# A concise introduction to the theory of numbers

ALAN BAKER
*Professor of Pure Mathematics in the University of Cambridge*

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge CB2 1RP, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, United Kingdom
40 West 20th Street, New York, NY 10011–4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia



First published 1984
Reprinted 1986 (twice), 1988, 1990, 1994, 1997

*A catalogue record for this book is available from the British Library*

Library of Congress catalogue card number: 84–1911

ISBN 0 521 28654 9 paperback

Transferred to digital printing 2002

# *Contents*

# 1

## *Divisibility*

### 1 Foundations

The set 1, 2, 3, ... of all natural numbers will be denoted by $\mathbb{N}$. There is no need to enter here into philosophical questions concerning the existence of $\mathbb{N}$. It will suffice to assume that it is a given set for which the Peano axioms are satisfied. They imply that addition and multiplication can be defined on $\mathbb{N}$ such that the commutative, associative and distributive laws are valid. Further, an ordering on $\mathbb{N}$ can be introduced so that either $m < n$ or $n < m$ for any distinct elements $m$, $n$ in $\mathbb{N}$. Furthermore, it is evident from the axioms that the principle of mathematical induction holds and that every non-empty subset of $\mathbb{N}$ has a least member. We shall frequently appeal to these properties.

As customary, we shall denote by $\mathbb{Z}$ the set of integers $0, \pm 1, \pm 2, \ldots$, and by $\mathbb{Q}$ the set of rationals, that is the numbers $p/q$ with $p$ in $\mathbb{Z}$ and $q$ in $\mathbb{N}$. The construction, commencing with $\mathbb{N}$, of $\mathbb{Z}$, $\mathbb{Q}$ and then the real and complex numbers $\mathbb{R}$ and $\mathbb{C}$ forms the basis of Mathematical Analysis and it is assumed known.

### 2 Division algorithm

Suppose that $a$, $b$ are elements of $\mathbb{N}$. One says that $b$ divides $a$ (written $b|a$) if there exists an element $c$ of $\mathbb{N}$ such that $a = bc$. In this case $b$ is referred to as a divisor of $a$, and $a$ is called a multiple of $b$. The relation $b|a$ is reflexive and transitive but not symmetric; in fact if $b|a$ and $a|b$ then $a = b$. Clearly also if $b|a$ then $b \leq a$ and so a natural number has only finitely many divisors. The concept of divisibility is readily extended

to $\mathbb{Z}$; if $a$, $b$ are elements of $\mathbb{Z}$, with $b \neq 0$, then $b$ is said to divide $a$ if there exists $c$ in $\mathbb{Z}$ such that $a = bc$.

We shall frequently appeal to the division algorithm. This asserts that for any $a$, $b$ in $\mathbb{Z}$, with $b > 0$, there exist $q$, $r$ in $\mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$. The proof is simple; indeed if $bq$ is the largest multiple of $b$ that does not exceed $a$ then the integer $r = a - bq$ is certainly non-negative and, since $b(q+1) > a$, we have $r < b$. The result plainly remains valid for any integer $b \neq 0$ provided that the bound $r < b$ is replaced by $r < |b|$.

### 3 Greatest common divisor

By the greatest common divisor of natural numbers $a$, $b$ we mean an element $d$ of $\mathbb{N}$ such that $d|a$, $d|b$ and every common divisor of $a$ and $b$ also divides $d$. We proceed to prove that a number $d$ with these properties exists; plainly it will be unique, for any other such number $d'$ would divide $a$, $b$ and so also $d$, and since similarly $d|d'$ we have $d = d'$.

Accordingly consider the set of all natural numbers of the form $ax + by$ with $x$, $y$ in $\mathbb{Z}$. The set is not empty since, for instance, it contains $a$ and $b$; hence there is a least member $d$, say. Now $d = ax + by$ for some integers $x$, $y$, whence every common divisor of $a$ and $b$ certainly divides $d$. Further, by the division algorithm, we have $a = dq + r$ for some $q$, $r$ in $\mathbb{Z}$ with $0 \leq r < d$; this gives $r = ax' + by'$, where $x' = 1 - qx$ and $y' = -qy$. Thus, from the minimal property of $d$, it follows that $r = 0$ whence $d|a$. Similarly we have $d|b$, as required.

