


9

ADVANCED NUMBER THEORY

Harvey Cohn



ADVANCED NUMBER THEORY

Harvey Cohn

Distinguished Professor of Mathematics
City University of New York

Dover Publications, Inc.
New York

Copyright © 1962 by Harvey Cohn.
All rights reserved under Pan American and International Copyright Conventions.

Published in Canada by General Publishing Company, Ltd., 30 Lesmill Road, Don Mills, Toronto, Ontario.

Published in the United Kingdom by Constable and Company, Ltd., 10 Orange Street, London WC2H 7EG.

This Dover edition, first published in 1980, is an unabridged and corrected republication of the work first published in 1962 by John Wiley & Sons, Inc., under the title *A Second Course in Number Theory*.

International Standard Book Number: 0-486-64023-X
Library of Congress Catalog Card Number: 80-65862

Manufactured in the United States of America
Dover Publications, Inc.
180 Varick Street
New York, N.Y. 10014

PREFACE

The prerequisites for this book are the "standard" first-semester course in number theory (with incidental elementary algebra) and elementary calculus. There is no lack of suitable texts for these prerequisites (for example, *An Introduction to the Theory of Numbers*, by I. Niven and H. S. Zuckerman, John Wiley and Sons, 1960, can be cited as a book that introduces the necessary algebra as part of number theory). Usually, very little else can be managed in that first semester beyond the transition from improvised combinatorial amusements of antiquity to the coherently organized background for quadratic reciprocity, which was achieved in the eighteenth century.

The present text constitutes slightly more than enough for a second-semester course, carrying the student on to the twentieth century by motivating some heroic nineteenth-century developments in algebra and analysis. The relation of this textbook to the great treatises will necessarily be like that of a historical novel to chronicles. We hope that once the student knows what to seek he will find "chronicles" to be as exciting as a "historical novel."

The problems in the text play a significant role and are intended to stimulate the spirit of experimentation which has traditionally ruled number theory and which has indeed become resurgent with the realization of the modern computer. A student completing this course should acquire an appreciation for the historical origins of linear algebra, for the zeta-function tradition, for ideal class structure, and for genus theory. These

ideas, although relatively old, still make their influence felt on the frontiers of modern mathematics. Fermat's last theorem and complex multiplication are unfortunate omissions, but the motive was not to depress the degree of difficulty so much as it was to make the most efficient usage of one semester.

My acknowledgments are many and are difficult to list. I enjoyed the benefits of courses under Bennington P. Gill at City College and Saunders MacLane at Harvard. The book profited directly from suggestions by my students and from the incidental advice of many readers, particularly Burton W. Jones and Louis J. Mordell. I owe a special debt to Herbert S. Zuckerman for a careful reading, to Gordon Pall for major improvements, and to the staff of John Wiley and Sons for their cooperation.

HARVEY COHN

Tucson, Arizona
October 1961

The preface for this book is the "standard" preface for a course in number theory (with incidental elementary algebra and elementary calculus). There is no lack of suitable texts for these prerequisites (for example, an introduction to the theory of numbers by I. M. Gelfand and H. S. Zuckerman, John Wiley and Sons, 1960) and can be cited as a book that introduces the necessary algebra as part of number theory. Usually, very little else can be merged in that first semester beyond the treatment from introductory combinatorial arguments of analogy to the recently organized background for quadratic reciprocity, which was achieved in the twentieth century.

The present text constitutes a first step toward a second semester course, roughly dependent on the twentieth century by involving some basic modern developments in algebra and number theory. The selection of the subject and great teacher will necessarily be the first of a historical novel. We hope that once the student knows what to look for in the "historical" to be as exciting as a "historical novel."

The program in the text gives a significant role and are intended to stimulate the spirit of experimentation which has traditionally ruled number theory and which has been more recently with the realization of the modern computer. A book of computer programs should acquire an appreciation for the historical nature of modern number theory for the relation between the ideal case structure and the theory. These

CONTENTS

Note: The sections marked with * or ** might be omitted in class use if there is a lack of time. (Here the ** sections are considered more truly optional.)

