Die Grundlehren der
mathematischen Wissenschaften in Einzeldarstellungen
Band 148

K. Chandrasekharan

Introduction to Analytic Number Theory

Springer-Verlag Berlin · Heidelberg · New York

Die Grundlehren der mathematischen Wissenschaften

in Einzeldarstellungen
mit besonderer Berücksichtigung
der Anwendungsgebiete

Band 148

Prof. Dr. K. Chandrasekharan
Eidgenössische Technische Hochschule Zürich

Geschäftsführende Herausgeber:

Prof. Dr. B. Eckmann
Eidgenössische Technische Hochschule Zürich

Prof. Dr. B. L. van der Waerden
Mathematisches Institut der Universität Zürich

Library of Congress Catalog Card Number 68-21990

Printed in Germany

Titel-Nr. 5131

Preface

This book has grown out of a course of lectures I have given at the Eidgenössische Technische Hochschule, Zürich. Notes of those lectures, prepared for the most part by assistants, have appeared in German. This book follows the same general plan as those notes, though in style, and in text (for instance, Chapters III, V, VIII), and in attention to detail, it is rather different. Its purpose is to introduce the non-specialist to some of the fundamental results in the theory of numbers, to show how analytical methods of proof fit into the theory, and to prepare the ground for a subsequent inquiry into deeper questions. It is published in this series because of the interest evinced by Professor Beno Eckmann.

I have to acknowledge my indebtedness to Professor Carl Ludwig Siegel, who has read the book, both in manuscript and in print, and made a number of valuable criticisms and suggestions. Professor Raghavan Narasimhan has helped me, time and again, with illuminating comments. Dr. Harold Diamond has read the proofs, and helped me to remove obscurities. I have to thank them all.

August 1968 K. C.

Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete

---

Lieferbare Bände:

2. Knopp: Theorie und Anwendung der unendlichen Reihen. DM 48,—; US $ 12.00
3. Hurwitz: Vorlesungen über allgemeine Funktionentheorie und elliptische Funktionen. DM 49,—; US $ 12.25
4. Madelung: Die mathematischen Hilfsmittel des Physikers. DM 49,70; US $ 12.45
10. Schouten: Ricci-Calculus. DM 58,60; US $ 14.65
14. Klein: Elementarmathematik vom höheren Standpunkt aus. 1. Band: Arithmetik. Algebra. Analysis. DM 24,—; US $ 6.00
15. Klein: Elementarmathematik vom höheren Standpunkt aus. 2. Band: Geometrie. DM 24,—; US $ 6.00
16. Klein: Elementarmathematik vom höheren Standpunkt aus. 3. Band: Präzisions- und Approximationsmathematik. DM 19,80; US $ 4.95
19. Pólya/Szegö: Aufgaben und Lehrsätze aus der Analysis I: Reihen, Integralrechnung, Funktionentheorie. DM 34,—; US $ 8.50
20. Pólya/Szegö: Aufgaben und Lehrsätze aus der Analysis II: Funktionentheorie, Nullstellen, Polynome, Determinanten, Zahlentheorie. DM 38,—; US $ 9.50
22. Klein: Vorlesungen über höhere Geometrie. DM 28,—; US $ 7.00
26. Klein: Vorlesungen über nicht-euklidische Geometrie. DM 24,—; US $ 6.00
27. Hilbert/Ackermann: Grundzüge der theoretischen Logik. DM 38,—; US $ 9.50
30. Lichtenstein: Grundlagen der Hydromechanik. DM 38,—; US $ 9.50
31. Kellogg: Foundations of Potential Theory. DM 32,—; US $ 8.00
32. Reidemeister: Vorlesungen über Grundlagen der Geometrie. DM 18,—; US $ 4.50
38. Neumann: Mathematische Grundlagen der Quantenmechanik. DM 28,—; US $ 7.00
40. Hilbert/Bernays: Grundlagen der Mathematik I. DM 68,—; US $ 17.00
50. Hilbert/Bernays: Grundlagen der Mathematik II. 2. Aufl. in Vorbereitung
52. Magnus/Oberhettinger/Soni: Formulas and Theorems for the Special Functions of Mathematical Physics. DM 66,—; US $ 16.50
57. Hamel: Theoretische Mechanik. DM 84,—; US $ 21.00
58. Blaschke/Reichardt: Einführung in die Differentialgeometrie. DM 24,—; US $ 6.00
59. Hasse: Vorlesungen über Zahlentheorie. DM 69,—; US $ 17.25
60. Collatz: The Numerical Treatment of Differential Equations. DM 78,—; US $ 19.50
61. Maak: Fastperiodische Funktionen. DM 38,—; US $ 9.50
62. Sauer: Anfangswertprobleme bei partiellen Differentialgleichungen. DM 41,—; US $ 10.25
64. Nevanlinna: Uniformisierung. DM 49,50; US $ 12.40
65. Tóth: Lagerungen in der Ebene, auf der Kugel und im Raum. DM 27,—; US $ 6.75
66. Bieberbach: Theorie der gewöhnlichen Differentialgleichungen. DM 58,50; US $ 14.65
68. Aumann: Reelle Funktionen. DM 59,60; US $ 14.90
69. Schmidt: Mathematische Gesetze der Logik I. DM 79,—; US $ 19.75
71. Meixner/Schäfke: Mathieusche Funktionen und Sphäroidfunktionen mit Anwendungen auf physikalische und technische Probleme. DM 52,60; US $ 13.15

