

数学·统计学系列 39

An Introduction to the

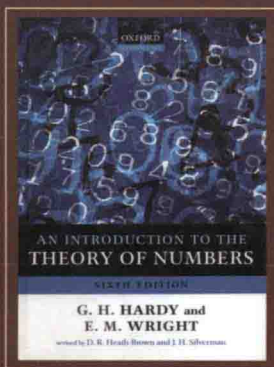
Theory of Numbers

哈代数论

(英文版·第6版)

[英] G. H. Hardy 著
E. M. Wright

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



人民邮电出版社
POSTS & TELECOM PRESS

An Introduction to the Theory of Numbers

哈代数论

(英文版·第6版)

“这本引人入胜的书对这一学科进行了生动、详尽的叙述，而且没有用到太多高深的理论。”

——*Mathematical Gazette* (数学公报)

“……一本非常重要的著作……它一定能继续保持长久、旺盛的生命力……”

——*Mathematical Reviews* (数学评论)

本书是数论领域的一部传世名著，也是现代数学大师哈代的代表作之一。书中从多个角度对数论进行了阐述，内容涉及素数、无理数、同余、费马定理、连分数、不定方程、二次域、算术函数、分划等。体现了哈代一贯的写作风格，深入浅出，娓娓道来。

新版与时俱进，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。

本书自出版以来一直备受学界推崇，被许多知名大学指定为教材或参考书，如牛津大学、麻省理工学院、斯坦福大学、加州大学伯克利分校等，具有深远的影响。

G. H. Hardy (1877–1947) 20世纪上半叶享有世界声誉的数学大师，是英国数学界和英国分析学派的领袖，对数论和分析学的发展有巨大的贡献和重大的影响。除了自己的研究工作之外，他还培养和指导了众多数学大家，包括印度数学奇才拉马努金和我国数学家华罗庚。

E. M. Wright (1906–2005) 英国著名数学家，毕业于牛津大学，是G. H. Hardy的学生。生前担任英国名校阿伯丁大学校长多年。爱丁堡皇家学会会士、伦敦数学会会士。曾任 *Journal of Graph Theory* 和 *Zentralblatt für Mathematik* 的名誉主编。



本书相关信息请访问：图灵网站 <http://www.turingbook.com>

读者/作者热线：(010)51095186

反馈/投稿/推荐信箱：contact@turingbook.com

分类建议：数学/基础数学

人民邮电出版社网址 www.ptpress.com.cn

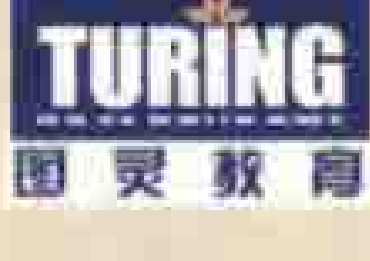
ISBN 978-7-115-21427-0



9 787115 214270 >

ISBN 978-7-115-21427-0

定价：59.00元



图灵教育

TOMS

39

哈 代 数 论

英文版

第6版

〔英〕

G. H. Hardy

著

E. M. Wright

〔英〕

D. R. Heath-Brown

修订

〔美〕

J. H. Silverman



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 著
E. M. Wright

[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

试读结束: 需要全本请在线购买: www.ertongbook.com

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 our personal interests to decide our 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 \rightarrow (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

I.	THE SERIES OF PRIMES (1)	1
1.1.	Divisibility of integers	1
1.2.	Prime numbers	2
1.3.	Statement of the fundamental theorem of arithmetic	3
1.4.	The sequence of primes	4
1.5.	Some questions concerning primes	6
1.6.	Some notations	7
1.7.	The logarithmic function	9
1.8.	Statement of the prime number theorem	10
II.	THE SERIES OF PRIMES (2)	14
2.1.	First proof of Euclid's second theorem	14
2.2.	Further deductions from Euclid's argument	14
2.3.	Primes in certain arithmetical progressions	15
2.4.	Second proof of Euclid's theorem	17
2.5.	Fermat's and Mersenne's numbers	18
2.6.	Third proof of Euclid's theorem	20
2.7.	Further results on formulae for primes	21
2.8.	Unsolved problems concerning primes	23
2.9.	Moduli of integers	23
2.10.	Proof of the fundamental theorem of arithmetic	25
2.11.	Another proof of the fundamental theorem	26
III.	FAREY SERIES AND A THEOREM OF MINKOWSKI	28
3.1.	The definition and simplest properties of a Farey series	28
3.2.	The equivalence of the two characteristic properties	29
3.3.	First proof of Theorems 28 and 29	30
3.4.	Second proof of the theorems	31
3.5.	The integral lattice	32
3.6.	Some simple properties of the fundamental lattice	33
3.7.	Third proof of Theorems 28 and 29	35
3.8.	The Farey dissection of the continuum	36
3.9.	A theorem of Minkowski	37
3.10.	Proof of Minkowski's theorem	39
3.11.	Developments of Theorem 37	40