INTRODUCTORY SURVEY	1
Diophantine Equations 1	
Motivating Problem in Quadratic Forms 2	
Use of Algebraic Numbers 5	
Primes in Arithmetic Progression 6	
PART 1. BACKGROUND MATERIAL	
1. Review of Elementary Number Theory and Group Theory	9
Number Theoretic Concepts	9
1. Congruence 9	
2. Unique factorization 10	
3. The Chinese remainder theorem 11	
4. Structure of reduced residue classes 12	
5. Residue classes for prime powers 13	
Group Theoretic Concepts	15
6. Abelian groups and subgroups 15	
7. Decomposition into cyclic groups 16	
Quadratic Congruences	18
8. Quadratic residues 18	
9. Jacobi symbol 20	

*2. Characters	22
1. Definitions	22
2. Total number of characters	24
3. Residue classes	27
4. Resolution modulus	28
5. Quadratic residue characters	32
6. Kronecker's symbol and Hasse's congruence	35
7. Dirichlet's lemma on real characters	36
3. Some Algebraic Concepts	39
1. Representation by quadratic forms	39
2. Use of surds	40
3. Modules	41
4. Quadratic integers	42
5. Hilbert's example	43
6. Fields	44
7. Basis of quadratic integers	45
8. Integral domain	47
9. Basis of σ_n	48
**10. Fields of arbitrary degree	49
4. Basis Theorems	54
1. Introduction of n dimensions	54
2. Dirichlet's boxing-in principle	54
3. Lattices	55
4. Graphic representation	57
5. Theorem on existence of basis	58
6. Other interpretations of the basis construction	63
7. Lattices of rational integers, canonical basis	65
8. Sublattices and index concept	68
9. Application to modules of quadratic integers	70
10. Discriminant of a quadratic field	72
**11. Fields of higher degree	73
**5. Further Applications of Basis Theorems	75
Structure of Finite Abelian Groups	75
1. Lattice of group relations	75
2. Need for diagonal basis	76
3. Elementary divisor theory	77
4. Basis theorem for abelian groups	81
5. Simplification of result	82
Geometric Remarks on Quadratic Forms	83
6. Successive minima	83
7. Binary forms	86
8. Korkine and Zolotareff's example	88

PART 2. IDEAL THEORY IN QUADRATIC FIELDS

- 6. Unique Factorization and Units 93**
1. The "missing" factors 93
 2. Indecomposable integers, units, and primes 94
 3. Existence of units in a quadratic field 95
 4. Fundamental units 98
 5. Construction of a fundamental unit 100
 6. Failure of unique factorization into indecomposable integers 102
 - *7. Euclidean algorithm 104
 - *8. Occurrence of the Euclidean algorithm 105
 - *9. Pell's equation 110
 - **10. Fields of higher degree 111
- 7. Unique Factorization into Ideals 113**
1. Set theoretical notation 113
 2. Definition of ideals 114
 3. Principal ideals 116
 4. Sum of ideals, basis 117
 5. Rules for transforming the ideal basis 119
 6. Product of ideals, the critical theorem, cancellation 120
 7. "To contain is to divide" 122
 8. Unique factorization 123
 9. Sum and product of factored ideals 124
 10. Two element basis, prime ideals 125
 11. The critical theorem and Hurwitz's lemma 128
- 8. Norms and Ideal Classes 131**
1. Multiplicative property of norms 131
 2. Class structure 134
 3. Minkowski's theorem 136
 4. Norm estimate 139
- 9. Class Structure in Quadratic Fields 142**
1. The residue character theorem 142
 2. Primary numbers 145
 3. Determination of principal ideals with given norms 147
 4. Determination of equivalence classes 148
 5. Some imaginary fields 149
 6. Class number unity 151
 7. Units and class calculation of real quadratic fields 151
 - *8. The famous polynomials $x^2 + x + q$ 155