73. Hermes: Einführung in die Verbandstheorie. DM 46,—; US $ 11.50
74. Boerner: Darstellungen von Gruppen. DM 58,—; US $ 14.50
75. Rado/Reichelderfer: Continuous Transformations in Analysis, with an Introduction to Algebraic Topology. DM 59,60; US $ 14.90
76. Tricomi: Vorlesungen über Orthogonalreihen. DM 37,60; US $ 9.40
77. Behnke/Sommer: Theorie der analytischen Funktionen einer komplexen Veränderlichen. DM 79,—; US $ 19.75
79. Saxer: Versicherungsmathematik. 1. Teil. DM 39,60; US $ 9.90
80. Pickert: Projektive Ebenen. DM 48,60; US $ 12.15
81. Schneider: Einführung in die transzendenten Zahlen. DM 24,80; US $ 6.20
82. Specht: Gruppentheorie. DM 69,60; US $ 17.40
83. Bieberbach: Einführung in die Theorie der Differentialgleichungen im reellen Gebiet. DM 32,80; US $ 8.20
84. Conforto: Abelsche Funktionen und algebraische Geometrie. DM 41,80; US $ 10.45
85. Siegel: Vorlesungen über Himmelsmechanik. DM 33,—; US $ 8.25
86. Richter: Wahrscheinlichkeitstheorie. DM 68,—; US $ 17.00
87. van der Waerden: Mathematische Statistik. DM 49,60; US $ 12.40
88. Müller: Grundprobleme der mathematischen Theorie elektromagnetischer Schwingungen. DM 52,80; US $ 13.20
89. Pfluger: Theorie der Riemannschen Flächen. DM 39,20; US $ 9.80
90. Oberhettinger: Tabellen zur Fourier Transformation. DM 39,50; US $ 9.90
91. Prachar: Primzahlverteilung. DM 58,—; US $ 14.50
92. Rehbock: Darstellende Geometrie. DM 29,—; US $ 7.25
93. Hadwiger: Vorlesungen über Inhalt, Oberfläche und Isoperimetrie. DM 49,80; US $ 12.45
94. Funk: Variationsrechnung und ihre Anwendung in Physik und Technik. DM 98,—; US $ 24.50
95. Maeda: Kontinuierliche Geometrien. DM 39,—; US $ 9.75
97. Greub: Linear Algebra. DM 39,20; US $ 9.80
98. Saxer: Versicherungsmathematik. 2. Teil. DM 48,60; US $ 12.15
99. Cassels: An Introduction to the Geometry of Numbers. DM 69,—; US $ 17.25
100. Koppenfels/Stallmann: Praxis der konformen Abbildung. DM 69,—; US $ 17.25
101. Rund: The Differential Geometry of Finsler Spaces. DM 59,60; US $ 14.90
103. Schütte: Beweistheorie. DM 48,—; US $ 12.00
104. Chung: Markov Chains with Stationary Transition Probabilities. DM 56,—; US $ 14.00
105. Rinow: Die innere Geometrie der metrischen Räume. DM 83,—; US $ 20.75
106. Scholz/Hasenjaeger: Grundzüge der mathematischen Logik. DM 98,—; US $ 24.50
107. Köthe: Topologische Lineare Räume I. DM 78,—; US $ 19.50
108. Dynkin: Die Grundlagen der Theorie der Markoffschen Prozesse. DM 33,80; US $ 8.45
109. Hermes: Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit. DM 49,80; US $ 12.45
110. Dinghas: Vorlesungen über Funktionentheorie. DM 69,—; US $ 17.25
111. Lions: Equations différentielles opérationnelles et problèmes aux limites. DM 64,—; US $ 16.00
112. Morgenstern/Szabó: Vorlesungen über theoretische Mechanik. DM 69,—; US $ 17.25
113. Meschkowski: Hilbertsche Räume mit Kernfunktion. DM 58,—; US $ 14.50

