Graduate Texts in Mathematics 84

Kenneth Ireland
Michael Rosen

A Classical Introduction to Modern Number Theory

With 1 Illustration

Kenneth Ireland
Michael Rosen

A Classical Introduction to Modern Number Theory

With 1 Illustration

Springer-Verlag
New York Heidelberg Berlin

Kenneth Ireland
Department of Mathematics
University of New Brunswick
Fredericton
New Brunswick E3B 5A3
Canada

Michael Rosen
Department of Mathematics
Brown University
Providence, RI 02906
U.S.A.

AMS Subject Classifications (1980): 10-01, 12-01

Library of Congress Cataloging in Publication Data

Ireland, Kenneth F.
A classical introduction to modern number theory.
(Graduate texts in mathematics; 84)
Bibliography: p.
Includes index.
1. Numbers, Theory of. I. Rosen, Michael I.
II. Title. III. Series.
QA241.I667 512'.7 81-23265
AACR2

"A Classical Introduction to Modern Number Theory" is a revised and expanded version of "Elements of Number Theory" published in 1972 by Bogden and Quigley, Inc. Publishers.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-90625-8 Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90625-8 Springer-Verlag Berlin Heidelberg New York

Preface

This book is a revised and greatly expanded version of our book *Elements of Number Theory* published in 1972. As with the first book the primary audience we envisage consists of upper level undergraduate mathematics majors and graduate students. We have assumed some familiarity with the material in a standard undergraduate course in abstract algebra. A large portion of Chapters 1–11 can be read even without such background with the aid of a small amount of supplementary reading. The later chapters assume some knowledge of Galois theory, and in Chapters 16 and 18 an acquaintance with the theory of complex variables is necessary.

Number theory is an ancient subject and its content is vast. Any introductory book must, of necessity, make a very limited selection from the fascinating array of possible topics. Our focus is on topics which point in the direction of algebraic number theory and arithmetic algebraic geometry. By a careful selection of subject matter we have found it possible to exposit some rather advanced material without requiring very much in the way of technical background. Most of this material is classical in the sense that is was discovered during the nineteenth century and earlier, but it is also modern because it is intimately related to important research going on at the present time.

In Chapters 1–5 we discuss prime numbers, unique factorization, arithmetic functions, congruences, and the law of quadratic reciprocity. Very little is demanded in the way of background. Nevertheless it is remarkable how a modicum of group and ring theory introduces unexpected order into the subject. For example, many scattered results turn out to be parts of the answer to a natural question: What is the structure of the group of units in the ring $\mathbb{Z}/n\mathbb{Z}$?

Reciprocity laws constitute a major theme in the later chapters. The law of quadratic reciprocity, beautiful in itself, is the first of a series of reciprocity laws which lead ultimately to the Artin reciprocity law, one of the major achievements of algebraic number theory. We travel along the road beyond quadratic reciprocity by formulating and proving the laws of cubic and biquadratic reciprocity. In preparation for this many of the techniques of algebraic number theory are introduced; algebraic numbers and algebraic integers, finite fields, splitting of primes, etc. Another important tool in this investigation (and in others!) is the theory of Gauss and Jacobi sums. This material is covered in Chapters 6–9. Later in the book we formulate and prove the more advanced partial generalization of these results, the Eisenstein reciprocity law.

A second major theme is that of diophantine equations, at first over finite fields and later over the rational numbers. The discussion of polynomial equations over finite fields is begun in Chapters 8 and 10 and culminates in Chapter 11 with an exposition of a portion of the paper "Number of solutions of equations over finite fields" by A. Weil. This paper, published in 1948, has been very influential in the recent development of both algebraic geometry and number theory. In Chapters 17 and 18 we consider diophantine equations over the rational numbers. Chapter 17 covers many standard topics from sums of squares to Fermat's Last Theorem. However, because of material developed earlier we are able to treat a number of these topics from a novel point of view. Chapter 18 is about the arithmetic of elliptic curves. It differs from the earlier chapters in that it is primarily an overview with many definitions and statements of results but few proofs. Nevertheless, by concentrating on some important special cases we hope to convey to the reader something of the beauty of the accomplishments in this area where much work is being done and many mysteries remain.

