Michal Křížek
Lawrence Somer
Alena Šolcová

From Great Discoveries in Number Theory to Applications

Springer

From Great Discoveries in Number Theory to Applications

Michal Křížek · Lawrence Somer · Alena Šolcová

From Great Discoveries in Number Theory to Applications

Springer

Michal Křížek
Institute of Mathematics
Czech Academy of Sciences
Prague, Czech Republic

Lawrence Somer
Department of Mathematics
Catholic University of America
Washington, DC, USA

Alena Šolcová
Department of Applied Mathematics
Czech Technical University in Prague
Prague, Czech Republic

ISBN 978-3-030-83898-0 ISBN 978-3-030-83899-7 (eBook)
https://doi.org/10.1007/978-3-030-83899-7

Mathematics Subject Classification (2010): 11-XX, 05Cxx, 11Dxx, 11B39, 28A80

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

Preface

For us, mathematical theorems and their proofs
are like gold nuggets to a prospector.
THE AUTHORS

We encounter integer numbers daily, and they are literally everywhere around us. It is not possible to avoid them, ignore them, or to be indifferent to them. So let us take together a journey through the world of integers, to get acquainted with their fascinating and sometimes magic properties. We will discover some surprising connections between number theory and geometry (see, e.g., Chaps. 1, 4, 7, and 8). We shall see which laws are followed by integers. We will also show that number theory has many practical applications without which we could not imagine the modern technical world. It has a big influence on everything we do.

This treatise on integer numbers is based on our more than 70 works on elementary and algebraic number theory that we published between the years 2001 and 2021 mostly in prestigious international journals such as *Journal of Number Theory, Integers, The Fibonacci Quarterly, Discrete Mathematics, Journal of Integer Sequences, Proceedings of the American Mathematical Society, and Czechoslovak Mathematical Journal* (see, e.g., dml.cz). Most of our results were reported at many international conferences on number theory and also the regular Friday seminar *Current Problems in Numerical Analysis,* which takes place at the Institute of Mathematics of the Czech Academy of Sciences in Prague [426].

The book is intended for a general mathematical audience—especially for those who can appreciate the beauty of both abstract and applied mathematics. We only assume that the reader is familiar with the basic rules of arithmetic and has no problem with adjustments of algebraic formulas. Only very rarely it is necessary to understand some relationships from linear algebra or calculus. Most chapters can be read independently from one another. Some parts are quite simple, others more complicated. If some part is too difficult, there is no problem in skipping it.

At the end of the book, there are several tables and a fairly extensive bibliography to attract attention to some important works in number theory. For inspiration, there are also several links to websites, although we are well aware that they are not subjected

to any review and change quite frequently. Newly defined terms are highlighted in italics in the text for the convenience of the reader. They can also be found in the Index.

In order to read the individual chapters, it is not necessary that the reader understands all theorems. There are 230 of them. Mathematicians formulate their ideas in the form of mathematical theorems that contain only what is relevant in the problem in question. We provide proofs of most statements so that one can verify their validity. For more complicated proofs, we only give a reference to the corresponding literature. The most beautiful feature of number theory is that the main ideas of proofs of every statement usually differ from each other. Formulations of mathematical theorems presented in this book often take only one or two lines, which makes it relatively easy to understand what a particular theorem says.

Mathematical theorems are valid forever. They are independent of position and time. Parliament does not decide about their validity by voting, nor the religious or political system in some country, nor does it depend on cultural customs. For example, the famous Pythagorean Theorem is valid on Earth as well as on the distant Andromeda galaxy M31, and it will also be valid after millions of years. Definitions of mathematical terms do not allow a double meaning. Also absolutely accurate formulations of mathematical problems do not allow more interpretations. The vague expressions we witness in daily life lead to a number of misunderstandings. Only a small percentage of our population is able to express their ideas accurately and perceive the beauty of mathematics. This was aptly stated by the well-known Hungarian mathematician Cornelius Lanczos (1893–1974) as follows:

> Most of the arts, as painting, sculpture, and music, have emotional appeal to the general public. This is because these arts can be experienced by one or more of our senses. Such is not true of the art of mathematics; this art can be appreciated only by mathematicians, and to become a mathematician requires a long period of intensive training. The community of mathematicians is similar to an imaginary community of musical composers whose only satisfaction is obtained by the interchange among themselves of the musical scores they compose.

There are many books on number theory. Let us mention, e.g., [6, 9, 28, 56, 82, 85, 91, 127, 132, 137, 138, 176, 235, 284, 291, 321–324, 327, 333, 344, 347, 350, 395, 413, 424]. However, our book contains some nonstandard topics. For instance, we will see how triangular numbers are related to the bell-work machinery of the Prague Astronomical Clock, what kind of mathematics is hidden in the traditional Chinese calendar, how the Fundamental Theorem of Arithmetic was used to design a message to extraterrestrial civilizations, how number theory is related to chaos, fractals, and graph theory. We will construct a $3 \times 3 \times 3$ magic cube containing only prime numbers. We will also get acquainted with the latest results from the hunt for the largest prime numbers and what prime numbers are good for. We shall present a number of their various real-life technical applications in completely different areas. We shall see how identification numbers of Czech organizations or bank account numbers are protected against possible errors with the help of prime numbers and error-detecting codes. We also discuss the so-called error-correcting codes, which automatically correct errors and we shall see how they are constructed. Further, we

show how large prime numbers are used to transmit secret messages, to generate pseudorandom numbers, and what is their significance for digital signatures. We also demonstrate how congruences can be applied in scheduling sport tournaments. We give other examples, where number theory is useful and charming at the same time.

In a number of discussions, many researchers helped us to improve the content of this book, in particular, L'ubomíra Balková, Jan Brandts, Karel Břinda, Yann Bugeaud, Pavel Burda, Walter Carlip, Antonín Čejchan, Karl Dilcher, Petr Golan, Václav Holub, Jan Chleboun, František Katrnoška, Petr Klán, Martin Klazar, Michal Kliment, Kurt Koltko, Sergey Korotov, Pavel and Filip Křížek, František Kuřina, Florian Luca, Attila Mészáros, Karel Micka, Jaroslav Mlýnek, Vladimír Novotný, Pavla Pavlíková, Edita Pelantová, Jan Pernička, Štefan Porubský, Andrzej Schinzel, Bangwei She, Ladislav Skula, László Szalay, Bedřich Šofr, Jakub Šolc, Pavel Trojovský, Jiří Tůma, Tomáš Vejchodský, and Václav Vopravil. We really appreciate their help, and they deserve our great thanks. Furthermore, we are deeply grateful to Hana Bílková and Eva Ritterová for their technical assistance in the final typesetting of the manuscript.

