

Erich Hecke

Lectures on the Theory of Algebraic Numbers

Erich Hecke

Lectures on the Theory of Algebraic Numbers

**Translated by George U. Brauer and Jay R. Goldman
with the assistance of R. Kotzen**



Springer-Verlag
New York Heidelberg Berlin

Erich Hecke

formerly of
Department of Mathematics
Universität Hamburg
Hamburg
Federal Republic of Germany

Translators:

George U. Brauer
Jay R. Goldman

School of Mathematics
University of Minnesota
Minneapolis, MN 55455
USA

Editorial Board

P. R. Halmos

Managing Editor
Department of Mathematics
Indiana University
Bloomington, Indiana 47401
USA

F. W. Gehring

Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48104
USA

C. C. Moore

Department of Mathematics
University of California
Berkeley, California 94720
USA

AMS Classification (1980) 12-01

Library of Congress Cataloging in Publication Data

Hecke, Erich, 1887-1947.

Lectures on the theory of algebraic numbers.

(Graduate texts in mathematics; 77)

Translation of: Vorlesung über die Theorie der algebraischen Zahlen.

Bibliography: p.

I. Algebraic number theory. I. Title. II. Series.

QA247.H3713 512'.74 81-894

AACR2

Title of the German Original Edition: Vorlesung über die Theorie der algebraischen Zahlen. Akademische Verlagsgesellschaft, Leipzig, 1923.

© 1981 by Springer-Verlag New York Inc.

All rights reserved. No part of this book may be translated or reproduced in any form without written permission from Springer-Verlag, 175 Fifth Avenue, New York, New York 10010, U.S.A.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1



ISBN 0-387-90595-2 Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90595-2 Springer-Verlag Berlin Heidelberg New York

Translators' Preface

... if one wants to make progress in mathematics one should study
the masters not the pupils.

N. H. Abel

Hecke was certainly one of the masters, and in fact, the study of Hecke L-series and Hecke operators has permanently embedded his name in the fabric of number theory. It is a rare occurrence when a master writes a basic book, and Hecke's *Lectures on the Theory of Algebraic Numbers* has become a classic. To quote another master, André Weil: "To improve upon Hecke, in a treatment along classical lines of the theory of algebraic numbers, would be a futile and impossible task."

We have tried to remain as close as possible to the original text in preserving Hecke's rich, informal style of exposition. In a very few instances we have substituted modern terminology for Hecke's, e.g., "torsion free group" for "pure group."

One problem for a student is the lack of exercises in the book. However, given the large number of texts available in algebraic number theory, this is not a serious drawback. In particular we recommend *Number Fields* by D. A. Marcus (Springer-Verlag) as a particularly rich source.

We would like to thank James M. Vaughn Jr. and the Vaughn Foundation Fund for their encouragement and generous support of Jay R. Goldman without which this translation would never have appeared.

Minneapolis
July 1981

George U. Brauer
Jay R. Goldman

Author's Preface to the German Original Edition

The present book, which arose from lectures which I have given on various occasions in Basel, Göttingen, and Hamburg, has as its goal to introduce the reader without any knowledge of number theory to an understanding of problems which currently form the summit of the theory of algebraic number fields. The first seven chapters contain essentially nothing new; as far as form is concerned, I have drawn conclusions from the development of mathematics, in particular from that of arithmetic, and have used the notation and methods of group theory to develop the necessary theorems about finite and infinite Abelian groups. This yields considerable formal and conceptual simplifications. Nonetheless there will perhaps be some items of interest for the person who is familiar with the theory, such as the proof of the fundamental theorem on Abelian groups (§8), the theory of relative discriminants (§36, 38) which I deal with by the original construction of Dedekind, and the determination of the class number without the zeta-function (§50).

The last chapter, Chapter VIII, leads the reader to the summit of the modern theory. This chapter yields a new proof of the most general quadratic reciprocity law in arbitrary algebraic number fields, which by using the theta function, is substantially shorter than those proofs known until now. Even if this method is not capable of generalization it has the advantage of giving the beginner an overview of the new kinds of concepts which appear in algebraic number fields, and from this, of making the higher reciprocity theorems more easily accessible. The book closes with the proof of the existence of the class field of relative degree two, which is obtained here as a consequence of the reciprocity theorem.

