 2, such as cubing (raising to the third power), or even raising to the fourth power, the 100th power, and so forth. Correspondingly, you can take the cube root of a number, the fourth root, the 100th root, and so on. To indicate a root other than a square root, the same radical symbol is used, but with a number called the index inserted into the radical sign, typically positioned within the "check mark" part.

Example 1.15 Index and argument

$$4^3 = 64 \iff \sqrt[3]{64} = 4$$

In this example, the "3" inside the radical sign is the **index** of the radical. The "64" is referred to as the argument of the **radical**, also known as the **radicand**. Since square roots are the most common type of radicals, the index is usually omitted for square roots. Although "$\sqrt[2]{2}$" would be technically correct, it is rarely used in practice.

Definition 1.2 (Rules for calculations involving radicals)

$\sqrt[n]{xy} = \sqrt[n]{x} \times \sqrt[n]{y}$	where $x, y \geq 0$
$\sqrt[n]{\frac{x}{y}} = \frac{\sqrt[n]{x}}{\sqrt[n]{y}}$	where $x \geq 0$ and $y > 0$
$\sqrt{x^2} = \lvert x \rvert$	where $x \in \mathbb{R}$
$(\sqrt[n]{x})^n = x$	If $x < 0$ and $n \in \mathbb{N}$, then $\sqrt[n]{x}$ is not defined
$\sqrt[n]{-x} = -\sqrt[n]{x}$	where $x \geq 0$ and $n \in \mathbb{N}$ is odd

♣

Raising a number to a **power**, also known as **exponentiation**, is a fundamental mathematical operation that involves multiplying a number by itself a certain number of times as we saw above. The **base** is the number being multiplied, and the **exponent** indicates how many times the base is used as a factor. For example, a^n means that the base a is multiplied by itself n times. Exponentiation is a powerful tool in mathematics, with a few essential rules that govern its application.

Definition 1.3 (Rules for calculations involving exponents 1)

Let $n, m \in \mathbb{N}$. Then the following applies:

1. $x^n \cdot x^m = x^{n+m}$
2. $\dfrac{x^n}{x^m} = x^{n-m}$ $\qquad x \neq 0$
3. $x^n \cdot y^n = (x \cdot y)^n$
4. $\dfrac{x^n}{y^n} = \left(\dfrac{x}{y}\right)^n$ $\qquad y \neq 0$
5. $(x^n)^m = x^{n \cdot m}$
6. $x^1 = x$

♣

Some of these rules allow the concept of powers (Definition 1.4) to be extended so that the exponent may be any integer. If you set $n = m$ in rule (2), you get:

$$\frac{x^n}{x^n} = x^{n-n} = x^0$$

But since $\frac{x^n}{x^n} = 1$, we obtain

$$x^0 = 1$$

Thus, the concept of exponentiation is extended to include $n \in \mathbb{N} \cup \{0\}$. If you now set $n = 0$ again in rule (2), you get:

$$\frac{x^0}{x^m} = x^{0-m} = x^{-m}$$

But according to the previous calculation, $x^0 = 1$. Therefore, you obtain

$$\frac{1}{x^m} = x^{-m}$$

Since m is a positive number, $-m$ must be a negative number. Thus, the concept of exponentiation is extended to apply to all integers. This means that definition our concept of powers holds for $n \in \mathbb{Z}$ and that the rules in definition 1.4 apply for $n \in \mathbb{Z}$ and $m \in \mathbb{Z}$. As a consequence, the following rules can be added:

Definition 1.4 (Rules for calculations involving exponents 2)

Let $n \in \mathbb{Z}$. Then the following applies:

7. $x^0 = 1$ $\qquad x \neq 0$
8. $\dfrac{1}{x^m} = x^{-m}$ $\qquad x \neq 0$

♣

Let us illustrate these rules with a couple of examples.

Example 1.16 Reduce the following expression

$$\left(3xy^6\right)^3 = 3^3 \cdot x^3 \cdot \left(y^6\right)^3 = 27x^3y^{18}$$

Example 1.17 Reduce the following expression

$$\frac{a^{-4}b^3}{a^7b^{-5}} = \frac{a^{-4}}{a^7} \cdot \frac{b^3}{b^{-5}} = a^{-4-7} \cdot b^{3-(-5)} = a^{-11} \cdot b^8 = \frac{b^8}{a^{11}}$$

For positive numbers x, the concept of exponentiation an be further extended to apply when the exponent is a rational number. Any rational number $r \in \mathbb{Q}$ can be written as $r = \frac{m}{n}$, where $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. For $x > 0$, we now define

$$y = x^r = x^{\frac{m}{n}}$$

From this, you obtain (using, among other things, rule (5)):

$$y^n = \left(x^{\frac{m}{n}}\right)^n = x^{\frac{m}{n} \cdot n} = x^m$$

Finally, by using the concept of radicals, we obtain

$$y^n = x^m \qquad \Longleftrightarrow \qquad y = \sqrt[n]{x^m}$$

Note that because $x > 0$, it follows that $y > 0$ as well. We are now ready to state ***the extended concept of exponentiation***.

Definition 1.5 (The extended concept of exponentiation)

Let $m \in \mathbb{Z}$ and let $n \in \mathbb{N}$ such that $\frac{m}{n} \in \mathbb{Q}$. Then the following applies:

$$x^{\frac{m}{n}} = \sqrt[n]{x^m} \qquad x > 0$$

And more specifically, the following holds true

$$x^{\frac{1}{n}} = \sqrt[n]{x} \qquad x > 0$$

♣

The denominator of a rational exponent corresponds to the index of the radical, while the numerator remains as the exponent of the base. Conversely, the index of a radical can be transformed into the denominator of an exponent in an equivalent exponential expression. This property allows us to convert any radical expression into an exponential form, providing a powerful tool for simplification.

Example 1.18

$$\sqrt[5]{x^3} = x^{\frac{3}{5}} \quad \text{vs.} \quad \sqrt[3]{x^5} = x^{\frac{5}{3}}$$

$$\frac{1}{\sqrt[7]{x^3}} = x^{-\frac{3}{7}}$$

$$\frac{1}{\sqrt[3]{x^2}} = \left(x^2\right)^{-\frac{2}{3}}$$

This property can also be reversed: any rational exponent can be rewritten as a radical expression by using the denominator as the radical's index. The ability to interchange between exponential and radical forms enables us to evaluate expressions that were previously difficult to handle by converting them into radicals.

Example 1.19

$$27^{-\frac{4}{3}} = \frac{1}{\sqrt[3]{27^4}} = \frac{1}{\left(\sqrt[3]{27}\right)^4} = \frac{1}{3^4} = \frac{1}{81}$$

One of the greatest advantages of converting a radical expression into an exponential form is that it allows us to apply all the properties of exponents to simplify the expression. The following examples illustrate how various properties can be utilised to simplify expressions with rational exponents.

Example 1.20

$$a^{\frac{2}{3}}b^{\frac{1}{2}}a^{\frac{1}{6}}b^{\frac{1}{5}} = a^{\frac{2}{3}+\frac{1}{6}}b^{\frac{1}{2}+\frac{1}{5}} = a^{\frac{4}{6}+\frac{1}{6}}b^{\frac{5}{10}+\frac{2}{10}} = a^{\frac{5}{6}}b^{\frac{7}{10}}$$

$$\left(x^{\frac{1}{3}}x^{\frac{2}{5}}\right)^{\frac{3}{4}} = x^{\frac{1}{3}\times\frac{3}{4}}x^{\frac{2}{5}\times\frac{3}{4}} = x^{\frac{3}{12}}x^{\frac{6}{20}} = x^{\frac{1}{4}}x^{\frac{3}{10}}$$

$$\frac{x^{\frac{4}{2}}x^{\frac{4}{6}}x^{\frac{1}{2}}x^{\frac{5}{6}}}{x^{\frac{7}{2}}x^{0}} = 2x^{\frac{4}{2}+\frac{1}{2}}x^{\frac{4}{6}+\frac{5}{6}}x^{\frac{7}{2}} = 2x^{\frac{5}{2}}x^{\frac{9}{6}}x^{\frac{7}{2}} = 2x^{-1}x^{\frac{3}{2}} = 2x^{\frac{3}{2}}$$

$$\left(25x^{\frac{1}{3}}x^{\frac{2}{5}}\right)^{-\frac{1}{2}} = \left(25x^{\frac{5}{15}}x^{\frac{4}{10}}\right)^{-\frac{1}{2}} = \left(25x^{-\frac{7}{15}}x^{\frac{19}{10}}\right)^{-\frac{1}{2}} = \left(\frac{9}{25x^{-\frac{7}{15}}x^{\frac{19}{10}}}\right)^{\frac{1}{2}} = \frac{9}{2}\cdot 25x^{-\frac{7}{30}}x^{\frac{19}{20}} = \frac{3x^{\frac{7}{30}}}{5x^{\frac{19}{20}}}$$

It is important to remember that when simplifying expressions with rational exponents, we are applying the same exponent rules that are used for integer exponents. The only difference is that we must also adhere to the rules for fractions.

1.4 Using Formulae and Substitution

In the study of engineering, physical quantities are often related to each other through formulas. These formulas consist of variables and constants that represent the physical quantities in question. To evaluate a formula, one must substitute numerical values for the variables.

For example, Ohm's law provides a formula that relates the voltage, v, across a resistor with a resistance value R, to the current i flowing through it. The formula is given by

$$v = iR$$

This formula allows us to calculate the voltage v if the values for i and R are known. For instance, if $i = 13\,\mathrm{A}$ and $R = 5\,\Omega$, then

$$v = iR = (13)(5) = 65$$

Thus, the voltage is 65 V.

This example highlights the importance of paying close attention to the units of any physical quantities involved. A formula is only valid if a consistent set of units is used.

Example 1.21 Inserting into formulae

The kinetic energy K of an object with mass M moving at speed v can be calculated using the formula:

$$K = \frac{1}{2}Mv^2$$

Calculate the kinetic energy of an object with a mass of 5 kg moving at a speed of $2\,\mathrm{m\,s^{-1}}$.

Solution:

$$K = \frac{1}{2}Mv^2 = \frac{1}{2}(5)(2^2) = 10$$

◀

In the SI system, the unit of energy is the joule, so the kinetic energy of the object is 10 joules.

Example 1.22 Inserting into formulae
The area A of a circle with radius r can be calculated using the formula $A = \pi r^2$.

Alternatively, if the diameter d of the circle is known, the equivalent formula can be used:

$$A = \frac{\pi d^2}{4}$$

Calculate the area of a circle with a diameter of 0.1 m. The value of π is pre-programmed in your calculator.

Solution:

$$A = \frac{\pi (0.1)^2}{4} = 0.00785\,\mathrm{m}^2$$

◀

Example 1.23 Inserting into formulae
The volume V of a circular cylinder is equal to its cross-sectional area A multiplied by its length h.

Calculate the volume of a cylinder with a diameter of 0.1 m and a length of 0.3 m.

Solution:

$$V = Ah = \frac{\pi (0.1)^2}{4} \times 0.3 = 0.00236$$

The volume is $0.00236\,\mathrm{m}^3$. ◀

1.5 Rearranging Formulae

In the formula for the area of a circle, $A = \pi r^2$, the variable A is referred to as the subject of the formula. A variable is considered the subject if it appears by itself on one side of the equation, usually on the left-hand side, and nowhere else in the formula. If we are asked to transpose the formula for r, or solve for r, we must rearrange the equation so that r becomes the subject. When transposing a formula, any operation performed on one side must also be applied to the other side. There are five key rules to follow during this process.

Rules for rearranging formulae

The following operations can be performed on both sides of the formula:

- Add the same quantity to both sides
- Subtract the same quantity from both sides
- Multiply both sides by the same quantity - remember to multiply all terms
- Divide both sides by the same quantity - remember to divide all terms
- Apply a function to both sides, such as squaring or finding the reciprocal

Example 1.24 Transpose the formula $p = 5t - 17$ to make t the subject.

Solution: To isolate t on the left-hand side, proceed in steps using the five rules. First, add 17 to both sides of the equation $p = 5t - 17$:

$$p + 17 = 5t - 17 + 17$$

Simplifying, we get:

$$p + 17 = 5t$$

Next, divide both sides by 5 to isolate t:

$$\frac{p + 17}{5} = t$$

Thus, the formula for t is:

$$t = \frac{p + 17}{5}$$

◀

Example 1.25 Transpose the formula $\sqrt{2q} = p$ to solve for q.

Solution: First, square both sides to eliminate the square root around $2q$. Note that $(\sqrt{2q})^2 = 2q$. This gives:

$$2q = p^2$$

Next, divide both sides by 2 to solve for q:

$$q = \frac{p^2}{2}$$

◀

Problem 1.1 Transpose the formula $v = \sqrt{t^2 + w}$ to solve for w. To isolate w, follow these steps:

a. First, square both sides to eliminate the square root around $t^2 + w$:
$$v^2 = t^2 + w$$
b. Next, subtract t^2 from both sides to isolate w:
$$v^2 - t^2 = w$$
c. Finally, write down the formula for w:
$$w = v^2 - t^2$$

Example 1.26 Transpose the formula $x = \frac{1}{y}$ to solve for y.