It is customary to signify the greatest common divisor of $a$, $b$ by $(a, b)$. Clearly, for any $n$ in $\mathbb{N}$, the equation $ax + by = n$ is soluble in integers $x$, $y$ if and only if $(a, b)$ divides $n$. In the case $(a, b) = 1$ we say that $a$ and $b$ are relatively prime or coprime (or that $a$ is prime to $b$). Then the equation $ax + by = n$ is always soluble.

Obviously one can extend these concepts to more than two numbers. In fact one can show that any elements $a_1, \ldots, a_m$ of $\mathbb{N}$ have a greatest common divisor $d = (a_1, \ldots, a_m)$ such that $d = a_1x_1 + \cdots + a_mx_m$ for some integers $x_1, \ldots, x_m$. Further, if $d = 1$, we say that $a_1, \ldots, a_m$ are relatively prime and then the equation $a_1x_1 + \cdots + a_mx_m = n$ is always soluble.

## 4 Euclid's algorithm

A method for finding the greatest common divisor $d$ of $a$, $b$ was described by Euclid. It proceeds as follows.

By the division algorithm there exist integers $q_1$, $r_1$ such that $a = bq_1 + r_1$ and $0 \leq r_1 < b$. If $r_1 \neq 0$ then there exist integers $q_2$, $r_2$ such that $b = r_1 q_2 + r_2$ and $0 \leq r_2 < r_1$. If $r_2 \neq 0$ then there exist integers $q_3$, $r_3$ such that $r_1 = r_2 q_3 + r_3$ and $0 \leq r_3 < r_2$. Continuing thus, one obtains a decreasing sequence $r_1, r_2, \ldots$ satisfying $r_{j-2} = r_{j-1} q_j + r_j$. The sequence terminates when $r_{k+1} = 0$ for some $k$, that is when $r_{k-1} = r_k q_{k+1}$. It is then readily verified that $d = r_k$. Indeed it is evident from the equations that every common divisor of $a$ and $b$ divides $r_1, r_2, \ldots, r_k$; and moreover, viewing the equations in the reverse order, it is clear that $r_k$ divides each $r_j$ and so also $b$ and $a$.

Euclid's algorithm furnishes another proof of the existence of integers $x$, $y$ satisfying $d = ax + by$, and furthermore it enables these $x$, $y$ to be explicitly calculated. For we have $d = r_k$ and $r_j = r_{j-2} - r_{j-1} q_j$ whence the required values can be obtained by successive substitution. Let us take, for example, $a = 187$ and $b = 35$. Then, following Euclid, we have

$$187 = 35 \cdot 5 + 12, \quad 35 = 12 \cdot 2 + 11, \quad 12 = 11 \cdot 1 + 1.$$

Thus we see that $(187, 35) = 1$ and moreover

$$1 = 12 - 11 \cdot 1 = 12 - (35 - 12 \cdot 2) = 3(187 - 35 \cdot 5) - 35.$$

Hence a solution of the equation $187x + 35y = 1$ in integers $x$, $y$ is given by $x = 3$, $y = -16$.

There is a close connection between Euclid's algorithm and the theory of continued fractions; this will be discussed in Chapter 6.

## 5 Fundamental theorem

A natural number, other than 1, is called a prime if it is divisible only by itself and 1. The smallest primes are therefore given by 2, 3, 5, 7, 11, ....

Let $n$ be any natural number other than 1. The least divisor of $n$ that exceeds 1 is plainly a prime, say $p_1$. If $n \neq p_1$ then, similarly, there is a prime $p_2$ dividing $n/p_1$. If $n \neq p_1 p_2$ then there is a prime $p_3$ dividing $n/p_1 p_2$; and so on. After a finite

number of steps we obtain $n = p_1 \cdots p_m$; and by grouping together we get the standard factorization (or canonical decomposition) $n = p_1^{j_1} \cdots p_k^{j_k}$, where $p_1, \ldots, p_k$ denote distinct primes and $j_1, \ldots, j_k$ are elements of $\mathbb{N}$.

The fundamental theorem of arithmetic asserts that the above factorization is unique except for the order of the factors. To prove the result, note first that if a prime $p$ divides a product $mn$ of natural numbers then either $p$ divides $m$ or $p$ divides $n$. Indeed if $p$ does not divide $m$ then $(p, m) = 1$ whence there exist integers $x$, $y$ such that $px + my = 1$; thus we have $pnx + mny = n$ and hence $p$ divides $n$. More generally we conclude that if $p$ divides $n_1 n_2 \cdots n_k$ then $p$ divides $n_l$ for some $l$. Now suppose that, apart from the factorization $n = p_1^{j_1} \cdots p_k^{j_k}$ derived above, there is another decomposition and that $p'$ is one of the primes occurring therein. From the preceding conclusion we obtain $p' = p_l$ for some $l$. Hence we deduce that, if the standard factorization for $n/p'$ is unique, then so also is that for $n$. The fundamental theorem follows by induction.