Finally, we are indebted to Ms. Elena Griniari, Ms. Tooba Shafique, Mrs. Kay Stoll, Mr. Vijayakumar Selvaraj, and Ms. Sindhu Sundararajan from Springer-Verlag for helpful cooperation in the preparation of this book. Our great thanks go to the Springer Publishing House for its care in the graphical design of the book and to the referees for valuable suggestions. We are also grateful to our families for patience and understanding.

The work on this book was supported by RVO 67985840 of the Czech Republic. Chapter 12 was partly supported also by Grant No. 20-01074S of the Grant Agency of the Czech Republic. These supports are gratefully acknowledged.

Prague, Czech Republic — Michal Křížek
Washington, DC, USA — Lawrence Somer
Prague, Czech Republic — Alena Šolcová
May 2021

Contents

Glossary of Symbols

$\mathbb{N} = \{1, 2, 3, \dots\}$	Set of natural numbers
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$	Set of integer numbers
$\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$	Set of prime numbers
$\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$	Set of rational numbers
$\mathbb{R}$	Set of real numbers
$\mathbb{C}$	Set of complex numbers
B_n	Bernoulli numbers
C_n	Cullen numbers
F_m	Fermat numbers
K_n	Fibonacci numbers
L_n	Lucas numbers
M_p	Mersenne numbers
$P_{k,n}$	Polygonal numbers
P_n	Pentagonal numbers
S_n	Square numbers
T_n	Triangular numbers
W_n	Woodall numbers
$(n_1, n_2, \dots, n_k)$	Greatest common divisor of $n_1, n_2, \dots, n_k$
$[n_1, n_2, \dots, n_k]$	Least common multiple $n_1, n_2, \dots, n_k$
$\{n_1, n_2, \dots, n_k\}$	Set of k numbers $n_1, n_2, \dots, n_k$ (the order does not matter)
$\langle n_1, n_2, \dots, n_k \rangle$	Ordered k-tuple of numbers $n_1, \dots, n_k$ (dependent on the order)
(a_i)	Sequence
$\lfloor a \rfloor$	Integer part of a real number a
$\lvert S \rvert$	Number of elements of the set S (also the absolute value)
$\approx$	Approximate equality
$n \equiv k \pmod{m}$	n is congruent to k modulo m
$n \not\equiv k \pmod{m}$	n is not congruent to k modulo m
$m \mid n$	m divides n
$m \nmid n$	m does divides n

$m^j \| n$	m^j exactly divides n for $1 < m \leq n$
$\max(m, n)$	Maximum of numbers m and n
$\min(m, n)$	Minimum of numbers m and n
sgn	Signum
$\mathrm{ord}_d n$	Order of n modulo d
$n!$	Product $1 \cdot 2 \cdots n$, n-factorial
det	Determinant
$\log_b$	Logarithm to the base b
log	Natural logarithm
e	Euler number 2.718 281 828…
$G(n)$	Directed graph (digraph) with n vertices
$\tau(n)$	Number of all positive divisors of n
$\omega(n)$	Number of all different prime divisors of n
$\sigma(n)$	Sum of all positive divisors of n
$s(n)$	Sum of all positive divisors of n less than n
ϕ	Euler totient function
λ	Carmichael lambda function
$\left(\frac{a}{p}\right)$	Legendre symbol for an odd prime p
$\left(\frac{a}{m}\right)$	Jacobi symbol for an odd number m
$\binom{n}{k}$	Binomial coefficient n over k
Re z	Real part of a complex number z
Im z	Imaginary part of a complex number z
$\bar{z}$	Complex conjugate number to z
i	Imaginary unit
i, j, k	Integer indices (subscripts)
$\exists$	There exist(s)
$\forall$	For all
$\mathcal{O}(\cdot)$	Landau symbol: $f(\alpha) = \mathcal{O}(g(\alpha))$ if there exists $C > 0$ such that $\lvert f(\alpha)\rvert \leq C\lvert g(\alpha)\rvert$ for $\alpha \to 0$ or $\alpha \to \infty$
$\emptyset$	Empty set
π	Ludolph number 3.141 592 653…
$\pi(x)$	Number of primes less than or equal to x
$\prod$	Product
$\sum$	Sum
$\cap$	Intersection
$\cup$	Union
$\setminus$	Set subtraction
$\subset$	Subset
$\in$	Is element of
$\notin$	Is not element of
$\{x \in A; \mathcal{P}(x)\}$	Set of all elements x from A which possess property $\mathcal{P}(x)$

$f: A \to B$	Mapping (function) f from the set A to the set B
$\Rightarrow$	Implication
$\Leftrightarrow$	Equivalence
$:=$	Assignment
$\square$	Halmos symbol

Chapter 1
Divisibility and Congruence

1.1 Introduction

According to ancient Chinese philosophy,
all phenomena arose from the dusty axis,
which split into two complete opposites,
yin *and* **yang**.

In one of the oldest Chinese books *I-Ching (Book of Changes)*, which dates approximately from the 8th century BC, there is a picture (so-called hexagram) containing 8×8 boxes. Each box contains 6 broken or full horizontal lines (see Fig. 1.1). The broken line indicates the old Chinese principle *yin* and the full principle of *yang*, which are in opposition. *Yin* is associated with the Moon, humidity, darkness, Earth, woman, and passivity, *yang* on the other hand with the Sun, drought, light, heaven, man, and activity.

The prominent German mathematician Gottfried Wilhelm Leibniz (1646–1716) associated this hexagram with the discovery of a binary system. Considering zero instead of the broken line and one instead of the full line, the symbols in particular boxes from left to right (starting from the top line) can be interpreted as the numbers $0, 1, 2, 3, \ldots$ written in the binary system. The first number in the upper left corner is therefore zero, even though this notation was not used for operations with numbers in the 8th century BC. The last number in the lower right corner corresponds to 63, which is written as 111111 in the binary system. The use of zero nowadays seems completely natural, but its discovery and in particular, its symbolic representation signified great progress in mathematics over the entire world (cf. Fig. 1.2).