CONTENTS

	11
IV. IRRATIONAL NUMBERS	45
4.1. Some generalities	45
4.2. Numbers known to be irrational	46
4.3. The theorem of Pythagoras and its generalizations	47
4.4. The use of the fundamental theorem in the proofs of Theorems 43–45	49
4.5. A historical digression	50
4.6. Geometrical proof of the irrationality of $\sqrt{5}$	52
4.7. Some more irrational numbers	53
V. CONGRUENCES AND RESIDUES	57
5.1. Highest common divisor and least common multiple	57
5.2. Congruences and classes of residues	58
5.3. Elementary properties of congruences	60
5.4. Linear congruences	60
5.5. Euler's function $\phi(m)$	63
5.6. Applications of Theorems 59 and 61 to trigonometrical sums	65
5.7. A general principle	70
5.8. Construction of the regular polygon of 17 sides	71
VI. FERMAT'S THEOREM AND ITS CONSEQUENCES	78
6.1. Fermat's theorem	78
6.2. Some properties of binomial coefficients	79
6.3. A second proof of Theorem 72	81
6.4. Proof of Theorem 22	82
6.5. Quadratic residues	83
6.6. Special cases of Theorem 79: Wilson's theorem	85
6.7. Elementary properties of quadratic residues and non-residues	87
6.8. The order of $a \pmod{m}$	88
6.9. The converse of Fermat's theorem	89
6.10. Divisibility of $2^{p-1} - 1$ by p^2	91
6.11. Gauss's lemma and the quadratic character of 2	92
6.12. The law of reciprocity	95
6.13. Proof of the law of reciprocity	97
6.14. Tests for primality	98
6.15. Factors of Mersenne numbers; a theorem of Euler	100
VII. GENERAL PROPERTIES OF CONGRUENCES	103
7.1. Roots of congruences	103
7.2. Integral polynomials and identical congruences	103
7.3. Divisibility of polynomials \pmod{m}	105
7.4. Roots of congruences to a prime modulus	106
7.5. Some applications of the general theorems	108

7.6.	Lagrange's proof of Fermat's and Wilson's theorems	110
7.7.	The residue of $\{\frac{1}{2}(p-1)!\}$	111
7.8.	A theorem of Wolstenholme	112
7.9.	The theorem of von Staudt	115
7.10.	Proof of von Staudt's theorem	116
VIII.	CONGRUENCES TO COMPOSITE MODULI	120
8.1.	Linear congruences	120
8.2.	Congruences of higher degree	122
8.3.	Congruences to a prime-power modulus	123
8.4.	Examples	125
8.5.	Bauer's identical congruence	126
8.6.	Bauer's congruence: the case $p=2$	129
8.7.	A theorem of Leudesdorf	130
8.8.	Further consequences of Bauer's theorem	132
8.9.	The residues of 2^{p-1} and $(p-1)!$ to modulus p^2	135
IX.	THE REPRESENTATION OF NUMBERS BY DECIMALS	138
9.1.	The decimal associated with a given number	138
9.2.	Terminating and recurring decimals	141
9.3.	Representation of numbers in other scales	144
9.4.	Irrationals defined by decimals	145
9.5.	Tests for divisibility	146
9.6.	Decimals with the maximum period	147
9.7.	Bachet's problem of the weights	149
9.8.	The game of Nim	151
9.9.	Integers with missing digits	154
9.10.	Sets of measure zero	155
9.11.	Decimals with missing digits	157
9.12.	Normal numbers	158
9.13.	Proof that almost all numbers are normal	160
X.	CONTINUED FRACTIONS	165
10.1.	Finite continued fractions	165
10.2.	Convergents to a continued fraction	166
10.3.	Continued fractions with positive quotients	168
10.4.	Simple continued fractions	169
10.5.	The representation of an irreducible rational fraction by a simple continued fraction	170
10.6.	The continued fraction algorithm and Euclid's algorithm	172
10.7.	The difference between the fraction and its convergents	175
10.8.	Infinite simple continued fractions	177