Solution: To isolate y, notice that y appears in the denominator. Multiplying both sides by y removes the fraction:

$$yx = y \times \frac{1}{y}$$

This simplifies to:

$$yx = 1$$

Finally, divide both sides by x to solve for y:

$$y = \frac{1}{x}$$

Alternatively, you can simply invert both sides directly to obtain:

$$y = \frac{1}{x}$$

◀

Example 1.27 Make R the subject of the formula:

$$\frac{2}{R} = \frac{3}{x+y}$$

Solution: Since R appears in a fraction, invert both sides:

$$\frac{R}{2} = \frac{x+y}{3}$$

Multiplying both sides by 2 yields: $R = \dfrac{2(x+y)}{3}$ ◀

Example 1.28 Make R the subject of the formula:

$$\frac{1}{R} = \frac{1}{R_1} + \frac{1}{R_2}$$

Solution: The two terms on the right-hand side can be combined:

$$\frac{1}{R_1} + \frac{1}{R_2} = \frac{R_2 + R_1}{R_1 R_2}$$

The formula then becomes:

$$\frac{1}{R} = \frac{R_2 + R_1}{R_1 R_2}$$

Finally, inverting both sides gives:

$$R = \frac{R_1 R_2}{R_2 + R_1}$$

◀

1.6 Functions

In mathematics, a function assigns each element of one set to a specific element of another set (which may be the same set). For example, consider a Mathematics for Software Engineering class where each student is assigned a grade from the set $\{12, 10, 7, 4, 02\}$. Suppose the grades are as follows:

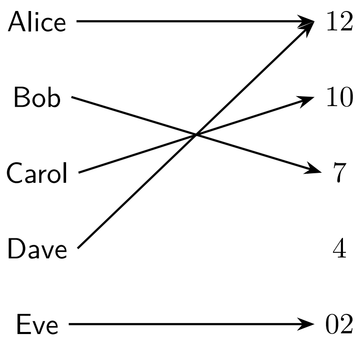


Figure 1.1: Example of a function mapping names to numbers.

This assignment of grades, illustrated in figure 1.1, exemplifies a function.

Functions play a crucial role in mathematics and computer science. They define discrete structures such as sequences and strings and are used to analyse the time complexity of algorithms. Many computer programs are designed to compute values of functions. Recursive functions, defined in terms of themselves, are especially significant in computer science. This section provides an overview of the fundamental concepts of functions needed in the mathematics for software engineering.

Definition 1.6

Let A and B be nonempty sets. A function f from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write $f : A \to B$. ♣

Remark: Functions are sometimes also called mappings or transformations.

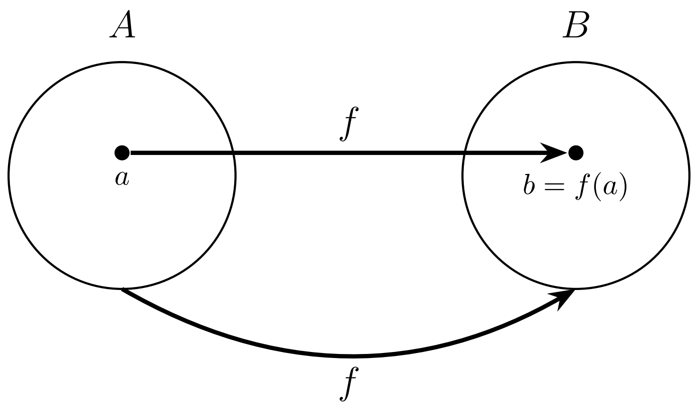


Figure 1.2: A function f mapping an element a from set A to an element $b = f(a)$ in set B.

Functions can be specified in various ways. Sometimes, we explicitly state the assignments, as shown in Figure 1.1. Often, a formula such as $f(x) = x + 1$ is used to define a function. In other cases, a computer program may specify the function.

Definition 1.7

If f is a function from A to B, we say that A is the **domain** of f and B is the **co-domain** of f. If $f(a) = b$, we say that b is the **image** of a and a is a **preimage** of b. The **range**, or image, of f is the set of all images of elements of A. Also, if f is a function from A to B, we say that f **maps** A to B. ♣

When defining a function, we specify its domain, co-domain, and the mapping of elements from the domain to the co-domain. Two functions are equal if they have the same domain, the same co-domain, and map each element of their domain to the same element in the co-domain.

It's important to note that altering the domain or co-domain results in a different function. Similarly, changing the mapping of elements also produces a different function.

The following examples illustrate various functions. In each example, we describe the domain, co-domain, range, and the assignment of values to the elements of the domain.

Example 1.29 What are the domain, co-domain, and range of the function that assigns grades to students described in the first paragraph of the introduction of this section?

Solution: Let G be the function that assigns a grade to a student in our Software engineering mathematics class. Note that $G(\text{Alice}) = 12$, for instance. The domain of G is the set {Alice, Bob, Carol, David, Eve }, and the co-domain is the set $\{12, 10, 7, 4, 02\}$. The range of G is the set $\{12, 10, 7, 02\}$, because each grade except 4 is assigned to some student. ◀

Example 1.30 Let f be the function that assigns the last two bits of a bit string of length 2 or greater to that string. For example, $f(11010) = 10$. Then, the domain of f is the set of all bit strings of length 2 or greater, and both the co-domain and range are the set $\{00, 01, 10, 11\}$.

Example 1.31 Let $f : \mathbb{Z} \to \mathbb{Z}$ assign the square of an integer to this integer. Then, $f(x) = x^2$, where the domain of f is the set of all integers, the co-domain of f is the set of all integers, and the range of f is the set of all integers that are perfect squares, namely, $\{0, 1, 4, 9, \ldots\}$.

One-to-One and Onto Functions

In mathematics, functions are a fundamental concept used to describe the relationship between two sets. However, not all functions behave the same way. To understand these differences, we introduce the concepts of one-to-one (injective) and onto (surjective) functions.

Some functions never assign the same value to two different domain elements. These functions are said to be **one-to-one**.

Definition 1.8 (One-to-One functions (Injective))

A function $f : A \to B$ is called **one-to-one** (or **injective**) if different elements in A map to different elements in B. In other words, if $f(a_1) = f(a_2)$, then $a_1 = a_2$. This property ensures that no two distinct elements in A are mapped to the same element in B. ♣

Graphically, a function is one-to-one if no horizontal line intersects the graph of the function at more than one point.

Definition 1.9 (Onto Functions (Surjective))

A function $f : A \to B$ is called **onto** (or **surjective**) if every element in B is the image of at least one element in A. In other words, for every $b \in B$, there exists at least one $a \in A$ such that $f(a) = b$. This property ensures that the function "covers" the entire set B. ♣

Inverse Functions

Now, consider a function $f : A \to B$ that is both one-to-one and onto. Because f is onto, every element of B is the image of some element in A. Furthermore, because f is one-to-one, every element of B is the image of a unique element of A. This unique correspondence allows us to define a new function from B to A that "reverses" the mapping given by f.

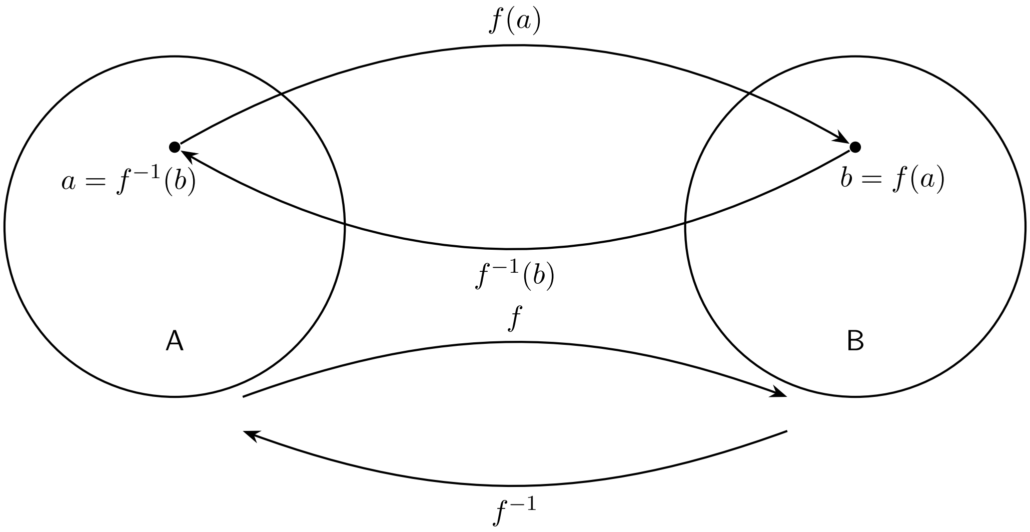


Figure 1.3: The function f^{-1} is the inverse of function f.

This new function is called the **inverse function** of f, denoted by $f^{-1} : B \to A$. The inverse function

f^{-1} satisfies the following properties:

$$f(f^{-1}(b)) = b \quad \text{for every } b \in B.$$

$$f^{-1}(f(a)) = a \quad \text{for every } a \in A.$$

We can summarise these considerations in the following definition

Definition 1.10 (Inverse Functions)

Let f be a one-to-one correspondence from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$. The inverse function of f is denoted by f^{-1}. Hence, $f^{-1}(b) = a$ when $f(a) = b$. ♣

These properties show that f^{-1} effectively undoes the work of f, mapping each element of B back to the corresponding element in A.

Example 1.32

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x + 3$. We can check that f is both one-to-one and onto:

- **One-to-One**: If $f(x_1) = f(x_2)$, then $2x_1 + 3 = 2x_2 + 3$. Subtracting 3 from both sides gives $2x_1 = 2x_2$, and dividing by 2 yields $x_1 = x_2$. Thus, f is one-to-one.
- **Onto**: Given any $y \in \mathbb{R}$, we can solve $y = 2x + 3$ for x to find $x = \frac{y-3}{2}$. Since this x exists for every y, f is onto.

Since f is both one-to-one and onto, it has an inverse function f^{-1} defined by

$$f^{-1}(y) = \frac{y-3}{2}.$$

Composite Functions

In mathematics, functions can be combined to form new functions. One important way of combining functions is through the composition of functions. The composite of two functions is essentially applying one function to the results of another.

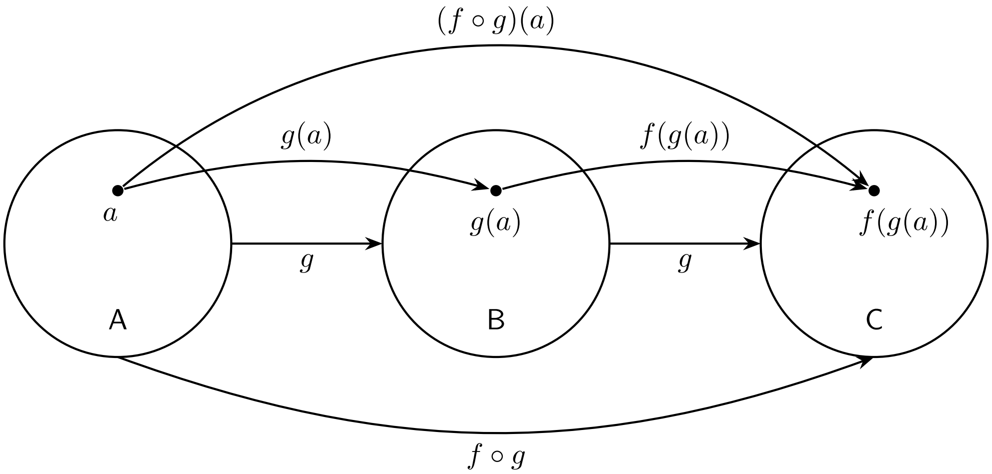


Figure 1.4: The composition of f and g.

Definition 1.11

Let $f : B \to C$ and $g : A \to B$ be two functions. The **composite function** of f and g, denoted by $f \circ g$, is a function from A to C defined by

$$(f \circ g)(x) = f(g(x)),$$

for every $x \in A$. ♣

In other words, the composite function $f \circ g$ means that you first apply the function g to the input x, and then apply the function f to the result of $g(x)$. In figure 1.4 the composition of functions is shown.

Example 1.33

Consider the functions $f(x) = 2x + 3$ and $g(x) = x^2$. The composite function $f \circ g$ is given by:

$$(f \circ g)(x) = f(g(x)) = f(x^2) = 2x^2 + 3.$$

Here, the function $g(x)$ squares the input x, and then the function $f(x)$ multiplies the result by 2 and adds 3.

Now, let's reverse the composition and compute $g \circ f$:

$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = (2x + 3)^2.$$

Notice that $f \circ g$ and $g \circ f$ are generally different functions, illustrating that the composition of functions is not commutative.

Example 1.34 Let g be the function from the set $\{a, b, c\}$ to itself such that $g(a) = b, g(b) = c$, and $g(c) = a$. Let f be the function from the set $\{a, b, c\}$ to the set $\{1, 2, 3\}$ such that $f(a) = 3, f(b) = 2$, and $f(c) = 1$. What is the composition of f and g, and what is the composition of g and f ?

Solution: The composition $f \circ g$ is defined by $(f \circ g)(a) = f(g(a)) = f(b) = 2$, $(f \circ g)(b) = f(g(b)) = f(c) = 1$, and $(f \circ g)(c) = f(g(c)) = f(a) = 3$.