Although the ancient Chinese did not perform with the symbols *yin–yang* any arithmetic operations, we cannot deny they were the first to represent numbers by the binary system. The discovery of the binary system found practical application

M. Křížek et al., *From Great Discoveries in Number Theory to Applications*,
https://doi.org/10.1007/978-3-030-83899-7_1

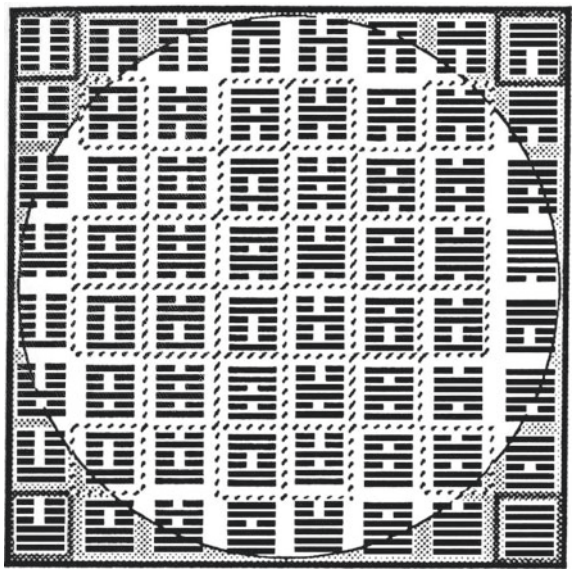


Fig. 1.1 The first depiction of a binary system from the 8th century BC

Fig. 1.2 Symbols *yin–yang* can be found on the current South Korean flag

only in today's computer age, i.e. almost three thousand years later. Computers display and process all information (including numbers) in the binary system. This is the easiest way in electronic circuits of a computer to process data. Thus, the functioning of e-mail, scanners, copiers, digital cameras, compact disks CD and DVD, cell phones, and the worldwide network of Internet is actually based on the ancient Chinese principles of *yin* (= 0) and *yang* (= 1).

However, nature has discovered the binary (or if you wish quartic base 4) system in the course of evolution more than three billion years ago. On the double helix of deoxyribonucleic acid (DNA), which is contained in each cell, there are four bases: adenine A, cytosine C, guanine G, and thymine T. If we replace them by the pairs 00, 01, 10, and 11, then each strand of DNA will correspond to a sequence of zeros and ones that actually represents genetic information recorded in the binary system. Note that the genetic code is nearly universal for animals and plants [290] with a few exceptions, see [193].

By means of the replication $R(A) = T$, $R(C) = G$, $R(G) = C$, and $R(T) = A$ one gets the second strand of DNA, thereby forming a double helix (see [162]). Nature thus actually discovered a simple logical operation: negation. For example,

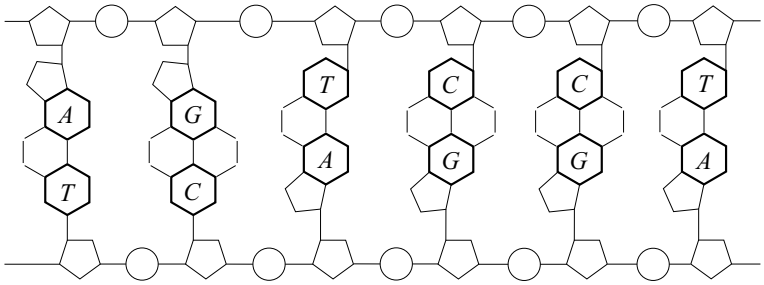


Fig. 1.3 Schematic illustration of DNA structure. Nucleotides are denoted by A, C, G, and T. Molecules of deoxyribose sugar (marked by pentagons) and phosphoric acid (marked by circles) are connected by strong covalent bonds. In this way, they protect genetic information against damage. The whole DNA molecule is actually twisted into a double helix

the nucleotides $\ldots AGTCCT\ldots$ on the upper strand (see Fig. 1.3) corresponding to the sequence of bits

$$\ldots 001011010111\ldots$$

pass during DNA replication on $\ldots TCAGGA\ldots$ corresponding to the complementary sequence

$$\ldots 110100101000\ldots,$$

where $A = 00$, $C = 01$, $G = 10$, and $T = 11$. The human genome in one cell is 750 MB (1 Byte = 8 bits).

Putting $A = 0$, $C = 1$, $G = 2$, and $T = 3$, the entire genetic information is transferred to the base 4 system. The sum of these numerical values is for all permissible pairs $A - T$, $C - G$, $G - C$, and $T - A$ always equal to 3. According to George Gamow, number theory could be used to elucidate the functioning of genes.

Here allow us a small detour. When designing the model for the structure of DNA in 1953, the fact that one of the authors Francis H.C. Crick was a physicist with abstract mathematical-physical thinking, played an important role. Already in 1950 Crick realized that if we connect the same molecules exactly in the same way, they will lie on a space helix (or especially on a circle or a straight line), see [73]. He received the Nobel Prize together with James D. Watson for the discovery of the double helix of DNA. Similarly, the founder of genetics Johann Gregor Mendel was a mathematician. His precise work with statistical data from crossing peas allowed him to discover laws of heredity (see [163, 269]). We further note that there are deep connections between the structure and function of DNA and topology and other areas of mathematics (see Benham et al. [29]).

In antiquity and the Middle Ages, number systems of different bases were used. For example, it is documented that the ancient Babylonians used a system with a base of 60. The origin of the words dozen (12) and pile (60) also illustrates that not only the decimal system was not used.

Recall that a positive integer n in a system of base b can be uniquely written in the form

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

where $c_i \in \{0, 1, \ldots, b-1\}$ are its digits, i.e., the set of digits has exactly b elements and $c_k \neq 0$. (The existence of such an expression can be proved by induction and the uniqueness can be obtained similarly as in Theorem 2.2.) If $b \geq 10$, then letters can play the role of other digits. For instance, in the hexadecimal system the following digits are used: 0, 1, 2, ..., 9, A, B, C, D, E, F. In this book, however, we will mostly use the decimal or binary system.