114. MacLane: Homology. DM 62,—; US $ 15.50
115. Hewitt/Ross: Abstract Harmonic Analysis. Vol. 1: Structure of Topological Groups. Integration Theory. Group Representations. DM 76,—; US $ 19.00
116. Hörmander: Linear Partial Differential Operators. DM 42,—; US $ 10.50
117. O'Meara: Introduction to Quadratic Forms. DM 48,—; US $ 12.00
118. Schäfke: Einführung in die Theorie der speziellen Funktionen der mathematischen Physik. DM 49,40; US $ 12.35
119. Harris: The Theory of Branching Processes. DM 36,—; US $ 9.00
120. Collatz: Funktionalanalysis und numerische Mathematik. DM 58,—; US $ 14.50
121.
122. Dynkin: Markov Processes. DM 96,—; US $ 24.00
123. Yosida: Functional Analysis. DM 66,—; US $ 16.50
124. Morgenstern: Einführung in die Wahrscheinlichkeitsrechnung und mathematische Statistik. DM 34,50; US $ 8.65
125. Itô/McKean: Diffusion Processes and Their Sample Paths. DM 58,—; US $ 14.50
126. Lehto/Virtanen: Quasikonforme Abbildungen. DM 38,—; US $ 9.50
127. Hermes: Enumerability, Decidability, Computability. DM 39,—; US $ 9.75
128. Braun/Koecher: Jordan-Algebren. DM 48,—; US $ 12.00
129. Nikodým: The Mathematical Apparatus for Quantum-Theories. DM 144,—; US $ 36.00
130. Morrey: Multiple Integrals in the Calculus of Variations. DM 78,—; US $ 19.50
131. Hirzebruch: Topological Methods in Algebraic Goemetry. DM 38,—; US $ 9.50
132. Kato: Perturbation theory for linear operators. DM 79,20; US $ 19.80
133. Haupt/Künneth: Geometrische Ordnungen. DM 68,—; US $ 17.00
134. Huppert: Endliche Gruppen I. DM 156,—; US $ 39.00
135. Handbook for Automatic Computation. Vol. 1/Part a: Rutishauser: Description of ALGOL 60. DM 58,—; US $ 14.50
136. Greub: Multilinear Algebra. DM 32,—; US $ 8.00
137. Handbook for Automatic Computation. Vol. 1/Part b: Grau/Hill/Langmaack: Translation of ALGOL 60. DM 64,—; US $ 16.00
138. Hahn: Stability of Motion. DM 72,—; US $ 18.00
139. Mathematische Hilfsmittel des Ingenieurs. Herausgeber: Sauer/Szabó. 1. Teil. DM 88,—; US $ 22.00
141. Mathematische Hilfsmittel des Ingenieurs. Herausgeber: Sauer/Szabó. 3. Teil. DM 98,—; US $ 24.50
143. Schur/Grunsky: Vorlesungen über Invariantentheorie. DM 32,—; US $ 8.00
144. Weil: Basic Number Theory. DM 48,—; US $ 12.00
145. Butzer/Berens: Semi-Groups of Operators and Approximation. DM 56,—; US $ 14.00
146. Treves: Locally Convex Spaces and Linear Partial Differential Equations. DM 36,—; US $ 9.00
147. Lamotke: Semisimpliziale algebraische Topologie. DM 48,—; US $ 12.00
148. Chandrasekharan: Introduction to Analytic Number Theory. DM 28,—; US $ 7.00
149. Sario/Oikawa: Capacity Functions. In Vorbereitung
150. Iosifescu/Theodorescu: Random Processes and Learning. DM 68,—; US $ 17.00
151. Mandl: Analytical Treatment of One-Dimensional Markov Processes. DM 36,—; US $ 9.00
152. Hewitt/Ross: Abstract Harmonic Analysis. Vol. 2. In Vorbereitung
153. Federer: Geometric Measure Theory. In Vorbereitung