The third, and final, major theme is that of zeta functions. In Chapter 11 we discuss the congruence zeta function associated to varieties defined over finite fields. In Chapter 16 we discuss the Riemann zeta function and the Dirichlet L-functions. In Chapter 18 we discuss the zeta function associated to an algebraic curve defined over the rational numbers and Hecke L-functions. Zeta functions compress a large amount of arithmetic information into a single function and make possible the application of the powerful methods of analysis to number theory.

Throughout the book we place considerable emphasis on the history of our subject. In the notes at the end of each chapter we give a brief historical sketch and provide references to the literature. The bibliography is extensive containing many items both classical and modern. Our aim has been to provide the reader with a wealth of material for further study.

There are many exercises, some routine, some challenging. Some of the exercises supplement the text by providing a step by step guide through the proofs of important results. In the later chapters a number of exercises have been adapted from results which have appeared in the recent literature. We

hope that working through the exercises will be a source of enjoyment as well as instruction.

In the writing of this book we have been helped immensely by the interest and assistance of many mathematical friends and acquaintances. We thank them all. In particular we would like to thank Henry Pohlmann who insisted we follow certain themes to their logical conclusion, David Goss for allowing us to incorporate some of his work into Chapter 16, and Oisin McGuiness for his invaluable assistance in the preparation of Chapter 18. We would like to thank Dale Cavanaugh, Janice Phillips, and especially Carol Ferreira, for their patience and expertise in typing large portions of the manuscript. Finally, the second author wishes to express his gratitude to the Vaughn Foundation Fund for financial support during his sabbatical year in Berkeley, California (1979/80).

July 25, 1981

Kenneth Ireland
Michael Rosen

Contents

Chapter 1

Unique Factorization

The notion of prime number is fundamental in number theory. The first part of this chapter is devoted to proving that every integer can be written as a product of primes in an essentially unique way.

After that, we shall prove an analogous theorem in the ring of polynomials over a field.

On a more abstract plane, the general idea of unique factorization is treated for principal ideal domains.

Finally, returning from the abstract to the concrete, the general theory is applied to two special rings that will be important later in the book.

§1 Unique Factorization in $\mathbb{Z}$

As a first approximation, number theory may be defined as the study of the natural numbers 1, 2, 3, 4, ... L. Kronecker once remarked (speaking of mathematics generally) that God made the natural numbers and all the rest is the work of man. Although the natural numbers constitute, in some sense, the most elementary mathematical system, the study of their properties has provided generations of mathematicians with problems of unending fascination.

We say that a number a divides a number b if there is a number c such that $b = ac$. If a divides b, we use the notation $a|b$. For example, $2|8$, $3|15$, but $6 \nmid 21$. If we are given a number, it is tempting to factor it again and again until further factorization is impossible. For example, $180 = 18 \times 10 = 2 \times 9 \times 2 \times 5 = 2 \times 3 \times 3 \times 2 \times 5$. Numbers that cannot be factored further are called primes. To be more precise, we say that a number p is a prime if its only divisors are 1 and p. Prime numbers are very important because every number can be written as a product of primes. Moreover, primes are of great interest because there are many problems about them that are easy to state but very hard to prove. Indeed many old problems about primes are unsolved to this day.

The first prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ... One may ask if there are infinitely many prime numbers. The answer is yes. Euclid gave an elegant proof of this fact over 2000 years ago. We shall give his proof and several others in Chapter 2. One can ask other questions

of this nature. Let $\pi(x)$ be the number of primes between 1 and x. What can be said about the function $\pi(x)$? Several mathematicians found by experiment that for large x the function $\pi(x)$ was approximately equal to $x/\ln(x)$. This assertion, known as the prime number theorem, was proved toward the end of the nineteenth century by J. Hadamard and independently by Ch.-J. de la Vallé Poussin. More precisely, they proved

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Even from a small list of primes one can notice that they have a tendency to occur in pairs, for example, 3 and 5, 5 and 7, 11 and 13, 17 and 19. Do there exist infinitely many prime pairs? The answer is unknown.