We set out on a journey to find secrets of integer numbers and will introduce some of their literally magical and unexpected features. In particular, we want to convey that numbers are not just for fun, but that number theory also has a huge number of practical applications. In the past, Euclid, Fermat, Euler, and many others actually only "played" with numbers, proved various statements about them, without knowing what a huge amount of their results would appear and what practical use their mathematical theorems would have. Moreover, the same result can often be used in a number of completely different situations. In this book, we will see this, for example, in the Chinese Remainder Theorem or Fermat's Little Theorem. Most statements from number theory wait for their practical use and many of them will never find applications. But this does not diminish their beauty.

Humanity has been dealing with investigation of prime numbers and their sometimes surprising properties for several millennia. But not until the 20th century was it discovered that prime numbers also have a number of useful applications. For example, since 1986 birth numbers ($\approx$ social security numbers) in the Czech Republic are formed to be divisible by the prime number 11. This is because the computer immediately detects an error as soon as you type a given birth number wrongly in one of its digits. If we are wrong in more than one digit, then there is a large probability that the computer is also able to detect an error. This is one example of a so-called error-detecting code. A somewhat more complicated code based on the prime 11 protects against a possible error appearing in bank account numbers, identification numbers of organizations, ISSN numbers of journals, and ISBN numbers of publications.

Larger primes having more than a hundred of digits, are used in modern cryptographic systems with public encryption key (for instance in the RSA method for the transmission of secret messages). Also, a digital signature is based on large primes. Efficient pseudo-random generators or algorithms for very fast multiplication of large numbers can be constructed using prime numbers. Prime numbers have a number of applications in signal analysis as well as in image processing using various theoretical transformations, such as when filtering data obtained from radars, sonar, modems, and radiotelescopes.

With the publication of the fundamental work *Disquisitiones arithmeticae* [118] by Gauss at the beginning of the 19th century, number theory established itself as a systematic mathematical discipline whose main subject is the study of properties of integers. Then in the 20th century it has found wide application in various fields of human activities.

It is used in a number of software products, in information security, in data compression, mathematical genetics, in physics, astronomy, robotics, and crystallography. Bar codes are commonly encountered in the commercial sphere today thanks to the enormous advances of optoelectronics. Their introduction in stores increases the speed of sales up to 400%. Error-correcting codes are used in data transmission from interplanetary probes or on railways to ensure their reliable operation. Also the functioning of digital cameras, telecommunication satellites, and music players is based on number theory. These modern achievements of civilization would never have been possible without number theory. Although they were not here in the 19th century, we would hardly give them up at present. Unfortunately, the general public does not realize this and considers them to be obvious. It is often underestimated how much human ingenuity, intellectual effort, and mathematical results are hidden in these technical equipments. For example, computer tomographs would not work without complex numbers. The reason is that the fast Fourier transform relies on complex arithmetic and it is needed for a fast calculation of the Radon inverse transformation in real time (see [185]).

In the following chapters, we will focus on geometric imagination, which can to a large extent facilitate the understanding of some algebraic statements, relations and basic concepts of number theory, such as the famous algebraic identities $(a \pm b)^2 = a^2 \pm 2ab + b^2$, $a^2 - b^2 = (a + b)(a - b)$, the Pythagorean Theorem (see Fig. 2.1) and the relation for the sum of an arithmetic sequence (see Fig. 1.4). In total, there are about 70 pictures in this book and it contains notes on the historical background of some concepts and methods.

Finally, let us mention that in solving equations we must exactly specify the set of admissible solutions. For example, the equation

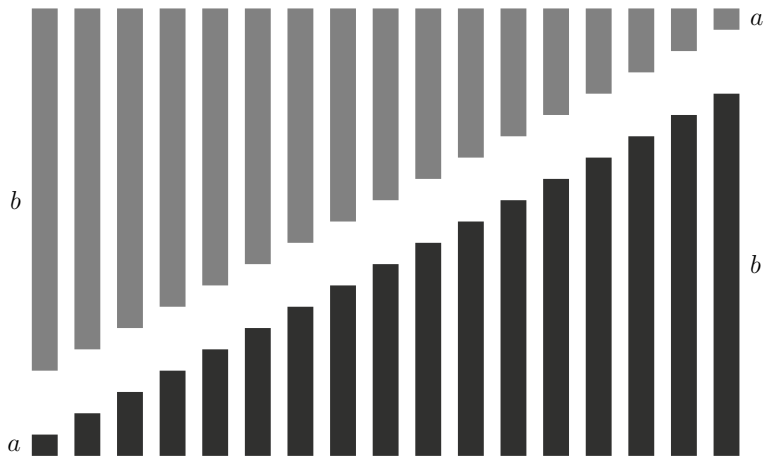


Fig. 1.4 Geometric interpretation of the well-known Gaussian relation for the sum of the first n members of an arithmetic sequence $a + (a + d) + (a + 2d) + \cdots + b = \frac{1}{2}n(a + b)$, where d is the difference of two neighboring terms and $b = a + (n - 1)d$

$$x^2 + y^2 = 2$$

has no solution in the set of even numbers. It has only one solution $(x, y) = (1, 1)$ in the set of natural numbers $\mathbb{N}$ and exactly four solutions $(\pm 1, \pm 1)$ in the set of integer numbers $\mathbb{Z}$. There are countably many solutions in the set of rational numbers $\mathbb{Q}$, e.g., $(\frac{1}{5}, \frac{7}{5})$, $(\frac{7}{13}, \frac{17}{13})$, $(\frac{7}{17}, \frac{23}{17})$, and there are uncountably many solutions in the set of real numbers $\mathbb{R}$ or complex numbers $\mathbb{C}$.

1.2 Natural Numbers

From ancient times people used the numbers $1, 2, 3, \ldots$ to express the number of some objects. The oldest use of zero was recorded in India. For a long time, zero was not even considered to be a number. Moreover, at present historians still do not have a year zero (but it is used by astronomers).

Sometimes we encounter the question of whether zero is or is not a natural number. Unfortunately, it is not possible to give a clear answer to this question of the YES/NO type, since whether or not we consider zero to be a natural number is a matter of definition. It is advisable to include zero in the set of natural numbers, for example, when determining the number of elements of finite sets, because the number of elements of the empty set is zero.