Contents

Chapter VI

Arithmetical functions and lattice points

Chapter VII

Chebyshev's theorem on the distribution of prime numbers

Chapter VIII

Weyl's theorems on uniform distribution and Kronecker's theorem

Chapter IX

Minkowski's theorem on lattice points in convex sets

Chapter X

Dirichlet's theorem on primes in an arithmetical progression

Chapter XI

The prime number theorem

Chapter I

The unique factorization theorem

§ 1. Primes. We assume as known the *positive integers* $1, 2, 3, \ldots$, the *negative integers* $-1, -2, -3, \ldots$, and *zero*, which we reckon as an integer. By the *non-negative integers* we mean the positive integers together with zero. We assume as known the elementary arithmetical operations on integers.

An integer a is said to be *divisible* by an integer $b \neq 0$, if there exists an integer c, such that $a = bc$. We then say that b *divides* a, or b is a *divisor* of a, and indicate this by writing $b|a$. We also say that a is an *integral multiple* or just a *multiple* of b. We write $b \nmid a$ to indicate that b does *not* divide a. The following propositions are easily verified:

if $b|a$, and $a > 0$, and $b > 0$, then $1 \leqslant b \leqslant a$;

if $b|a$, and $c|b$, then $c|a$;

if $b|a$, and $c \neq 0$, then $bc|ac$;

if $c|a$, and $c|b$, then $c|(ma+nb)$, for all integers m and n.

Given two integers a and b, $b \neq 0$, there exist unique integers q and r, such that $a = bq + r$, where $0 \leqslant r < |b|$. We call q the *quotient*, and r the *remainder* in the division of a by b. If $b|a$, then $r = 0$.

An integer p, where $p > 1$, is a *prime number*, or a *prime*, if its only positive divisors are 1 and p. An integer greater than 1, which is not a prime, is called *composite*.

In this chapter we shall prove that every integer greater than 1 can be represented as a product of primes, and that such a representation as a product is *unique*, except for the order of the factors. We shall also prove that there exist infinitely many primes.

§ 2. The unique factorization theorem. We begin with the following simple

THEOREM 1. *If n is an integer greater than 1, then n is a product of primes.*

PROOF. Either n is a prime, or it is composite. In the former case, there is nothing more to prove. If n is composite, then, by definition, there exist integers d, such that $1 < d < n$, and $d|n$. Let m be the least of such

divisors. Then m must be a prime, for otherwise there exists an integer k, such that $1<k<m$, and $k|m$. That would imply that $k|n$, and $1<k<m$, which contradicts the definition of m. Thus m is a prime p_1, say. We then write $n=p_1\cdot r$, where $1<r<n$, and repeat the same process with r, to obtain $n=p_1\cdot p_2\cdot s$, where $p_2\geqslant p_1$, and $1\leqslant s<r<n$. This process clearly breaks off after a finite number of steps, since there are only finitely many integers between 1 and n. We therefore obtain

$$n=p_1 p_2\dots p_t, \quad \text{with} \quad p_1\leqslant p_2\leqslant\cdots\leqslant p_t, \tag{1}$$

which concludes the proof.

We note, in passing, that if $n=ab$, then a and b cannot both be greater than $\sqrt{n}$. It follows that any composite integer n has a prime factor p, such that $p\leqslant\sqrt{n}$.

By grouping together the equal primes in the representation (1), and changing the indices, if necessary, we can rewrite (1) as

$$n=p_1^{a_1} p_2^{a_2}\dots p_k^{a_k}, \tag{2}$$

where $p_1<p_2<\cdots<p_k$, and $a_i>0$, for $i=1,2,\dots,k$. This is called the *standard form* of n.

We are now in a position to prove the unique factorization theorem, which is also known as the fundamental theorem of arithmetic (Theorem 2).

THEOREM 2. *The standard form of an integer n, which is greater than* 1, *is unique.*

We shall give three proofs of this theorem. The first proof uses only Theorem 1. The second is connected with the solution of linear equations in integers, while the third makes use of the theory of *Farey sequences.*

FIRST PROOF OF THEOREM 2. The standard form of a prime is clearly unique.