Note that $g \circ f$ is not defined, because the range of f is not a subset of the domain of g. ◀

Example 1.35 label: Let f and g be the functions from the set of integers to the set of integers defined by $f(x) = 2x + 3$ and $g(x) = 3x + 2$. What is the composition of f and g ? What is the composition of g and f?

Solution: Both the compositions $f \circ g$ and $g \circ f$ are defined. Moreover,

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

and

$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11.$$

◀

Remark: Even though $f \circ g$ and $g \circ f$ are defined for the functions f and g in example 35, $f \circ g$ and $g \circ f$ are not equal. In other words, the commutative law does not hold for the composition of functions.

When the composition of a function and its inverse is formed, in either order, an identity function is obtained. To see this, suppose that f is a one-to-one correspondence from the set A to the set B. Then the inverse function f^{-1} exists and is a one-to-one correspondence from B to A. The inverse function reverses the correspondence of the original function, so $f^{-1}(b) = a$ when $f(a) = b$, and $f(a) = b$ when $f^{-1}(b) = a$.

Hence,

$$\left(f^{-1} \circ f\right)(a) = f^{-1}(f(a)) = f^{-1}(b) = a,$$

and

$$\left(f \circ f^{-1}\right)(b) = f\left(f^{-1}(b)\right) = f(a) = b.$$

Consequently, $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_B$, where I_A and I_B are the identity functions on the sets A and B, respectively. That is, $\left(f^{-1}\right)^{-1} = f$.

Example 1.36 If $f : \mathbb{R} \to \mathbb{R}$ is defined as $f(x) = 2x + 3$, then $f^{-1}(x) = \frac{x-3}{2}$. The composition $f \circ f^{-1}$ would be the identity function $I_{\mathbb{R}}$ on the real numbers, meaning $f\left(f^{-1}(x)\right) = x$ for all $x \in \mathbb{R}$.

1.7 Graphical Identification of Function Types

Understanding the behaviour of different types of functions is fundamental in mathematics. Functions can be classified based on their graphical patterns, which provide valuable insights into their characteristics. In this section, we will explore various types of functions, including linear, quadratic, exponential, and more. By examining their graphs, we can identify key features such as intercepts, slopes, curvature, and asymptotic behaviour, enabling us to distinguish between these different types of functions effectively.

Linear Functions

The general equation for a linear function is given by

$$y = ax + b \quad \text{(often written as } y = mx + b\text{)},$$

where a (or m) represents the slope and b is the y-intercept. The domain of this function is all real numbers. This equation is in slope-intercept form because a (or m) gives the slope and b gives the y-intercept. If $a = 0$, the function simplifies to $y = b$, which is a constant function.

The parent function for a linear equation is

$$y = x.$$

The transformed function can be written in the point-slope form as

$$y = y_1 + a(x - x_1),$$

where the graph contains the point (x_1, y_1) and has slope a. In this form:

- a is the vertical dilation (slope),
- y_1 represents the vertical translation,

- x_1 represents the horizontal translation.

This point-slope form can also be written as

$$y - y_1 = a(x - x_1),$$

where the coordinates of the fixed point (x_1, y_1) appear with a negative sign. The form $y = y_1 + a(x - x_1)$ expresses y explicitly in terms of x, making it easier to enter into a graphing calculator.

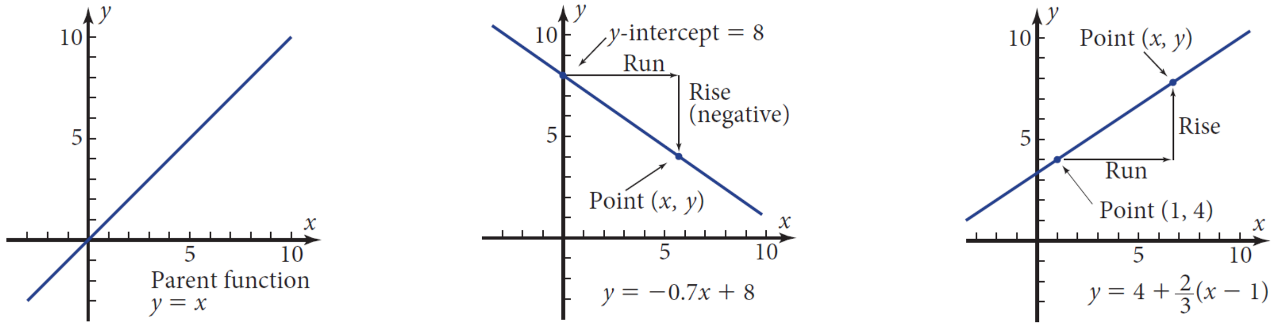


Figure 1.5: Linear functions

The graph of a linear function is a straight line. The parent function $y = x$ is shown on the left in figure 1.5, the slope-intercept form in the middle, and the point-slope form on the right.

For the slope-intercept form: "Start at b on the y-axis, move x units horizontally, and rise ax units vertically." For the point-slope form: "Start at (x_1, y_1), move $(x - x_1)$ units horizontally, and rise $a(x - x_1)$ units vertically."

Quadratic Functions

The general equation for a quadratic function is given by

$$y = ax^2 + bx + c,$$

where $a \neq 0$, and a, b, and c are constants. The domain of this function is all real numbers.

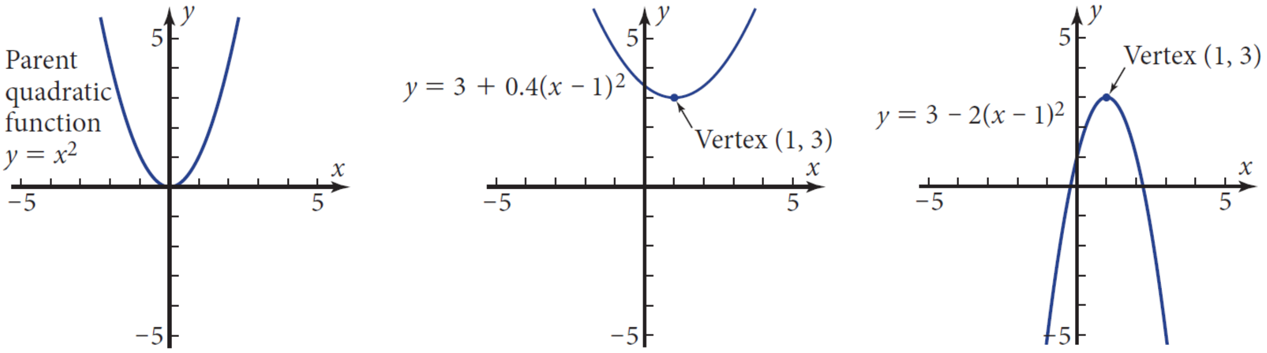


Figure 1.6: Quadratic functions

The parent function for a quadratic equation is

$$y = x^2,$$

where the vertex of the parabola is at the origin $(0, 0)$.

The transformed function can be written in vertex form as

$$y = k + a(x - h)^2,$$

where the vertex of the parabola is located at (h, k). In this form:

- k represents the vertical translation,
- h represents the horizontal translation,
- a represents the vertical dilation.

Vertex form can also be written as

$$y - k = a(x - h)^2,$$

but expressing y explicitly in terms of x makes the equation easier to enter into a graphing calculator.

The graph of a quadratic function is a parabola (from the Greek word for "along the path of a ball"). The parabola is concave up if $a > 0$ and concave down if $a < 0$. This behaviour is illustrated in figure 1.6.

Power Functions

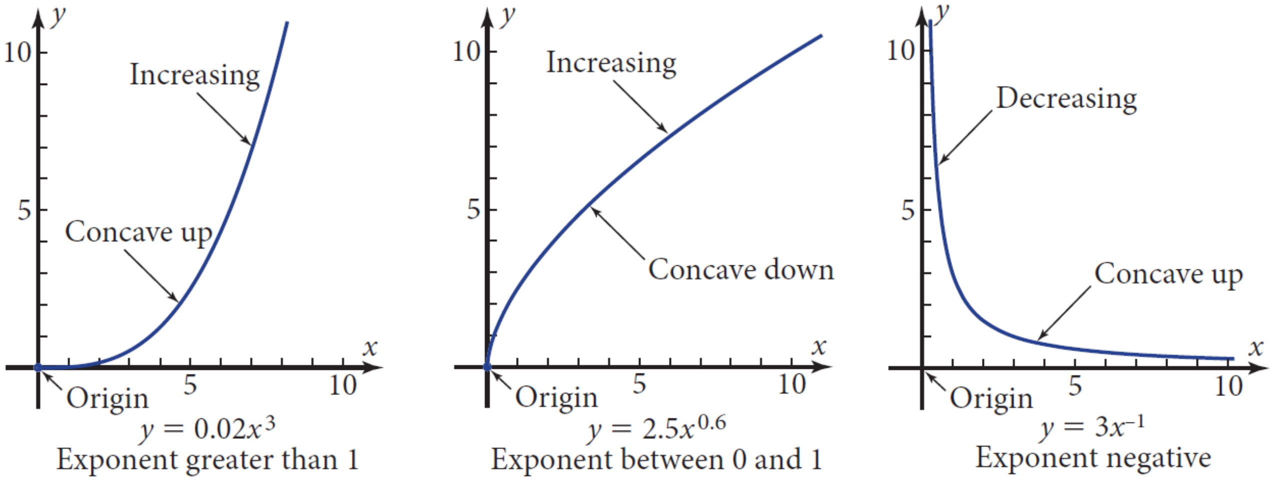
The general equation for a power function is given by

$$y = ax^b,$$

where a and b are nonzero constants. The domain of the function depends on the value of b:

- If $b > 0$, the domain is all real numbers.
- If $b < 0$, the domain excludes $x = 0$ to avoid division by zero.
- If b is not an integer, the domain usually excludes negative numbers to avoid taking roots of negative numbers.

In most applications, the domain is restricted to non-negative numbers.



$y = 0.02x^3$
Exponent greater than 1

$y = 2.5x^{0.6}$
Exponent between 0 and 1

$y = 3x^{-1}$
Exponent negative

Figure 1.7: Power functions

The parent function for a power function is

$$y = x^b.$$

For the general power function $y = ax^b$:

- If $b > 0$, then y varies directly with the bth power of x, meaning y is directly proportional to the bth power of x.
- If $b < 0$, then y varies inversely with the bth power of x, meaning y is inversely proportional to the bth power of x.

The dilation factor a serves as the proportionality constant.

The translated form of a power function is

$$y = d + a(x - c)^b,$$

where c and d are the horizontal and vertical translations, respectively. This can be compared with the translated forms of linear and quadratic functions:

$$y = y_1 + a(x - x_1) \qquad \text{(linear function)},$$
$$y = k + a(x - h)^2 \qquad \text{(quadratic function)}.$$

Unless otherwise stated, "power function" will imply the untranslated form, $y = ax^b$.

Figure 1.7 shows the graphs of power functions for different values of b. In all cases, $a > 0$. The shape and concavity of the graph depend on the value of b:

- If $b > 0$, the graph contains the origin.
- If $b < 0$, the graph has the axes as asymptotes.
- The function is increasing if $b > 0$ and decreasing if $b < 0$.
- The graph is concave up if $b > 1$ or $b < 0$, and concave down if $0 < b < 1$.

The concavity of the graph describes the rate at which y increases. For $b > 0$, concave up indicates that y is increasing at an increasing rate, while concave down indicates that y is increasing at a decreasing rate.

Exponential Functions

The general equation for an exponential function is given by

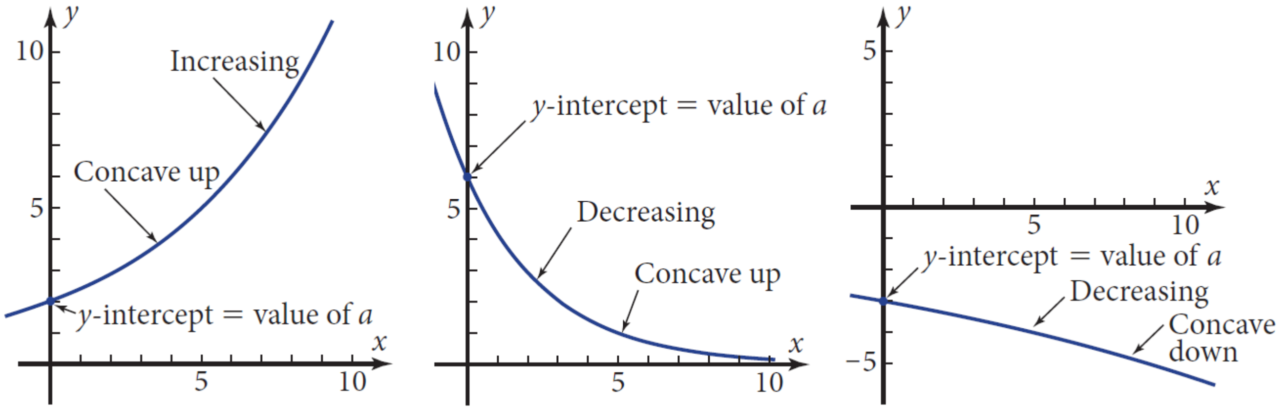
$$y = ab^x,$$

where a and b are constants, $a \neq 0$, $b > 0$, and $b \neq 1$. The domain of this function is all real numbers.

