John Vince

Foundation Mathematics for Computer Science

A Visual Approach

Second Edition

Springer

John Vince
Bournemouth University
Breinton, Hereford, UK

ISBN 978-3-030-42077-2 ISBN 978-3-030-42078-9 (eBook)
https://doi.org/10.1007/978-3-030-42078-9

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Chapter 1
Visual Mathematics

1.1 Visual Brains Versus Analytic Brains

I consider myself a *visual* person, as pictures help me understand complex problems. I also don't find it too difficult to visualise objects from different view points. I remember learning about electrons, neutrons and protons for the first time, where our planetary system provided a simple model to visualise the hidden structure of matter. My mental image of electrons was one of small orange spheres, spinning around a small, central nucleus containing blue protons and grey neutrons. And although this visual model was seriously flawed, it provided a first step towards understanding the structure of matter.

As my knowledge of mathematics grew, this, too, was image based. Equations were curves and surfaces, simultaneous equations were intersecting or parallel lines, etc., and when I embarked upon computer science, I found a natural application for mathematics. For me, mathematics is a visual science, although I do appreciate that many professional mathematicians need only a formal, symbolic notation for constructing their world. Such people do not require visual scaffolding—they seem to be able to manipulate abstract mathematical concepts at a symbolic level. Their books do not require illustrations or diagrams—Greek symbols, upside-down and back-to-front Latin fonts are sufficient to annotate their ideas.

Today, when reading popular science books on quantum theory, I still try to form images of 3D fields of energy and probability oscillating in space—to no avail—and I have accepted that human knowledge of such phenomena is best left to a mathematical description. Nevertheless, mathematicians, such as Sir Roger Penrose, know the importance of visual models in communicating complex mathematical ideas. His book *The Road to Reality: A Complete Guide to the Laws of the Universe* is decorated with beautiful, informative, hand-drawn illustrations, which help readers understand the mathematics of science. In this book I rely heavily on images to communicate an idea. They are simple and are the first step on a ladder towards understanding a difficult idea. Eventually, when that *Eureka* moment arrives, that moment when

J. Vince, *Foundation Mathematics for Computer Science*,
https://doi.org/10.1007/978-3-030-42078-9_1

"I understand what you are saying," the image becomes closely associated with the mathematical notation.

1.2 Learning Mathematics

I was fortunate in my studies in that I was taught by people interested in mathematics, and their interest rubbed off on me. I feel sorry for children who have given up on mathematics, simply because they are being taught by teachers whose primary subject is not mathematics. I was never too concerned about the uses of mathematics, although applied mathematics is of special interest.

One of the problems with mathematics is its incredible breadth and depth. It embraces everything from 2D geometry, calculus, topology, statistics, complex functions to number theory and propositional calculus. All of these subjects can be studied superficially or to a mind-numbing complexity. Fortunately, no one is required to understand everything, which is why mathematicians tend to specialise in one or two areas and develop a specialist knowledge.

1.3 What Makes Mathematics Difficult?

"What makes mathematics difficult?" is also a difficult question to answer, but one that has to be asked and answered. There are many answers to this question, and I believe that problems begin with mathematical notation and how to read it; how to analyse a problem and express a solution using mathematical statements. Unlike learning a foreign language—which I find very difficult—mathematics is a language that needs to be learned by discovering facts and building upon them to discover new facts. Consequently, a good memory is always an advantage, as well as a sense of logic.

Mathematics can be difficult for anyone, including mathematicians. For example, when the idea of $\sqrt{-1}$ was originally proposed, it was criticised and looked down upon by mathematicians, mainly because its purpose was not fully understood. Eventually, it transformed the entire mathematical landscape, including physics. Similarly, when the German mathematician Georg Cantor (1845–1919), published his papers on set theory and transfinite sets, some mathematicians hounded him in a disgraceful manner. The German mathematician Leopold Kronecker (1823–1891), called Cantor a "scientific charlatan", a "renegade", and a "corrupter of youth", and did everything to hinder Cantor's academic career. Similarly, the French mathematician and physicist Henri Poincaré (1854–1912), called Cantor's ideas a "grave disease", whilst the Austrian-British philosopher and logician Ludwig Wittgenstein (1889–1951) complained that mathematics is "ridden through and through with the pernicious idioms of set theory." How wrong they all were. Today, set theory is a major branch of mathematics and has found its way into every math curriculum. So don't be surprised to discover that some mathematical ideas are initially difficult to understand—you are in good company.

1.4 Does Mathematics Exist Outside Our Brains?

Many people have considered the question "What is mathematics?" Some mathematicians and philosophers argue that numbers and mathematical formulae have some sort of external existence and are waiting to be discovered by us. Personally, I don't accept this idea. I believe that we enjoy searching for patterns and structure in anything that finds its way into our brains, which is why we love poetry, music, storytelling, art, singing, architecture, science, as well as mathematics. The piano, for example, is an instrument for playing music using different patterns of notes. When the piano was invented—a few hundred years ago—the music of Chopin, Liszt and Rachmaninoff did not exist in any form—it had to be composed by them. Similarly, by building a system for counting using numbers, we have an amazing tool for composing mathematical systems that help us measure quantity, structure, space and change. Such systems have been applied to topics such as fluid dynamics, optimisation, statistics, cryptography, game theory probability theory, and many more. I will attempt to develop this same idea by showing how the concept of number, and the visual representation of number reveals all sorts of patterns, that give rise to number systems, algebra, trigonometry, geometry, analytic geometry and calculus. The universe does not need any of these mathematical ideas to run its machinery, but we need these ideas to understand its operation.

1.5 Symbols and Notation

One of the reasons why many people find mathematics inaccessible is due to its symbols and notation. Let's look at symbols first. The English alphabet possesses a reasonable range of familiar character shapes:

a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z
A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z

which find their way into every branch of mathematics and physics, and permit us to write equations such as

$$E = mc^2$$

and

$$A = \pi r^2.$$

It is important that when we see an equation, we are able to read it as part of the text. In the case of $E = mc^2$, this is read as "E equals m, c squared", where E stands for energy, m for mass, and c the speed of light. In the case of $A = \pi r^2$, this is read as "A equals pi, r squared", where A stands for area, π the ratio of a circle's circumference to its diameter, and r the circle's radius. Greek symbols, which happen to look nice and impressive, have also found their way into many equations, and often disrupt the flow of reading, simply because we don't know their English names. For example, the English theoretical physicist Paul Dirac (1902–1984) derived an equation for a moving electron using the symbols α_i and β, which are 4×4 matrices, where

$$\alpha_i \beta + \beta \alpha_i = 0$$

and is read as

"the sum of the products alpha-i beta, and beta alpha-i, equals zero."

Although we will not come across moving electrons in this book, we will have to be familiar with the following Greek symbols:

α	alpha	ν	nu
β	beta	ξ	xi
γ	gamma	o	o
δ	delta	π	pi
ϵ	epsilon	ρ	rho
ζ	zeta	σ	sigma
η	eta	τ	tau
θ	theta	υ	upsilon
ι	iota	ϕ	phi
κ	kappa	χ	chi
λ	lambda	ψ	psi
μ	mu	ω	omega

and some upper-case symbols:

$\varGamma$	Gamma	$\varSigma$	Sigma
$\varDelta$	Delta	$\varUpsilon$	Upsilon
$\varTheta$	Theta	$\varPhi$	Phi
$\varLambda$	Lambda	$\varPsi$	Psi
$\varXi$	Xi	$\varOmega$	Omega
$\varPi$	Pi.		

Being able to read an equation does not mean that we understand it—but we are a little closer than just being able to stare at a jumble of symbols! Therefore, in future, when I introduce a new mathematical object, I will tell you how it should be read.

Chapter 2
Numbers

2.1 Introduction

This chapter revises the sets of numbers employed in mathematics such as natural, integer, rational, irrational, real, algebraic, transcendental, imaginary, complex, quaternions and octonions. It also describes how these numbers behave in the context of three laws: commutative law, associative law and the distributive law. Apart from the every-day base of 10, the three important bases in computer science are covered: binary, octal and hexadecimal.

As prime numbers find their way into all aspects of cryptography, the chapter introduces the fundamental theorem of arithmetic, prime number distribution, perfect numbers and Mersenne numbers. The chapter concludes with the concept of infinity and some worked examples.

2.2 Counting

Our brain's visual cortex possesses some incredible image processing features. For example, children know instinctively when they are given less sweets than another child, and adults know instinctively when they are short-changed by a Parisian taxi driver, or driven around the Arc de Triumph several times, on the way to the airport! Intuitively, we can assess how many donkeys are in a field without counting them, and generally, we seem to know within a second or two, whether there are just a few, dozens, or hundreds of something. But when accuracy is required, one can't beat counting. But what is counting?

Well normally, we are taught to count by our parents by memorising first, the counting words *one, two, three, four, five, six, seven, eight, nine, ten,* .. and second, associating them with our fingers, so that when asked to count the number of donkeys in a picture book, each donkey is associated with a counting word. When each donkey has been identified, the number of donkeys equals the last word mentioned.