Another famous unsolved problem is known as the Goldbach conjecture (C. H. Goldbach). Can every even number be written as the sum of two primes? Goldbach came to this conjecture experimentally. Nowadays electronic computers make it possible to experiment with very large numbers. No counterexample to Goldbach's conjecture has ever been found. Great progress toward a proof has been given by I. M. Vinogradov and L. Schnirelmann. In 1937 Vinogradov was able to show that every sufficiently large odd number is the sum of three odd primes.

In this book we shall not study in depth the distribution of prime numbers or "additive" problems about them (such as the Goldbach conjecture). Rather our concern will be about the way primes enter into the multiplicative structure of numbers. The main theorem along these lines goes back essentially to Euclid. It is the theorem of unique factorization. This theorem is sometimes referred to as the fundamental theorem of arithmetic. It deserves the title. In one way or another almost all the results we shall discuss depend on it. The theorem states that every number can be factored into a product of primes in a unique way. What uniqueness means will be explained below.

As an illustration consider the number 180. We have seen that $180 = 2 \times 2 \times 3 \times 3 \times 5 = 2^2 \times 3^2 \times 5$. Uniqueness in this case means that the only primes dividing 180 are 2, 3, and 5 and that the exponents 2, 2, and 1 are uniquely determined by 180.

$\mathbb{Z}$ will denote the ring of integers, i.e., the set $0, \pm 1, \pm 2, \pm 3, \ldots$, together with the usual definition of sum and product. It will be more convenient to work with $\mathbb{Z}$ rather than restricting ourselves to the positive integers. The notion of divisibility carries over with no difficulty to $\mathbb{Z}$. If p is a positive prime, $-p$ will also be a prime. We shall not consider 1 or -1 as primes even though they fit the definition. This is simply a useful convention. Note that 1 and -1 divide everything and that they are the only integers with this property. They are called the units of $\mathbb{Z}$. Notice also that every nonzero integer divides zero. As is usual we shall exclude division by zero.

There are a number of simple properties of division that we shall simply list. The reader may wish to supply the proofs.

(1) $a|a$, $a \neq 0$.
(2) If $a|b$ and $b|a$, then $a = \pm b$.
(3) If $a|b$ and $b|c$, then $a|c$.
(4) If $a|b$ and $a|c$, then $a|b + c$.

Let $n \in \mathbb{Z}$ and let p be a prime. Then if n is not zero, there is a nonnegative integer a such that $p^a|n$ but $p^{a+1} \nmid n$. This is easy to see if both p and n are positive for then the powers of p get larger and larger and eventually exceed n. The other cases are easily reduced to this one. The number a is called the order of n at p and is denoted by $\text{ord}_p n$. Roughly speaking $\text{ord}_p n$ is the number of times p divides n. If $n = 0$, we set $\text{ord}_p 0 = \infty$. Notice that $\text{ord}_p n = 0$ if and only if (iff) $p \nmid n$.

Lemma 1. *Every nonzero integer can be written as a product of primes.*

PROOF. Assume that there is an integer that cannot be written as a product of primes. Let N be the smallest positive integer with this property. Since N cannot itself be prime we must have $N = mn$, where $1 < m, n < N$. However, since m and n are positive and smaller than N they must each be a product of primes. But then so is $N = mn$. This is a contradiction.

The proof can be given in a more positive way by using mathematical induction. It is enough to prove the result for all positive integers. 2 is a prime. Suppose that $2 < N$ and that we have proved the result for all numbers m such that $2 \leq m < N$. We wish to show that N is a product of primes. If N is a prime, there is nothing to do. If N is not a prime, then $N = mn$, where $2 \leq m, n < N$. By induction both m and n are products of primes and thus so is N. □

By collecting terms we can write $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$, where the p_i are primes and the a_i are nonnegative integers. We shall use the following notation:

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)},$$

where $\varepsilon(n) = 0$ or 1 depending on whether n is positive or negative and where the product is over all positive primes. The exponents $a(p)$ are nonnegative integers and, of course, $a(p) = 0$ for all but finitely many primes. For example, if $n = 180$, we have $\varepsilon(n) = 0, a(2) = 2, a(3) = 2$, and $a(5) = 1$, and all other $a(p) = 0$.

