国外数学名著系列

（影印版）79

Harold M. Edwards

Fermat's Last Theorem

A Genetic Introduction to Algebraic Number Theory

费马大定理

代数数论的原始导引

科 学 出 版 社

国外数学名著系列(影印版)　79

Fermat's Last Theorem

A Genetic Introduction to Algebraic Number Theory

费马大定理

代数数论的原始导引

Harold M. Edwards

科 学 出 版 社
北　京

图字：01-2011-3334

Harold M. Edwards: Fermat's Last Theorem: A Genetic Introduction to Algeberaic Number Theory
© Springer-Verlag Berlin Heidelberg 1977

图书在版编目 (CIP) 数据

费马大定理：代数数论的原始导引= Fermat's Last Theorem: A Genetic Introduction to Algeberaic Number Theory /（美）爱德华兹(Edwards, H. M.) 编著. —影印版. —北京：科学出版社, 2011

(国外数学名著系列; 79)

ISBN 978-7-03-031384-3

I. ①费… II. ①爱… III. ①费马大定理-英文 IV. ①O156

中国版本图书馆 CIP 数据核字(2011) 第 105010 号

责任编辑:赵彦超 徐园园/责任印刷:钱玉芬/封面设计:陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com
北京佳信达欣艺术印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2011 年 6 月第 一 版 开本：B5(720 × 1000)
2011 年 6 月第一次印刷 印张：27
印数: 1—2 000 字数：520 000

定价：68.00 元

(如有印装质量问题，我社负责调换)

《国外数学名著系列》(影印版)序

要使我国的数学事业更好地发展起来，需要数学家淡泊名利并付出更艰苦地努力。另一方面，我们也要从客观上为数学家创造更有利的发展数学事业的外部环境，这主要是加强对数学事业的支持与投资力度，使数学家有较好的工作与生活条件，其中也包括改善与加强数学的出版工作。

从出版方面来讲，除了较好较快地出版我们自己的成果外，引进国外的先进出版物无疑也是十分重要与必不可少的。从数学来说，施普林格(Springer)出版社至今仍然是世界上最具权威的出版社。科学出版社影印一批他们出版的好的新书，使我国广大数学家能以较低的价格购买，特别是在边远地区工作的数学家能普遍见到这些书，无疑是对推动我国数学的科研与教学十分有益的事。

这次科学出版社购买了版权，一次影印了23本施普林格出版社出版的数学书，就是一件好事，也是值得继续做下去的事情。大体上分一下，这23本书中，包括基础数学书5本，应用数学书6本与计算数学书12本，其中有些书也具有交叉性质。 这些书都是很新的，2000年以后出版的占绝大部分，共计16本，其余的也是1990年以后出版的。这些书可以使读者较快地了解数学某方面的前沿，例如基础数学中的数论、代数与拓扑三本，都是由该领域大数学家编著的“数学百科全书”的分册。对从事这方面研究的数学家了解该领域的前沿与全貌很有帮助。按照学科的特点，基础数学类的书以“经典”为主，应用和计算数学类的书以“前沿”为主。这些书的作者多数是国际知名的大数学家，例如《拓扑学》一书的作者诺维科夫是俄罗斯科学院的院士，曾获“菲尔兹奖”和“沃尔夫数学奖”。这些大数学家的著作无疑将会对我国的科研人员起到非常好的指导作用。

当然，23本书只能涵盖数学的一部分，所以，这项工作还应该继续做下去。更进一步，有些读者面较广的好书还应该翻译成中文出版，使之有更大的读者群。

总之，我对科学出版社影印施普林格出版社的部分数学著作这一举措表示热烈的支持，并盼望这一工作取得更大的成绩。

王　元

2005年12月3日

Preface

Since it is likely that many people will open this book wanting to know what the current state of knowledge about Fermat's Last Theorem is, and since the book itself will not answer this question, perhaps the preface should contain a few indications on the subject. Fermat's Last Theorem is of course the assertion (not a theorem) that the equation $x^n + y^n = z^n$ has no solution in positive whole numbers when $n > 2$. It is elementary (see Section 1.5) to prove that $x^4 + y^4 = z^4$ is impossible. Therefore the original equation is impossible whenever n is divisible by 4. (If $n = 4k$ then $x^n + y^n = z^n$ would imply the impossible equation $X^4 + Y^4 = Z^4$ where $X = x^k$, $Y = y^k$, and $Z = z^k$.) Similarly, if $x^m + y^m = z^m$ can be proved to be impossible for any particular m, it will follow that the original equation is impossible for any n that is divisible by m. Since every $n > 2$ is divisible either by 4 or by an odd prime, *in order to prove Fermat's Last Theorem it will suffice to prove it in the cases where the exponent n is a prime.*

For the exponent 3, the theorem is not too difficult to prove (see Chapter 2). For the exponents 5 and 7 the difficulties are greater (Sections 3.3 and 3.4), but the theorem can be proved by essentially elementary methods. The main topic of this book is the powerful theory of ideal factorization which Kummer developed in the 1840s and used to prove the theorem at one stroke for all prime exponents less than 100 other than 37, 59, and 67. Specifically, Kummer's theorem states: *Let p be an odd prime. A sufficient condition for Fermat's Last Theorem to be true for the exponent p is that p not divide the numerators of the Bernoulli numbers* $B_2, B_4, \ldots, B_{p-3}$. (See Sections 5.5 and 6.19.) A prime which satisfies Kummer's sufficient condition is called "regular."