J. Vince, *Foundation Mathematics for Computer Science*,
https://doi.org/10.1007/978-3-030-42078-9_2

However, this still assumes that we know the meaning of *one, two, three, four, ..* etc. Memorising these counting words is only part of the problem—getting them in the correct sequence is the real challenge. The incorrect sequence *one, two, five, three, nine, four, ..* etc., introduces an element of randomness into any calculation, but practice makes perfect, and it's useful to master the correct sequence before going to university!

2.3 Sets of Numbers

A *set* is a collection of distinct objects called its *elements* or *members*. For example, each system of number belongs to a set with given a name, such as $\mathbb{N}$ for the natural numbers, $\mathbb{R}$ for real numbers, and $\mathbb{Q}$ for rational numbers. When we want to indicate that something is whole, real or rational, etc., we use the notation

$$n \in \mathbb{N}$$

which reads "n is a member of ($\in$) the set $\mathbb{N}$", i.e. n is a whole number. Similarly,

$$x \in \mathbb{R}$$

stands for "x is a real number."

A *well-ordered set* possesses a unique order, such as the natural numbers $\mathbb{N}$. Therefore, if P is the well-ordered set of prime numbers and $\mathbb{N}$ is the well-ordered set of natural numbers, we can write

$$\begin{aligned} P &= \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \dots\} \\ \mathbb{N} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, \dots\}. \end{aligned}$$

By pairing the prime numbers in P with the numbers in $\mathbb{N}$, we have

$$\{2, 1\}, \{3, 2\}, \{5, 3\}, \{7, 4\}, \{11, 5\}, \{13, 6\}, \{17, 7\}, \{19, 8\}, \{23, 9\}, \dots$$

and we can reason that 2 is the 1st prime, and 3 is the 2nd prime, etc. However, we still have to declare what we mean by 1, 2, 3, 4, 5, ... etc., and without getting too philosophical, I like the idea of defining them as follows. The word *one*, represented by 1, stands for one-ness of anything: one finger, one house, one tree, one donkey, etc. The word *two*, represented by 2, is "one more than one". The word *three*, represented by 3, is "one more than two", and so on.

We are now in a position to associate some mathematical notation with our numbers by introducing the $+$ and $=$ signs. We know that $+$ means *add*, but it also can stand for *more*. We also know that $=$ means *equal*, and it can also stand for *is the same as*. Thus the statement

$$2 = 1 + 1$$

is read as “two is the same as one more than one.”

We can also write

$$3 = 1 + 2$$

which is read as “three is the same as one more than two.” But as we already have a definition for 2, we can write

$$\begin{aligned} 3 &= 1 + 2 \\ &= 1 + 1 + 1. \end{aligned}$$

Developing this idea, and including some extra combinations, we have

$$\begin{aligned} 2 &= 1 + 1 \\ 3 &= 1 + 2 \\ 4 &= 1 + 3 = 2 + 2 \\ 5 &= 1 + 4 = 2 + 3 \\ 6 &= 1 + 5 = 2 + 4 = 3 + 3 \\ 7 &= 1 + 6 = 2 + 5 = 3 + 4 \\ &\text{etc.} \end{aligned}$$

and can be continued without limit. The numbers, 1, 2, 3, 4, 5, 6, etc., are called *natural numbers*, and are the set $\mathbb{N}$.

2.4 Zero

The concept of zero has a well-documented history, which shows that it has been used by different cultures over a period of two-thousand years or more. It was the Indian mathematician and astronomer Brahmagupta (598-c.–670) who argued that zero was just as valid as any natural number, with the definition: *the result of subtracting any number from itself*. However, even today, there is no universal agreement as to whether zero belongs to the set $\mathbb{N}$, consequently, the set $\mathbb{N}^0$ stands for the set of natural numbers including zero.

In today’s positional decimal system, which is a *place value system*, the digit 0 is a placeholder. For example, 203 stands for: two hundreds, no tens and three units. Although $0 \in \mathbb{N}^0$, it does have special properties that distinguish it from other members of the set, and Brahmagupta also gave rules showing this interaction.

If $x \in \mathbb{N}^0$, then the following rules apply:

$$\begin{aligned} \text{addition:} \quad & x + 0 = x \\ \text{subtraction:} \quad & x - 0 = x \\ \text{multiplication:} \quad & x \times 0 = 0 \times x = 0 \\ \text{division:} \quad & 0/x = 0 \\ \text{undefined division:} \quad & x/0. \end{aligned}$$

The expression $0/0$ is called an *indeterminate form*, as it is possible to show that under different conditions, especially limiting conditions, it can equal anything. So for the moment, we will avoid using it until we cover calculus.

2.5 Negative Numbers

When negative numbers were first proposed, they were not accepted with open arms, as it was difficult to visualise -5 of something. For instance, if there are 5 donkeys in a field, and they are all stolen to make salami, the field is now empty, and there is nothing we can do in the arithmetic of donkeys to create a field of -5 donkeys. However, in applied mathematics, numbers have to represent all sorts of quantities such as temperature, displacement, angular rotation, speed, acceleration, etc., and we also need to incorporate ideas such as left and right, up and down, before and after, forwards and backwards, etc. Fortunately, negative numbers are perfect for representing all of the above quantities and ideas.

Consider the expression $4 - x$, where $x \in \mathbb{N}^0$. When x takes on certain values, we have

$$\begin{aligned} 4 - 1 &= 3 \\ 4 - 2 &= 2 \\ 4 - 3 &= 1 \\ 4 - 4 &= 0 \end{aligned}$$

and unless we introduce negative numbers, we are unable to express the result of $4 - 5$. Consequently, negative numbers are visualised as shown in Fig. 2.1, where the *number line* shows negative numbers to the left of the natural numbers, which are *positive*, although the $+$ sign is omitted for clarity.

Fig. 2.1 The number line showing negative and positive numbers

Moving from left to right, the number line provides a numerical continuum from large negative numbers, through zero, towards large positive numbers. In any calculation we could agree that angles above the horizon are positive, and angles below the horizon, negative. Similarly, a movement forwards is positive, and a movement backwards is negative. So now we are able to write

$$
\begin{gathered}
4-5=-1 \\
4-6=-2 \\
4-7=-3 \\
\text{etc.,}
\end{gathered}
$$

without worrying about creating impossible conditions.

2.5.1 The Arithmetic of Positive and Negative Numbers

Once again, Brahmagupta compiled all the rules, Tables 2.1 and 2.2, supporting the addition, subtraction, multiplication and division of positive and negative numbers. The real fly in the ointment, being negative numbers, which cause problems for children, math teachers and occasional accidents for mathematicians. Perhaps, the one rule we all remember from our school days is that "two negatives make a positive".

Another problem with negative numbers arises when we employ the square-root function. As the product of two positive or negative numbers results in a positive result, the square-root of a positive number gives rise to a positive **and** a negative answer. For example, $\sqrt{4} = \pm 2$. This means that the square-root function only applies to positive numbers. Nevertheless, it did not stop the invention of the *imaginary* unit i, where $i^2 = -1$. However, i is not a number, but an operator, which is described later.

Table 2.1 Rules for adding and subtracting positive and negative numbers

$+$	b	$-b$	$-$	b	$-b$
a	$a+b$	$a-b$	a	$a-b$	$a+b$
$-a$	$b-a$	$-(a+b)$	$-a$	$-(a+b)$	$b-a$

Table 2.2 Rules for multiplying and dividing positive and negative numbers

$\times$	b	$-b$	$/$	b	$-b$
a	ab	$-ab$	a	a/b	$-a/b$
$-a$	$-ab$	ab	$-a$	$-a/b$	a/b

2.6 Observations and Axioms

The following *axioms* or laws provide a formal basis for mathematics, and in the descriptions a *binary operation* is an arithmetic operation such as $+$, $-$, $\times$, / which operates on two operands.

2.6.1 Commutative Law

The *commutative law* in algebra states that when two elements are linked through some binary operation, the result is independent of the order of the elements. The commutative law of addition is

$$\begin{aligned} a + b &= b + a \\ \text{e.g. } 1 + 2 &= 2 + 1. \end{aligned}$$

The commutative law of multiplication is

$$\begin{aligned} a \times b &= b \times a \\ \text{e.g. } 1 \times 2 &= 2 \times 1. \end{aligned}$$

Note that subtraction is not commutative

$$\begin{aligned} a - b &\neq b - a \\ \text{e.g. } 1 - 2 &\neq 2 - 1. \end{aligned}$$

2.6.2 Associative Law

The *associative law* in algebra states that when three or more elements are linked together through a binary operation, the result is independent of how each pair of elements is grouped. The associative law of addition is

$$\begin{aligned} a + (b + c) &= (a + b) + c \\ \text{e.g. } 1 + (2 + 3) &= (1 + 2) + 3. \end{aligned}$$

The associative law of multiplication is

$$\begin{aligned} a \times (b \times c) &= (a \times b) \times c \\ \text{e.g. } 1 \times (2 \times 3) &= (1 \times 2) \times 3. \end{aligned}$$

However, note that subtraction is not associative

$$a - (b - c) \neq (a - b) - c$$
$$\text{e.g. } 1 - (2 - 3) \neq (1 - 2) - 3.$$

which may seem surprising, but at the same time confirms the need for clear axioms.