The parent function for an exponential equation is

$$y = b^x,$$

where the asymptote is the x-axis.



$y = 2 \cdot 1.2^x$
Base greater than 1

$y = 6 \cdot 0.7^x$
Base between 0 and 1

$y = -3 \cdot 1.06^x$
Coefficient negative

Figure 1.8: Exponential functions

In the equation $y = ab^x$, we say that "y varies exponentially with x." This means that y changes by a constant factor b for each unit increase in x.

The translated form of the exponential function is

$$y = ab^x + c,$$

where the asymptote is the line $y = c$. Unless otherwise stated, "exponential function" will refer to the untranslated form $y = ab^x$.

Figure 1.8 illustrates exponential functions for different values of a and b. The key properties of the graph are as follows:

- The constant a is the y-intercept of the graph.
- The function is increasing if $b > 1$ and decreasing if $0 < b < 1$, provided $a > 0$.
- If $a < 0$, the function's behavior is reversed: it is decreasing if $b > 1$ and increasing if $0 < b < 1$.
- The graph is concave up if $a > 0$ and concave down if $a < 0$.

Mathematicians often use one of two particular constants as the base for an exponential function: either 10, which is the base of the decimal system, or the naturally occurring number e, which approximately equals 2.71828. These bases are significant in various mathematical applications.

Definition 1.12 (Special Exponential Functions)

$y = a \cdot 10^{bx}$	base-10 exponential function
$y = a \cdot e^{bx}$	natural (base-e) exponential function

where a and b are constants and the domain is all real numbers. ♣

To generalise the exponential function, the variable in the exponent is often multiplied by a constant. The (untranslated) general forms of these exponential functions are given below:

$$y = a \cdot 10^{bx} \quad \text{and} \quad y = a \cdot e^{bx}$$

These functions can be further generalized by incorporating translations in both the x- and y-directions.

The translated forms are:

$$y = a \cdot 10^{b(x-c)} + d \quad \text{and} \quad y = a \cdot e^{b(x-c)} + d$$

The base-e exponential function, in particular, has a significant advantage when studying calculus, as the rate of change of e^x is equal to e^x itself.

1.8 Logarithms

Any positive number can be written as a power of 10. For instance,

$$\begin{aligned} 3 &= 10^{0.477\ldots} \\ 5 &= 10^{0.6989\ldots} \\ 15 &= 10^{1.1760\ldots} \end{aligned}$$

The exponents $0.4771\ldots$, $0.6989\ldots$, and $1.1760\ldots$ are called the base-10 logarithms of 3, 5, and 15, respectively:

$$\begin{aligned} \log 3 &= 0.4771\ldots \\ \log 5 &= 0.6989\ldots \\ \log 15 &= 1.1760\ldots \end{aligned}$$

To better understand the meaning of logarithms, press `LOG` 3 on your calculator. You will get:

$$\log 3 = 0.477121254\ldots$$

Then, without rounding, raise 10 to this power. You will obtain:

$$10^{0.477121254\ldots} = 3$$

The powers of 10 have the normal properties of exponentiation. For instance,

$$\begin{aligned} 15 = (3)(5) &= \left(10^{0.4771\ldots}\right)\left(10^{0.6999\ldots}\right) \\ &= 10^{0.4771\ldots+0.6599\ldots} \\ &= 10^{1.1760\ldots} \end{aligned}$$

This means $10^{0.4771\ldots+0.6599\ldots} = 10^{1.1760\ldots}$. Here, you add the exponents while keeping the same base. You can verify with your calculator that $10^{1.1760\ldots}$ indeed equals 15.

From this example, you can infer that logarithms have the same properties as exponents. This is expected because logarithms *are* exponents. For instance,

$$\log(3 \cdot 5) = \log 3 + \log 5 \quad \textit{The logarithm of a product equals the sum of the logarithms of the factors.}$$

From the values given earlier, you can also show that:

$$\log \frac{15}{3} = \log 15 - \log 3 \quad \textit{The logarithm of a quotient.}$$

This property is reasonable because you divide powers of equal bases by subtracting the exponents:

$$\frac{15}{3} = \frac{10^{1.1760\ldots}}{10^{0.477\ldots}} = 10^{1.1760\ldots-0.4771\ldots} = 10^{0.6989\ldots} = 5$$

Since a power can be written as a product, you can find the logarithm of a power as follows:

$$\log 34 = \log(3 \cdot 3 \cdot 3 \cdot 3) = \log 3 + \log 3 + \log 3 + \log 3$$
$$= 4 \log 3 \quad \textit{Combine like terms.}$$

The logarithm of a power equals the exponent of that power times the logarithm of the base. To verify this result, observe that $3^4 = 81$. Press $4 \times \texttt{LOG}\,3$ on your calculator, and you'll find it equals $1.9084\ldots$.

Definition 1.13 (Base-10 Logarithms)

$$\log x = y \iff 10^y = x$$

Verbally: $\log x$ is the exponent in the power of 10 that gives x ♣

Properties of base-10 logarithms

- Log of a Product:
  $$\log xy = \log x + \log y$$
  Verbally: The log of a product equals the sum of the logs of the factors.
- Log of a Quotient:
  $$\log \frac{x}{y} = \log x - \log y$$
  Verbally: The log of a quotient equals the log of the numerator minus the log of the denominator.
- Log of a Power:
  $$\log x^y = y \log x$$
  Verbally: The log of a power equals the exponent times the log of the base.

Property

The term logarithm comes from the Greek words *logos*, meaning "ratio," and *arithmos*, meaning "number." Before the invention of calculators, base-10 logarithms were calculated approximately using infinite series and recorded in tables. Products involving many factors, such as

$$(357)(4.367)(22.4)(3.142)$$

could be calculated by adding their logarithms (exponents) rather than tediously multiplying several pairs of numbers. This method was invented by Englishman Henry Briggs (1561–1630) and Scotsman John Napier (1550–1616). The name logarithm, thus, reflects this "logical way to do arithmetic,".

The most important thing to remember about logarithms is this

A logarithm is an exponent.

Example 1.37 Find x if $\log 10^{3.721} = x$

Solution: By definition, the logarithm is the exponent of 10. So $x = 3.721$. ◀

Example 1.38 Find x if $0.258 = 10^x$

Solution: By definition, x, the exponent of 10 , is the logarithm of 0.258 .

$$x = \log 0.258 = -0.5883\ldots$$

◀

Logarithms with Any Base: The Change-of-Base Property

If $x = 10^y$, then y is the base-10 logarithm of x. Similarly, if $x = 2^y$, then y is the base-2 logarithm of x. The only difference between these logarithms is the number that serves as the base. To distinguish among logarithms with different bases, the base is written as a subscript after the abbreviation "log." For instance:

$$3 = \log_2 8 \Leftrightarrow 2^3 = 8,$$
$$4 = \log_3 81 \Leftrightarrow 3^4 = 81,$$
$$2 = \log_{10} 100 \Leftrightarrow 10^2 = 100.$$

The symbol $\log_2 8$ is pronounced "log to the base 2 of 8." The symbol $\log_{10} 100$ is, of course, equivalent to $\log 100$, as defined in the previous section. Note that in all cases, a logarithm represents an exponent.

Definition 1.14 (Logarithm with Any Base)

Algebraically:

$\log_b x = y$ if and only if $b^y = x$, where $b > 0, b \neq 1$, and $x > 0$

Verbally:

$\log_b x = y$ means that y is the exponent of b that gives x as the answer. ♣

The way you pronounce the symbol for logarithm gives you a way to remember the definition. The next two examples show you how to do this.

Example 1.39 Write $\log_5 c = a$ in exponential form.

Solution:

Think this:

- "$\log_5 \ldots$" is read as "log base 5 . . .," meaning 5 is the base.
- A logarithm is an exponent. Since the $\log$ equals a, a must be the exponent.
- The "answer" obtained from 5^a is the argument of the logarithm, denoted as c.

Write only this:

$$5^a = c$$

◀

Example 1.40 Write $z^4 = m$ in logarithmic form.

Solution: $\log_z m = 4$ ◀

Two bases of logarithms are used frequently enough to have their own key on most calculators. One is the base-10 logarithm, also known as the common logarithm, as discussed in the previous section. The other is the base-e logarithm, known as the natural logarithm, where $e = 2.71828\ldots$, a naturally occurring number (like π) that will be advantageous in your future mathematical studies.

The symbol $\ln x$ (pronounced "el en of x") is used for natural logarithms, and is defined as:

$$\ln x = \log_e x$$

Definition 1.15 (Common Logarithm and Natural Logarithm)

Common: The symbol $\log x$ means $\log_{10} x$.

Natural: The symbol $\ln x$ means $\log_e x$, where e is a constant equal to $2.71828182845\ldots$ ♣

Example 1.41 Find $\log_5 17$. Check your answer by an appropriate numerical method.

Solution: Let $x = \log_5 17$.

$$5^x = 17$$
$$\log_{10} 5^x = \log_{10} 17$$
$$x \log_{10} 5 = \log_{10} 17$$
$$x = \frac{\log_{10} 17}{\log_{10} 5} = 1.7603\ldots$$
$$\log_5 17 = 1.7603\ldots$$
$$5^{1.7603\ldots} = 17$$

◀

In this example, note that the base-5 logarithm of a number is directly proportional to the base-10 logarithm of that number. The conclusion of the example can be expressed as follows:

$$\log_5 17 = \frac{1}{\log_{10} 5} \cdot \log_{10} 17 = 1.4306\ldots \log_{10} 17$$

To find the base-5 logarithm of any number, simply multiply its base-10 logarithm by $1.4306\ldots$ (that is, divide by $\log_{10} 5$).

This proportional relationship is known as the change-of-base property. From the results of Example 3, you can write:

$$\log_5 17 = \frac{\log_{10} 17}{\log_{10} 5}$$

Notice that the logarithm with the desired base is isolated on the left side of the equation, while the two logarithms on the right side share the same base—typically one that is available on your calculator. The box below illustrates this property for bases a and b with argument x:

The Change-of-Base Property of Logarithms

$$\log_a x = \frac{\log_b x}{\log_b a} \quad \text{or} \quad \log_a x = \frac{1}{\log_b a}(\log_b x)$$

Example 1.42 Find $\ln 29$ using the change-of-base property with base-10 logarithms. Check your answer directly by pressing $\ln 29$ on your calculator.

Solution:

$$\ln 29 = \frac{\log 29}{\log e} = \frac{1.4623\ldots}{0.4342\ldots} = 3.3672\ldots$$

Directly: $\ln 29 = 3.3672\ldots$

which agrees with the answer we got using the change-of-base property. ◀

Properties of Logarithms

The Logarithm of a Power:

$$\log_b x^y = y \log_b x$$

Verbally: The logarithm of a power equals the product of the exponent and the logarithm of the base. The Logarithm of a Product:

$$\log_b(xy) = \log_b x + \log_b y$$

Verbally: The logarithm of a product equals the sum of the logarithms of the factors. The Logarithm of a Quotient:

$$\log_b \frac{x}{y} = \log_b x - \log_b y$$

Verbally: The logarithm of a quotient equals the logarithm of the numerator minus the logarithm of the denominator.

Solving Exponential and Logarithmic Equations

Logarithms provide a way to solve an equation with a variable in the exponent or to solve an equation that already contains logarithms. We will demonstrate this through the next few examples.

Example 1.43 Solve the exponential equation $7^{3x} = 983$ algebraically, using logarithms.

Solution:

$$7^{3x} = 983$$

$$\log 7^{3x} = \log 983$$ `Take the base-10 logarithm of both sides.`

$$3x \log 7 = \log 983$$ `Apply the logarithm power property.`

$$x = \frac{\log 983}{3 \log 7}$$ `Divide both sides by the coefficient of x.`

$$x = 1.1803\ldots$$

◀

Example 1.44 Solve the equation

$$\log_2(x-1) + \log_2(x-3) = 3$$

Solution:

$$\log_2(x-1)+\log_2(x-3)=3$$

$$\log_2[(x-1)(x-3)]=3$$ `Apply the logarithm of a product property.`

$$2^3=(x-1)(x-3)$$ `Use the definition of logarithm.`

$$8=x^2-4x+3$$ `Expand the product.`

$$x^2-4x-5=0$$ `Reduce one side to zero. Use the symmetric property of equality.`

$$(x-5)(x+1)=0$$ `Solve by factoring.`

$x=5$ or $x=-1$

We need to be cautious here because the solutions in the final step are the solutions of the quadratic equation, and we must make sure they are also solutions of the original logarithmic equation. Check by substituting the solutions into the original equation.