It is simple to express the greatest common divisor $(a, b)$ of elements $a$, $b$ of $\mathbb{N}$ in terms of the primes occurring in their decompositions. In fact we can write $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, where $p_1, \ldots, p_k$ are distinct primes and the $\alpha$s and $\beta$s are non-negative integers; then $(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$, where $\gamma_l = \min(\alpha_l, \beta_l)$. With the same notation, the lowest common multiple of $a, b$ is defined by $\{a, b\} = p_1^{\delta_1} \cdots p_k^{\delta_k}$, where $\delta_l = \max(\alpha_l, \beta_l)$. The identity $(a, b)\{a, b\} = ab$ is readily verified.

### 6 Properties of the primes

There exist infinitely many primes, for if $p_1, \ldots, p_n$ is any finite set of primes then $p_1 \cdots p_n + 1$ is divisible by a prime different from $p_1, \ldots, p_n$; the argument is due to Euclid. It follows that, if $p_n$ is the $n$th prime in ascending order of magnitude, then $p_m$ divides $p_1 \cdots p_n + 1$ for some $m \geq n + 1$; from this we deduce by induction that $p_n < 2^{2^n}$. In fact a much stronger result is known; indeed $p_n \sim n \log n$ as $n \to \infty$.† The result is equivalent to the assertion that the number $\pi(x)$ of primes $p \leq x$ satisfies $\pi(x) \sim x/\log x$ as $x \to \infty$. This is called the prime-number

† The notation $f \sim g$ means that $f/g \to 1$; and one says that $f$ is asymptotic to $g$.

theorem and it was proved by Hadamard and de la Vallée Poussin independently in 1896. Their proofs were based on properties of the Riemann zeta-function about which we shall speak in Chapter 2. In 1737 Euler proved that the series $\sum 1/p_n$ diverges and he noted that this gives another demonstration of the existence of infinitely many primes. In fact it can be shown by elementary arguments that, for some number $c$,

$$\sum_{p \leq x} 1/p = \log\log x + c + O(1/\log x).$$

Fermat conjectured that the numbers $2^{2^n}+1$ $(n = 1, 2, \ldots)$ are all primes; this is true for $n = 1, 2, 3$ and 4 but false for $n = 5$, as was proved by Euler. In fact 641 divides $2^{32}+1$. Numbers of the above form that are primes are called Fermat primes. They are closely connected with the existence of a construction of a regular plane polygon with ruler and compasses only. In fact the regular plane polygon with $p$ sides, where $p$ is a prime, is capable of construction if and only if $p$ is a Fermat prime. It is not known at present whether the number of Fermat primes is finite or infinite.

Numbers of the form $2^n - 1$ that are primes are called Mersenne primes. In this case $n$ is a prime, for plainly $2^m - 1$ divides $2^n - 1$ if $m$ divides $n$. Mersenne primes are of particular interest in providing examples of large prime numbers; for instance it is known that $2^{44\,497} - 1$ is the 27th Mersenne prime, a number with 13 395 digits.

It is easily seen that no polynomial $f(n)$ with integer coefficients can be prime for all $n$ in $\mathbb{N}$, or even for all sufficiently large $n$, unless $f$ is constant. Indeed by Taylor's theorem, $f(mf(n)+n)$ is divisible by $f(n)$ for all $m$ in $\mathbb{N}$. On the other hand, the remarkable polynomial $n^2-n+41$ is prime for $n = 1, 2, \ldots, 40$. Furthermore one can write down a polynomial $f(n_1, \ldots, n_k)$ with the property that, as the $n_j$ run through the elements of $\mathbb{N}$, the set of positive values assumed by $f$ is precisely the sequence of primes. The latter result arises from studies in logic relating to Hilbert's tenth problem (see Chapter 8).