2.6.3 Distributive Law

The *distributive law* in algebra describes an operation which when performed on a combination of elements is the same as performing the operation on the individual elements. The distributive law does not work in all cases of arithmetic. For example, multiplication over addition holds

$$a(b + c) = ab + ac$$
$$\text{e.g. } 2(3 + 4) = 6 + 8,$$

whereas addition over multiplication does not:

$$a + (b \times c) \neq (a + b) \times (a + c)$$
$$\text{e.g. } 3 + (4 \times 5) \neq (3 + 4) \times (3 + 5).$$

Although these laws are natural for numbers, they do not necessarily apply to all mathematical objects. For instance, the vector product, which multiplies two vectors together, is not commutative. The same applies for matrix multiplication.

2.7 The Base of a Number System

2.7.1 Background

Over recent millennia, mankind has invented and discarded many systems for representing number. People have counted on their fingers and toes, used pictures (hieroglyphics), cut marks on clay tablets (cuneiform symbols), employed Greek symbols (Ionic system) and struggled with, and abandoned Roman numerals (I, V, X, L, C, D, M, etc.), until we reach today's decimal place system, which has Hindu-Arabic and Chinese origins. And since the invention of computers, we have witnessed the emergence of binary, octal and hexadecimal number systems, where 2, 8 and 16 respectively, replace the 10 in our decimal system.

The decimal number 23 means "two tens and three units", and in English is written "twenty-three", in French "vingt-trois" (twenty-three), and in German "dreiundzwanzig" (three and twenty). Let's investigate the algebra behind the decimal system and see how it can be used to represent numbers to any base. The expression

$$a \times 1000 + b \times 100 + c \times 10 + d \times 1$$

where a, b, c, d take on any value between 0 and 9, describes any whole number between 0 and 9999. By including

$$e \times 0.1 + f \times 0.01 + g \times 0.001 + h \times 0.0001$$

where e, f, g, h take on any value between 0 and 9, any decimal number between 0 and 9999.9999 can be represented.

Indices bring the notation alive and reveal the true underlying pattern:

$$\dots a10^3 + b10^2 + c10^1 + d10^0 + e10^{-1} + f10^{-2} + g10^{-3} + h10^{-4} \dots.$$

Remember that any number raised to the power 0 equals 1. By adding extra terms both left and right, any number can be accommodated.

In this example, 10 is the base, which means that the values of a to h range between 0 and 9, 1 less than the base. Therefore, by substituting B for the base we have

$$\dots aB^3 + bB^2 + cB^1 + dB^0 + eB^{-1} + fB^{-2} + gB^{-3} + hB^{-4} \dots$$

where the values of a to h range between 0 and $B - 1$.

2.7.2 Octal Numbers

The octal number system has $B = 8$, and a to h range between 0 and 7

$$\dots a8^3 + b8^2 + c8^1 + d8^0 + e8^{-1} + f8^{-2} + g8^{-3} + h8^{-4} \dots$$

and the first 17 octal numbers are

$$1_8, 2_8, 3_8, 4_8, 5_8, 6_8, 7_8, 10_8, 11_8, 12_8, 13_8, 14_8, 15_8, 16_8, 17_8, 20_8, 21_8.$$

The subscript 8, reminds us that although we may continue to use the words "twenty-one", it is an octal number, and not a decimal. But what is 14_8 in decimal? Well, it stands for

$$1 \times 8^1 + 4 \times 8^0 = 12.$$

Thus 356.4_8 in decimal, equals

$$\begin{gathered}(3 \times 8^2) + (5 \times 8^1) + (6 \times 8^0) + (4 \times 8^{-1})\\(3 \times 64) + (5 \times 8) + (6 \times 1) + (4 \times 0.125)\\(192 + 40 + 6) + (0.5)\\238.5.\end{gathered}$$

Counting in octal appears difficult, simply because we have never been exposed to it, like the decimal system. If we had evolved with 8 fingers, instead of 10, we would be counting in octal!

2.7.3 Binary Numbers

The binary number system has $B = 2$, and a to h are 0 or 1

$$\dots a2^3 + b2^2 + c2^1 + d2^0 + e2^{-1} + f2^{-2} + g2^{-3} + h2^{-4} \dots$$

and the first 13 binary numbers are

$$1_2, 10_2, 11_2, 100_2, 101_2, 110_2, 111_2, 1000_2, 1001_2, 1010_2, 1011_2, 1100_2, 1101_2.$$

Thus 11011.11_2 in decimal, equals

$$\begin{gathered}(1 \times 2^4) + (1 \times 2^3) + (0 \times 2^2) + (1 \times 2^1) + (1 \times 2^0) + (1 \times 2^{-1}) + (1 \times 2^{-2})\\(1 \times 16) + (1 \times 8) + (0 \times 4) + (1 \times 2) + (1 \times 0.5) + (1 \times 0.25)\\(16 + 8 + 2) + (0.5 + 0.25)\\26.75.\end{gathered}$$

The reason why computers work with binary numbers—rather than decimal—is due to the difficulty of designing electrical circuits that can store decimal numbers in a stable fashion. A switch, where the open state represents 0, and the closed state represents 1, is the simplest electrical component to emulate. No matter how often it is used, or how old it becomes, it will always behave like a switch. The main advantage of electrical circuits is that they can be switched on and off trillions of times a second, and the only disadvantage is that the encoded binary numbers and characters contain a large number of bits, and humans are not familiar with binary.

2.7.4 Hexadecimal Numbers

The hexadecimal number system has $B = 16$, and a to h can be 0 to 15, which presents a slight problem, as we don't have 15 different numerical characters. Consequently, we use 0 to 9, and the letters A, B, C, D, E, F to represent 10, 11, 12, 13, 14, 15 respectively

$$\dots a16^3 + b16^2 + c16^1 + d16^0 + e16^{-1} + f16^{-2} + g16^{-3} + h16^{-4} \dots$$

and the first 17 hexadecimal numbers are

$$1_{16}, 2_{16}, 3_{16}, 4_{16}, 5_{16}, 6_{16}, 7_{16}, 8_{16}, 9_{16}, A_{16}, B_{16}, C_{16}, D_{16}, E_{16}, F_{16}, 10_{16}, 11_{16}.$$

Thus $1E.8_{16}$ in decimal, equals

$$\begin{gathered}(1 \times 16) + (E \times 1) + (8 \times 16^{-1})\\(16 + 14) + (8/16)\\30.5.\end{gathered}$$

Although it is not obvious, binary, octal and hexadecimal numbers are closely related, which is why they are part of a programmer's toolkit. Even though computers work with binary, it's the last thing a programmer wants to use. So to simplify the man-machine interface, binary is converted into octal or hexadecimal. To illustrate this, let's convert the 16-bit binary code 1101011000110001 into octal.

Using the following general binary integer

$$a2^8 + b2^7 + c2^6 + d2^5 + e2^4 + f2^3 + g2^2 + h2^1 + i2^0$$

we group the terms into threes, starting from the right, because $2^3 = 8$

$$(a2^8 + b2^7 + c2^6) + (d2^5 + e2^4 + f2^3) + (g2^2 + h2^1 + i2^0).$$

Simplifying

$$\begin{gathered}2^6(a2^2 + b2^1 + c2^0) + 2^3(d2^2 + e2^1 + f2^0) + 2^0(g2^2 + h2^1 + i2^0)\\8^2(a2^2 + b2^1 + c2^1) + 8^1(d2^2 + e2^1 + f2^0) + 8^0(g2^2 + h2^1 + i2^0)\\8^2R + 8^1S + 8^0T\end{gathered}$$

where

$$\begin{aligned}R &= a2^2 + b2^1 + c\\S &= d2^2 + e2^1 + f\\T &= g2^2 + h2^1 + i\end{aligned}$$

and the values of R, S, T vary between 0 and 7. Therefore, given 1101011000110001, we divide the binary code into groups of three, starting at the right, and adding two leading zeros

$$(001)(101)(011)(000)(110)(001).$$

For each group, multiply the zeros and ones by 4, 2, 1, right to left

$$\begin{gathered}(0+0+1)(4+0+1)(0+2+1)(0+0+0)(4+2+0)(0+0+1)\\(1)(5)(3)(0)(6)(1)\\153061_8.\end{gathered}$$

Therefore, $1101011000110001_2 \equiv 153061_8$, ($\equiv$ stands for "equivalent to") which is much more compact. The secret of this technique is to memorise the patterns

$$\begin{aligned}000_2 &\equiv 0_8\\001_2 &\equiv 1_8\\010_2 &\equiv 2_8\\011_2 &\equiv 3_8\\100_2 &\equiv 4_8\\101_2 &\equiv 5_8\\110_2 &\equiv 6_8\\111_2 &\equiv 7_8.\end{aligned}$$

Here are a few more examples, with the binary digits grouped in threes:

$$\begin{aligned}111_2 &\equiv 7_8\\101\ 101_2 &\equiv 55_8\\100\ 000_2 &\equiv 40_8\\111\ 000\ 111\ 000\ 111_2 &\equiv 70707_8.\end{aligned}$$

It's just as easy to reverse the process, and convert octal into binary. Here are some examples:

$$\begin{aligned}567_8 &\equiv 101\ 110\ 111_2\\23_8 &\equiv 010\ 011_2\\1741_8 &\equiv 001\ 111\ 100\ 001_2.\end{aligned}$$

A similar technique is used to convert binary to hexadecimal, but this time we divide the binary code into groups of four, because $2^4 = 16$, starting at the right, and adding leading zeros, if necessary. To illustrate this, let's convert the 16-bit binary code 1101 0110 0011 0001 into hexadecimal.