On the other hand, there are good reasons why it is sometimes advantageous not to include zero in the set of natural numbers. This is, for example, to avoid division by zero or when raising natural numbers to a natural power. In particular, the symbol 0^0 cannot be unambiguously assigned to one value that would naturally correspond to standard arithmetical operations with real numbers. For example, for $n = 1, 2, \ldots$ we have $0^n = 0$, while $n^0 = 1$. Archimedes' axiom presented below could not be applied if 0 would be a natural number. It is also not possible to define reasonably the least common multiple of, for example, the numbers 0 and 3, as we shall see in Sect. 1.4. Therefore, more often zero is not considered to be a natural number.

The *set of natural numbers (positive integers)* will be denoted by

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

It took a long time for mathematicians to figure out how in fact, natural numbers should be introduced. Among several options, the following four axioms formulated around 1891 by the Italian mathematician Giuseppe Peano (1858–1939) were defined. They use a special function "successor", truthfully characterize the set of natural numbers and are called *Peano's axioms* after him:

(A1) *There exists a unique natural number that is not a successor of any natural numbers.* We will denote this number by the symbol 1.

(A2) *Each natural number has exactly one successor.*

(A3) *Each natural number is a successor of at most one natural number.*
(A4) *Any set that contains the natural number* 1 *and for each natural number also contains its successor, is the set of natural numbers.*

The main idea of the principle of mathematical induction is based on these axioms. If we want to prove that some property $V(n)$ holds for all natural numbers n, then first we prove that $V(n)$ is valid for $n = 1$. Then we prove that if the property $V(n)$ holds for some natural number n, then $V(n+1)$ also holds for the successor $n+1$ of the number n.

The *set of integer numbers* is denoted by

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

This set therefore consists of natural numbers, numbers opposite to them (i.e. with minus sign), and zero. It is closed under the addition and multiplication operations, i.e., for any $m, n \in \mathbb{Z}$ we have $m + n \in \mathbb{Z}$ and $m \cdot n \in \mathbb{Z}$. The following relations $=$, $<$, $>$, $\leq$, and $\geq$ are also established on the set $\mathbb{Z}$.

Convention. Integer numbers in this book will mostly denoted by i, j, k, ℓ, m, n, p, q, r, s, t,..., unless otherwise specified.

The set of natural numbers $\mathbb{N}$ is *well ordered,* which means that an arbitrary nonempty subset has a least element. The sets of integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, and real numbers $\mathbb{R}$ do not have a similar property.

The fact that the set of natural numbers is well ordered is equivalent to the principle of mathematical induction (see e.g. [395, p. 40]). It is actually an axiom, i.e., a statement which is accepted without proof, because it does not contradict our intuition.

Already in antiquity, Archimedes (287–212 BC) realized that the set of natural numbers is well ordered.

Archimedes' axiom. *For any natural numbers j and k there exists a natural number n such that $nj \geq k$.*

Archimedes' axiom can be proved. So it is a mathematical theorem, but for historical reasons, it is called an axiom. If it were not true, then there would exist $j, k \in \mathbb{N}$ such that $nj < k$ for each $n \in \mathbb{N}$. Since the set $\mathbb{N}$ is well ordered, there exists a smallest element $k - mj$ of the subset $M = \{k - nj\,;\ n \in \mathbb{N}\} \subset \mathbb{N}$ However, the element $k - (m+1)j$ is also in M and satisfies

$$k - (m+1)j = (k - mj) - j < k - mj,$$

which contradicts the minimality of the element $k - mj$ from the set M.

Archimedes' axiom has a nice geometric interpretation. It says, in fact, how many line segments of length j cover a line of length k.

1.3 Simple Criteria of Divisibility

We say that d *divides* (without remainder) a natural number n, if there exists $k \in \mathbb{N}$ such that $n = d \cdot k$. In this case we shall write

$$d \mid n,$$

for instance, $3 \mid 6$. The number d is called a *divisor* of the number n and the numbers 1 and n are called *trivial divisors* of n. If $1 < d < n$, then d is called a *nontrivial divisor*, and if $d < n$, then d is called a *proper divisor* of n. If m does not divide n, we shall write $m \nmid n$, for instance, $5 \nmid 6$. Similar definitions can also be introduced for integer numbers when $m \neq 0$. An integer divisible by 2 is called *even*, otherwise *odd*.

Theorem 1.1 *A natural number n written in the decimal system is divisible by*

(a) *two, if its last digit is even,*
(b) *three, if the sum of all its digits is divisible by* 3*,*
(c) *four, if the number formed by the last two digits of n is divisible by* 4*,*
(d) *five, if its last digit is* 0 *or* 5*,*
(e) *six, if it is even and divisible by* 3*,*
(f) *seven, if twice the number of hundreds increased by the number formed by the last two digits is divisible by* 7*,*
(g) *eight, if the number formed by the last three digits of n is divisible by* 8*,*
(h) *nine, if the sum of all its digits is divisible by* 9*,*
(i) *ten, if its last digit is* 0*.*

Proof Let n be an arbitrary natural number. In the decimal system it can be uniquely written in the form

$$n = c_k 10^k + \cdots + c_2 10^2 + c_1 10 + c_0, \tag{1.1}$$

where its digits $c_k, \ldots, c_2, c_1, c_0$ are from the set $\{0, 1, 2, \ldots, 9\}$ and $c_k \neq 0$. From (1.1) we immediately get (a), (c), (d), (g), and (i).

Denote by s the sum of all digits of the number n, i.e.,

$$s = c_k + \cdots + c_2 + c_1 + c_0.$$

Then

$$n - s = c_k(10^k - 1) + \cdots + c_2 99 + c_1 9,$$

where each term on the right-hand side is divisible by nine. That is why, n is divisible by three (respectively nine) exactly when s is divisible by three (respectively nine). Hence, (b) and (h) hold.

We observe that (e) follows immediately from (a) and (b). It remains to prove (f). The next proof of this criterion comes from Václav Holub. Twice the number of hundreds of n increased by the number formed by the last two digits is equal to

$$m = 2c_k 10^{k-2} + \cdots + 2c_2 + 10c_1 + c_0.$$

By (1.1) we see that the difference

$$n - m = 98c_k 10^{k-2} + \cdots + 98c_2$$

is divisible by seven, since $7 \mid 98$. Now if 7 divides m, then 7 also divides the sum $m + (n - m) = n$. □

Example By Theorem 1.1 we have $7 \mid 1239$, since 7 divides $2 \cdot 12 + 39 = 63$.