We can now state the main theorem.

Theorem 1. *For every nonzero integer n there is a prime factorization*

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)},$$

with the exponents uniquely determined by n. In fact, we have $a(p) = \text{ord}_p n$.

The proof of this theorem is not as easy as it may seem. We shall postpone the proof until we have established a few preliminary results.

Lemma 2. *If $a, b \in \mathbb{Z}$ and $b > 0$, there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < b$.*

PROOF. Consider the set of all integers of the form $a - xb$ with $x \in \mathbb{Z}$. This set includes positive elements. Let $r = a - qb$ be the least nonnegative element in this set. We claim that $0 \leq r < b$. If not, $r = a - qb \geq b$ and so $0 \leq a - (q + 1)b < r$, which contradicts the minimality of r. □

Definition. If $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, we define $(a_1, a_2, \ldots, a_n)$ to be the set of all integers of the form $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ with $x_1, x_2, \ldots, x_n \in \mathbb{Z}$.

Let $A = (a_1, a_2, \ldots, a_n)$. Notice that the sum and difference of two elements in A are again in A. Also, if $a \in A$ and $r \in \mathbb{Z}$, then $ra \in A$. In ring-theoretic language, A is an *ideal* in the ring $\mathbb{Z}$.

Lemma 3. *If $a, b \in \mathbb{Z}$, then there is a $d \in \mathbb{Z}$ such that $(a, b) = (d)$.*

PROOF. We may assume that not both a and b are zero so that there are positive elements in (a, b). Let d be the smallest positive element in (a, b). Clearly $(d) \subseteq (a, b)$. We shall show that the reverse inclusion also holds.

Suppose that $c \in (a, b)$. By Lemma 2 there exist integers q and r such that $c = qd + r$ with $0 \leq r < d$. Since both c and d are in (a, b) it follows that $r = c - qd$ is also in (a, b). Since $0 \leq r < d$ we must have $r = 0$. Thus $c = qd \in (d)$. □

Definition. Let $a, b \in \mathbb{Z}$. An integer d is called a *greatest common divisor* of a and b if d is a divisor of both a and b and if every other common divisor of a and b divides d.

Notice that if c is another greatest common divisor of a and b, then we must have $c \mid d$ and $d \mid c$ and so $c = \pm d$. Thus the greatest common divisor of two numbers, if it exists, is determined up to sign.

As an example, one may check that 14 is a greatest common divisor of 42 and 196. The following lemma will establish the existence of the greatest common divisor, but it will not give a method for computing it. In the Exercises we shall outline an efficient method of computation known as the Euclidean algorithm.

Lemma 4. *Let $a, b \in \mathbb{Z}$. If $(a, b) = (d)$ then d is a greatest common divisor of a and b.*

PROOF. Since $a \in (d)$ and $b \in (d)$ we see that d is a common divisor of a and b. Suppose that c is a common divisor. Then c divides every number of the form $ax + by$. In particular $c \mid d$. □

Definition. We say that two integers a and b are *relatively prime* if the only common divisors are ± 1, the units.

It is fairly standard to use the notation (a, b) for the greatest common divisor of a and b. The way we have defined things, (a, b) is a set. However, since $(a, b) = (d)$ and d is a greatest common divisor (if we require d to be positive, we may use the article *the*) it will not be too confusing to use the symbol (a, b) for both meanings. With this convention we can say that a and b are relatively prime if $(a, b) = 1$.

Proposition 1.1.1. *Suppose that $a|bc$ and that $(a, b) = 1$. Then $a|c$.*

PROOF. Since $(a, b) = 1$ there exist integers r and s such that $ra + sb = 1$. Therefore, $rac + sbc = c$. Since a divides the left-hand side of this equation we have $a|c$. □

This proposition is false if $(a, b) \neq 1$. For example, $6|24$ but $6 \nmid 3$ and $6 \nmid 8$.