Suppose, if possible, that some positive integers >1 have two different standard forms. Let N be the *smallest* such integer, with

$$N=p_1 p_2\cdots p_k=q_1 q_2\cdots q_m.$$

Every p is distinct from every q, since any prime common to both the representations would divide N to yield an integer $N'<N$ with the same property as N, which is impossible by the definition of N.

We may assume that

$$p_1\leqslant p_2\leqslant\cdots\leqslant p_k, \quad \text{and} \quad q_1\leqslant q_2\leqslant\cdots\leqslant q_m.$$

Now $p_1 \neq q_1$. Let us suppose, as we may, that $p_1 < q_1$. We define the number

$$P = p_1 q_2 \dots q_m.$$

Since $p_1 | P$, and $p_1 | N$, it follows that $p_1 | (N - P)$, where

$$N - P = (q_1 - p_1) q_2 \dots q_m > 1.$$

Therefore we can write

$$N - P = p_1 t_1 \dots t_h, \tag{3}$$

where the t_i are primes for $i = 1, 2, \dots, h$. We can also write $q_1 - p_1$ as a product of primes, say

$$q_1 - p_1 = r_1 r_2 \dots r_s,$$

if $q_1 - p_1 > 1$. Then we get

$$N - P = r_1 r_2 \dots r_s \cdot q_2 \dots q_m, \tag{4}$$

as another representation of $N - P$ as a product of primes. We have seen that none of the p's is equal to a q. In particular, p_1 is not equal to any q. Nor is p_1 equal to any r, for it is clear that $p_1 \nmid (q_1 - p_1)$, so that no factorization of $q_1 - p_1$ can contain p_1. Thus the integer $N - P$ has two factorizations, namely (3) and (4), which are distinct, since only one of them contains p_1. This is the case even if $q_1 - p_1 = 1$. But $1 < N - P < N$, which contradicts the minimality of N. Hence there exists no integer $n > 1$ with more than one standard form.

§ 3. A second proof of Theorem 2. This is based on the solution of certain linear equations in integers. We need some preparation.

Let a and b denote integers, not both zero. Their *greatest common divisor*, denoted by (a, b), is defined to be the largest positive integer which divides both a and b. If $(a, b) = 1$, we say that a is *prime to* b, or that a and b are *relatively prime*. We shall see that if $(a, b) = d$, the equation $ax + by = d$ has a solution in integers x, y. It follows from this that if p is a prime, and $p | ab$, then $p | a$ or $p | b$, and this, in turn, implies the unique factorization theorem.

A non-empty set of integers S with the property

$$m \in S \text{ and } n \in S \Rightarrow m - n \in S,$$

is called a *module*. It follows from the definition that if $m, n \in S$, then

$$0 = m - m \in S, \quad -n = 0 - n \in S, \quad m + n = m - (-n) \in S.$$

More generally, if $a\in S$, $b\in S$, then $ax+by\in S$, where x and y are integers. If a module contains only 0, we call it *the trivial module.* A non-trivial module obviously contains infinitely many positive, and negative, integers. We can say a little more.

THEOREM 3. *Every non-trivial module S consists of all integral multiples of a positive integer.*

PROOF. Since S is not the trivial module, it contains some positive integers. Let d be the smallest such integer. Then S contains all integral multiples of d. In order to show that these are the only elements of S, take any $n\in S$. We can write $n=dk+c$, where k and c are integers, and $0\leqslant c<d$. Since $d\in S$, it follows that $dk\in S$. Since $n\in S$, we have $n-dk\in S$, that is $c\in S$. But $c<d$, and d is the smallest positive integer in S. Hence $c=0$. Therefore n is an integral multiple of d.

From this we deduce

THEOREM 4. *If a and b are given integers, the module $S=\{ax+by\}$, where x and y are integers, is the set of all integral multiples of $d=(a,b)$.*

PROOF. It is easy to see that the set S *is* a module. By Theorem 3 we know that S is the set of all integral multiples of some positive integer e. Therefore e divides all elements of S; in particular, $e|a$, and $e|b$. Since d is the *greatest* common divisor of a and b, we must have $e\leqslant d$. On the other hand, $d|(ax+by)$ for all integers x, y, so that d divides every element of S. In particular, $d|e$. Hence $d\leqslant e$. Thus $e=d$, and the result follows.