Example For larger numbers it is usually necessary to apply an appropriate rule several times. For instance,

$$3 \mid 188887777788885,$$

whose sum of digits 105, which is divisible by 3, since $3 \mid (1 + 5)$.

We will deal with divisibility by 11 in Theorem 11.1. Let us further introduce rules for divisibility by the numbers 13, 17, and 19.

Remark Let n be a given natural number, let k be the number of tens in n, and let $c_0 \in \{0, 1, \ldots, 9\}$ be the last digit of n. Then

$$n = 10k + c_0.$$

A natural number n is divisible by 13 if four times the last digit added to the number of tens is divisible by 13. To see this we set $m = k + 4c_0$. Then

$$13 \mid n = 10k + c_0 = 10(m - 4c_0) + c_0 = 10m - 39c_0 \Leftrightarrow 13 \mid 10m \Leftrightarrow 13 \mid m.$$

For instance, $13 \mid 507$, since 13 divides $4 \cdot 7 + 50 = 78$.

A natural number n is divisible by 17, if five times the last digit subtracted from the number of tens is divisible by 17. To prove this we put $m = k - 5c_0$. Then

$$17 \mid n = 10k + c_0 = 10(m + 5c_0) + c_0 = 10m + 51c_0 \Leftrightarrow 17 \mid 10m \Leftrightarrow 17 \mid m.$$

For example, $17 \mid 357$, since 17 divides $35 - 5 \cdot 7 = 0$.

A natural number n is divisible by 19, if double the last digit added to the number of tens is divisible by 19. We set $m = k + 2c_0$. Then

$$19 \mid n = 10k + c_0 = 10(m - 2c_0) + c_0 = 10m - 19c_0 \Leftrightarrow 19 \mid 10m \Leftrightarrow 19 \mid m.$$

For instance, $19 \mid 1026$, since 19 divides $2 \cdot 6 + 102 = 114$ and 19 divides $11 + 2 \cdot 4 = 19$.

The divisibility tests by 13 and 19 are applications of a theorem by Carl Fredrik Liljevalch in 1838 (see [176, p. 283]).

Recall that the *binomial coefficient* $\binom{n}{m}$ (read n over m) is defined by

$$\binom{n}{m} = \frac{n!}{m!(n-m)!} \quad \text{for integers } n \geq m \geq 0,$$

where

$$n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n \quad \text{for } n \in \mathbb{N}, \quad 0! = 1.$$

The symbol $n!$ is called *n factorial*.

Remark Let $k = n - m$ be a natural number. Then we have

$$k!\binom{n}{m} = k!\frac{n!}{m!k!} = \frac{n!}{m!} = (m+1)(m+2)\cdots(m+k).$$

Thus we see that the product of k consecutive numbers on the right-hand side is always divisible by $k!$. Moreover, it can be proved that $(m+1)(m+2)\cdots(m+k)$ for $k \geq 2$ and $m \geq 2$ is never equal to the power ℓ^j for some $j \geq 2$ and $\ell \geq 2$ (see Erdős and Selfridge [105]).

1.4 The Least Common Multiple and the Greatest Common Divisor

Let m and n be arbitrary natural numbers. Denote by $M \subset \mathbb{N}$ a subset of all common multiples of m and n. The set M is clearly nonempty, because it contains e.g. the product mn. Since $\mathbb{N}$ is well ordered, M must contain a smallest element, which we denote by $[m, n]$ and call the *least common multiple* of the numbers $m, n \in \mathbb{N}$. Thus, it is the smallest natural number divisible by both m and n.

Similarly, the *greatest common divisor* of two integer numbers m and n, which are not zero at the same time, is the largest integer that divides both m and n. The greatest common divisor of numbers m and n will be denoted by (m, n).

A basic property of the largest common divisor and least common multiple is obviously

$$(m, n) = (n, m), \quad [m, n] = [n, m].$$

For $k, m, n \in \mathbb{N}$ the following distributive properties hold

$$[k, (m, n)] = ([k, m], [k, n]) \quad \text{and} \quad (k, [m, n]) = [(k, m), (k, n)].$$

Theorem 1.2 *For any natural numbers m and n we have*

$$mn = (m, n)[m, n]. \tag{1.2}$$

Proof Denote by $d \geq 1$ an arbitrary common divisor of m and n. Then $\frac{m}{d}$ and $\frac{n}{d}$ are natural numbers, $\frac{m}{d}n$ is an integer multiple of the number n, and $\frac{n}{d}m$ is an integer multiple of the number m. Therefore, $\frac{mn}{d}$ is a common multiple of the numbers m and n. Now if d is the greatest common divisor of the numbers m and n, then $\frac{mn}{d}$ has to be the least common multiple m and n. □

Example For $m = 18$ and $n = 27$ we have $(m, n) = 9$, $[m, n] = 54$, and hence $18 \cdot 27 = 9 \cdot 54$.

The greatest common divisor and the least common multiple of more than two numbers can be defined by induction similarly as for two numbers. For $k > 2$ and integer numbers $n_1, \ldots, n_k$ we set

$$\begin{aligned}(n_1, \ldots, n_{k-1}, n_k) &= \big((n_1, \ldots, n_{k-1}), n_k\big) \quad \text{if } n_1 \neq 0,\\ [n_1, \ldots, n_{k-1}, n_k] &= \big[[n_1, \ldots, n_{k-1}], n_k\big] \quad \text{if } n_1 n_2 \cdots n_k \neq 0.\end{aligned}$$

1.5 Coprime Numbers

Natural numbers m and n are called *coprime,* if $(m, n) = 1$. An interesting real-life technical application of coprime numbers is depicted in Fig. 1.5. It shows two gear ratios. In the left part of the figure, the larger wheel has 20 teeth and the smaller one 10 teeth. If there is one tooth slightly damaged on the larger wheel (it is marked with a dot in Fig. 1.5), then it fits into exactly the same gap in the smaller wheel after each turn of the larger wheel. Just at this gap, the smaller wheel will be very quickly worn out. In the right part of Fig. 1.5 we see two wheels with 25 and 12 teeth. Since $(25, 12) = 1$, there will be completely uniform wear. Let us still note that the ratio of the teeth is actually almost the same in both cases: 2 and 2.083.