Corollary 1. *If p is a prime and $p|bc$, then either $p|b$ or $p|c$.*

PROOF. The only divisors of p are ± 1 and $\pm p$. Thus $(p, b) = 1$ or p; i.e., either $p|b$ or p and b are relatively prime. If $p|b$, we are done. If not, $(p, b) = 1$ and so, by the proposition, $p|c$. □

We can state the corollary in a slightly different form that is often useful: If p is a prime and $p \nmid b$ and $p \nmid c$, then $p \nmid bc$.

Corollary 2. *Suppose that p is a prime and that $a, b \in \mathbb{Z}$. Then* $\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b$.

PROOF. Let $\alpha = \operatorname{ord}_p a$ and $\beta = \operatorname{ord}_p b$. Then $a = p^\alpha c$ and $b = p^\beta d$, where $p \nmid c$ and $p \nmid d$. Then $ab = p^{\alpha+\beta} cd$ and by Corollary 1 $p \nmid cd$. Thus $\operatorname{ord}_p ab = \alpha + \beta = \operatorname{ord}_p a + \operatorname{ord}_p b$. □

We are now in a position to prove the main theorem.

Apply the function ord_q to both sides of the equation

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)}$$

and use the property of ord_q given by Corollary 2. The result is

$$\operatorname{ord}_q n = \varepsilon(n) \operatorname{ord}_q(-1) + \sum_p a(p) \operatorname{ord}_q(p).$$

Now, from the definition of ord_q we have $\operatorname{ord}_q(-1) = 0$ and $\operatorname{ord}_q(p) = 0$ if $p \neq q$ and 1 if $p = q$. Thus the right-hand side collapses to the single term $a(q)$, i.e., $\operatorname{ord}_q n = a(q)$, which is what we wanted to prove.

It is to be emphasized that the key step in the proof is Corollary 1 : namely, if $p|ab$, then $p|a$ or $p|b$. Whatever difficulty there is in the proof is centered about this fact.

§2 Unique Factorization in $k[x]$

The theorem of unique factorization can be formulated and proved in more general contexts than that of Section 1. In this section we shall consider the ring $k[x]$ of polynomials with coefficients in a field k. In Section 3 we shall consider principal ideal domains. It will turn out that the analysis of these situations will prove useful in the study of the integers.

If $f, g \in k[x]$, we say that f divides g if there is an $h \in k[x]$ such that $g = fh$.

If $\deg f$ denotes the degree of f, we have $\deg fg = \deg f + \deg g$. Also, remember that $\deg f = 0$ iff f is a nonzero constant. It follows that $f|g$ and $g|f$ iff $f = cg$, where c is a nonzero constant. It also follows that the only polynomials that divide all the others are the nonzero constants. These are the units of $k[x]$. A nonconstant polynomial p is said to be irreducible if $q|p$ implies that q is either a constant or a constant times p. Irreducible polynomials are the analog of prime numbers.

Lemma 1. *Every nonconstant polynomial is the product of irreducible polynomials.*

PROOF. The proof is by induction on the degree. It is easy to see that polynomials of degree 1 are irreducible. Assume that we have proved the result for all polynomials of degree less than n and that $\deg f = n$. If f is irreducible, we are done. Otherwise $f = gh$, where $1 \leq \deg g, \deg h < n$. By the induction assumption both g and h are products of irreducible polynomials. Thus so is $f = gh$. □

It is convenient to define *monic polynomial*. A polynomial f is called monic if its leading coefficient is 1. For example, $x^2 + x - 3$ and $x^3 - x^2 + 3x + 17$ are monic but $2x^3 - 5$ and $3x^4 + 2x^2 - 1$ are not. Every polynomial (except zero) is a constant times a monic polynomial.

Let p be a monic irreducible polynomial. We define $\operatorname{ord}_p f$ to be the integer a defined by the property that $p^a|f$ but that $p^{a+1} \nmid f$. Such an integer must exist since the degree of the powers of p gets larger and larger. Notice that $\operatorname{ord}_p f = 0$ iff $p \nmid f$.

Theorem 2. *Let $f \in k[x]$. Then we can write*

$$f = c \prod_p p^{a(p)},$$