Using the following general binary integer number

$$a2^{11} + b2^{10} + c2^9 + d2^8 + e2^7 + f2^6 + g2^5 + h2^4 + i2^3 + j2^2 + k2^1 + l2^0$$

from the right, we divide the binary code into groups of four:

$$(a2^{11} + b2^{10} + c2^9 + d2^8) + (e2^7 + f2^6 + g2^5 + h2^4) + (i2^3 + j2^2 + k2^1 + l2^0).$$

Simplifying

$$\begin{gathered}
2^8(a2^3 + b2^2 + c2^1 + d2^0) + 2^4(e2^3 + f2^2 + g2^1 + h2^0) + 2^0(i2^3 + j2^2 + k2^1 + l2^0) \\
16^2(a2^3 + b2^2 + c2^1 + d) + 16^1(e2^3 + f2^2 + g2^1 + h) + 16^0(i2^3 + j2^2 + k2^1 + l) \\
16^2R + 16^1S + 16^0T
\end{gathered}$$

where

$$\begin{aligned}
R &= a2^3 + b2^2 + c2^1 + d \\
S &= e2^3 + f2^2 + g2^1 + h \\
T &= i2^3 + j2^2 + k2^1 + l
\end{aligned}$$

and the values of R,S,T vary between 0 and 15. Therefore, given 1101011000110001_2, we divide the binary code into groups of fours, starting at the right:

$$(1101)(0110)(0011)(0001).$$

For each group, multiply the zeros and ones by 8, 4, 2, 1 respectively, right to left:

$$\begin{gathered}
(8 + 4 + 0 + 1)(0 + 4 + 2 + 0)(0 + 0 + 2 + 1)(0 + 0 + 0 + 1) \\
(13)(6)(3)(1) \\
D631_{16}.
\end{gathered}$$

Therefore, $1101\ 0110\ 0011\ 0001_2 \equiv D631_{16}$, which is even more compact than its octal value 153061_8.

I have deliberately used whole numbers in the above examples, but they can all be extended to include a fractional part. For example, when converting a binary number such as 11.1101_2 to octal, the groups are formed about the binary point:

$$(011).(110)(100) \equiv 3.64_8.$$

Similarly, when converting a binary number such as 101010.100110_2 to hexadecimal, the groups are also formed about the binary point:

$$(0010)(1010).(1001)(1000) \equiv 2A.98_{16}.$$

Table 2.3 shows the first twenty decimal, binary, octal and hexadecimal numbers.

Table 2.3 The first twenty decimal, binary, octal, and hexadecimal numbers

decimal	binary	octal	hex	decimal	binary	octal	hex
1	1	1	1	11	1011	13	B
2	10	2	2	12	1100	14	C
3	11	3	3	13	1101	15	D
4	100	4	4	14	1110	16	E
5	101	5	5	15	1111	17	F
6	110	6	6	16	10000	20	10
7	111	7	7	17	10001	21	11
8	1000	10	8	18	10010	22	12
9	1001	11	9	19	10011	23	13
10	1010	12	A	20	10100	24	14

2.7.5 Adding Binary Numbers

When we are first taught the addition of integers containing several digits, we are advised to solve the problem digit by digit, working from right to left. For example, to add 254 to 561 we write:

$$\begin{array}{r} 561 \\ \underline{254} \\ \underline{815} \end{array}$$

where $4 + 1 = 5$, $5 + 6 = 1$ with a $carry = 1$, $2 + 5 + carry = 8$.

Table 2.4 shows all the arrangements for adding two digits with the $carry$ shown as ${}^{carry}n$. However, when adding binary numbers, the possible arrangements collapse to the four shown in Table 2.5, which greatly simplifies the process.

For example, to add 124 to 188 as two 16-bit binary integers, we write, showing the status of the $carry$ bit:

$$\begin{array}{l} 0000000011111000 \; carry \\ 0000000010111100 = 188 \\ \underline{0000000001111100 = 124} \\ \underline{0000000100111000 = 312} \end{array}$$

Such addition is easily undertaken by digital electronic circuits, and instead of having separate circuitry for subtraction, it is possible to perform subtraction using the technique of *two's complement*.

Table 2.4 Addition of two decimal integers showing the *carry*

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	$^{1}0$
2	2	3	4	5	6	7	8	9	$^{1}0$	$^{1}1$
3	3	4	5	6	7	8	9	$^{1}0$	$^{1}1$	$^{1}2$
4	4	5	6	7	8	9	$^{1}0$	$^{1}1$	$^{1}2$	$^{1}3$
5	5	6	7	8	9	$^{1}0$	$^{1}1$	$^{1}2$	$^{1}3$	$^{1}4$
6	6	7	8	9	$^{1}0$	$^{1}1$	$^{1}2$	$^{1}3$	$^{1}4$	$^{1}5$
7	7	8	9	$^{1}0$	$^{1}1$	$^{1}2$	$^{1}3$	$^{1}4$	$^{1}5$	$^{1}6$
8	8	9	$^{1}0$	$^{1}1$	$^{1}2$	$^{1}3$	$^{1}4$	$^{1}5$	$^{1}6$	$^{1}7$
9	9	$^{1}0$	$^{1}1$	$^{1}2$	$^{1}3$	$^{1}4$	$^{1}5$	$^{1}6$	$^{1}7$	$^{1}8$

Table 2.5 Addition of two binary integers showing the *carry*

+	0	1
0	0	1
1	1	$^{1}0$

2.7.6 Subtracting Binary Numbers

Two's complement is a technique for converting a binary number into a form such that when it is added to another binary number, it results in a subtraction. There are two stages to the conversion: inversion, followed by the addition of 1. For example, 24 in binary is 0000000000110000, and is inverted by switching every 1 to 0, and *vice versa*: 1111111111100111. Next , we add 1: 1111111111101000, which now represents -24. If this is added to binary 36: 0000000000100100, we have

$$
\begin{array}{l}
0000000000100100 = +36 \\
1111111111101000 = -24 \\
\hline
0000000000001100 = +12 \\
\hline
\end{array}
$$

Note that the last high-order addition creates a *carry* of 1, which is ignored. Here is another example, $100 - 30$:

	0000000000011110	$= +30$
Inversion	1111111111100001	
Add 1	0000000000000001	
	1111111111100010	$= -30$
Add 100	0000000001100100	$= +100$
	0000000001000110	$= +70$

2.8 Types of Numbers

As mathematics evolved, mathematicians introduced different types of numbers to help classify equations and simplify the language employed to describe their work. These are the various types and their set names.

2.8.1 Natural Numbers

The *natural numbers* $\{1,\ 2,\ 3,\ 4, \dots\}$ are used for counting, ordering and labelling and represented by the set $\mathbb{N}$. When zero is included, $\mathbb{N}^0$ or $\mathbb{N}_0$ is used:

$$\mathbb{N}^0 = \mathbb{N}_0 = \{0, 1, 2, \dots\}.$$

Note that negative numbers are not included. Natural numbers are used to subscript a quantity to distinguish one element from another, e.g. $x_1,\ x_2,\ x_3,\ x_4, \dots$.

2.8.2 Integers

Integer numbers include the natural numbers, both positive and negative, and zero, and are represented by the set $\mathbb{Z}$:

$$\mathbb{Z} = \{\dots,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \dots\}.$$

The reason for using $\mathbb{Z}$ is because the German for whole number is *ganzen Zahlen*. Leopold Kronecker apparently criticised Georg Cantor for his work on set theory with the jibe: "*Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk*", which translates: "*God made the integers, and all the rest is man's work*", implying that the rest are artificial. However, Cantor's work on set theory and transfinite numbers proved to be far from artificial.

2.8.3 Rational Numbers

Any number that equals the quotient of one integer divided by another non-zero integer, is a *rational number*, and represented by the set $\mathbb{Q}$. For example, 2, $\sqrt{16}$, 0.25 are rational numbers because

$$\begin{aligned} 2 &= 4/2 \\ \sqrt{16} &= 4 = 8/2 \\ 0.25 &= 1/4. \end{aligned}$$

Some rational numbers can be stored accurately inside a computer, but many others can only be stored approximately. For example, $4/3$ produces an infinite sequence of threes $1.333333\dots$ and is truncated when stored as a binary number.