As prerequisites only the elements of differential and integral calculus and of algebra, and for the last chapter the elements of complex function theory, will be assumed.

I am indebted for help with corrections and various suggestions to Messrs. Behnke, Hamburger, and Ostrowski. The publisher has held the plan of the book, conceived already before the war, with perseverance which is worthy of thanks, and despite the most unfavorable circumstances, has made possible the appearance of the book. My particular thanks are due to him for his pains.

Mathematical Seminar
Hamburg
March 1923

Erich Hecke

Contents

CHAPTER I

Elements of Rational Number Theory

1. Divisibility, Greatest Common Divisors, Modules, Prime Numbers, and the Fundamental Theorem of Number Theory (Theorems 1–5) 1
2. Congruences and Residue Classes (Euler's function $\psi(n)$. Fermat's theorem. Theorems 6–9) 6
3. Integral Polynomials, Functional Congruences, and Divisibility mod p (Theorems 10–13a) 10
4. Congruences of the First Degree (Theorems 14–15) 13

CHAPTER II

Abelian Groups

5. The General Group Concept and Calculation with Elements of a Group (Theorems 16–18) 16
6. Subgroups and Division of a Group by a Subgroup (Order of elements. Theorems 19–21) 20
7. Abelian Groups and the Product of Two Abelian Groups (Theorems 22–25) 22
8. Basis of an Abelian Group (The basis number of a group belonging to a prime number. Cyclic groups. Theorems 26–28) 24
9. Composition of Cosets and the Factor Group (Theorem 29) 28
10. Characters of Abelian Groups (The group of characters. Determination of all subgroups. Theorems 30–33) 30
11. Infinite Abelian Group (Finite basis of such a group and basis for a subgroup. Theorems 34–40) 34

CHAPTER III

Abelian Groups in Rational Number Theory

40

12. Groups of Integers under Addition and Multiplication
(*Theorem 41*) 40
13. Structure of the Group $\mathfrak{R}(n)$ of the Residue Classes mod n
Relatively Prime to n (*Primitive numbers mod p and mod p^2 .
Theorems 42–45*) 42
14. Power Residues (*Binomial congruences. Theorems 46–47*) 45
15. Residue Characters of Numbers mod n 48
16. Quadratic Residue Characters mod n (*On the quadratic
reciprocity law*) 50

CHAPTER IV

Algebra of Number Fields

54

17. Number Fields, Polynomials over Number Fields, and
Irreducibility (*Theorems 48–49*) 54
18. Algebraic Numbers over k (*Theorems 50–51*) 57
19. Algebraic Number Fields over k (*Simultaneous adjunction of
several numbers. The conjugate numbers. Theorems 52–55*) 59
20. Generating Field Elements, Fundamental Systems, and
Subfields of $K(\theta)$ (*Theorems 56–59*) 63

CHAPTER V

General Arithmetic of Algebraic Number Fields

68

21. Definition of Algebraic Integers, Divisibility, and Units
(*Theorems 60–63*) 68
22. The Integers of a Field as an Abelian Group: Basis and
Discriminant of the Field (*Moduli. Theorem 64*) 71
23. Factorization of Integers in $K(\sqrt{-5})$: Greatest Common
Divisors which Do Not Belong to the Field 73
24. Definition and Basic Properties of Ideals (*Product of ideals.
Prime ideals. Two definitions of divisibility. Theorems 65–69*) 77
25. The Fundamental Theorem of Ideal Theory (*Theorems 70–72*) 83
26. First Applications of the Fundamental Theorem (*Theorems 73–75*) 85
27. Congruences and Residue Classes Modulo Ideals and the
Group of Residue Classes under Addition and under
Multiplication (*Norm of an ideal. Fermat's theorem for ideal
theory. Theorems 76–85*) 87
28. Polynomials with Integral Algebraic Coefficients (*Content of
polynomials. Theorems 86–87*) 91
29. First Type of Decomposition Laws for Rational Primes:
Decomposition in Quadratic Fields (*Theorems 88–90*) 94
30. Second Type of Decomposition Theorem for Rational Primes:
Decomposition in the Field $K(e^{2\pi i/m})$ (*Theorems 91–92*) 98
31. Fractional Ideals (*Theorem 93*) 100
32. Minkowski's Theorem on Linear Forms (*Theorems 94–95*) 102

