TURING 图灵原版数学·统计学系列 39

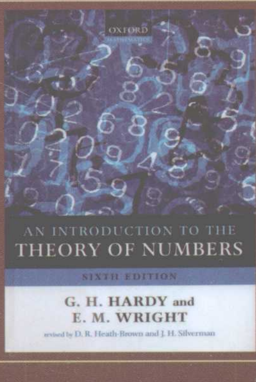
An Introduction to the Theory of Numbers

哈代数论

（英文版·第6版）

[英] G. H. Hardy
E. M. Wright 著

[英] D. R. Heath-Brown
[美] J. H. Silverman 修订



人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵原版数学·统计学系列

An Introduction to the Theory of Numbers

哈代数论

（英文版·第6版）

[英] G. H. Hardy
E. M. Wright 著
[英] D. R. Heath-Brown
[美] J. H. Silverman 修订

人民邮电出版社
北京

图书在版编目（CIP）数据

哈代数论：第6版：英文/（英）哈代
(Hardy, G. H.)，（英）莱特（Wright, E. M.）著.—北京：
人民邮电出版社，2009.11
（图灵原版数学·统计学系列）
书名原文：An Introduction to the Theory of
Numbers, sixth edition
ISBN 978-7-115-21427-0

I. ①哈… II. ①哈… ②莱… III. ①数论－英文
IV. ①O156

中国版本图书馆CIP数据核字（2009）第176007号

内 容 提 要

本书是数论领域的一部传世名著，成书于作者在牛津大学、剑桥大学等学校授课的讲义. 书中从各个不同角度对数论进行了阐述，内容包括素数、无理数、同余、费马定理、连分数、不定式、二次域、算术函数、分化等. 新版修订了每章末的注解，简要介绍了数论最新的发展；增加了一章讲述椭圆曲线，这是数论中最重要的突破之一. 还列出进一步阅读的文献.

本书适合数学专业本科生、研究生和教师用作教材或参考书，也适合对数论感兴趣的专业人士阅读参考.

图灵原版数学·统计学系列

哈代数论（英文版·第6版）

- 著　[英] G. H. Hardy　E. M. Wright
  修订　[英] D. R. Heath-Brown　[美] J. H. Silverman
  责任编辑　明永玲
- 人民邮电出版社出版发行　北京市崇文区夕照寺街14号
  邮编　100061　电子函件　315@ptpress.com.cn
  网址　http://www.ptpress.com.cn
  北京顺义振华印刷厂印刷
- 开本：880×1230　1/32
  印张：20
  字数：576千字　2009年11月第1版
  印数：1-2 000册　2009年11月北京第1次印刷

著作权合同登记号　图字：01-2009-5551号

ISBN 978-7-115-21427-0

定价：59.00元

读者服务热线：（010）51095186　印装质量热线：（010）67129223

反盗版热线：（010）67171154

FOREWORD BY ANDREW WILES

I had the great good fortune to have a high school mathematics teacher who had studied number theory. At his suggestion I acquired a copy of the fourth edition of Hardy and Wright's marvellous book *An Introduction to the Theory of Numbers*. This, together with Davenport's *The Higher Arithmetic*, became my favourite introductory books in the subject. Scouring the pages of the text for clues about the Fermat problem (I was already obsessed) I learned for the first time about the real breadth of number theory. Only four of the chapters in the middle of the book were about quadratic fields and Diophantine equations, and much of the rest of the material was new to me; Diophantine geometry, round numbers, Dirichlet's theorem, continued fractions, quaternions, reciprocity ... The list went on and on.

The book became a starting point for ventures into the different branches of the subject. For me the first quest was to find out more about algebraic number theory and Kummer's theory in particular. The more analytic parts did not have the same attraction then and did not really catch my imagination until I had learned some complex analysis. Only then could I appreciate the power of the zeta function. However, the book was always there as a starting point which I could return to whenever I was intrigued by a new piece of theory, sometimes many years later. Part of the success of the book lay in its extensive notes and references which gave navigational hints for the inexperienced mathematician. This part of the book has been updated and extended by Roger Heath-Brown so that a 21st-century-student can profit from more recent discoveries and texts. This is in the style of his wonderful commentary on Titchmarsh's *The Theory of the Riemann Zeta Function*. It will be an invaluable aid to the new reader but it will also be a great pleasure to those who have read the book in their youth, a bit like hearing the life stories of one's erstwhile school friends.