It is now clear that the following theorem holds:

THEOREM 5. *The equation $ax+by=n$ is soluble in integers x and y if and only if $(a,b)|n$.*

COROLLARY 1. *If $(a,b)=d$, then $ax+by=d$ is soluble in integers x and y. In other words, the greatest common divisor of a and b is a linear combination of these integers with integer coefficients.*

COROLLARY 2. *Any common divisor of a and b divides (a,b).*

These results lead to

THEOREM 6 (EUCLID). *If $a|bc$, and $(a,b)=1$, then $a|c$.*

PROOF. Since $(a,b)=1$, there exist integers x and y, such that $ax+by=1$. If we multiply by c, we get $acx+bcy=c$, and since $a|bc$, it follows that $a|(acx+bcy)$, or $a|c$.

COROLLARY. *If p is a prime, and $p\left|\prod_{i=1}^{r} p_i\right.$, where p_i is a prime for $i=1,2,\ldots,r$, then $p=p_i$ for at least one i.*

We are now in a position to give

A SECOND PROOF OF THEOREM 2. Suppose that an integer N has two different standard forms,

$$N = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \dots q_r^{b_r}.$$

Then $p_1 | q_1^{b_1} q_2^{b_2} \dots q_r^{b_r}$, hence, by the Corollary of Theorem 6, $p_1 = q_i$ for some i, $1 \leqslant i \leqslant r$. In the same way we see that every p equals some q, and every q equals some p. Therefore $k = r$, and since both forms are arranged in ascending order, we have

$$p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k},$$

with $p_1 < p_2 < \dots < p_k$. We shall see that $a_i = b_i$ for $i = 1, 2, \dots, k$. For if $a_i > b_i$ for some i, we can divide both sides by $p_i^{b_i}$ and obtain

$$p_1^{a_1} \dots p_i^{a_i - b_i} \dots p_k^{a_k} = p_1^{b_1} \dots p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} \dots p_k^{b_k},$$

where p_i divides the left-hand side, but not the right-hand side, which is impossible. Similarly it is impossible that $a_i < b_i$. Hence $a_i = b_i$ for all i, and the standard form is unique.

§ 4. Greatest common divisor and least common multiple. Related to the greatest common divisor of two integers a and b, defined in § 3, is the *least common multiple.*

DEFINITION. *The least common multiple* $\{a, b\}$ *of two integers* a *and* b, *where* $ab \neq 0$, *is the smallest positive integer which is divisible by both* a *and* b.

The relationship between (a, b) and $\{a, b\}$, where $ab > 0$, is expressed by the identity

$$ab = (a, b) \cdot \{a, b\}. \tag{5}$$

To prove this, consider the integer $\mu = ab/(a, b)$. Since $(a, b) | b$, μ is an integral multiple of a. Similarly μ is an integral multiple of b. Thus μ is a common multiple of a and b. Let ν be an integer which is some other common integral multiple of a and b, and consider the number

$$\frac{\nu}{\mu} = \frac{\nu \cdot (a, b)}{ab}.$$

We know that $(a, b) = ax + by$ for some integers x and y. Hence

$$\frac{\nu}{\mu} = \frac{\nu \cdot (ax + by)}{ab} = \frac{\nu x}{b} + \frac{\nu y}{a}.$$

But v/a and v/b are integers, hence v/μ is an integer. Thus any common integral multiple of a and b is an integral multiple of μ. Hence μ is their least common multiple, and

$$\mu = \frac{ab}{(a,b)} = \{a,b\}.$$

Incidentally we have shown that the least common multiple of a and b divides any common multiple of a and b.

If a is a positive integer, we can write

$$a = \prod p^{\alpha}, \qquad \alpha \geqslant 0,$$

where the product extends over all primes p, and α is a non-negative integer which is zero except for finitely many p. If a prime p does *not* divide a, then the corresponding exponent α is zero. Similarly we have

$$b = \prod p^{\beta}, \qquad \beta \geqslant 0.$$

It is easy to see that

$$(a,b) = \prod p^{\min[\alpha,\beta]}, \qquad \{a,b\} = \prod p^{\max[\alpha,\beta]}. \tag{6}$$

§ 5. Farey sequences. If h and k are integers, and $k>0$, we call h/k a *fraction*, with *numerator* h, and with *denominator* k.

A fraction h/k is called *irreducible*, or *reduced*, if $(h,k)=1$. A fraction h/k is called *proper*, if $0 \leqslant h/k \leqslant 1$.