PART 3. APPLICATIONS OF IDEAL THEORY

*10. Class Number Formulas and Primes in Arithmetic Progression	159
1. Introduction of analysis into number theory	159
2. Lattice points in ellipse	160
3. Ideal density in complex fields	161
4. Ideal density in real fields	163
5. Infinite series, the zeta-function	166
6. Euler factorization	167
7. The zeta-function and L -series for a field	169
8. Connection with ideal classes	170
9. Some simple class numbers	173
10. Dirichlet L -series and primes in arithmetic progression	174
11. Behavior of the L -series, conclusion of proof	176
**12. Weber's theorem on primes in ideal classes	179
11. Quadratic Reciprocity	183
1. Rational use of class numbers	183
2. Results on units	184
3. Results on class structure	187
4. Quadratic reciprocity preliminaries	190
5. The main theorem	192
6. Kronecker's symbol reappraised	193
12. Quadratic Forms and Ideals	195
1. The problem of distinguishing between conjugates	195
2. The ordered bases of an ideal	196
3. Strictly equivalent ideals	197
4. Equivalence classes of quadratic forms	198
5. The correspondence procedure	200
6. The correspondence theorem	204
7. Complete set of classes of quadratic forms	207
8. Some typical representation problems	209
**13. Compositions, Orders, and Genera	212
1. Composition of forms	212
2. Orders, ideals, and forms	216
3. Genus theory of forms	221
4. Hilbert's description of genera	228
*CONCLUDING SURVEY	231
Cyclotomic Fields and Gaussian Sums	232
Class Fields	234
Global and Local Viewpoints	238

Bibliography and Comments	243
Some Classics Prior to 1900	243
Some Recent Books (After 1900)	244
Special References by Chapter	245
Appendix Tables	247
I. Minimum Prime Divisors of Numbers Not Divisible by 2, 3, or 5 from 1 to 18,000	247
II. Power Residues for Primes Less than 100	255
III. Class Structures of Quadratic Fields of \sqrt{m} for m Less than 100	261
Index	275

INTRODUCTORY SURVEY

DIOPHANTINE EQUATIONS

The most generally enduring problem of number theory is probably that of diophantine equations. Greek mathematicians were quite adept at solving in integers x and y the equation

$$ax + by = c,$$

where a , b , and c are any given integers. The close relation with the greatest common divisor algorithm indicated the necessity of treating *unique factorization* as a primary tool in the solution of diophantine equations.

The Greek mathematicians gave some sporadic attention to forms of the more general equation

$$(1) \quad f(x, y) = Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0,$$

but achieved no sweeping results. They probably did not know that every equation of this kind can be solved "completely" by characterizing all solutions in a finite number of steps, although they had success with special cases such as $x^2 - 3y^2 = 1$. In fact, they used continued fraction techniques in both linear and quadratic problems, indicating at least esthetically a sense of unity. About 1750 Euler and his contemporaries became aware

This section presupposes some familiarity with elementary concepts of group, congruence, Euclidean algorithm, and quadratic reciprocity (which are reviewed in Chapter I).

2 INTRODUCTORY SURVEY

of the systematic solvability in a finite number of steps. Yet it was not until 1800 that Gauss gave in his famous *Disquisitiones Arithmeticae* the solution that still remains a model of perfection.

Now a very intimate connection developed between Gauss's solution and *quadratic reciprocity*, making unique factorization (in the linear case) and quadratic reciprocity (in the quadratic case) parallel tools. Finally, about 1896, Hilbert achieved the reorganization of the quadratic theory, making full use of this coincidence and thus completing the picture.

MOTIVATING PROBLEM IN QUADRATIC FORMS

The first step in a general theory of quadratic diophantine equations was probably the famous theorem of Fermat (1640) relating to a (homogeneous) quadratic form in x, y .

A prime number p is representable in an essentially unique manner by the form $x^2 + y^2$ for integral x and y if and only if $p \equiv 1$ modulo 4 (or $p = 2$).

It is easily verified that $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, $29 = 5^2 + 2^2$, etc., whereas the primes 3, 7, 11, 19, etc., have no such representation. The proof of Fermat's theorem is far from simple and is achieved later on as part of a larger result.

At the same time, Fermat used an identity from antiquity:

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' - yy')^2 + (xy' + x'y)^2,$$

easily verifiable, since both sides equal $x^2x'^2 + y^2y'^2 + x'^2y^2 + x^2y'^2$. He used this formula to build up solutions to the equation

$$(2) \quad x^2 + y^2 = m$$

for values of m which are not necessarily prime. For example, from the results

$$3^2 + 2^2 = 13, \quad (x = 3, y = 2),$$

$$2^2 + 1^2 = 5, \quad (x' = 2, y' = 1),$$

we obtain

$$7^2 + 4^2 = 65, \quad (xx' - yy' = 4, xy' + x'y = 7).$$

If we interpret the representation for 13 as

$$(-3)^2 + 2^2 = 13 \quad (x = -3, y = 2),$$

whereas

$$2^2 + 1^2 = 5, \quad (x' = 2, y' = 1),$$

then we obtain

$$(-8)^2 + 1^2 = 65, \quad (xx' - yy' = -8, xy' + x'y = 1);$$

but the reader can verify that $65 = 7^2 + 4^2 = 8^2 + 1^2$ are the only representations obtainable for 65 in the form $x^2 + y^2$, to within rearrangements of summands or changes of sign. If we allow the trivial additional operation of using (x, y) , which are not relatively prime ($(kx)^2 + (ky)^2 = k^2m$), we can build up all solutions to (2), from those for prime m .