33. Ideal Classes, the Class Group, and Ideal Numbers (Theorems 96–98)	105
34. Units and an Upper Bound for the Number of Fundamental Units (Theorems 99–100)	108
35. Dirichlet's Theorem about the Exact Number of Fundamental Units (The regulator of the field)	113
36. Different and Discriminant (Number rings. Theorems 101–105)	116
37. Relative Fields and Relations between Ideals in Different Fields (Theorem 106)	122
38. Relative Norms of Numbers and Ideals, Relative Differents, and Relative Discriminants (The prime factors of the relative different. Theorems 107–115)	125
39. Decomposition Laws in the Relative Fields $K(\sqrt{\mu})$ (Theorems 116–120)	132

CHAPTER VI

Introduction of Transcendental Methods into the Arithmetic of Number Fields

40. The Density of the Ideals in a Class (Theorem 121)	139
41. The Density of Ideals and the Class Number (The number of ideals with given norm. Theorem 122)	143
42. The Dedekind Zeta-Function (Dirichlet series. Dedekind's zeta-function and its behavior at $s = 1$. Representation by products. Theorems 123–125)	144
43. The Distribution of Prime Ideals of Degree 1, in Particular the Rational Primes in Arithmetic Progressions (The Dirichlet series with residue characters mod n . Degree of the cyclotomic fields. Theorems 126–131)	148

CHAPTER VII

The Quadratic Number Field

44. Summary and the System of Ideal Classes (Numerical examples)	155
45. The Concept of Strict Equivalence and the Structure of the Class Group (Theorems 132–134)	159
46. The Quadratic Reciprocity Law and a New Formulation of the Decomposition Laws in Quadratic Fields (Theorems 135–137)	163
47. Norm Residues and the Group of Norms of Numbers (Theorems 138–141)	168
48. The Group of Ideal Norms, the Group of Genera, and Determination of the Number of Genera (Theorems 142–145)	172
49. The Zeta-Function of $k(\sqrt{d})$ and the Existence of Primes with Prescribed Quadratic Residue Characters (Theorems 146–147)	176
50. Determination of the Class Number of $k(\sqrt{d})$ without Use of the Zeta-Function (Theorem 148)	179

51. Determination of the Class Number with the Help of the Zeta-Function (<i>Theorem 149</i>)	181
52. Gauss Sums and the Final Formula for the Class Number (<i>Theorems 150–152</i>)	184
53. Connection between Ideals in $k(\sqrt{d})$ and Binary Quadratic Forms (<i>Theorems 153–154</i>)	187

CHAPTER VIII

The Law of Quadratic Reciprocity in Arbitrary Number Fields

195

54. Quadratic Residue Characters and Gauss Sums in Arbitrary Number Fields (<i>Theorems 155–156</i>)	195
55. Theta-functions and Their Fourier Expansions (<i>Theorems 157–158</i>)	200
56. Reciprocity between Gauss Sums in Totally Real Fields (<i>The transformation formula of the theta function and the reciprocity between Gauss sums for totally real fields. Theorems 159–161</i>)	205
57. Reciprocity between Gauss Sums in Arbitrary Algebraic Number Fields (<i>The transformation formula of the theta function and the reciprocity between Gauss sums for arbitrary fields. Theorems 162–163</i>)	210
58. The Determination of the Sign of Gauss Sums in the Rational Number Field (<i>Theorem 164</i>)	215
59. The Quadratic Reciprocity Law and the First Part of the Supplementary Theorem (<i>Theorems 165–167</i>)	217
60. Relative Quadratic Fields and Applications to the Theory of Quadratic Residues (<i>Existence of prime ideals with prescribed residue characters. Theorems 168–169</i>)	224
61. Number Groups, Ideal Groups, and Singular Primary Numbers	227
61. Number Groups, Ideal Groups, and Singular Primary Numbers	227
62. The Existence of the Singular Primary Numbers and Supplementary Theorems for the Reciprocity Law (<i>Theorems 170–175</i>)	230
63. A Property of Field Differents and the Hilbert Class Field of Relative Degree 2 (<i>Theorems 176–179</i>)	234