2.8.4 Irrational Numbers

An *irrational number* cannot be expressed as the quotient of two integers. Irrational numbers never terminate, nor contain repeated sequences of digits, consequently, they are always subject to a small error when stored within a computer. Examples are:

$$\begin{aligned} \sqrt{2} &= 1.41421356\dots \\ \phi &= 1.61803398\dots \text{(golden section)} \\ \mathrm{e} &= 2.71828182\dots \\ \pi &= 3.14159265\dots \end{aligned}$$

2.8.5 Real Numbers

Rational and irrational numbers comprise the set of *real numbers* $\mathbb{R}$. Examples are 1.5, 0.004, 12.999 and 23.0.

2.8.6 Algebraic and Transcendental Numbers

Polynomial equations with rational coefficients have the form:

$$f(x) = ax^n + bx^{n-1} + cx^{n-2} \cdots + C$$

such as

$$y = 3x^2 + 2x - 1$$

and their roots belong to the set of *algebraic numbers* $\mathbb{A}$. A consequence of this definition implies that all rational numbers are algebraic, since if

$$x = \frac{p}{q}$$

then

$$qx - p = 0$$

which is a polynomial. Numbers that are not roots to polynomial equations are *transcendental numbers* and include most irrational numbers, but not $\sqrt{2}$, since if

$$x = \sqrt{2}$$

then

$$x^2 - 2 = 0$$

which is a polynomial.

2.8.7 Imaginary Numbers

Imaginary numbers employ the symbol i to represent the impossible operation $\sqrt{-1}$. When combined with a real number they form a *complex number* which possesses vector-like properties. An imaginary number such as bi is defined as

$$b \in \mathbb{R}, \quad i^2 = -1.$$

Imaginary numbers obey all the axioms associated with real numbers: they can be added, subtracted, multiplied and divided. For example, given

$$\begin{aligned} x &= -6i \\ y &= 3i \end{aligned}$$

then

$$\begin{aligned} x + y &= -6i + 3i = -3i \\ x - y &= -6i - 3i = -9i \\ xy &= (-6i)(3i) = -18i^2 = 18 \\ \frac{x}{y} &= \frac{-6i}{3i} = -2. \end{aligned}$$

2.8.8 Complex Numbers

A *complex number* has a real and imaginary part: $z = a + ib$, and represented by the set $\mathbb{C}$:

$$z = a + bi, \qquad z \in \mathbb{C}, \quad a, b \in \mathbb{R}, \quad i^2 = -1.$$

Examples are

$$\begin{aligned} z &= 1 + i \\ z &= 3 - 2i \\ z &= -23 + \sqrt{23}i. \end{aligned}$$

Complex numbers obey all the axioms associated with real numbers. For example, if we multiply $a + bi$ by $c + di$ we have

$$(a + bi)(c + di) = ac + adi + bci + bdi^2.$$

Collecting up like terms and substituting -1 for i^2 we get

$$(a + bi)(c + di) = ac + (ad + bc)i - bd$$

which simplifies to

$$(a + bi)(c + di) = ac - bd + (ad + bc)i$$

which is another complex number.

For example, given

$$\begin{aligned} x &= 2 + 3i \\ y &= 3 + 4i \end{aligned}$$

then

$$\begin{aligned} x + y &= (2 + 3i) + (3 + 4i) = 5 + 7i \\ x - y &= (2 + 3i) - (3 + 4i) = -1 - i \\ xy &= (2 + 3i)(3 + 4i) = 6 + 8i + 9i + 12i^2 = -6 + 17i. \end{aligned}$$

Something interesting happens when we multiply a complex number by its *complex conjugate*, which is the same complex number but with the sign of the imaginary part reversed:

$$(a + bi)(a - bi) = a^2 - abi + bai - b^2i^2.$$

Collecting up like terms and simplifying we obtain

$$(a + bi)(a - bi) = a^2 + b^2$$

which is a real number, as the imaginary part has been cancelled out by the action of the complex conjugate. Given a complex number y, its complex conjugate is represented by $\bar{y}$. This permits us to divide one complex number by another as follows:

$$\begin{aligned} x &= 2 + 3i \\ y &= 3 + 4i \\ \bar{y} &= 3 - 4i \\ \frac{x}{y} &= \frac{x}{y}\frac{\bar{y}}{\bar{y}} = \frac{(2+3i)}{(3+4i)}\frac{(3-4i)}{(3-4i)} = \frac{6 - 8i + 9i + 12}{9 + 16} = \frac{18 + i}{25} = \tfrac{18}{25} + \tfrac{1}{25}i. \end{aligned}$$

Chapter 12 provides more information on complex numbers.

2.8.9 *Quaternions and Octonions*

In 1843, the brilliant Irish mathematician and physicist Sir William Rowan Hamilton (1805–1865) invented *quaternions*, represented by the set $\mathbb{H}$, in honour of its inventor, which were the first non-commutative algebra:

$$q = a + bi + cj + dk$$

where

$$q \in \mathbb{H}, \quad a, b, c, d \in \mathbb{R}, \quad i^2 = j^2 = k^2 = -1,$$

$$ij = k, \quad ji = -k, \quad jk = i, \quad kj = -i, \quad ki = j, \quad ik = -j, \quad ijk = -1.$$

The imaginary products are shown in Table 2.6.

Given two quaternions:

$$\begin{aligned} x &= a + bi + cj + dk \\ y &= e + fi + gj + hk \end{aligned}$$

their product xy equals

$$\begin{aligned} xy = {} & (ae - bf - cg - dh) + (af + be + ch - dg)i \\ & + (ag + ce + df - bh)j + (ah + de + bg - cf)k. \end{aligned}$$

Table 2.6 The quaternion's imaginary products

$\times$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

The American mathematician Josiah Willard Gibbs (1839–1903), realised that a quaternion's imaginary part could be isolated and represent quantities with magnitude and direction, and 3D vectors were born:

$$\mathbf{v} = a\mathbf{i} + b\mathbf{j} + c\mathbf{k}.$$

Almost immediately quaternions were invented, the hunt began for the next complex algebra, which was discovered simultaneously in 1843 by a colleague of Hamilton, John Thomas Graves (1806–1870), who called them *octaves*, and by the young English mathematician Arthur Cayley (1821–1895), who called them *Cayley Numbers*:

$$z = a + bi + cj + dk + ep + fq + gr + hs$$

$$a, b, c, d, e, f, g, h \in \mathbb{R}, \quad i^2, j^2, k^2, p^2, q^2, r^2, s^2 = -1.$$

They are now called *octonions*, and are not only non-commutative, but non-associative, which means that in general, given three octonions A, B, C, then $(AB)C \neq A(BC)$. In 1898, the German mathematician Adolf Hurwitz (1859–1919), proved that there are only four algebras where it is possible to multiply and divide in the accepted sense: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$. Figure 2.2 shows the sets of numbers diagrammatically.

2.8.10 Transcendental and Algebraic Numbers

Given a polynomial built from integers, for example

$$y = 3x^3 - 4x^2 + x + 23,$$

if the result is an integer, it is called an *algebraic number*, otherwise it is a *transcendental number*. Familiar examples of the latter being $\pi = 3.141\,592\,653\ldots$, and $\mathrm{e} = 2.718\,281\,828\ldots$, which can be represented as various continued fractions:

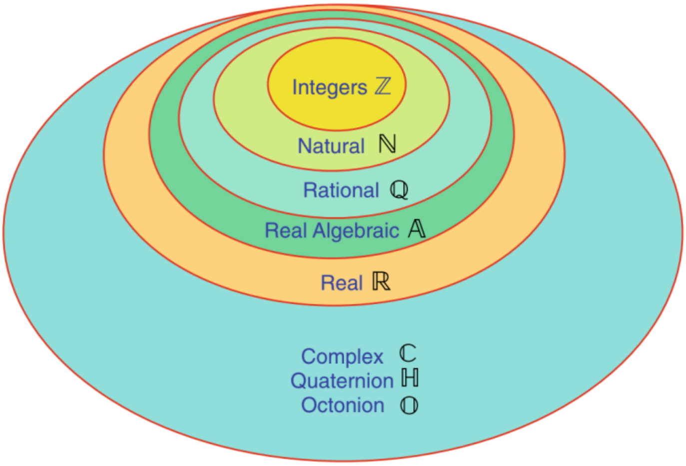


Fig. 2.2 The nested sets of numbers

$$\pi = \cfrac{4}{1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \cdots}}}}}$$

$$\mathrm{e} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cdots}}}}}$$

2.9 Prime Numbers

A *prime number* is defined as a positive integer that can only be divided by 1 and itself, without leaving a remainder. The first five prime numbers are 2, 3, 5, 7, 11. We can prove that *any* positive integer must either be a prime, or the product of two or more primes, using the following reasoning.