Thus Fermat's result, stated more compactly, is the following:

$$\text{Let} \quad Q(x, y) = x^2 + y^2.$$

Then all relatively prime solutions (x, y) to the problem of representing

$$Q(x, y) = m$$

for m any integer are achieved by means of the successive application of two results called *genus and composition theorems*.

GENUS THEOREM

$$(3) \quad Q(x, y) = p$$

can be solved in integral x, y for p a prime if and only if $p \equiv 1 \pmod{4}$, or $p = 2$. The representation is unique, except for obvious changes of sign or rearrangements of x and y .

COMPOSITION THEOREM

$$(4) \quad Q(x, y) Q(x', y') = Q(xx' - yy', x'y + xy').$$

In the intervening years until about 1800, Euler, Lagrange, Legendre, and others invented analogous results for a variety of quadratic forms. Gauss (1800) was the first one to see the larger problem and to achieve a complete generalization of the genus and composition theorems. The main result is too involved even to state here, but a slightly more difficult special result will give the reader an idea of what to expect. (See Chapter XIII.)

$$\text{Let} \quad Q_1(x, y) = x^2 + 5y^2,$$

$$Q_2(x, y) = 2x^2 + 2xy + 3y^2.$$

Then all relatively prime solutions (x, y) to the problem of representing

$$Q_1(x, y) = m$$

or

$$Q_2(x, y) = m$$

4 INTRODUCTORY SURVEY

for m any integer are achieved by means of the successive application of the following two results.

GENUS THEOREM

$$(5) \quad \begin{bmatrix} Q_1(x, y) \\ Q_2(x, y) \end{bmatrix} = p, \text{ a prime, if and only if } p \equiv \begin{pmatrix} 1, 9 \\ 3, 7 \end{pmatrix} \pmod{20},$$

in an essentially unique fashion. (The only special exceptions are, $Q_1(0, 1) = 5$, $Q_2(1, 0) = 2$.)

COMPOSITION THEOREM

$$(6a) \quad \begin{cases} Q_1(x, y) Q_1(x', y') = Q_1(xx' - 5yy', x'y + xy') \\ Q_1(x, y) Q_2(x', y') = Q_2(xx' - x'y - 3yy', xy' + 2x'y + yy') \\ Q_2(x, y) Q_2(x', y') = Q_1(2xx' + xy' + x'y - 2yy', xy' + x'y + yy'). \end{cases}$$

One may protest (in vain) that he is interested only in $Q_1(x, y)$, but it is impossible to separate $Q_1(x, y)$ and $Q_2(x, y)$ in the composition process. For instance,

$$Q_2(1, 1) = 7, \quad (x = 1, y = 1),$$

$$Q_2(0, 1) = 3, \quad (x' = 0, y' = 1),$$

and, from the last of the composition formulas,

$$Q_1(-1, 2) = 21, \quad (2xx' + xy' + x'y - 2yy' = -1, xy' + x'y + yy' = 2).$$

Thus, to represent 21 by Q_1 , we are forced to consider possible representations of factors of 21 by Q_2 . The reader may find the following exercise instructive along these lines:

Find a solution to $Q_1(x, y) = 29$ by trial and error and build from the preceding results solutions to $Q_1(x, y) = 841$ and $Q_2(x, y) = 203$.

Those readers who are familiar with the concept of a group will recognize system (6a) symbolically as

$$(6b) \quad \begin{cases} Q_1^2 = Q_1 \text{ (identity),} \\ Q_1 Q_2 = Q_2, \\ Q_2^2 = Q_1. \end{cases}$$

In this manner we are led from quadratic forms into algebra!