Here is another practical use of coprime numbers. The fixed part of the caliper is equipped with a scale in which each centimeter is divided into 10 mm. On the moving part, the so-called vernier is divided into 10 equally long pieces, which together have 9 mm (see Fig. 1.6). The fact that 9 and 10 are coprime allows us to determine the dimensions of small objects with precision to the nearest tenth of a millimeter. When measuring, we determine which line of the vernier merges with some line on the millimeter scale of the caliper. So many tenths of a millimeter is then added to the measured millimeters (i.e. to their largest integer value). If we were to choose instead of 9 mm another length that divides 10 mm, then several lines could merge so we would not know which data applies.

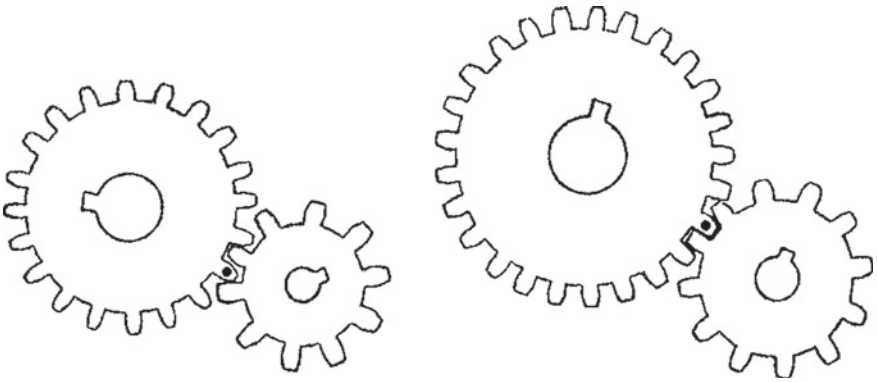
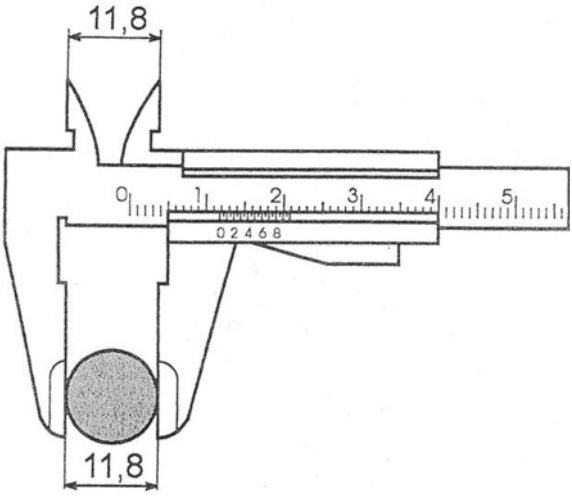


Fig. 1.5 For the number of teeth on the left and right gears we have $(20, 10) = 10$ and $(25, 12) = 1$, respectively

Fig. 1.6 Vernier on a caliper



The author of this elegant idea is a Portuguese royal mathematician and cosmographer Pedro Nunes (1502–1578), who first used it for accurate angle measurements. At present, a vernier-like device is used also in micrometers and is called the *nonius* in his honor.

1.6 Euclidean Algorithm

To calculate the greatest common divisor (m, n) of two large natural numbers $m \geq n$ the well-known *Euclidean algorithm* is often used. It can be briefly characterized as follows:

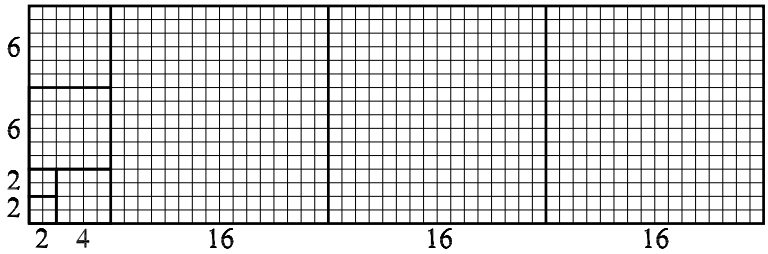


Fig. 1.7 Geometric illustration of the reduction of input data during the use of the Euclidean algorithm for calculating the greatest common divisor (54, 16)

If n divides m, then $(m, n) = n$, otherwise we have

$$(m, n) = (n, z),$$

where $z \geq 1$ is the remainder when dividing the number m by the number n. Since $z < m$, larger problem is thus converted to a smaller one. The next steps of the algorithm then proceed similarly. The original problem is thus reduced to smaller and smaller parts until we get the remainder 0.

For instance, if $m = 54$ and $n = 16$, then by the Euclidean algorithm we get

$$(54, 16) = (16, 6) = (6, 4) = (4, 2) = 2.$$

Now let us imagine that we have a squared paper with dimensions 54×16 (see Fig. 1.7). From this we will gradually cut off squares as large as possible and we will perform this as long as possible (see [188]), i.e., in the first step we cut off 3 squares 16×16, in the next step we cut 2 squares 6×6, etc. The length of the side of the square that we have left, is the result of the Euclidean algorithm, i.e. the largest common divisor of numbers 54 and 16.

If the numbers m and n are coprime, the Euclidean algorithm ends with the least possible square 1×1. For example, two consecutive natural numbers are always coprime.

To calculate the least common multiple of $[m, n]$, it is also useful to apply the Euclidean algorithm first, because $(m, n) \leq [m, n]$, and then use the relation (1.2). We return to the Euclidean algorithm in Theorem 7.7.

1.7 Linear Diophantine Equations

The name Diophantine equation is derived from the name of the Greek mathematician *Diophantus*, who lived in Alexandria in the 3rd century AD and dealt with solving various problems in number theory. Diophantine equations are equations with integer

coefficients, whose solution is sought in integers. In solving systems of Diophantine equations we usually have more unknowns than equations. In this section we shall deal only with one linear Diophantine equation with two integer unknowns.

Theorem 1.3 *Let $k = (m, n)$ for some integers m and n, which are not simultaneously zero. Then there exist integers x and y such that*

$$mx + ny = k. \tag{1.3}$$

Proof Let S be a set of all integers of the form $ma + nb$, where a and b are integers. The number m or n is not zero, and thus the set S contains nonzero integers. Since $t = ma + nb$ is in S, the number $-t = m(-a) + n(-b)$ is also in S. Hence, S contains natural numbers. Since $\mathbb{N}$ is well ordered (see Sect. 1.2), there exists a smallest natural number d in S of the form $d = mx + ny$. We claim that $d = (m, n)$.