The set of natural numbers comprises two sets: primes and non-primes. A prime, by definition, has no factors, apart from 1 and itself. A non-prime has factors and is called *composite*. However, these factors are natural numbers, which must either be

Table 2.7 The prime factors for the first 30 numbers

number	factors	number	factors	number	factors
1		11	11	21	3×7
2	2	12	$2^2\times3$	22	2×11
3	3	13	13	23	23
4	2^2	14	2×7	24	$2^3\times3$
5	5	15	3×5	25	5^2
6	2×3	16	2^4	26	2×13
7	7	17	17	27	3^3
8	2^3	18	2×3^2	28	$2^2\times7$
9	3^2	19	19	29	29
10	2×5	20	$2^2\times5$	30	$2\times3\times5$

prime or non-prime. Eventually, the composite factors *must* decompose into composite primes.

For example, $72 = 8 \times 9$, but $8 = 2^3$ and $9 = 3^2$, therefore, $72 = 2^3 \times 3^2$. Even starting with $72 = 6 \times 12$, but $6 = 2 \times 3$ and $12 = 2^2 \times 3$, therefore, $72 = 2^3 \times 3^2$. Table 2.7 shows the prime factors for the first 30 numbers.

2.9.1 The Fundamental Theorem of Arithmetic

Original work by the Greek mathematician Euclid (Mid-4th to mid-3rd century BC), revealed the *Fundamental Theorem of Arithmetic* (FTAr), also called the *Unique Factorisation Theorem*, which states that every integer greater than 1, is either prime or the unique product of primes, and is expressed symbolically as follows. Let $p_1, p_2, p_3, \dots, p_k$ be prime numbers, and $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_k$ be their associated positive integer powers: $p_1^{\alpha_1}, p_2^{\alpha_2}, p_3^{\alpha_3}, \dots, p_k^{\alpha_k}$. We now use the product function Pi, $\prod$ to create the product: $p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}, \dots, p_k^{\alpha_k}$, and introduce the variable i with a range of 1 to k, which permits the FTAr to be written as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}, \dots, p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

where $\prod$ is shorthand for "multiply together the associated terms".

For example, 2250 equals the unique product: $2^1 3^2 5^3$, and $245 = 5^1 7^2$. To prove that these prime products are unique, let's first assume that they are not, and show that this leads to a contradiction.

Table 2.8 Examples of primes and prime factors

2	3	5	7	11	13	17	19	23	29	31	N
2											3
2	3										7
2	3	5									31
2	3	5	7								211
2	3	5	7	11							2,311
2	3	5	7	11	13						$30,031 = 59 \times 509$
2	3	5	7	11	13	17					$510,511 = 19 \times 97 \times 277$
2	3	5	7	11	13	17	19				$9,699,691 = 347 \times 27,953$
2	3	5	7	11	13	17	19	23			$223,092,871 = 317 \times 703,763$
2	3	5	7	11	13	17	19	23	29		$6,469,693,231 = 331 \times 571 \times 34,231$
2	3	5	7	11	13	17	19	23	29	31	200,560,490,131

See www.compoasso.free.fr for an amazing list of prime numbers and related features. Also, readers interested in learning more about prime numbers should investigate Prime Numbers (2006).

2.9.5 Perfect Numbers

A *perfect number* equals the sum of its factors. For example, the factors of 6 are 1, 2 and 3, whose sum is also 6. One would imagine that there would be a large quantity of small perfect numbers, but the first five are: 6, 28, 496, 8128 and 33,550,336, which are all even. And as the search continues to discover higher values, using computers, no odd perfect number has emerged. Euclid proved that if m is prime, and of the form $2^k - 1$, then $m(m+1)/2$ is an even perfect number. For example, 3 is prime and

$$3 = 2^2 - 1 \quad \text{and} \quad \frac{3 \times 4}{2} = 6.$$

Similarly, 7 is prime and

$$7 = 2^3 - 1 \quad \text{and} \quad \frac{7 \times 8}{2} = 28.$$

2.9.6 Mersenne Numbers

Numbers of the form $2^k - 1$ are called *Mersenne numbers*, some of which, are also prime. The French theologian and mathematician Marin Mersenne (1588–1648) became interested in them towards the end of his life, and today they are known as *Mersenne primes*.

By the end of the 16th-century, the highest Mersenne prime was 524,287 which equals $2^{19} - 1$. At the start of the 21st-century, $2^{43,112,609} - 1$ was the highest, containing approximately 13 million digits!

Apart from the fact that prime numbers are so mysterious, they are very important in public key cryptography, which is central to today's Internet security systems.

2.10 Infinity

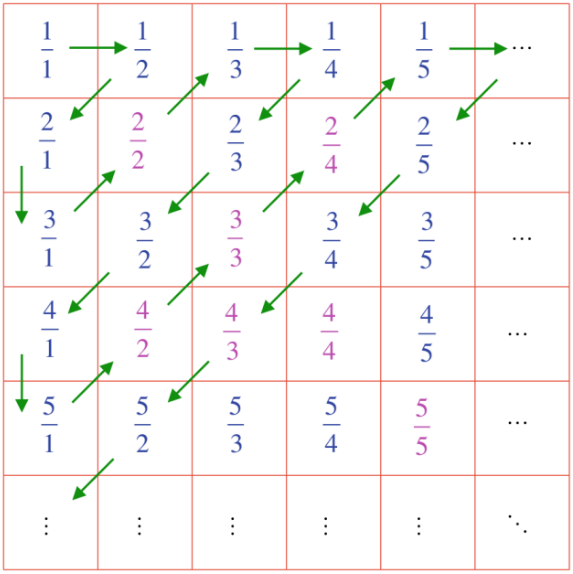
The term *infinity* is used to describe the size of unbounded systems. For example, prime numbers are infinite, so too are the sets of other numbers. Consequently, no matter how we try, it is impossible to visualise the size of infinity. Nevertheless, this did not stop Georg Cantor from showing that one infinite set could be infinitely larger than another.

Cantor distinguished between those infinite number sets that could be "counted", and those that could not. For Cantor, counting meant the one-to-one correspondence of a natural number with the members of another infinite set. If there was a clear correspondence, without leaving any gaps, then the two sets shared a common infinite size, called its *cardinality* using the first letter of the Hebrew alphabet aleph: $\aleph$. The cardinality of the natural numbers $\mathbb{N}$ is $\aleph_0$, called aleph-zero.

Cantor discovered a way of representing the rational numbers as a grid, which is traversed diagonally, back and forth, as shown in Fig. 2.3. Some ratios appear several times, such as $\frac{2}{2}$, $\frac{3}{3}$ etc., which are not counted. Nevertheless, the one-to-one correspondence with the natural numbers means that the cardinality of rational numbers is also $\aleph_0$.

A real surprise was that there are infinitely more transcendental numbers than natural numbers. Furthermore, there are an infinite number of cardinalities rising to $\aleph_\aleph$. Cantor had been alone working in this esoteric area, and as he published his results, he shook the very foundations of mathematics, which is why he was treated so badly by his fellow mathematicians.

Fig. 2.3 Rational number grid



2.11 Worked Examples

2.11.1 Algebraic Expansion

Expand $(a+b)(c+d)$, $(a-b)(c+d)$, and $(a-b)(c-d)$.
Solution:

$$\begin{aligned}
(a+b)(c+d) &= a(c+d) + b(c+d) \\
&= ac + ad + bc + bd. \\
(a-b)(c+d) &= a(c+d) - b(c+d) \\
&= ac + ad - bc - bd. \\
(a-b)(c-d) &= a(c-d) - b(c-d) \\
&= ac - ad - bc + bd.
\end{aligned}$$

2.11.2 Binary Subtraction

Using two's complement, subtract 12 from 50.
Solution:

	$0000000000001100 = +12$
Inversion	1111111111110011
Add 1	0000000000000001
	$1111111111110100 = -12$
Add 50	$0000000000110010 = +50$
	$0000000000100110 = +38$

2.11.3 Complex Numbers

Compute $(3+2\text{i})+(2+2\text{i})+(5-3\text{i})$ and $(3+2\text{i})(2+2\text{i})(5-3\text{i})$.
Solution:

$$(3+2\text{i})+(2+2\text{i})+(5-3\text{i}) = 10+\text{i}.$$

$$\begin{aligned}(3+2\text{i})(2+2\text{i})(5-3\text{i}) &= (3+2\text{i})(10-6\text{i}+10\text{i}+6)\\ &= (3+2\text{i})(16+4\text{i})\\ &= 48+12\text{i}+32\text{i}-8\\ &= 40+44\text{i}.\end{aligned}$$

2.11.4 Complex Rotation

Rotate the complex point $3+2\text{i}$ by $\pm 90°$ and $\pm 180°$.
Solution:
To rotate $+90°$ (anticlockwise) multiply by i.

$$\text{i}(3+2\text{i}) = 3\text{i}-2 = -2+3\text{i}.$$

To rotate $-90°$ (clockwise) multiply by $-\text{i}$.

$$-\text{i}(3+2\text{i}) = -3\text{i}+2 = 2-3\text{i}.$$

To rotate $+180°$ (anticlockwise) multiply by -1.

$$-1(3+2\text{i}) = -3-2\text{i}.$$

To rotate $-180°$ (clockwise) multiply by -1.