A final chapter has been added giving an account of the theory of elliptic curves. Although this theory is not described in the original editions (except for a brief reference in the notes to §13.6) it has proved to be critical in the study of Diophantine equations and of the Fermat equation in particular. Through the Birch and Swinnerton-Dyer conjecture on the one hand and through the extraordinary link with the Fermat equation on the other it has become a central part of the number theorist's life. It even played a central role in the effective resolution of a famous class number problem of Gauss. All this would have seemed absurdly improbable when the book was written. It is thus an appropriate ending for the new edition to have a lucid exposition of this theory by Joe Silverman. Of course it is only a quick sketch of the theory and the reader will surely be tempted to devote many hours, if not the best part of a lifetime, to unravelling its many mysteries.

A.J.W.

January, 2008

PREFACE TO THE SIXTH EDITION

This sixth edition contains a considerable expansion of the end-of-chapter notes. There have been many exciting developments since these were last revised, which are now described in the notes. It is hoped that these will provide an avenue leading the interested reader towards current research areas. The notes for some chapters were written with the generous help of other authorities. Professor D. Masser updated the material on Chapters 4 and 11, while Professor G.E. Andrews did the same for Chapter 19. A substantial amount of new material was added to the notes for Chapter 21 by Professor T.D. Wooley, and a similar review of the notes for Chapter 24 was undertaken by Professor R. Hans-Gill. We are naturally very grateful to all of them for their assistance.

In addition, we have added a substantial new chapter, dealing with elliptic curves. This subject, which was not mentioned in earlier editions, has come to be such a central topic in the theory of numbers that it was felt to deserve a full treatment. The material is naturally connected with the original chapter on Diophantine Equations.

Finally, we have corrected a significant number of misprints in the fifth edition. A large number of correspondents reported typographical or mathematical errors, and we thank everyone who contributed in this way.

The proposal to produce this new edition originally came from Professors John Maitland Wright and John Coates. We are very grateful for their enthusiastic support.

D.R.H.-B.
J.H.S.

September, 2007

D. R. Heath-Brown 著名数学家，牛津大学教授，英国皇家学会会员，分别于1981年和1996年获得伦敦数学会颁发的贝维克奖（Berwick Prize）.

J. H. Silverman 著名数学家，美国布朗大学教授，1982年哈佛大学博士毕业. 著有*The Arithmetic of Elliptic Curves*等十多本书，发表学术论文100多篇.

PREFACE TO THE FIFTH EDITION

The main changes in this edition are in the Notes at the end of each chapter. I have sought to provide up-to-date references for the reader who wishes to pursue a particular topic further and to present, both in the Notes and in the text, a reasonably accurate account of the present state of knowledge. For this I have been dependent on the relevant sections of those invaluable publications, the *Zentralblatt* and the *Mathematical Reviews*. But I was also greatly helped by several correspondents who suggested amendments or answered queries. I am especially grateful to Professors J. W. S. Cassels and H. Halberstam, each of whom supplied me at my request with a long and most valuable list of suggestions and references.

There is a new, more transparent proof of Theorem 445 and an account of my changed opinion about Theodorus'method in irrationals. To facilitate the use of this edition for reference purposes, I have, so far as possible, kept the page numbers unchanged. For this reason, I have added a short appendix on recent progress in some aspects of the theory of prime numbers, rather than insert the material in the appropriate places in the text.

E. M. W.

ABERDEEN
October 1978

PREFACE TO THE FIRST EDITION

This book has developed gradually from lectures delivered in a number of universities during the last ten years, and, like many books which have grown out of lectures, it has no very definite plan.

It is not in any sense (as an expert can see by reading the table of contents) a systematic treatise on the theory of numbers. It does not even contain a fully reasoned account of any one side of that many-sided theory, but is an introduction, or a series of introductions, to almost all of these sides in turn. We say something about each of a number of subjects which are not usually combined in a single volume, and about some which are not always regarded as forming part of the theory of numbers at all. Thus chs. XII–XV belong to the 'algebraic' theory of numbers, Chs. XIX–XXI to the 'addictive', and Ch. XXII to the 'analytic' theories; while Chs. III, XI, XXIII, and XXIV deal with matters usually classified under the headings of 'geometry of numbers' or 'Diophantine approximation'. There is plenty of variety in our programme, but very little depth; it is impossible, in 400 pages, to treat any of these many topics at all profoundly.