First we show that d is a common divisor of m and n. Let $u = ma_0 + nb_0$ be an arbitrary element in S. By division we find that $u = qd + r$, where $0 \leq r < d$ is the remainder. Thus we have

$$ma_0 + nb_0 = q(mx + ny) + r,$$

i.e.,

$$r = m(a_0 - qx) + n(b_0 - qy)$$

and $r \in S$. Since $r \geq 0$ and $r < d$, it follows that $r = 0$ due to the choice of d. Therefore, d divides u for all $u \in S$. However, $m = m \cdot 1 + n \cdot 0 \in S$ and $n = m \cdot 0 + n \cdot 1 \in S$, which means that d divides both m and n.

Finally, let e be an arbitrary common divisor of m and n. Then e divides $mx + ny = d$, and thus $d = (m, n) = k$. □

Theorem 1.3 has a very nice geometric interpretation (see Burton [56, p. 22]). Each line $mx + ny = k$ passes through the grid points (x, y), which are solutions of the linear Diophantine equation (see Fig. 1.8 for $m = 2$, $n = -3$, and $k = 1$). Relation (1.3) is called *Bézout's identity*.

Example Let us show how to solve the following Diophantine equation

$$8x - 27y = 1$$

by a method similar to the Euclidean algorithm. Since $(8, 27) = 1$, this equation has by Theorem 1.3 a solution and we have

$$x = 3y + \frac{3y + 1}{8}.$$

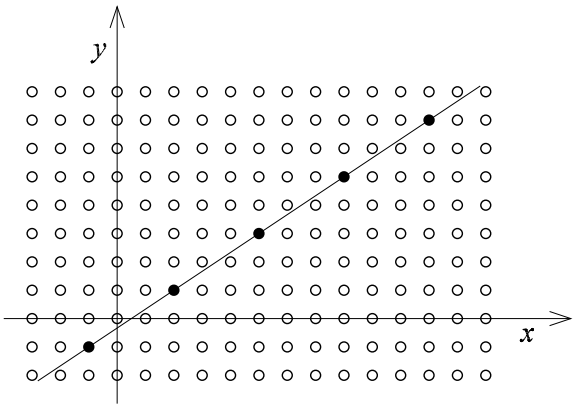


Fig. 1.8 A straight line corresponding to the linear Diophantine equation $2x - 3y = 1$ passes through points with coordinates $\ldots, (-1, -1), (2, 1), (5, 3), (8, 5), (11, 7), \ldots$

To get an integer solution, $3y + 1$ must be a multiple of 8, i.e., there exists an integer v such that

$$3y + 1 = 8v, \quad \text{and thus } y = 2v + \frac{2v - 1}{3}.$$

Hence, we can choose $v = 2$ and by backward substitution we get that the pair $y = 5$ and $x = 17$ is a solution. For $v = 5, 8, 11, \ldots$ and $v = -1, -4, -7, \ldots$ we obtain further pairs of solutions.

1.8 Congruence

In this section we will discuss the concept of congruence, introduced by the German mathematician Carl Friedrich Gauss. He used it for various calculations, such as which day falls on Easter Sunday (see Remark below). Congruences have many other practical applications in cryptography, in astronomy when creating calendars (see [56, p. 122]), in generating pseudorandom numbers, etc., as we shall see in Sects. 11.2–11.5.

Let n, z be integers and $m \in \mathbb{N}$. Then we say that *n is congruent to z modulo m* and write

$$n \equiv z \pmod{m},$$

if $n - z$ is divisible by m. The number m is called the *modulus*.

The notion congruence modulo 12 can be clearly demonstrated on the dial of a classical clock.

We now derive some practical rules for calculating congruences. Obviously $a \equiv a \pmod{m}$ for any integer a. If $a \equiv b \pmod{m}$, then for arbitrary integers a, b, c and $k \geq 0$ we easily find that

$$\begin{aligned} b &\equiv a \pmod{m}, \\ a \pm c &\equiv b \pm c \pmod{m}, \\ ac &\equiv bc \pmod{m}, \\ a^k &\equiv b^k \pmod{m}, \end{aligned} \tag{1.4}$$

where the last congruence follows from the equality

$$a^k - b^k = (a-b)\left(a^{k-1} + a^{k-2}b + \cdots + b^{k-1}\right), \quad k > 1.$$

From the above relationships, it is clear that the relation "$\equiv$" modulo m is reflexive and symmetric. Since transitivity holds as well, it is actually an equivalence relation on the set of integers.

If $(c, m) = 1$, then the congruence $ac \equiv bc \pmod{m}$ can be canceled by c, i.e., $a \equiv b \pmod{m}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then obviously

$$\begin{aligned} a + c &\equiv b + d \pmod{m}, \\ a - c &\equiv b - d \pmod{m}, \end{aligned}$$

and moreover,

$$ac \equiv bd \pmod{m}. \tag{1.5}$$

For $a = b + im$ and $c = d + jm$ it indeed holds that $ac = bd + (jb + id + ijm)m$, and thus congruence (1.5) is satisfied. Moreover, by (1.4) we also get that

$$f(a) \equiv f(b) \pmod{m}$$

for an arbitrary polynomial f with integer coefficients.

Remark The Gaussian algorithm on which day of the year y is Easter Sunday proceeds as follows:

For the period 1900–2099 we set $m = 24$ and $n = 5$. Let a, b, c, d, e be the smallest nonnegative numbers satisfying the congruences

$$\begin{aligned} a &\equiv y \pmod{19}, \\ b &\equiv y \pmod{4}, \\ c &\equiv y \pmod{7}, \\ d &\equiv (m + 19a) \pmod{30}, \\ e &\equiv (n + 2b + 4c + 6d) \pmod{7}. \end{aligned}$$

Here $a + 1$ is called *golden number* (the ordinal number of the year in the Metonic cycle having a period of 19 years in which there are 235 lunations). If $d + e < 10$ then the Easter Sunday will be on the $(22 + d + e)$th March, if $d + e = 35$ it will be on the $(d + e - 16)$th April and otherwise it will be on the $(d + e - 9)$th April.