The primes are well distributed in the sense that, for every $n > 1$, there is always a prime between $n$ and $2n$. This result, which is commonly referred to as Bertrand's postulate, can be

regarded as the forerunner of extensive researches on the difference $p_{n+1}-p_n$ of consecutive primes. In fact estimates of the form $p_{n+1}-p_n = O(p_n^{\kappa})$ are known with values of $\kappa$ just a little greater than $\frac{1}{2}$; but, on the other hand, the difference is certainly not bounded, since the consecutive integers $n!+m$ with $m = 2, 3, \ldots, n$ are all composite. A famous theorem of Dirichlet asserts that any arithmetical progression $a$, $a+q$, $a+2q, \ldots$, where $(a, q) = 1$, contains infinitely many primes. Some special cases, for instance the existence of infinitely many primes of the form $4n+3$, can be deduced simply by modifying Euclid's argument given at the beginning, but the general result lies quite deep. Indeed Dirichlet's proof involved, amongst other things, the concepts of characters and $L$-functions, and of class numbers of quadratic forms, and it has been of far-reaching significance in the history of mathematics.

Two notorious unsolved problems in prime-number theory are the Goldbach conjecture, mentioned in a letter to Euler of 1742, to the effect that every even integer ($>2$) is the sum of two primes, and the twin-prime conjecture, to the effect that there exist infinitely many pairs of primes, such as 3, 5 and 17, 19, that differ by 2. By ingenious work on sieve methods, Chen showed in 1974 that these conjectures are valid if one of the primes is replaced by a number with at most two prime factors (assuming, in the Goldbach case, that the even integer is sufficiently large). The oldest known sieve, incidentally, is due to Eratosthenes. He observed that if one deletes from the set of integers $2, 3, \ldots, n$, first all multiples of 2, then all multiples of 3, and so on up to the largest integer not exceeding $\sqrt{n}$, then only primes remain. Studies on Goldbach's conjecture gave rise to the Hardy–Littlewood circle method of analysis and, in particular, to the celebrated theorem of Vinogradov to the effect that every sufficiently large odd integer is the sum of three primes.

## 7 Further reading

For a good account of the Peano axioms see E. Landau, *Foundations of analysis* (Chelsea Publ. Co., New York, 1951).

The division algorithm, Euclid's algorithm and the fundamental theorem of arithmetic are discussed in every elementary text on number theory. The tracts are too numerous to list here

but for many years the book by G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford U.P., 5th edn, 1979) has been regarded as a standard work in the field. The books of similar title by T. Nagell (Wiley, New York, 1951) and H. M. Stark (MIT Press, Cambridge, Mass., 1978) are also to be recommended, as well as the volume by E. Landau, *Elementary number theory* (Chelsea Publ. Co., New York, 1958).

For properties of the primes, see the book by Hardy and Wright mentioned above and, for more advanced reading, see, for instance, H. Davenport, *Multiplicative number theory* (Springer-Verlag, Berlin, 2nd ed, 1980) and H. Halberstam and H. E. Richert, *Sieve methods* (Academic Press, London and New York, 1974). The latter contains, in particular, a proof of Chen's theorem. The result referred to on a polynomial in several variables representing primes arose from work of Davis, Robinson, Putnam and Matiyasevich on Hilbert's tenth problem; see, for instance, the article in *American Math. Monthly* **83** (1976), 449–64, where it is shown that 12 variables suffice.

## 8 Exercises

(i) Find integers $x$, $y$ such that $95x+432y=1$.

(ii) Find integers $x$, $y$, $z$ such that $35x+55y+77z=1$.

(iii) Prove that $1+\frac{1}{2}+\cdots+1/n$ is not an integer for $n>1$.

(iv) Prove that
$(\{a, b\}, \{b, c\}, \{c, a\}) = \{(a, b), (b, c), (c, a)\}$.

(v) Prove that if $g_1, g_2, \ldots$ are integers $>1$ then every natural number can be expressed uniquely in the form $a_0+a_1g_1+a_2g_1g_2+\cdots+a_kg_1\cdots g_k$, where the $a_j$ are integers satisfying $0\leq a_j<g_{j+1}$.

(vi) Show that there exist infinitely many primes of the form $4n+3$.

(vii) Show that, if $2^n+1$ is a prime then it is in fact a Fermat prime.

(viii) Show that, if $m>n$, then $2^{2^n}+1$ divides $2^{2^m}-1$ and so $(2^{2^m}+1, 2^{2^n}+1)=1$.

(ix) Deduce that $p_{n+1}\leq 2^{2^n}+1$, whence $\pi(x)\geq \log\log x$ for $x\geq 2$.