References

239

CHAPTER I

Elements of Rational Number Theory

§1 Divisibility, Greatest Common Divisors, Modules, Prime Numbers, and the Fundamental Theorem of Number Theory

For the time being the objects of arithmetic are the whole numbers, $0, \pm 1, \pm 2, \dots$ which can be combined by addition, subtraction, multiplication and division (not always) to form integers. Higher arithmetic uses methods of investigation analogous to those of real or complex numbers. Moreover it also uses analytic methods which belong to other areas of mathematics, such as infinitesimal calculus and complex function theory, in the derivation of its theorems. Since these will also be discussed in the latter part of this book, we will assume as known the totality of complex numbers, a number domain, in which the four types of operations (except division by 0) can be carried out unrestrictedly. The complex domain is usually developed more precisely in the elements of algebra or of differential calculus. In this domain the number 1 is distinguished as the one which satisfies the equation

$$1 \cdot a = a$$

for each number a . All successive integers are obtained by the process of addition and subtraction from the number 1, and if the process of division is then carried out the set of *rational numbers* is obtained as the totality of quotients of integers. Later, from §21 on, the concept of "integer" will be subjected to an essential extension.

In this introductory part the basic facts of rational arithmetic will be presented, briefly, as far as they concern divisibility properties of integers.

While, from two rational integers a, b , integers are always obtained in the form $a + b, a - b$, and $a \cdot b, a/b$ need not be an integer. If a/b is an integer, a special property of a and b is present, which we wish to express by the symbol $b|a$, in words: b divides a , or b goes evenly into a , or b is a divisor (factor) of a , or a is a multiple of b . Each integer a ($\neq 0$) has the trivial divisors $\pm a, \pm 1$; a and $-a$ have the same divisors; the only numbers which divide every number are the two "units" 1 and -1 . An integer a , different from zero, always has only finitely many divisors, as these cannot be larger in absolute value than $|a|$; on the other hand every non-zero integer divides 0.

If $b \neq 0$ and integral, then, among the multiples of b which are not larger than a given integer a there is exactly one largest multiple, say qb , and therefore $a - qb = r$ is a non-negative integer which is less than $|b|$. This integer r , uniquely determined by a and b by the requirement

$$a = qb + r, \quad q \text{ integral, } 0 \leq r < |b|$$

is called the remainder of the division of a by b , or the *remainder of a modulo b* . The statement $b|a$ is thus equivalent to $r = 0$.

If we now direct our attention to the common divisors c of two integers a, b which satisfies $c|a$ and $c|b$, then there is, to begin with, a uniquely determined *greatest common divisor* (abbreviated GCD); we denote it by $(a, b) = d$. According to this definition we always have $d \geq 1$. In order to find properties of this number (a, b) we consider that we always have $d|ax + by$ for all integers x, y . If we now consider the set of all numbers $L(x, y) = ax + by$, where x, y runs through all the integers, then d is obviously also the GCD of all $L(x, y)$; for it divides all $L(x, y)$ and there is no larger number with this property, since there can be no larger number which divides both $a = L(1, 0)$ and $b = L(0, 1)$. Among the positive integers $L(x, y)$, let $d_0 = L(x_0, y_0)$ be the smallest; thus from

$$L(x, y) > 0 \quad \text{it immediately follows that} \quad L(x, y) \geq d_0. \quad (1)$$

We now show that each $n = L(x, y)$ is a multiple of d_0 and that $d = d_0$. Let the remainder r of $n \bmod d_0$ be determined by

$$r = n - q \cdot d_0 = L(x - qx_0, y - qy_0).$$

Here we have $0 \leq r < d_0$; however by (1) it would follow from $r > 0$ that $r \geq d_0$. Thus we can have only $r = 0$, i.e., $n = qd_0$. Accordingly the numbers $L(x, y)$ are identical with the multiples of d_0 for each multiple $qd_0 = L(qx_0, qy_0)$ also appears among the $L(x, y)$. Consequently d_0 is likewise the GCD of all $L(x, y)$, hence it is identical with d . In particular this yields:

Theorem 1. If $(a, b) = d$, then the equation

$$n = ax + by$$

is solvable with integers x, y if and only if $d|n$.