If $x=5$, then

$$\begin{aligned}&\log_2(5-1)+\log_2(5-3)\\&=\log_2 4+\log_2 2\\&=2+1=3\end{aligned}$$

If $x=-1$, then

$$\begin{aligned}&\log_2(-1-1)+\log_2(-1-3)\\&=\log_2(-2)+\log_2(-4)\end{aligned}$$

which is undefined. ◀

Example 1.45 Solve the equation

$$e^{2x}-3e^x+2=0$$

Solution:

$$\begin{aligned}&e^{2x}-3e^x+2=0\\&(e^x)^2-3e^x+2=0\end{aligned}$$

We realise that this is a quadratic equation in the variable e^x. Using the quadratic formula, you get

$$e^x=\frac{+3\pm\sqrt{9-4(2)}}{2}=\frac{3\pm1}{2}$$

$e^x=2$ or $e^x=1$

You now have to solve these two equations.

$$\begin{aligned}&e^x=2 &\qquad& e^x=1\\&x=\ln 2=0.6931\ldots && x=0\end{aligned}$$

Check:

$$\begin{aligned}&e^{2\ln 2}-3e^{\ln 2}+2 &\qquad& (e^0)^2-3e^0+2\\&=\left(e^{\ln 2}\right)^2-3e^{\ln 2}+2 && =1^2-3(1)+2=0\\&=2^2-3(2)+2=0\end{aligned}$$

Both solutions are correct. ◀

Example 1.46 Solve the logarithmic equation $\ln(x+3)+\ln(x+5)=0$

Solution:

$$\begin{aligned}
&\ln(x+3)+\ln(x+5)=0\\
&\ln[(x+3)(x+5)]=0\\
&(x+3)(x+5)=e^0=1\\
&x^2+8x+15=1\\
&x^2+8x+14=0\\
&x=-2.5857\ldots \quad \text{or} \quad x=-5.4142\ldots
\end{aligned}$$

Check:

$$\begin{aligned}
&x=-2.5857\ldots:\\
&\ln(-2.5857\ldots+3)+\ln(-2.5857\ldots+5)\\
&=\ln(0.4142\ldots)+\ln(2.4142\ldots)\\
&=-0.8813\ldots+0.8813\ldots=0
\end{aligned}$$

which is ok.

$$\begin{aligned}
&x=-5.4142\ldots:\\
&\ln(-5.4142\ldots+3)+\ln(-5.4142\ldots+5)\\
&=\ln(-2.4142\ldots)+\ln(-0.4142\ldots)
\end{aligned}$$

which is undefined.

The only valid solution is $x=-2.5857\ldots$.

◀

Chapter 2 Fundamental Concepts in Number Theory

Numbers are the foundation of mathematics, representing quantities, measurements, and relationships in both abstract and concrete forms. The study of numbers dates back thousands of years, with early civilisations like the Babylonians, Egyptians, and Greeks laying the groundwork for modern number theory. These ancient cultures developed basic arithmetic, including addition, subtraction, multiplication, and division, which are still taught today.

Number theory, often called the "Queen of Mathematics," is a branch of mathematics devoted to the study of integers and the relationships between them. It encompasses a wide range of topics, including prime numbers, divisibility, modular arithmetic, and the properties of number systems. Number theory has a rich history, with significant contributions from mathematicians such as Euclid, who proved the infinitude of prime numbers around 300 BCE, and Pierre de Fermat, known for Fermat's Last Theorem, a problem that puzzled mathematicians for over 350 years until it was finally solved by Andrew Wiles in 1994.

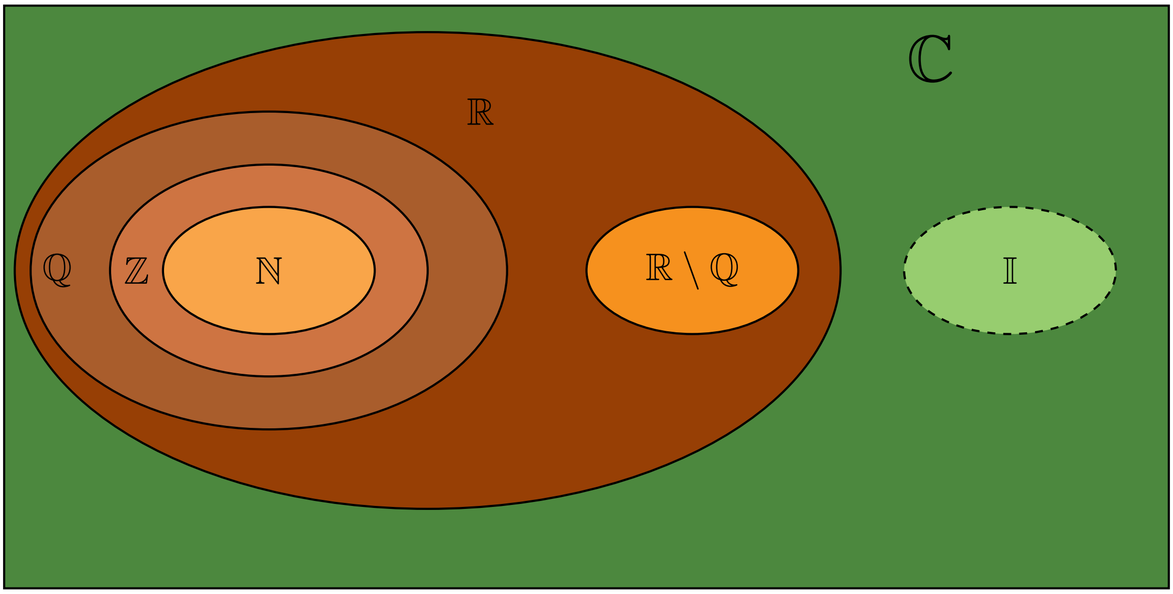


Figure 2.1: Venn diagram of numbers

Throughout history, number theory has evolved from a purely theoretical pursuit to a field with practical applications in modern technology. For example, cryptography, the science of securing communication, relies heavily on number theory, particularly the properties of prime numbers and modular arithmetic. The algorithms that protect our online transactions and digital communications are built upon the principles of number theory.

In this chapter, we will explore various aspects of numbers and number theory, starting with the basics of integers, prime numbers, and number systems, and gradually advancing to more complex topics. By understanding the fundamental properties of numbers, we gain insights into the mathematical structures that underpin the digital world and beyond.

Remark: Many numbers are included in more than one set. Table 2.1 offers an overview of the names, properties of and symbols used for the main number types.

Table 2.1: Types of Numbers and Their Properties

Natural Numbers	$\mathbb{N}$	Numbers used for counting (all positive integers).	$0, 1, 2, \ldots$
Integers	$\mathbb{Z}$	All positive and negative whole numbers.	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
Rational Numbers	$\mathbb{Q}$	All real numbers which can be expressed as a fraction, $\frac{p}{q}$, where p and q are integers and $q \neq 0$. All integers are rational numbers as 1 is a non-zero integer.	$\frac{1}{5}, \frac{5}{1}(=5), \frac{2}{3}, \frac{3}{2}, \frac{0}{3}(=0)$
Irrational Numbers	$\mathbb{R} \setminus \mathbb{Q}$	All real numbers which cannot be expressed as a fraction whose numerator and denominator are integers (i.e., all real numbers which aren't rational).	$\pi, \sqrt{2}, \sqrt{3}$
Real Numbers	$\mathbb{R}$	Includes all numbers on the number line.	$\frac{1}{5}, \sqrt{\frac{1}{5}}, 0, -2$
Imaginary Numbers	$\mathbb{I}$	Numbers which are the product of a real number and the imaginary unit i (where $i = \sqrt{-1}$).	$3i = \sqrt{-9},\ -5i = \sqrt{-25},$ $3\sqrt{2}i = \sqrt{-18}$
Complex Numbers	$\mathbb{C}$	All numbers which can be expressed in the form $a + bi$ where a and b are real numbers and $i = \sqrt{-1}$. Each complex number is a combination of a real number (a) and an imaginary number (bi).	$1 + 2i, 1, i, -3i, 0, -5 + i$

Remark: Figure 2.1 may appear misleading at first glance, as it suggests that there are real numbers which are neither rational nor irrational (depicted by the blue region). However, this is not the case. The set of real numbers is exclusively comprised of rational and irrational numbers. This is precisely why the set of irrational numbers is denoted as $\mathbb{R} \setminus \mathbb{Q}$, meaning "all real numbers except the rational numbers". The same is true of the complex numbers; the are all composed of the real numbers and the imaginary numbers.

2.1 Types of Numbers

Let's explore the various types of numbers, including natural numbers, whole numbers, integers, rational numbers, irrational numbers, and real numbers - imaginary numbers and complex numbers are left out of this discussion.

Natural Numbers

We begin with the natural numbers. We distinguish between whole numbers: $0, 1, 2, 3, \ldots$ and counting numbers: $1, 2, 3, \ldots$. These numbers are primarily used for counting. Natural numbers are often regarded as exact values (e.g., there are 4 tires on a car, 8 legs on a spider). However, in some contexts, they may be used as approximations (e.g., there were approximately 1000 people in the crowd).

One of the key properties of natural numbers is that they are *closed* under addition and multiplication. This means that if you take any two natural numbers and add or multiply them, the result will always be another natural number.

One of the key properties of natural numbers is that they are *closed* under certain operations, such as addition and multiplication. This means that if you take any two natural numbers and add or multiply them, the result will always be another natural number. For example, if a and b are natural numbers, then both $a + b$ and $a \times b$ are also natural numbers.

There is very little consensus as to whether the symbol $\mathbb{N}$ includes 0. Therefore, the set of whole numbers (that include 0) is often denoted $\mathbb{W}$.

Integers

Integers are the basic building blocks of number theory, consisting of the set of whole numbers and their negatives. Formally, integers include numbers like $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$ Basic arithmetic operations, such as addition and multiplication, follow certain properties:

Commutative, Associative, and Distributive Laws

- Commutativity: $a + b = b + a$
- Associativity: $(a + b) + c = a + (b + c)$
- Distributive property: $a \times (b + c) = a \times b + a \times c$

Integers are a fundamental set of numbers in mathematics, denoted by the symbol $\mathbb{Z}$. This set includes all the positive and negative whole numbers, as well as zero. Integers extend the natural numbers by incorporating their additive inverses, thereby allowing for the complete operation of subtraction within the set.

Additive Identity: The number 0 is known as the additive identity. This is because for any integer a, adding zero does not change the value of a. In mathematical terms, this property is expressed as $0 + a = a + 0 = a$. This identity is crucial because it ensures that the set of integers remains stable under addition.

Multiplicative Identity: Similarly, the number 1 serves as the multiplicative identity. For any integer a, multiplying by one leaves the value of a unchanged: $1 \times a = a \times 1 = a$. This property underpins the stability of integers under multiplication, maintaining the integrity of the set.

Additive Inverse: For each integer a, there exists a corresponding additive inverse, denoted as $-a$. The additive inverse is defined such that when a and $-a$ are added together, the result is the additive identity, zero: $a + (-a) = 0$. This property allows for the operation of subtraction within the set of integers, as subtraction can be viewed as the addition of an additive inverse.

Closure Property

Addition: The set of integers is closed under the operation of addition. This means that if you take any two integers and add them together, the sum will always be an integer. For example, if a and b are integers, then $a + b$ is also an integer. This closure property ensures that the set of integers is stable and complete under addition, meaning that no matter how many times you add integers together, the result will remain within the set of integers.
Multiplication: The set of integers is also closed under multiplication. If you multiply any two integers, the product will always be an integer. For instance, if a and b are integers, then $a \times b$ is also an integer. This property guarantees that the operation of multiplication, like addition, does not produce results outside the set of integers, thereby preserving the integrity of the set under multiplication.

It is universally agreed upon that the definition of an integer is clear and precise. Therefore, when in doubt, it is advisable to refer to numbers within this set as ”integers.” When you specifically need to refer to only the positive integers, it is both accurate and professional to explicitly state ”positive integers.” This terminology not only ensures clarity but also reflects a sound understanding of mathematical conventions.

Remember, zero is neither positive nor negative, so when discussing subsets of integers, careful consideration of this fact is necessary:

- **Integers:** $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$
- **Negative Integers:** $\mathbb{Z}^- = \{\ldots, -4, -3, -2, -1\}$
- **Positive Integers:** $\mathbb{Z}^+ = \{1, 2, 3, 4, \ldots\}$
- **Non-Negative Integers:** $\mathbb{Z}_0^+ = \mathbb{Z}_{\geq 0}+ = \{0, 1, 2, 3, 4, \ldots\}$
- **Non-Positive Integers:** $\mathbb{Z}_0^- = \mathbb{Z}_{\leq 0}\{\ldots, -4, -3, -2, -1, 0\}$

This notation should be consistent with standard mathematical conventions.

Rational Numbers

Rational numbers, denoted by the symbol $\mathbb{Q}$, are numbers that can be expressed as the quotient of two integers, where the numerator is any integer and the denominator is a non-zero integer. Formally, a rational number can be written as $\frac{a}{b}$, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$. This set of numbers is fundamental in mathematics as it provides a means to represent fractions and ratios, allowing for a wide range of arithmetic operations, and as such are a generalisation of common fractions which we saw in chapter 1. They can represent any number that can be written as a finite or repeating decimal.

One of the key properties of rational numbers is that each non-zero rational number has a *multiplicative inverse*. The multiplicative inverse of a rational number $\frac{a}{b}$ is the rational number $\frac{b}{a}$, provided that $a \neq 0$. The importance of the multiplicative inverse lies in the fact that when a number is multiplied by its inverse, the result is the *multiplicative identity*, which is 1. In other words, for any rational number $\frac{a}{b}$, its inverse is denoted by $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, and we have:

$$\frac{a}{b} \times \frac{b}{a} = \frac{ab}{ba} = 1$$

This property ensures that rational numbers are closed under multiplication and division (except division by zero), making them a robust and versatile set of numbers for various mathematical operations.