$$-1(3+2\text{i}) = -3-2\text{i}.$$

2.11.5 Quaternions

Compute $(2+3i+4j+k)+(6+2i+j+2k)$ and $(2+3i+4j+k)(6+2i+j+2k)$.
Solution:

$$(2+3i+4j+k)+(6+2i+j+2k)=8+5i+5j+3k.$$

$$\begin{aligned}(2+3i+4j+k)(6+2i+j+2k) &= 12+4i+2j+4k+18i+6i^2+3ij+6ik\\ &\quad +24j+8ji+4j^2+8jk+6k+2ki+kj+2k^2\\ &= 12+4i+2j+4k+18i-6+3k-6j\\ &\quad +24j-8k-4+8i+6k+2j-i-2\\ &= 0+29i+22j+5k.\end{aligned}$$

References

www.compoasso.free.fr
Crandall R, Pomerance C (2006) Prime numbers: a computational perspective, 2nd edn

example, the expression $ax + by - d$ equals zero for a straight line. The variables x and y are the coordinates of any point on the line and the values of a, b and d determine the position and orientation of the line. The $=$ sign permits the line equation to be expressed as a self-evident statement:

$$0 = ax + by - d.$$

Such a statement implies that the expressions on the left- and right-hand sides of the $=$ sign are "equal" or "balanced", and in order to maintain equality or balance, whatever is done to one side, must also be done to the other. For example, adding d to both sides, the straight-line equation becomes

$$d = ax + by.$$

Similarly, we could double or treble both expressions, divide them by 4, or add 6, without disturbing the underlying relationship. When we are first taught algebra, we are often given the task of rearranging a statement to make different variables the subject. For example, (3.1) can be rearranged such that x is the subject:

$$y = \frac{x+4}{2-\frac{1}{z}} \tag{3.1}$$

$$y\left(2-\frac{1}{z}\right) = x+4$$

$$x = y\left(2-\frac{1}{z}\right) - 4.$$

Making z the subject requires more effort:

$$\begin{aligned} y &= \frac{x+4}{2-\frac{1}{z}} \\ y\left(2-\frac{1}{z}\right) &= x+4 \\ 2y - \frac{y}{z} &= x+4 \\ 2y - x - 4 &= \frac{y}{z} \\ z &= \frac{y}{2y-x-4}. \end{aligned}$$

Parentheses are used to isolate part of an expression in order to select a subexpression that is manipulated in a particular way. For example, the parentheses in $c(a + b) + d$ ensure that the variables a and b are added together before being multiplied by c, and finally added to d.

3.3.1 Solving the Roots of a Quadratic Equation

Problem solving is greatly simplified if one has solved it before, and having a good memory is always an advantage. In mathematics, we keep coming across problems that have been encountered before, apart from different numbers. For example, $(a+b)(a-b)$ always equals a^2-b^2, therefore factorising the following is a trivial exercise:

$$
\begin{aligned}
a^2-16 &= (a+4)(a-4)\\
x^2-49 &= (x+7)(x-7)\\
x^2-2 &= (x+\sqrt{2})(x-\sqrt{2}).
\end{aligned}
$$

A perfect square has the form:

$$a^2+2ab+b^2=(a+b)^2.$$

Consequently, factorising the following is also a trivial exercise:

$$
\begin{aligned}
a^2+4ab+4b^2 &= (a+2b)^2\\
x^2+14x+49 &= (x+7)^2\\
x^2-20x+100 &= (x-10)^2.
\end{aligned}
$$

Now let's solve the roots of the quadratic equation $ax^2+bx+c=0$, i.e. those values of x that make the equation equal zero. As the equation involves an x^2 term, we will exploit any opportunity to factorise it. We begin with the quadratic where $a \neq 0$:

$$ax^2+bx+c=0.$$

Step 1: Subtract c from both sides to begin the process of creating a perfect square:

$$ax^2+bx=-c.$$

Step 2: Divide both sides by a to create an x^2 term:

$$x^2+\frac{b}{a}x=-\frac{c}{a}.$$

Step 3: Add $b^2/4a^2$ to both sides to create a perfect square on the left side:

$$x^2+\frac{b}{a}x+\frac{b^2}{4a^2}=\frac{b^2}{4a^2}-\frac{c}{a}.$$

Step 4: Factorise the left side:

$$\left(x+\frac{b}{2a}\right)^2=\frac{b^2}{4a^2}-\frac{c}{a}.$$

Step 5: Make $4a^2$ the common denominator for the right side:

$$\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}.$$

Step 6: Take the square root of both sides:

$$x+\frac{b}{2a}=\frac{\pm\sqrt{b^2-4ac}}{2a}.$$

Step 7: Subtract $b/2a$ from both sides:

$$x=\frac{\pm\sqrt{b^2-4ac}}{2a}-\frac{b}{2a}.$$

Step 8: Rearrange the right side:

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

which provides the roots for any quadratic equation.

The discriminant $\sqrt{b^2-4ac}$ may be positive, negative or zero. A positive value reveals two real roots:

$$x_1=\frac{-b+\sqrt{b^2-4ac}}{2a},\quad x_2=\frac{-b-\sqrt{b^2-4ac}}{2a}. \tag{3.2}$$

A negative value reveals two complex roots:

$$x_1=\frac{-b+i\sqrt{|b^2-4ac|}}{2a},\quad x_2=\frac{-b-i\sqrt{|b^2-4ac|}}{2a}.$$

And a zero value reveals a single root:

$$x=\frac{-b}{2a}.$$

For example, Fig. 3.1 shows the graph of $y=x^2+x-2$, where we can see that $y=0$ at two points: $x=-2$ and $x=1$. In this equation

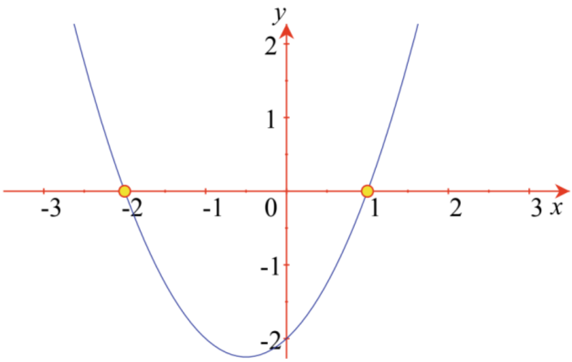


Fig. 3.1 Graph of $y = x^2 + x - 2$

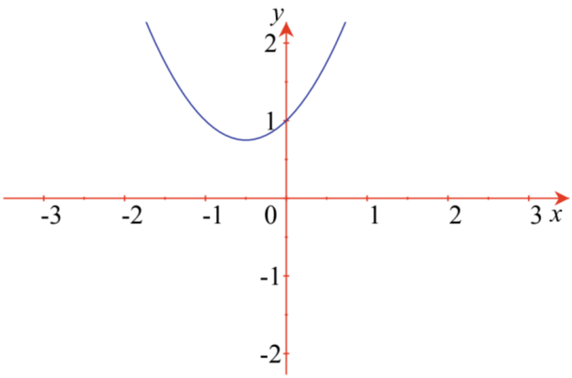


Fig. 3.2 Graph of $y = x^2 + x + 1$

$$a = 1$$
$$b = 1$$
$$c = -2$$

which when plugged into (3.2) confirms the graph:

$$x_1 = \frac{-1 + \sqrt{1+8}}{2} = 1$$
$$x_2 = \frac{-1 - \sqrt{1+8}}{2} = -2.$$

Figure 3.2 shows the graph of $y = x^2 + x + 1$, where at no point does $y = 0$. In this equation

$$a = 1$$
$$b = 1$$
$$c = 1$$

which when plugged into (3.2) confirms the graph by giving complex roots:

$$
\begin{aligned}
x_1 &= \frac{-1+\sqrt{1-4}}{2} = -\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2} \\
x_2 &= \frac{-1-\sqrt{1-4}}{2} = -\tfrac{1}{2} - i\tfrac{\sqrt{3}}{2}.
\end{aligned}
$$

Let's show that x_1 satisfies the original equation:

$$
\begin{aligned}
y &= x_1^2 + x_1 + 1 \\
&= \left(-\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}\right)^2 - \tfrac{1}{2} + i\tfrac{\sqrt{3}}{2} + 1 \\
&= \tfrac{1}{4} - i\tfrac{\sqrt{3}}{2} - \tfrac{3}{4} - \tfrac{1}{2} + i\tfrac{\sqrt{3}}{2} + 1 \\
&= 0.
\end{aligned}
$$

x_2 also satisfies the same equation.

Algebraic expressions also contain a wide variety of functions, such as

$$
\begin{aligned}
\sqrt{x} &= \text{square root of } x \\
\sqrt[n]{x} &= n\text{-th root of } x \\
x^n &= x \text{ to the power } n \\
n! &= \text{factorial } n \\
\sin x &= \text{sine of } x \\
\cos x &= \text{cosine of } x \\
\tan x &= \text{tangent of } x \\
\log x &= \text{logarithm of } x \\
\ln x &= \text{natural logarithm of } x.
\end{aligned}
$$

Trigonometric functions are factorised as follows:

$$
\begin{aligned}
\sin^2 x - \cos^2 x &= (\sin x + \cos x)(\sin x - \cos x) \\
\sin^2 x - \tan^2 x &= (\sin x + \tan x)(\sin x - \tan x) \\
\sin^2 x + 4\sin x\cos x + 4\cos^2 x &= (\sin x + 2\cos x)^2 \\
\sin^2 x - 6\sin x\cos x + 9\cos^2 x &= (\sin x - 3\cos x)^2.
\end{aligned}
$$

3.4 Indices

Indices are used to imply repeated multiplication and create a variety of situations where laws are required to explain how the result is to be computed.