Moreover it follows from this that every common divisor of a and b divides the GCD of a, b .

To ascertain the GCD one uses, as is well-known, a process which goes back to Euclid, the so-called Euclidean algorithm. The main point of this algorithm consists of reducing the calculation of (a, b) to the calculation of the GCD of two smaller numbers. It follows from $a = qb + r$ that the common divisors of a and b are identical with those of b and r , hence we have $(a, b) = (b, r)$. Assume $a > 0$, $b > 0$ for the sake of convenience, set $a = a_1$, $b = a_2$ because of symmetry, and then let the remainder of $a_1 \bmod a_2$ be a_3 . In general let

a_{i+2} be the remainder of $a_i \bmod a_{i+1}$ for $i = 1, 2, \dots$

as long as the remainder can be determined, that is, $a_{i+1} > 0$, and indeed let

$$a_i = q_i a_{i+1} + a_{i+2}, \quad 0 \leq a_{i+2} < a_{i+1}.$$

Since, according to this procedure, the a_i form a monotone decreasing sequence of integers for $i \geq 2$, the process must reach an end after finitely many steps, which will occur when the remainder becomes zero. Suppose $a_{i+2} = 0$. Since

$$\begin{aligned} (a_1, a_2) &= (a_2, a_3) = \dots (a_i, a_{i+1}) \\ &= (a_{i+1}, a_{i+2}) = (a_{k+1}, a_{k+2}) \\ &= (a_{k+1}, 0) = a_{k+1}, \end{aligned}$$

the last non-vanishing remainder a_{k+1} is the GCD sought.

In the proof of Theorem 1 we have used only one property of the set of numbers $L(x, y)$, namely the property that this set is a module. Here we define:

Definition. A system S of integers is a *module* if it contains at least one number different from 0 and if along with m and n , $m + n$ and $m - n$ also always belong to S .

Thus if m belongs to S , then $m + m = 2m$, $m + 2m = 3m \dots$ belong to S ; moreover $m - m = 0$, $m - 2m = -m$, $m - 3m = -2m \dots$ belong to S . Hence, in general, mx belongs to S for each integer x provided m belongs to S , and consequently $mx + ny$ also belongs to S for integers x, y if this holds for m, n .

We can prove the following very general theorem about modules with the help of the proof of Theorem 1.

Theorem 2. The numbers in a module S are identical with the multiples of certain number d . d is determined by S up to the factor ± 1 .

For the proof we consider that S contains positive numbers in any case. Let d be the smallest positive number occurring in S . If n belongs to S , then

by what has gone before, $n - qd$ also belongs to S for each integer q , in particular so must the remainder of $n \bmod d$, which is $< d$ but ≥ 0 , and thus must $= 0$. Consequently each n from S is a multiple of d and since d belongs to S so do all multiples of d . Let d' be a second number which also has the property: the numbers of S are identical with the multiples of d' —then d must be a multiple of d' and conversely, that is, $d' = \pm d$.

If in an arbitrary linear form $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ with integral coefficients one lets the $x_1, \dots, x_n$ run through all integers, then the range of values defined in this way is obviously a module. Hence in particular we have

Theorem 3. *The range of values of an arbitrary linear form in n variables with integral coefficients, not all vanishing, is identical with the range of values of a certain form of one variable $d \cdot x$. Here d is the GCD of the coefficients of the original form.*

In order that the equation (a so-called Diophantine equation)

$$k = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

be solvable in integers $x_1, \dots, x_n$, it is necessary and sufficient that the GCD of $a_1, \dots, a_n$ divides k .

If $(a, b) = 1$, we call a and b *coprime* or *relatively prime*. By Theorem 1, in order that $(a, b) = 1$, the solvability of

$$ax + by = 1$$

in integers x, y is necessary and sufficient.