Rational numbers are dense on the number line, meaning that between any two rational numbers, there exists another rational number. This property makes the set of rational numbers particularly important in the study of real numbers, as it allows for the approximation of irrational numbers to any desired degree of accuracy.

Irrational Numbers

Irrational numbers, denoted by the symbol $\mathbb{R} \setminus \mathbb{Q}$, are real numbers that cannot be expressed as the quotient of two integers. Unlike rational numbers, which have a repeating or terminating decimal expansion, the decimal expansion of an irrational number neither repeats nor terminates. This property makes irrational numbers fundamentally different from rational numbers, as they cannot be precisely represented as fractions.

Some of the most famous examples of irrational numbers include:

- **Pi** (π): Perhaps the most well-known irrational number, π is the ratio of the circumference of a circle to its diameter. Its value is approximately $3.14159\ldots$, but its decimal expansion goes on infinitely without repeating. π plays a crucial role in geometry, trigonometry, and calculus.
- **The Golden Ratio** (ϕ): The golden ratio, $\phi \approx 1.61803\ldots$, is an irrational number that appears frequently in nature, art, and architecture. It is defined as the positive solution to the equation $x^2 - x - 1 = 0$, and it is the limit of the ratio of successive Fibonacci numbers.
- **The Square Root of 2** ($\sqrt{2}$): The square root of 2, approximately $1.41421\ldots$, is the length of the diagonal of a square with side length 1. This number is historically significant because its discovery by the ancient Greeks, particularly the Pythagoreans, revealed the existence of numbers that could not be expressed as the ratio of two integers. The Pythagorean theorem states that in a right triangle, the square of the hypotenuse is equal to the sum of the squares of the other two sides. For a right triangle with both legs of length 1, the hypotenuse is $\sqrt{2}$, demonstrating that $\sqrt{2}$ cannot be a rational number.
- **Euler's Number** (e): The number $e \approx 2.71828\ldots$ is the base of the natural logarithm and is a fundamental constant in mathematics, particularly in calculus and complex analysis. The number e arises naturally in various growth processes, such as compound interest and population growth.

Irrational numbers fill the gaps between rational numbers on the number line, making the real numbers a continuous set. However, like rational numbers, they too have important properties. For instance, while irrational numbers do not have a simple fractional representation, they are nonetheless essential in representing the lengths, areas, and volumes that cannot be captured by rational numbers alone.

Real Numbers

Real numbers, denoted by the symbol $\mathbb{R}$, form the foundation of most mathematical analysis and are essential in describing continuous quantities. The set of real numbers is composed of both rational numbers ($\mathbb{Q}$) and irrational numbers ($\mathbb{R} \setminus \mathbb{Q}$), thus encompassing all numbers that can be placed on the number line. While both rational and irrational numbers are part of the real number system, they differ significantly in their properties:

Similarities and Differences of Rational and Irrational Numbers

- **Representation:** Rational numbers can be represented as fractions, while irrational numbers cannot. This distinction makes irrational numbers more complex to handle, especially in arithmetic operations.
- **Decimal Expansion:** The decimal expansion of rational numbers is either finite or periodic, while that of irrational numbers is infinite and non-repeating.
- **Closure Properties:** Rational numbers are closed under addition, subtraction, multiplication, and division (except by zero). Irrational numbers are not closed under these operations; for example, the sum or product of two irrational numbers can sometimes be rational.
- **Density:** Rational numbers are dense on the real number line, meaning that between any two rational numbers, there exists another rational number. Irrational numbers are also densely distributed but in a complementary manner, filling in the ”gaps” left by the rationals, ensuring that the real number line is continuous without any breaks.

The real number line is a continuous, unbroken line that extends infinitely in both directions. Every point on this line corresponds to a unique real number, whether rational or irrational. This continuity is what allows the real numbers to model continuous phenomena in nature, such as time, distance, and temperature.

2.2 Integer Properties and Modular Arithmetic

In 1 we introduced the concept of a factor. A factor is a portion of a quantity, usually an integer or polynomial that, when multiplied by other factors, gives the entire quantity.

In number theory, a factor of a number n is synonymous with a **divisor** of n. Specifically, a divisor of an integer n is an integer d that divides n and results in another integer.

A positive **proper divisor** is a positive divisor of a number n, excluding n itself. Similarly, a **proper factor** of a positive integer n is a factor of n other than 1 or n.

For example, the factors of 12 are:

$$1, 2, 3, 4, 6, 12$$

In this list, 2, 3, 4, and 6 are proper factors of 12, meaning they are less than 12 itself but greater than 1.

A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself. In other words, a prime number cannot be formed by multiplying two smaller natural numbers. The first few prime numbers are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

Notice that 2 is the only even prime number because any other even number can be divided by 2, making it *composite*. A **composite number**, in contrast to a prime, is a natural number greater than 1 that can be divided evenly by at least one positive integer other than 1 and itself. For example, 6 is a composite number because it can be expressed as $6 = 2 \times 3$.

Prime factorisation

Prime factorisation is the process of breaking down a composite number into a product of its prime factors. For any composite number, this factorisation is unique, except for the order of the factors. For instance, consider the number 60:

$$60 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3 \times 5$$

Here, 2, 3, and 5 are prime factors of 60 and $2^2 \times 3 \times 5$ is the **canonical factorisation** of 60 - we usually just call it the prime factorisation.

Theorem 2.1 (The Fundamental Theorem of Arithmetic)

Every integer greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors. ♡

This theorem underscores the importance of prime numbers as the "building blocks" of all natural numbers.

Example 2.1

$$84 = 2^2 \times 3 \times 7$$

No matter how you factorise 84, you will always end up with this set of prime numbers (2, 3, and 7), though the order might differ.

The prime factorisation allows for a unique representation of the number in terms of its prime factors.

Greatest Common Divisor (GCD)

The Greatest Common Divisor (GCD), also referred to as the *highest common factor* (HCF) or *greatest common factor* (GFC), of two or more integers is the largest positive integer that divides each of the given integers without leaving a remainder. To determine the GCD, one commonly employs the prime factorisation of the numbers involved. The GCD is then found by multiplying the common prime factors with the smallest exponents from the prime factorisation of the numbers.

For example, consider finding the GCD of 24 and 36:

$$24 = 2^3 \times 3, \quad 36 = 2^2 \times 3^2$$

The common prime factors are 2 and 3. Thus, the GCD is:

$$\text{GCD} = 2^2 \times 3 = 12$$

Example 2.2 Find the GCD of 36 and 120

Solution:

The arrows indicate the numbers that we chose.

$$36 = \overset{\downarrow}{\enclose{circle}{2^2}} \times \enclose{circle}{3^2}$$

$$120 = \enclose{circle}{2^3} \times \underset{\uparrow}{\enclose{circle}{3}} \times 5$$

We see that 2 and 3 are common factors, and choose the ones with the smallest exponents:

$$GCD = 2^2 \times 3 = 12$$

◀

Least Common Multiple (LCM)

The Least Common Multiple (LCM) of two or more integers is the smallest positive integer that is evenly divisible by each of the given integers. The LCM can also be determined using the prime factorisation of the numbers.

For instance, to find the LCM of 24 and 36:

$$24 = 2^3 \times 3, \quad 36 = 2^2 \times 3^2$$

The LCM is obtained by taking the highest power of each prime factor that appears in the factorisation of either number:

$$\text{LCM} = 2^3 \times 3^2 = 72$$

Example 2.3 Find the LCM of 12 and 18

Solution:

$$15 = 3 \times 5$$

$$18 = 2 \times 3^2$$

So the factors with the highest exponents in either factorisation is 2, 3^2, and 5, so

$$LCM = 2 \times 3^2 \times 5 = 90$$

◀

Example 2.4 Find the LCM of 80 and 120

Solution:

The arrows indicate the numbers that we chose.

$$80 = \overset{\downarrow}{\enclose{circle}{2^4}} \times \overset{\downarrow}{\enclose{circle}{5}}$$

$$120 = \underset{\uparrow}{\enclose{circle}{2^3}} \times 3 \times \underset{\uparrow}{\enclose{circle}{5}}$$

We see that 2 and 5 are common factors and choose the ones with the smallest exponents (5 has the same exponents so we just take one of them):

$$LCM = 2^4 \times 3 \times 5 = 240$$

◀

Connection Between GCD and LCM

An important relationship between the GCD and LCM of two numbers a and b is given by the formula:

$$\text{GCD}(a, b) \times \text{LCM}(a, b) = a \times b$$

For example, using the numbers 24 and 36:

$$12 \times 72 = 24 \times 36 = 864$$

This relationship is a powerful tool in solving problems related to divisibility, number theory, and algebra.

The study of primes and factors is foundational in mathematics, providing essential tools for understanding the structure of numbers. The concepts of prime factorisation, the Fundamental Theorem of Arithmetic, and the calculations of GCD and LCM are not only critical in theoretical mathematics but also in practical applications, such as cryptography, coding theory, and the analysis of algorithms.

Divisors and Remainders

Division involving integers can be tricky since the result might not always be an integer. Often, division produces a remainder. For example,

$$9 = 2 \times 4 + 1.$$

In this case, dividing 9 by 4 leaves a *remainder* of 1.

In general, for any integers a and b, we can express this as:

$$b = k \times a + r,$$

where r is the remainder. If r is zero, then we say that a divides b, denoted as $a \mid b$. The vertical bar is used to signify divisibility. For instance, $2 \mid 128$ and $7 \mid 49$, but 3 does not divide 4, which is written as $3 \nmid 4$.

Above, we made no distinction between factors and divisors. Some argue that they differ slightly:

- If $a \mid b$ and $a > 0$, a is a *divisor* of b.
- If $a \notin \{1, b\}$ and $a \mid b$, a is a factor of b.

In this definition, primes have no factors, only two divisors 1 and itself. We will make no further distinction between primes and factors and use the terms interchangeably.

Modular Arithmetic

The mod operator, commonly encountered in computer programming, provides the remainder after division. For example:

1. $25 \bmod 4 = 1$ because $25 \div 4 = 6$ with a remainder of 1.
2. $19 \bmod 5 = 4$ since $19 = 3 \times 5 + 4$.
3. $24 \bmod 5 = 4$.
4. $99 \bmod 11 = 0$.

While there are some complexities when dealing with negative numbers, we will focus on positive integers for simplicity. It's also worth noting that the results of the modulus operation are often expressed differently. For instance, $24 = 4 \bmod 5$ or $21 = 0 \bmod 7$, which means $24 \bmod 5 = 4$ and $21 \bmod 7 = 0$.

Modular arithmetic is sometimes referred to as clock arithmetic. Imagine using a 24-hour clock: 09:00 represents 9 in the morning, while 21:00 represents 9 in the evening. If a journey starts at 07:00 and lasts 25 hours, the arrival time would be 08:00 the next day. Mathematically, this can be expressed as $7 + 25 = 32$ and $32 \bmod 24 = 8$. Essentially, we start at 7 and move 25 hours forward on the clock face, landing at 8.

Chapter 3 Numeral Systems

We are so accustomed to working within the decimal system that we often forget it is a relatively recent invention and was once considered revolutionary. It is time to carefully examine how we represent numbers. Typically, we use the decimal system, where a number like 3459 is shorthand for $3 \times 1000 + 4 \times 100 + 5 \times 10 + 9$. The position of each digit is crucial, as it allows us to distinguish between values like 30 and 3. The decimal system is a **positional numeral system**, meaning it has designated positions for units, tens, hundreds, and so forth. Each digit's position implies the multiplier (a power of ten) that should be used with that digit, and each position has a value ten times that of the position to its right.

Notice that we can save space by writing 1000 as 10^3, where the exponent 3 indicates the number of zeros. Thus, $100000 = 10^5$. If the exponent is negative, it represents a fraction, e.g., $10^{-3} = \frac{1}{1000}$. Perhaps the most ingenious aspect of the positional system was the addition of the decimal point, which allows us to include decimal fractions. For example, the number 123.456 is equivalent to:

$$1 \times 100 + 2 \times 10 + 3 \times 1 + 4 \times \frac{1}{10} + 5 \times \frac{1}{100} + 6 \times \frac{1}{1000}.$$

This can be visualised as:

$$\begin{array}{rccccccccc}
\text{Multiplier:} & \ldots & 10^2 & 10^1 & 10^0 & . & 10^{-1} & 10^{-2} & 10^{-3} & \ldots \\
\text{Digits:} & \ldots & 1 & 2 & 3 & . & 4 & 5 & 6 & \ldots \\
 & & & & & \uparrow & & & & \\
 & & & & & \text{Decimal Point:} & & & &
\end{array}$$

However, there is no inherent reason why we must use powers of 10, or base 10. The Babylonians, for instance, used base 60, and base 12 was very common in medieval Europe. Today, the most widely used numeral systems are summarised table 3.1

Numeral system	Symbols	Base	Additional information
Decimal	0-9	10	-
Binary	0, 1	2	-
Hexadecimal	0-9, A-F	16	$\mathrm{A} \equiv 10, \mathrm{B} \equiv 11, \mathrm{C} \equiv 12, \mathrm{D} \equiv 13, \mathrm{E} \equiv 14, \mathrm{F} \equiv 15$
Octal	0-7	8	-

Table 3.1: Summary of Common Numeral Systems

We begin by focusing on binary which will also receive the most detailed attention in this chapter.