From the above notation, it is evident that

$$\log(ab) = \log a + \log b$$
$$\log\left(\frac{a}{b}\right) = \log a - \log b$$
$$\log(a^n) = n \log a.$$

3.6 Further Notation

All sorts of symbols are used to stand in for natural language expressions; here are some examples:

$<$ less than
$>$ greater than
$\leq$ less than or equal to
$\geq$ greater than or equal to
$\approx$ approximately equal to
$\equiv$ equivalent to
$\neq$ not equal to
$|x|$ absolute value of x.

For example, $0 \leq t \leq 1$ is interpreted as: t is greater than or equal to 0, and is less than or equal to 1. Basically, this means t varies between 0 and 1.

3.7 Functions

The theory of *functions* is a large subject, and at this point in the book, I will only touch upon some introductory ideas that will help you understand the following chapters.

The German mathematician Gottfried von Leibniz (1646–1716) is credited with an early definition of a function, based upon the slope of a graph. However, it was the Swiss mathematician Leonhard Euler (1707–1783) who provided a definition along the lines: "A function is a variable quantity, whose value depends upon one or more independent variables." Other mathematicians have introduced more rigorous definitions, which are examined later on in the chapter on calculus.

3.7.1 Explicit and Implicit Equations

The equation

$$y = 3x^2 + 2x + 4$$

associates the value of y with different values of x. The directness of the equation: "$y =$", is why it is called an *explicit equation*, and their explicit nature is extremely useful. However, simply by rearranging the terms, creates an *implicit equation*:

$$4 = y - 3x^2 - 2x$$

which implies that certain values of x and y combine to produce the result 4. Another implicit form is

$$0 = y - 3x^2 - 2x - 4$$

which means the same thing, but expresses the relationship in a slightly different way.

An implicit equation can be turned into an explicit equation using algebra. For example, the implicit equation

$$4x + 2y = 12$$

has the explicit form:

$$y = 6 - 2x$$

where it is clear what y equals.

3.7.2 Function Notation

The explicit equation

$$y = 3x^2 + 2x + 4$$

tells us that the value of y depends on the value of x, and not the other way around. For example, when $x = 1$, $y = 9$; and when $x = 2$, $y = 20$. As y depends upon the value of x, it is called the *dependent variable*; and as x is independent of y, it is called the *independent variable*.

We can also say that y is a function of x, which can be written as

$$y = f(x)$$

where the letter "f" is the name of the function, and the independent variable is enclosed in brackets. We could have also written $y = g(x)$, $y = h(x)$, etc.

Eventually, we have to identify the nature of the function, which in this case is

$$f(x) = 3x^2 + 2x + 4.$$

Nothing prevents us from writing

$$y = f(x) = 3x^2 + 2x + 4$$

which means: y equals the value of the function $f(x)$, which is determined by the independent variable x using the expression $3x^2 + 2x + 4$.

An equation may involve more than one independent variable, such as the volume of a cylinder:

$$V = \pi r^2 h$$

where r is the radius, and h, the height, and is written:

$$V(r, h) = \pi r^2 h.$$

3.7.3 Intervals

An *interval* is a continuous range of numerical values associated with a variable, which can include or exclude the upper and lower values. For example, a variable such as x is often subject to inequalities like $x \geq a$ and $x \leq b$, which can also be written as

$$a \leq x \leq b$$

and implies that x is located in the *closed interval* $[a, b]$, where the square brackets indicate that the interval includes a and b. For example,

$$1 \leq x \leq 10$$

means that x is located in the closed interval [1, 10], which includes 1 and 10.

When the boundaries of the interval are not included, then we would state $x > a$ and $x < b$, which is written

$$a < x < b$$

and means that x is located in the *open interval* $]a, b[$, where the reverse square brackets indicate that the interval excludes a and b. For example,

$$1 < x < 10$$

means that x is located in the open interval]1, 10[, which excludes 1 and 10.

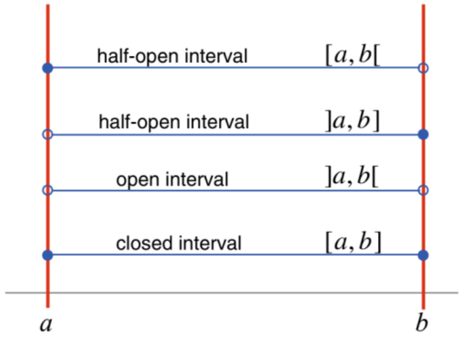


Fig. 3.5 Closed, open and half-open intervals. The filled circles indicate that a or b are included in the interval

Closed and open intervals may be combined as follows. If $x \geq a$ and $x < b$ then

$$a \leq x < b$$

and means that x is located in the *half-open interval* $[a, b[$. For example,

$$1 \leq x < 10$$

means that x is located in the half-open interval $[1, 10[$, which includes 1, but not 10.

Similarly, if

$$1 < x \leq b$$

means that x is located in the half-open interval $]1, 10]$, which includes 10, but not 1.

An alternative notation employs parentheses instead of reversed brackets:

$$
\begin{aligned}
]a, b[&= (a, b) \\
[a, b[&= [a, b) \\
]a, b] &= (a, b].
\end{aligned}
$$

Figure 3.5 shows open, closed and half-open intervals diagrammatically.

3.7.4 Function Domains and Ranges

The following descriptions of domains and ranges only apply to functions with one independent variable: $f(x)$.

Returning to the above function:

$$y = f(x) = 3x^2 + 2x + 4$$

the independent variable x, can take on any value from $-\infty$ to $+\infty$, which is called the *domain* of the function. In this case, the domain of $f(x)$ is the set of real numbers $\mathbb{R}$. The notation used for intervals, is also used for domains, which in this case is

$$]-\infty, +\infty[$$

and is open, as there are no precise values for $-\infty$ and $+\infty$.

As the independent variable takes on different values from its domain, so the dependent variable, y or $f(x)$, takes on different values from its *range*. Therefore, the range of $y = f(x) = 3x^2 + 2x + 4$ is also the set of real numbers $\mathbb{R}$.

The domain of $\log x$ is

$$]0, +\infty[$$

which is open, because $x \neq 0$. Whereas, the range of $\log x$ is

$$]-\infty, +\infty[.$$

The domain of $\sqrt{x}$ is

$$[0, +\infty[$$

which is half-open, because $\sqrt{0} = 0$, and $+\infty$ has no precise value. Similarly, the range of $\sqrt{x}$ is

$$[0, +\infty[.$$

Sometimes, a function is sensitive to one specific number. For example, in the function

$$y = f(x) = \frac{1}{x-1},$$

when $x = 1$, there is a divide by zero, which is meaningless. Consequently, the domain of $f(x)$ is the set of real numbers $\mathbb{R}$, apart from 1.

3.7.5 Odd and Even Functions

An *odd function* satisfies the condition:

$$f(-x) = -f(x)$$

where x is located in a valid domain. Consequently, the graph of an odd function is symmetrical relative to the x-axis, relative to the origin. For example, $\sin\alpha$ is odd because

$$\sin(-\alpha) = -\sin\alpha$$

$$
\begin{aligned}
e^y &= \frac{23}{x-1} \\
y &= \ln\left(\frac{23}{x-1}\right).
\end{aligned}
$$

Solution:

$$
\begin{aligned}
23 &= \frac{x+68}{3-\sin y} \\
3-\sin y &= \frac{x+68}{23} \\
\sin y &= 3-\frac{x+68}{23} \\
&= \frac{1-x}{23} \\
y &= \arcsin\left(\frac{1-x}{23}\right).
\end{aligned}
$$

3.8.2 Solving a Quadratic Equation

Solve the following quadratic equations, and test the answers.

$$0 = x^2+4x+1, \quad 0 = 2x^2+4x+2, \quad 0 = 2x^2+4x+4.$$

Solution: $0 = x^2+4x+1$

$$
\begin{aligned}
x &= \frac{-b \pm \sqrt{b^2-4ac}}{2a} \\
&= \frac{-4 \pm \sqrt{16-4}}{2} \\
&= \frac{-4 \pm \sqrt{12}}{2} \\
&= -2 \pm \sqrt{3}.
\end{aligned}
$$

Test with $x = -2+\sqrt{3}$.

$$
\begin{aligned}
x^2+4x+1 &= (-2+\sqrt{3})^2 + 4(-2+\sqrt{3}) + 1 \\
&= 4-4\sqrt{3}+3-8+4\sqrt{3}+1 \\
&= 0.
\end{aligned}
$$