As the most important rule of calculation with the symbol (a, b) we state:

Theorem 4. *For every three integers a, b, c , where $c > 0$*

$$(a, b)c = (ac, bc). \quad (2)$$

In fact if $(a, b) = d$, then the equation $acx + bcy = cd$ follows by Theorem 1 from the known solvable equation $ax + by = d$; consequently cd is a multiple of (ac, bc) , again by Theorem 1. On the other hand, however, cd is a common divisor of ac, bc and hence must be equal to (ac, bc) .

In addition we note the concept of *least common multiple* of two numbers a and b . This is the smallest positive number v which is divisible by a as well as by b . For this number we have

$$v = \frac{|a \cdot b|}{d}, \quad \text{where } (a, b) = d. \quad (3)$$

For by (2),

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1, \quad v = \left(\frac{a}{d}v, \frac{b}{d}v\right).$$

However ab/d is a common divisor of $(a/d)v$ and $(b/d)v$ and thus it divides v , that is, $v \geq |ab/d|$; on the other hand, ab/d is a number which is divisible

by a as well as by b , and consequently it has absolute value $\geq v$. Hence ab/d can only be $= \pm v$.

Since the numbers divisible by a and by b form a module and v is the smallest positive number occurring in it, every number divisible by a and by b must be a multiple of v .

We now turn to the *multiplicative decomposition* of a number a . If, except for the trivial decomposition into integral factors, in which one factor is ± 1 and the other is $\pm a$, there is no other, we call a a *prime number* (or *prime*). Such numbers exist, e.g., $\pm 2, \pm 3, \pm 5, \dots$. We do not wish to count the units ± 1 as prime numbers. If, for the sake of simplicity, we restrict ourselves to the decomposition of positive numbers a into positive factors we see first of all that every $a > 1$ is divisible by at least one positive prime number since the smallest positive factor of a , which is > 1 , obviously can only be a prime. Now we split off a prime number p_1 from the number a by the decomposition $a = p_1 a_1$, if $a_1 > 1$ we again split off another prime p_2 from a_1 by $a_1 = p_2 a_2$, and so on. Since the $a_1, a_2, \dots$ form a decreasing sequence of positive integers we must arrive at an end of the process after finitely many steps, that is, some a_k must be $= 1$. With this, a is represented as a product of primes $p_1 \cdot p_2 \cdots p_k$. Hence the primes are building blocks from which each integer can be built up by multiplication. We now have

Theorem 5. (Fundamental Theorem of Arithmetic). *Each positive number > 1 can be represented in one—and except for the order of the factors—in only one way as a product of primes.*

For this it is sufficient to show that a prime p can divide a product of two numbers $a \cdot b$ only if it divides at least one factor. But this follows from Theorem 4. Namely, if the prime number does not divide a , then as a prime it cannot have any factor at all in common with a ; hence $(a, p) = 1$. Then for each positive integer b , we have by Theorem 4

$$(ab, pb) = b.$$

Now if $p|ab$, then we must also have $p|b$, i.e., the prime p divides the other factor b of the product ab . This theorem carries over at once to a product of several factors.

In order to prove Theorem 5 we consider two representations of a positive number a as a product of powers of distinct positive primes p_i, q_i :

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}.$$

By what was just proved each prime q divides at least one prime factor of the left-hand side and is thus identical with some p_k . Thus the $q_1, \dots, q_k$ agree with $p_1, \dots, p_r$, except possibly for order; hence we also have $k = r$. We choose the numbering so that $p_i = q_i$. Now if corresponding exponents were not equal, say $a_1 > b_1$, then after division of the equation by $q_1^{b_1}$ it follows that the left-hand side still has the factor $p_1 = q_1$, but the right-hand side no longer has this factor. Hence $a_1 = b_1$ and in general $a_i = b_i$.