3.1 Binary numbers

In the binary scale, we express numbers in powers of 2 rather than the 10s of the decimal scale. For some numbers, this is easy. Recall $2^0 = 1$,

As in decimal, we write this with the position of the digit representing the power, the first place after the decimal being the 2^0 position, the next the 2^1, and so on. To convert a decimal number to binary, we can

Decimal number		In powers of 2	Power of 2				Binary number
			3	2	1	0	
8	=	2^3	1	0	0	0	1000
7	=	$2^2 + 2^1 + 2^0$	0	1	1	1	111
6	=	$2^2 + 2^1$	0	1	1	0	110
5	=	$2^2 + 2^0$	0	1	0	1	101
4	=	2^2	0	1	0	0	100
3	=	$2^1 + 2^0$	0	0	1	1	11
2	=	2^1	0	0	1	0	10
1	=	2^0	0	0	0	1	1

Table 3.2: Decimal Numbers in Binary Representation

use the `mod` operator.

As an example, consider 88 in decimal or 88_{10}. We would like to write it as a binary number. We take the number and successively divide `mod` 2. See below:

Step Number n	x_n	$x_n/2$	$x_n \bmod 2$
0	88	44	0
1	44	22	0
2	22	11	0
3	11	5	1
4	5	2	1
5	2	1	0
6	1	0	1

Table 3.3: Conversion of Decimal 88 to Binary

Writing the last column in reverse, that is from the bottom up, we have 1011000, which is the binary form of 88, i.e., $88_{10} = 1011000_2$.

Binary decimals are less common but quite possible. Thus, 101.1011 is just $2^2 + 2^0 + 2^{-1} + 2^{-3} + 2^{-4}$, which is, after some calculation, 5.6875. We have seen how to turn the integer part of a decimal number into a binary number, and we can do the same with a decimal fraction. Consider 0.6875. As before, we draw up a table:

Giving, reading down, $0.6875_{10} = 1011_2$.

Binary Expansion

The process outlined in the previous section is called **binary expansion** and refers to the representation of a number in the binary (base-2) numeral system. Every decimal number can be expressed as a sum of powers of 2, where each power corresponds to a binary digit (bit) in the number's binary form.

Step Number n	x_n	$x_n \times 2$	$\lfloor x_n \times 2 \rfloor$
0	0.6875	1.375	1
1	0.375	0.75	0
2	0.75	1.5	1
3	0.5	1	1

Table 3.4: Conversion of Decimal Fraction 0.6875 to Binary

Let's reconsider the decimal number 88. To find its binary expansion, we identify the largest power of 2 less than or equal to 88 and continue subtracting powers of 2 until we reach 0.

First, we note that $2^6 = 64$ is the largest power of 2 less than 88:

$$88 = 64 + 24$$

Next, we find that $2^4 = 16$ is the largest power of 2 less than 24:

$$24 = 16 + 8$$

Finally, $2^3 = 8$ exactly matches the remainder:

$$8 = 8 + 0$$

Thus, we have:

$$88 = 2^6 + 2^4 + 2^3$$

In binary, each of these powers of 2 is represented by a '1' in the corresponding place value, with '0' in place values where no power of 2 contributes:

$$88_{10} = 1011000_2$$

To summarise:

- $2^6 = 64$ corresponds to the leftmost '1' in the binary expansion.
- $2^4 = 16$ corresponds to the next '1'.
- $2^3 = 8$ corresponds to the next '1'.
- The remaining digits are '0' because 2^5, 2^2, 2^1, and 2^0 do not contribute to the value 88.

Thus, the binary expansion of 88 is 1011000_2. This method of representing numbers is fundamental in computer science and digital electronics, where binary representation is the standard for data storage and processing.

Binary Operations

Binary operations are basic arithmetic operations performed on binary numbers. These operations are essential in computing and digital systems, as they form the foundation for how computers process and manipulate data.

Binary addition, subtraction, and multiplication are similar to their decimal counterparts but follow simpler rules due to the binary system's limited digits. For example, binary addition follows these rules:

$$0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=10$$

In this case, $1+1$ results in 10_2, which means 0 with a carry of 1 to the next higher bit. Binary subtraction and multiplication follow similar straightforward rules that are easy to implement in digital systems.

The XOR (exclusive OR) operation is another important binary operation. XOR produces a 1 if the two bits being compared are different and a 0 if they are the same:

$$0 \oplus 0=0, \quad 0 \oplus 1=1, \quad 1 \oplus 0=1, \quad 1 \oplus 1=0$$

In binary addition, the XOR operation is used to add two bits without considering any carry from a previous bit. This is because XOR effectively performs addition modulo 2, which aligns perfectly with how binary addition works. For example:

Bit 1	Bit 2	XOR (Sum)	AND (Carry)
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

In the case of $1+1$, XOR gives a sum of 0 and an AND operation (which detects the carry) gives a carry of 1, resulting in the binary number 10.

$$\begin{aligned}
0+0&=0\\
0+1&=1\\
1+1&=10 \quad \text{so we carry 1 and leave a zero}\\
1+1+1=1+(1+0)&=1+10=11.
\end{aligned}$$

We can write this in very much the same way as for a decimal addition:

$$\begin{array}{c|c|c|c|c|c|c|l}
 & 1 & 1 & 0 & 1 & 0 & 1 & \\
+ & 1 & 0 & 1 & 1 & 1 & 0 & \\
\hline
1 & 1 & 0 & 0 & 0 & 1 & 1 & \text{Sum} \\
\uparrow & & & & \uparrow & & & \\
 & & & & & & &
\end{array}$$

The right-hand arrow shows where we carry a 1. The left-hand arrow shows where we have $1+1+1$ so we carry a 1 and have a 1 left over.

As we will see below, we will often need to handle multiple carries. There are two ways to handle this which resemble the methods we know from the decimal system. We will explain using an example.

Method 1: Column-wise Binary Addition with Multiple Carries

Consider

$$\begin{array}{cccccc}
 & 1 & 1 & 1 & 1 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 1 & 1 \\
\hline
\end{array}$$

Step 1: Add the Rightmost Column
Start by adding the rightmost bits:

$$1 + 1 + 1 + 1 = 100_2 \quad (\text{ which is binary for } 4)$$

Reading the result from right to left (i.e. from *least significant bit* (LSB) to the *most significant bit*(MSB))

- write down the 0
- carry the 0 to the next column
- carry the 1 to the third column

You end up with

$$\begin{array}{cccccc}
 & & & {\scriptstyle 1} & {\scriptstyle 0} & \\
 & 1 & 1 & 1 & 1 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 1 & 1 \\
\hline
 & & & & & 0
\end{array}$$

Step 2: Add the Second Column from the Right
Next, add the second column:

$$0 + 1 + 0 + 0 + 1 = 10_2 \quad (\text{ which is binary for } 2)$$

Reading the result from LSB to MSB:

- write down the 0
- carry the 1 to the next column

You end up with

$$\begin{array}{cccccc}
 & & & {\scriptstyle 1} & & \\
 & & & {\scriptstyle 1} & & \\
 & 1 & 1 & 1 & 1 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 1 & 1 \\
\hline
 & & & & 0 & 0
\end{array}$$

Step 3: Add the Third Column from the Right
Now, add the third column:

$$1 + 1 + 1 + 1 + 1 + 1 = 110_2 \quad (\text{ which is binary for } 6)$$

Reading the result from LSB to MSB

- write down the 0
- carry the 1 to the fourth column
- carry the 1 to the fifth column

You end up with

Our sum so far:

$$
\begin{array}{cccccc}
 & {\scriptstyle 1} & {\scriptstyle 1} & & & \\
 & 1 & 1 & 1 & 1 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 1 & 1 \\
\hline
 & & & 0 & 0 & 0
\end{array}
$$

Step 4: Add the Fourth Column from the Right
Move to the fourth column:

$$1 + 1 + 1 + 1 + 1 = 101_2 \quad (\text{ which is binary for } 5)$$

Reading the result from LSB to MSB

- write down the 1
- carry the 0 to the fifth column
- carry the 1 to the sixth column

You end up with

$$
\begin{array}{ccccccc}
 & & {\scriptstyle 0} & & & & \\
 & {\scriptstyle 1} & {\scriptstyle 1} & & & & \\
 & & 1 & 1 & 1 & 1 & 1 \\
+ & & 1 & 1 & 1 & 0 & 1 \\
+ & & 1 & 1 & 1 & 0 & 1 \\
+ & & 1 & 1 & 1 & 1 & 1 \\
\hline
 & & & 1 & 0 & 0 & 0
\end{array}
$$

Step 5: Add the Leftmost Column
Add the leftmost column:

$$1+1+1+1+1 = 101_2 \quad (\text{ which is binary for } 5)$$

Reading the result from LSB to MSB

- write down the 1
- carry the 0 to the sixth column
- carry the 1 to the seventh column

This results in

$$\begin{array}{cccccccc}
 & & {\scriptstyle 0} & & & & & \\
 & {\scriptstyle 1} & {\scriptstyle 1} & & & & & \\
 & & & 1 & 1 & 1 & 1 & 1 \\
+ & & & 1 & 1 & 1 & 0 & 1 \\
+ & & & 1 & 1 & 1 & 0 & 1 \\
+ & & & 1 & 1 & 1 & 1 & 1 \\
\hline
 & & & 1 & 1 & 0 & 0 & 0
\end{array}$$

Step 6: Add the Remaining Carries
Finally, add the remaining carries:

$$\begin{array}{cccccccc}
 & & & 1 & 1 & 1 & 1 & 1 \\
+ & & & 1 & 1 & 1 & 0 & 1 \\
+ & & & 1 & 1 & 1 & 0 & 1 \\
+ & & & 1 & 1 & 1 & 1 & 1 \\
\hline
 & 1 & 1 & 1 & 1 & 0 & 0 & 0
\end{array}$$

The following example demonstrates the entire process by using different colors to distinguish each column and the corresponding carries they produce. Note that the last two digits in the sum are colored black, as they do not result from any specific column but are instead generated solely from the carries.

$$\begin{array}{cccccccc}
 & {\scriptstyle 1} & {\scriptstyle 0} & & & & & \\
 & & {\scriptstyle 1} & {\scriptstyle 0} & & {\scriptstyle 1} & & \\
 & & & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 0} & \\
 & & & 1 & 1 & 1 & 1 & 1 \\
+ & & & 1 & 1 & 1 & 0 & 1 \\
+ & & & 1 & 1 & 1 & 0 & 1 \\
+ & & & 1 & 1 & 1 & 1 & 1 \\
\hline
 & 1 & 1 & 1 & 1 & 0 & 0 & 1
\end{array}$$

Method 2: Direct Summation and Simplification

We will illustrate the second method using the same example. In the previous case, we carried the actual binary number to the next columns. In this method, we write down 0 if the sum is even and 1 if the sum is odd. Every time a sum a multiple of 2, we carry a 1 to the next columns, and then continue this process for each column, including the carries in the calculation of that column.

Step 1: Add the Rightmost Column
Add bits in column 1 (from counting from MSB):

$$1 + 1 + 1 + 1 = 100_2 \quad (\text{ which is binary for } 4)$$

Reading the result from LSB to MSB

- write down the 0
- carry a 1 for the first multiple of 2
- carry a 1 for the second multiple of 2

This results in

$$\begin{array}{rccccc}
 & & & & {\scriptstyle 1} & \\
 & & & & {\scriptstyle 1} & \\
 & 1 & 1 & 1 & 1 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 1 & 1 \\
\hline
 & & & & & 0
\end{array}$$

Step 2: Add the Second Column from the Right
Add bits in column 2 (from counting from MSB):

$$1 + 1 + 1 + 1 = 100_2 \quad (\text{ which is binary for } 4)$$

Reading the result from LSB to MSB

- write down the 0
- carry a 1 for the first multiple of 2
- carry a 1 for the second multiple of 2

This results in

$$\begin{array}{rccccc}
 & & & {\scriptstyle 1} & & \\
 & & & {\scriptstyle 1} & & \\
 & 1 & 1 & 1 & 1 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 1 & 1 \\
\hline
 & & & & 0 & 0
\end{array}$$

Step 3: Add the Third Column from the Right

Add bits in column 3 (from counting from MSB):

$$1+1+1+1+1+1 = 110_2 \quad (\text{ which is binary for } 6)$$

Reading the result from LSB to MSB

- write down the 0
- carry a 1 for the first multiple of 2
- carry a 1 for the second multiple of 2
- carry a 1 for the third multiple of 2

This results in

$$\begin{array}{cccccc}
 & & \scriptstyle 1 & & & \\
 & & \scriptstyle 1 & & & \\
 & & \scriptstyle 1 & & & \\
 & 1 & 1 & 1 & 1 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 1 & 1 \\ \hline
 & & & 0 & 0 & 0
\end{array}$$

Step 4: Add the Fourth Column from the Right
Add bits in column 4 (from counting from MSB):

$$1+1+1+1+1+1+1 = 111_2 \quad (\text{ which is binary for } 7)$$

Reading the result from LSB to MSB

- write down the 1
- carry a 1 for the first multiple of 2
- carry a 1 for the second multiple of 2
- carry a 1 for the third multiple of 2

This results in

$$\begin{array}{cccccc}
 & \scriptstyle 1 & & & & \\
 & \scriptstyle 1 & & & & \\
 & \scriptstyle 1 & & & & \\
 & 1 & 1 & 1 & 1 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 0 & 1 \\
+ & 1 & 1 & 1 & 1 & 1 \\ \hline
 & & 1 & 0 & 0 & 0
\end{array}$$

Step 5: Add the Leftmost Column
Add bits in leftmost column):

$$1+1+1+1+1+1+1 = 111_2 \quad (\text{ which is binary for } 7)$$

Reading the result from LSB to MSB

- write down the result in binary, i.e. 1 1 1

This results in

$$\begin{array}{rccccccc}
 & & & 1 & 1 & 1 & 1 & 1 \\
+ & & & 1 & 1 & 1 & 0 & 1 \\
+ & & & 1 & 1 & 1 & 0 & 1 \\
+ & & & 1 & 1 & 1 & 1 & 1 \\
\hline
 & 1 & 1 & 1 & 1 & 0 & 0 & 0
\end{array}$$

which corresponds to the result we obtained above. While not demonstrated explicitly here, subtraction works in a similar fashion.