USE OF ALGEBRAIC NUMBERS

The reader will probably note that the decomposition theorem resembles the method of multiplication of complex numbers:

$$(7a) \quad (x + iy)(x' + iy') = (xx' - yy') + i(xy' + yx'),$$

where, of course, $i = \sqrt{-1}$. The composition theorems for $Q_1(x, y)$ and $Q_2(x, y)$ can be similarly explained by use of $\sqrt{-5}$ if we solve for x'' and y'' in each of the following equations:

$$(7b) \quad \begin{cases} (x + \sqrt{-5}y)(x' + \sqrt{-5}y') = (x'' + \sqrt{-5}y''), \\ (x + \sqrt{-5}y)(2x' + y' + \sqrt{-5}y') = (2x'' + y'' + \sqrt{-5}y''), \\ (2x + y + \sqrt{-5}y)(2x' + y' + \sqrt{-5}y') = 2(x'' + \sqrt{-5}y''), \end{cases}$$

but we shall defer all details to Chapter XIII.

The important point, historically, is that before the time of Gauss mathematicians strongly feared the possibility of developing a contradiction if reliance was placed on such numbers as $\sqrt{-1}$, $\sqrt{-5}$, and they would use these numbers "experimentally," although their final proofs were couched in the immaculate language of traditional integral arithmetic; yet eventually they had to accept radicals as a necessary simplifying device.

A second guiding influence in the introduction of radicals was the famous conjecture known as *Fermat's last theorem*:

If n is an integer ≥ 3 , the equation

$$x^n + y^n = z^n$$

has no solution in integers (x, y, z) , except for the trivial case in which $xyz = 0$. The result is still not proved for all n , nor is it contradicted. Here Cauchy, Kummer, and others achieved, for special n , remarkable results by factoring the left-hand side. We shall ignore this very important development in order to unify the material, but we cannot fail to see its relevance (say) for $n = 3$, if we write

$$\begin{aligned} x^3 + y^3 &= (x + y)(y + \rho y)(x + \rho^2 y), \\ \rho &= (-1 + \sqrt{-3})/2, \quad \rho^2 = (-1 - \sqrt{-3})/2. \end{aligned}$$

The introduction of such numbers as ρ , $\sqrt{-1}$, $\sqrt{-5}$ resulted in a further development by Dedekind (1870) of a systematic theory of algebraic numbers. These are quantities α defined by equations, for instance, of degree k ,

$$A_0\alpha^k + A_1\alpha^{k-1} + \cdots + A_k = 0$$

with integral coefficients. It turned out that quadratic surds ($k = 2$) were an extremely significant special case whose properties to this very day are not fully generalized to $k > 2$. Thus the importance of this special (quadratic) case cannot be overestimated in the theory of algebraic numbers of arbitrary degree k .

In this book we try to get the best of both worlds: we use quadratic forms with *integral* coefficients or factor the forms (using *algebraic* number theory), depending on which is more convenient.

PRIMES IN ARITHMETIC PROGRESSION

If we examine $Q_1(x, y)$ and $Q_2(x, y)$ more carefully, we find that in both cases the discriminant is -20 , (the discriminant is the usual value, $d = B^2 - 4AC$ for the form $Ax^2 + Bxy + Cy^2$). Actually, the number of forms required for a complete composition theorem associated with a discriminant is (essentially) a very important integer called the *class number*, written $h(d)$. Thus, referring to $Q(x, y)$, we find $h(-4) = 1$; and referring to $Q_1(x, y)$, $Q_2(x, y)$, we find $h(-20) = 2$. The value of the class number is one of the most *irregular* functions in number theory. Gauss (1800) and Dirichlet (1840), however, did obtain "exact" formulas for the class number. They used continuous variables and the limiting processes of calculus, or the tools of analysis.

One of the most startling results in number theory developed when Dirichlet used this class-number formula to show the following result:

There is an infinitude of primes in any arithmetic progression

$a, a + d, a + 2d, a + 3d, \dots,$
provided $(a, d) = 1$, and $d > 0$.

The fact that *quadratic* forms had originally provided the clue to a problem involving the *linear* form $a + xd$ has not been completely assimilated even today. Despite the occurrence of "direct" demonstrations of the result of Dirichlet, the importance of the original ideas is manifest in the wealth of unsolved related problems in algebraic number theory.

We are thus concerned with the remarkable interrelation between the theory of integers and analysis. The role of number theory as a fountain-head of algebra and analysis is the central idea of this book.

PART 1

BACKGROUND MATERIAL