There are large gaps in the book which will be noticed at once by any expert. The most conspicuous is the omission of any account of the theory of quadratic forms. This theory has been developed more systematically than any other part of the theory of numbers, and there are good discussions of it in easily accessible books. We had to omit something, and this seemed to us the part of the theory where we had the least to add to existing accounts.

We have often allowed out personal interests to decide out programme, and have selected subjects less because of their importance (though most of them are important enough) than because we found them congenial and because other writers have left us something to say. Our first aim has been to write an interesting book, and one unlike other books. We may have succeeded at the price of too much eccentricity, or we may have failed; but we can hardly have failed completely, the subject-matter being so attractive that only extravagant incompetence could make it dull.

The book is written for mathematicians, but it does not demand any great mathematical knowledge or technique. In the first eighteen chapters we assume nothing that is not commonly taught in schools, and any intelligent university student should find them comparatively easy reading. The last six are more difficult, and in them we presuppose a little more, but nothing beyond the content of the simpler university courses.

The title is the same as that of a very well-known book by Professor L. E. Dickson (with which ours has little in common). We proposed at one time to change it to *An introduction to arithmetic*, a more novel and in some ways a more appropriate title; but it was pointed out that this might lead to misunderstandings about the content of the book.

A number of friends have helped us in the preparation of the book. Dr. H. Heilbronn has read all of it both in manuscript and in print, and his criticisms and suggestions have led to many very substantial improvements, the most important of which are acknowledged in the text. Dr. H. S. A. Potter and Dr. S. Wylie have read the proofs and helped us to remove many errors and obscurities. They have also checked most of the references to the literature in the notes at the ends of the chapters. Dr. H. Davenport and Dr. R. Rado have also read parts of the book, and in particular the last chapter, which, after their suggestions and Dr. Heilbronn's, bears very little resemblance to the original draft.

We have borrowed freely from the other books which are catalogued on pp. 417–19 [pp. 596–9 in current 6th edn.], and especially from those of Landau and Perron. To Landau in particular we, in common with all serious students of the theory of numbers, owe a debt which we could hardly overstate.

G. H. H.
E. M. W.

OXFORD
August 1938

REMARKS ON NOTATION

We borrow four symbols from formal logic, viz.

$$\rightarrow, \equiv, \exists, \in .$$

$\rightarrow$ is to be read as 'implies'. Thus

$$l \mid m \rightarrow l \mid n \quad \text{(p. 2)}$$

means ' "l is a divisor of m" implies "l is a divisor of n" ', or, what is the same thing, 'if l divides m then l divides n'; and

$$b \mid a \,.\, c \mid b \rightarrow c \mid a \quad \text{(p. 1)}$$

means 'if b divides a and c divides b then c divides a'.

$\equiv$ is to be read 'is equivalent to'. Thus

$$m \mid ka - ka' \equiv m_1 \mid a - a' \quad \text{(p. 61)}$$

means that the assertions 'm divides ka—ka'' and 'm_1 divides a—a'' are equivalent; either implies the other.

These two symbols must be distinguished carefully from $\to$ (tends to) and $\equiv$ (is congruent to). There can hardly be any misunderstanding, since $\rightarrow$ and $\equiv$ are always relations between *propositions*.

$\exists$ is to be read as 'there is an'. Thus

$$\exists l \,.\, 1 < l < m \,.\, l \mid m \quad \text{(p. 2)}$$

means 'there is an l such that (i) $1 < l < m$ and (ii) l divides m'.

$\in$ is the relation of a member of a class to the class. Thus

$$m \in S \,.\, n \in S \rightarrow (m \pm n) \in S \quad \text{(p. 23)}$$

means 'if m and n are members of S then $m + n$ and $m - n$ are members of S'.

A star affixed to the number of a theorem (e.g. Theorem 15*) means that the proof of the theorem is too difficult to be included in the book. It is not affixed to theorems which are not proved but may be proved by arguments similar to those used in the text.

CONTENTS