A *Farey sequence of order* n, where n is a positive integer, is the sequence F_n of all irreducible, proper fractions h/k, with $1 \leqslant k \leqslant n$, arranged in non-decreasing order. For example, F_5 is the sequence

$$\tfrac{0}{1},\ \tfrac{1}{5},\ \tfrac{1}{4},\ \tfrac{1}{3},\ \tfrac{2}{5},\ \tfrac{1}{2},\ \tfrac{3}{5},\ \tfrac{2}{3},\ \tfrac{3}{4},\ \tfrac{4}{5},\ \tfrac{1}{1}.$$

A *Farey fraction* is a term in a Farey sequence of some order. We note that every rational number m/n, such that $0 \leqslant m/n \leqslant 1$, is *equal* to a Farey fraction.

It follows from the unique factorization theorem (Theorem 2) that a reduced fraction is unique. In other words, two reduced fractions which are equal must be identical. Since we do *not* wish to use Theorem 2, however, we have to allow for the possibility that two Farey fractions *may* be equal without being identical. In that case, we arrange them in increasing order of their numerators. The following theorem rules out such a possibility in fact, and prepares the ground for a third proof of Theorem 2.

THEOREM 7 (FAREY-CAUCHY). *If* l/m *is the immediate successor of* h/k *in the Farey sequence* F_N, *then* $kl - hm = 1$.

PROOF. The result is seen to be true, by actual verification, for F_N, $1 \leqslant N \leqslant 5$. We shall *assume* it true for F_N, and prove it for F_{N+1}.

Let a/b be a reduced proper fraction which does *not* belong to F_N. Then $b \geqslant N+1$, and a/b must lie between some two consecutive fractions h/k and l/m of F_N, say

$$\frac{h}{k} \leqslant \frac{a}{b} \leqslant \frac{l}{m},$$

equality being allowed, since the uniqueness of reduction of a fraction is *not* assumed.

Define the integers λ and μ as follows:

$$\lambda = ka - hb, \qquad \mu = bl - am.$$

Then $\lambda \geqslant 0$, $\mu \geqslant 0$, and $\lambda + \mu > 0$, since we have assumed the theorem to be true for F_N, to which h/k and l/m belong. Further

$$\lambda l + \mu h = kal - ham = a(kl - hm) = a,$$

since $kl - hm = 1$ by the induction hypothesis on F_N. Similarly

$$\lambda m + \mu k = b, \tag{7}$$

and $(\lambda, \mu) = 1$, since $(a,b) = 1$. Thus, if $h/k \leqslant a/b \leqslant l/m$, $(a,b) = 1$, then

$$\frac{a}{b} = \frac{\lambda l + \mu h}{\lambda m + \mu k}, \quad \lambda \geqslant 0, \quad \mu \geqslant 0, \quad \lambda + \mu > 0, \quad (\lambda, \mu) = 1.$$

Conversely, if λ and μ are integers, such that $\lambda \geqslant 0$, $\mu \geqslant 0$, $\lambda + \mu > 0$, $(\lambda, \mu) = 1$, and we *define* a,b by $a = \lambda l + \mu h$, $b = \lambda m + \mu k$, then *uniquely* $\lambda = ka - hb$, $\mu = bl - am$, *and* $(a,b) = 1$, so the fraction a/b is reduced, and $h/k \leqslant a/b \leqslant l/m$, since $kl - hm = 1$. Thus a/b belongs to F_M, for some M.

Since $k > 0$, $m > 0$, $(\lambda, \mu) = 1$, we also see that $b \leqslant m + k$ exactly in the three cases $\lambda, \mu = 0,1;\ 1,1;\ 1,0$; giving $a,b = h,k;\ l+h,\ m+k;\ l,m$. Now $\lambda \neq 0$, for if $\lambda = 0$, then $a/b = (\mu h)/(\mu k)$, which is *not* reduced unless $\mu = 1$, in which case $b = k$ by (7), and that contradicts the assumption that $b \geqslant N+1 > k$. Similarly $\mu \neq 0$. Hence $b \leqslant m + k$ only if $\lambda = \mu = 1$. Now $b \geqslant N+1$, and if $(a/b) \in F_{N+1}$, then $b = N+1$. Further $m + k \geqslant N+1$, since

$$\frac{l+h}{m+k} \notin F_N,$$