With this theorem about the *unique* decomposition of each number into prime factors we have a substantially different method of deciding the questions treated above, e.g., whether a given number b divides another number a , how (a, b) or the least common multiple of a and b is found, etc. Specifically, if we think of a and b as decomposed into their prime factors $p_1, \dots, p_r$,

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

$$b = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r},$$

where zero is also allowed for the exponents a_i, b_i , then obviously $b|a$ holds if and only if we always have $a_i \geq b_i$. Moreover we have

$$(a, b) = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}, \quad d_i = \min(a_i, b_i), \quad i = 1, 2, \dots, r,$$

$$v = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}, \quad c_i = \max(a_i, b_i), \quad i = 1, 2, \dots, r.$$

The existence of infinitely many primes follows immediately from the fact that

$$z = p_1 \cdot p_2 \cdots p_n + 1$$

is a number which is not divisible by any of the primes $p_1, \dots, p_n$. Hence z is divisible by at least one prime number distinct from $p_1, \dots, p_n$ and consequently if there are n primes, then there are $n + 1$ primes.

§2 Congruences and Residue Classes

By the preceding section, an integer $n \neq 0$ immediately determines a distribution of all integers according to the remainder which they yield mod n . We assign two integers a and b which have the same remainder mod n to the same *residue class mod n* or more simply, the same class mod n , and write

$$a \equiv b \pmod{n}, \quad (a \text{ is congruent to } b \text{ modulo } n),$$

which is equivalent to $n|a - b$. If a is not congruent to b relative to the modulus n we write $a \not\equiv b \pmod{n}$. $a \equiv 0 \pmod{n}$ asserts that a is divisible by n . Each number is called a *representative* of its class. Since the different remainders mod n are the numbers $0, 1, 2, \dots, |n| - 1$, the number of different residue classes mod n is $|n|$. The following easily verified rules hold for calculations with congruences: if a, b, c, d, n are integers, $n \neq 0$, then we have:

- (i) $a \equiv a \pmod{n}$.
- (ii) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
- (iii) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
- (iv) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a \pm c \equiv b \pm d \pmod{n}$.
- (v) If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.

In general from $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ it follows that $ac \equiv bd \pmod{n}$. In particular we have $a^k \equiv b^k \pmod{n}$ for each positive integer k whenever $a \equiv b \pmod{n}$. By repeated application of (iv) and (v) we obtain: if $a \equiv b \pmod{n}$, then $f(a) \equiv f(b) \pmod{n}$ when $f(x)$ is an integral rational function of x (polynomial in x) with integral coefficients.

Hence, to put it briefly, we can calculate with congruences of the same modulus in exactly the same way as with equations as far as the integral rational operations (addition, subtraction, multiplication) are concerned. With division it is different. If $ca \equiv cb \pmod{n}$, it does not follow that $a \equiv b \pmod{n}$, for the hypothesis means $n|c(a-b)$. Now if $(n, c) = d$, we further have

$$\left(\frac{n}{d}, \frac{c}{d}\right) = 1, \quad \frac{n}{d} \frac{c}{d} (a-b);$$

hence by Theorem 4,

$$\frac{n}{d} \Big| a-b, \quad \text{i.e.,} \quad a \equiv b \pmod{\frac{n}{d}}.$$

For example: It does not follow from $5 \cdot 4 \equiv 5 \cdot 1 \pmod{15}$ that $4 \equiv 1 \pmod{15}$, but rather only $\text{mod}(15/5) = 3$. Hence we have:

Theorem 6. If $ca \equiv cb \pmod{n}$, then

$$a \equiv b \pmod{\frac{n}{d}}, \quad \text{where } (c, n) = d,$$

and conversely.

In connection with this there is the fact:

A product of two integers may be congruent to zero mod n although neither of the factors has this property.

For example $2 \cdot 3 \equiv 0 \pmod{6}$ although neither 2 nor 3 is $\equiv 0 \pmod{6}$. Concerning the connection between congruences relative to different moduli we see directly from the definition: if a congruence holds mod n , then it also holds modulo each factor of n , in particular also modulo $-n$. Furthermore, if

$$a \equiv b \pmod{n_1} \quad \text{and} \quad a \equiv b \pmod{n_2},$$

then

$$a \equiv b \pmod{v},$$

where v is the least common multiple of n_1 and n_2 .

Since the residue classes modulo n and the residue classes modulo $-n$ coincide, it is sufficient to investigate the residue classes modulo a positive n .

A system of n integers which contains exactly one representative from each residue class mod n will be called a *complete system of residues mod n* .