10.9.	The representation of an irrational number by an infinite continued fraction	178
10.10.	A lemma	180
10.11.	Equivalent numbers	181
10.12.	Periodic continued fractions	184
10.13.	Some special quadratic surds	187
10.14.	The series of Fibonacci and Lucas	190
10.15.	Approximation by convergents	194
XI.	APPROXIMATION OF IRRATIONALS BY RATIONALS	198
11.1.	Statement of the problem	198
11.2.	Generalities concerning the problem	199
11.3.	An argument of Dirichlet	201
11.4.	Orders of approximation	202
11.5.	Algebraic and transcendental numbers	203
11.6.	The existence of transcendental numbers	205
11.7.	Liouville's theorem and the construction of transcendental numbers	206
11.8.	The measure of the closest approximations to an arbitrary irrational	208
11.9.	Another theorem concerning the convergents to a continued fraction	210
11.10.	Continued fractions with bounded quotients	212
11.11.	Further theorems concerning approximation	216
11.12.	Simultaneous approximation	217
11.13.	The transcendence of e	218
11.14.	The transcendence of π	223
XII.	THE FUNDAMENTAL THEOREM OF ARITHMETIC IN $k(1)$, $k(i)$, AND $k(\rho)$	229
12.1.	Algebraic numbers and integers	229
12.2.	The rational integers, the Gaussian integers, and the integers of $k(\rho)$	230
12.3.	Euclid's algorithm	231
12.4.	Application of Euclid's algorithm to the fundamental theorem in $k(1)$	232
12.5.	Historical remarks on Euclid's algorithm and the fundamental theorem	234
12.6.	Properties of the Gaussian integers	235
12.7.	Primes in $k(i)$	236
12.8.	The fundamental theorem of arithmetic in $k(i)$	238
12.9.	The integers of $k(\rho)$	241
XIII.	SOME DIOPHANTINE EQUATIONS	245
13.1.	Fermat's last theorem	245
13.2.	The equation $x^2 + y^2 = z^2$	245
13.3.	The equation $x^4 + y^4 = z^4$	247
13.4.	The equation $x^3 + y^3 = z^3$	248

13.5.	The equation $x^3+y^3=3z^3$	253
13.6.	The expression of a rational as a sum of rational cubes	254
13.7.	The equation $x^3+y^3+z^3=t^3$	257
XIV.	QUADRATIC FIELDS (1)	264
14.1.	Algebraic fields	264
14.2.	Algebraic numbers and integers; primitive polynomials	265
14.3.	The general quadratic field $k(\sqrt{m})$	267
14.4.	Unities and primes	268
14.5.	The unities of $k(\sqrt{2})$	270
14.6.	Fields in which the fundamental theorem is false	273
14.7.	Complex Euclidean fields	274
14.8.	Real Euclidean fields	276
14.9.	Real Euclidean fields (<i>continued</i>)	279
XV.	QUADRATIC FIELDS (2)	283
15.1.	The primes of $k(i)$	283
15.2.	Fermat's theorem in $k(i)$	285
15.3.	The primes of $k(\rho)$	286
15.4.	The primes of $k(\sqrt{2})$ and $k(\sqrt{5})$	287
15.5.	Lucas's test for the primality of the Mersenne number M_{4n+3}	290
15.6.	General remarks on the arithmetic of quadratic fields	293
15.7.	Ideals in a quadratic field	295
15.8.	Other fields	299
XVI.	THE ARITHMETICAL FUNCTIONS $\phi(n), \mu(n), d(n), \sigma(n), r(n)$	302
16.1.	The function $\phi(n)$	302
16.2.	A further proof of Theorem 63	303
16.3.	The Möbius function	304
16.4.	The Möbius inversion formula	305
16.5.	Further inversion formulae	307
16.6.	Evaluation of Ramanujan's sum	308
16.7.	The functions $d(n)$ and $\sigma_k(n)$	310
16.8.	Perfect numbers	311
16.9.	The function $r(n)$	313
16.10.	Proof of the formula for $r(n)$	315
XVII.	GENERATING FUNCTIONS OF ARITHMETICAL FUNCTIONS	318
17.1.	The generation of arithmetical functions by means of Dirichlet series	318
17.2.	The zeta function	320
17.3.	The behaviour of $\zeta(s)$ when $s \rightarrow 1$	321
17.4.	Multiplication of Dirichlet series	323