By using one of these methods for handling multiple carries, allow us to also multiply two binary numbers.

Multiplication in Binary

Multiplication in binary is technically easier than multiplication in decimal. In binary operations, we work exclusively with two digits: 0 and 1. This means that both the the multiplier[1] and multiplicand consist of 0's and 1' (and so does the multiplicand). The process of finding the binary product is analogous to traditional multiplication in the decimal system. The four five steps involved in multiplying binary digits are:

$$0 \times 0 = 0$$

$$0 \times 1 = 0$$

$$1 \times 0 = 0$$

$$1 \times 1 = 1$$

$$1 \times 10_2 = 10_2 \quad (\text{multiplying by base } 10_2 \text{ adds a 0 to the end})$$

The last step means that $101_2 \times 10_2 = 1010_2$ which is analogous to the decimal case: $143_{10} \times 10_{10} = 1430_{10}$.

We will illustrate the process by supplying a couple of examples.

Example 3.1

[1] The ”multiplicand” is the number that has to be multiplied, and the ”multiplier” is the number by which it is multiplied.

$$\begin{array}{ccrrrr}
 & (1) & & 1 & 0 & 0 \\
\times & (2) & & & 1 & 1 \\ \hdashline
 & (3) & & 1 & 0 & 0 \\
+ & (4) & 1 & 0 & 0 & 0 \\ \hline
 & (5) & 1 & 1 & 0 & 0
\end{array}$$

Here are the steps:

- Multiply the multiplicand (line 1) by the LSB of the multiplier (line 2), which in this case is 1.
- Record this result in line 3.
- Append a 0 to line 4 to account for the shift to the next power of 2 in the multiplier.
- Multiply the multiplicand (line 1) by the next bit of the multiplier (line 2), which is also 1 in this case.
- Add this result to line 4, after the 0 you appended earlier.
- Finally, sum the values in lines 3 and 4, as outlined in the previous section, to obtain the final result in line 5.

We offer two additional examples:

Example 3.2

$$\begin{array}{crrrrrr}
 & & & & 1 & 0 & 1 \\
\times & & & 1 & 0 & 1 & 1 \\ \hdashline
 & & & & 1 & 0 & 1 \\
+ & & & 1 & 0 & 1 & 0 \\
+ & & 0 & 0 & 0 & 0 & 0 \\
+ & 1 & 0 & 1 & 0 & 0 & 0 \\ \hline
 & 1 & 1 & 0 & 1 & 1 & 1
\end{array}$$

Example 3.3

$$\begin{array}{crrrrrrrrr}
 & & & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
\times & & & & & & & 1 & 0 & 1 \\ \hdashline
 & & & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
+ & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline
 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0
\end{array}$$

In example 3.3 notice that we omitted the row of zeroes that the second value of the multiplier would have produced, and notice even further that we added two 0's before restating the multiplicand in the sum.

Binary multiplication, like binary addition, is a core operation in computer arithmetic. By breaking the process down into manageable steps—multiplying individual bits and then summing the results—it becomes clear how similar it is to the multiplication methods we use in the decimal system. The main difference is the simplicity and efficiency of working within the binary system, where only the digits 0 and 1 are involved.

We notice how binary multiplication builds on binary addition. Each step, involving shifts and sums, essentially consists of repeated additions adjusted by powers of two. A strong grasp of binary addition naturally leads to a better understanding of binary multiplication and its applications.

3.2 Octal and Hexadecimal

Octal is a base-8 numbering system that uses the digits 0 through 7. It is closely related to binary, which is a base-2 system. The connection between the two lies in how easily binary numbers can be converted to octal and vice versa. Each octal digit corresponds to exactly three binary digits (bits), making conversions straightforward. For example, the binary number '110' converts directly to the octal digit '6'. Because of this close relationship, octal is often used as a shorthand for binary in computing, particularly in contexts where grouping binary digits in sets of three simplifies reading and interpreting binary data.

$$12_8 = 1 \cdot 8^1 + 2 \cdot 8^0 = 10_{10}$$
$$3021_8 = 3 \cdot 8^3 + 0 \cdot 8^2 + 2 \cdot 8^1 + 1 \cdot 8^0 = 1553_{10}$$

Since 8 is 2^3, we can express it in binary:

$3 \rightarrow 011$

$0 \rightarrow 000$

$2 \rightarrow 010$

$1 \rightarrow 001$

Thus, $3021_8 = 011000010001_2 = 11000010001_2$

We obtain the final result by removing leading zeros.

Hexadecimal is a base-16 numbering system that uses sixteen distinct symbols: the digits 0-9 and the letters A-F, where A represents 10, B represents 11, and so on up to F, which represents 15. Hexadecimal is closely related to binary because each hexadecimal digit corresponds exactly to four binary digits (bits). This direct relationship makes it easy to convert between the two systems. For example, the hexadecimal digit 'A' translates to the binary sequence '1010'. Due to this efficiency in grouping, hexadecimal is often used in computing as a more compact and readable way to represent binary data, particularly in areas like memory addresses and colour codes in web design.

$$123_{16} = 1 \cdot 16^2 + 2 \cdot 16^1 + 3 \cdot 16^0 = 256 + 32 + 3 = 291_{10}$$
$$A2E_{16} = 10 \cdot 16^2 + 2 \cdot 16^1 + 14 \cdot 16^0 = 2560 + 32 + 14 = 2606_{10}$$

Since 16 is 2^4, we can express it in binary:

$5 \rightarrow 0101$

$E \rightarrow 1110$

$B \rightarrow 1011$

$5 \rightarrow 0101$

$2 \rightarrow 0010$

Thus, $A2E_{16} = 101000101110_2$

Again, notice that we removed the leading 0's from 5_{16} when writing the result.

3.3 Converting Between Systems

Understanding how to convert numbers between binary, decimal, octal, and hexadecimal systems is essential in computer science and digital electronics. Each system is a different base, and each has its own applications. Here's a step-by-step guide to help you convert numbers from one system to another.

Decimal to Binary Conversion

To convert a decimal number to binary:

1. Divide the decimal number by 2.
2. Record the remainder (it will be 0 or 1).
3. Divide the quotient by 2 and record the remainder.
4. Repeat until the quotient is 0.
5. The binary number is the sequence of remainders read from bottom to top.

Example 3.4 Convert 23_{10} to binary.

Solution:

$$\begin{aligned}
23 \div 2 &= 11 \quad \text{remainder } 1 \\
11 \div 2 &= 5 \quad \text{remainder } 1 \\
5 \div 2 &= 2 \quad \text{remainder } 1 \\
2 \div 2 &= 1 \quad \text{remainder } 0 \\
1 \div 2 &= 0 \quad \text{remainder } 1
\end{aligned}$$

Thus, $23_{10} = 10111_2$. ◀

Decimal to Octal Conversion

To convert a decimal number to octal:

1. Divide the decimal number by 8.
2. Record the remainder.
3. Divide the quotient by 8 and record the remainder.
4. Repeat until the quotient is 0.
5. The octal number is the sequence of remainders read from bottom to top.

Example 3.5 Convert 78_{10} to octal.

Solution:

$$\begin{aligned} 78 \div 8 &= 9 \quad \text{remainder } 6 \\ 9 \div 8 &= 1 \quad \text{remainder } 1 \\ 1 \div 8 &= 0 \quad \text{remainder } 1 \end{aligned}$$

Thus, $78_{10} = 116_8$. ◀

Decimal to Hexadecimal Conversion

To convert a decimal number to hexadecimal:

1. Divide the decimal number by 16.
2. Record the remainder (use A, B, C, D, E, F for remainders 10, 11, 12, 13, 14, 15 respectively).
3. Divide the quotient by 16 and record the remainder.
4. Repeat until the quotient is 0.
5. The hexadecimal number is the sequence of remainders read from bottom to top.

Example 3.6 Convert 255_{10} to hexadecimal.

Solution:

$$\begin{aligned} 255 \div 16 &= 15 \quad \text{remainder } 15 \quad (\text{F}) \\ 15 \div 16 &= 0 \quad \text{remainder } 15 \quad (\text{F}) \end{aligned}$$

Thus, $255_{10} = FF_{16}$. ◀

Binary to Decimal Conversion

To convert a binary number to decimal:

1. Multiply each bit by 2 raised to the power of its position, starting from 0 on the right.
2. Sum all the products.

Notice that this amounts to the method outlined above about binary expansion.

Example 3.7 Convert 1101_2 to decimal.

Solution:

$$1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 8 + 4 + 0 + 1 = 13_{10}$$

◀

Binary to Octal Conversion

To convert a binary number to octal:

1. Group the binary digits into sets of three, starting from the right. Add leading zeros if necessary.
2. Convert each group of three binary digits to its octal equivalent.

Example 3.8 Convert 110110_2 to octal.

Solution:

$$110 \to 6$$

$$110 \to 6$$

Thus, $110110_2 = 66_8$. ◀

Binary to Hexadecimal Conversion

To convert a binary number to hexadecimal:

1. Group the binary digits into sets of four, starting from the right. Add leading zeros if necessary.
2. Convert each group of four binary digits to its hexadecimal equivalent.

Example 3.9 Convert 10110101_2 to hexadecimal.

Solution:

$$1011 \to B$$

$$0101 \to 5$$

Thus, $10110101_2 = B5_{16}$. ◀

Octal to Binary Conversion

To convert an octal number to binary:

1. Convert each octal digit to its 3-bit binary equivalent.

Example 3.10 Convert 57_8 to binary.

Solution:

$$5 \to 101$$

$$7 \to 111$$

Thus, $57_8 = 101111_2$. ◀

Octal to Decimal Conversion

To convert an octal number to decimal:

1. Multiply each digit by 8 raised to the power of its position, starting from 0 on the right.
2. Sum all the products.

Example 3.11 Convert 157_8 to decimal.

Solution:

$$1 \cdot 8^2 + 5 \cdot 8^1 + 7 \cdot 8^0 = 64 + 40 + 7 = 111_{10}$$

◀

Octal to Hexadecimal Conversion

To convert an octal number to hexadecimal:

1. First, convert the octal number to binary.
2. Then, convert the binary number to hexadecimal by grouping the binary digits in sets of four.

Example 3.12 Convert 157_8 to hexadecimal.

Solution:

$$1 \to 001$$
$$5 \to 101$$
$$7 \to 111$$

Thus, $157_8 = 001101111_2 = 6F_{16}$. ◀

Hexadecimal to Binary Conversion

To convert a hexadecimal number to binary:

1. Convert each hexadecimal digit to its 4-bit binary equivalent.

Example 3.13 Convert $2B_16$ to binary.

Solution:

$$2 \to 0010$$
$$B \to 1011$$

Thus, $2B_{16} = 00101011_2$. ◀

Hexadecimal to Decimal Conversion

To convert a hexadecimal number to decimal:

1. Multiply each digit by 16 raised to the power of its position, starting from 0 on the right.
2. Sum all the products.

Example 3.14 Convert $2B_16$ to decimal.

Solution:

$$2 \cdot 16^1 + 11 \cdot 16^0 = 32 + 11 = 43_{10}$$

◀

Hexadecimal to Octal Conversion

To convert a hexadecimal number to octal:

1. First, convert the hexadecimal number to binary.
2. Then, convert the binary number to octal by grouping the binary digits in sets of three.

Example 3.15 Convert $2B_16$ to octal.

Solution:

$$\begin{aligned} 2 &\rightarrow 0010 \\ B &\rightarrow 1011 \end{aligned}$$

Thus, $2B_{16} = 00101011_2 = 53_8$.

Final Thoughts on Conversion

The concept of expansion plays a central role in these conversions. Whether you are expanding a decimal number into its binary, octal, or hexadecimal form, or converting a binary number into its octal or hexadecimal equivalent, you are more or less expressing the number in terms of powers of the base. The expansion method is essentially the same for each system as it boils down to dividing by the highest power of the base recursively:

$$\begin{aligned} 7562_{10} &= 1 \cdot 16^3 + 3466 = 1 \cdot 16^3 + 13 \cdot 16^2 + 138 \\ &= 1 \cdot 16^3 + 13 \cdot 16^2 + 8 \cdot 16^1 + 10 \cdot 16^0 = 1\,D\,8\,A \end{aligned}$$

By understanding these expansions and the relationships between these number systems, you can efficiently switch between them, allowing you to represent and manipulate data in the most suitable format for any given situation.