Since 1850, work on the theorem has centered on proving more and more inclusive sufficient conditions. In one sense the best known sufficient conditions are now very inclusive, and in another sense they are very disappointing. The sense in which they are inclusive is that *they include all primes less than* 100,000 [W1]. The sense in which they are disappointing is that *no sufficient condition for Fermat's Last Theorem has ever been shown to include an infinite set of prime exponents*. Thus one is in the position of being able to prove Fermat's Last Theorem for virtually any prime within computational range, but one cannot rule out the possibility that the Theorem is *false* for *all* primes beyond some large bound.

The basic method of the book is, as the subtitle indicates, the genetic method. The dictionary defines the genetic method as "the explanation or evaluation of a thing or event in terms of its origin and development." In this book I have attempted to explain the basic techniques and concepts of the theory, and to make them seem natural, manageable, and effective, by tracing their origin and development in the works of some of the great masters—Fermat, Euler, Lagrange, Legendre, Gauss, Dirichlet, Kummer, and others.

It is important to distinguish the genetic method from history. The distinction lies in the fact that the genetic method primarily concerns itself with the subject—its "explanation or evaluation" in the definition above—whereas the primary concern of history is an accurate record of the men, ideas, and events which played a part in the evolution of the subject. In a history there is no place for detailed descriptions of the theory unless it is essential to an understanding of the events. In the genetic method there is no place for a careful study of the events unless it contributes to the appreciation of the subject.

This means that the genetic method tends to present the historical record from a false perspective. Questions which were never successfully resolved are ignored. Ideas which led into blind alleys are not pursued. Months of fruitless effort are passed over in silence and mountains of exploratory calculations are dispensed with. In order to get to the really fruitful ideas, one pretends that human reason moves in straight lines from problems to solutions. I want to emphasize as strongly as I can that this notion that reason moves in straight lines is an outrageous fiction which should not for a moment be taken seriously.

Samuel Johnson once said of the writing of biography that "If nothing but the bright side of characters should be shown, we should sit down in despondency, and think it utterly impossible to imitate them in anything. The sacred writers related the vicious as well as the virtuous actions of men; which had this moral effect, that it kept mankind from despair." This book does, for the most part, show only the bright side, only the ideas that work, only the guesses that are correct. You should bear in mind that this is *not* a history or biography and you should not despair.

You may well be interested less in the contrast between history and the genetic method than in the contrast between the genetic method and the more usual method of mathematical exposition. As the mathematician

Otto Toeplitz described it, the essence of the genetic method is to look to the historical origins of an idea in order to find the best way to motivate it, to study the context in which the originator of the idea was working in order to find the "burning question" which he was striving to answer [T1]. In contrast to this, the more usual method pays no attention to the questions and presents only the answers. From a logical point of view only the answers are needed, but from a psychological point of view, learning the answers without knowing the questions is so difficult that it is almost impossible. That, at any rate, is my own experience. I have found that the best way to overcome the difficulty of learning an abstract mathematical theory is to follow Toeplitz's advice and to ignore the modern treatises until I have studied the genesis in order to learn the questions.

The first three chapters of the book deal with elementary aspects of the question of Fermat's Last Theorem. They are written at a much more elementary level than the rest of the book. I hope that the reader who already has the mathematical maturity to read the later chapters will still find these first three chapters interesting and worthwhile, if easy, reading. At the same time, I hope that the less experienced reader who must work his way more gradually through the first chapters will in the course of that reading acquire enough experience to enable him, with effort, to make his way through the later chapters as well.

The next three chapters, Chapters 4–6, are devoted to the development of Kummer's theory of ideal factors and its application to prove his famous theorem, stated above, that Fermat's Last Theorem is true for regular prime exponents. This is as far as the present book takes the study of Fermat's Last Theorem. I plan to write a second volume to deal with work on Fermat's Last Theorem which goes beyond Kummer's theorem, but these later developments are difficult, and Kummer's theorem is a very natural point at which to end this volume.

The final three chapters deal with matters less directly related to Fermat's Last Theorem, namely, the theory of ideal factorization for quadratic integers, Gauss's theory of binary quadratic forms, and Dirichlet's class number formula. To study Kummer's work on Fermat's Last Theorem without studying these other aspects of number theory would be as foolish as to study the history of Germany without studying the history of France. Kummer was aware at the very outset of his work on ideal theory that it was closely related to Gauss's theory of binary quadratic forms. While the application to Fermat's Last Theorem was one of Kummer's motives for developing the theory, others (and by his own testimony more immediate ones) were the quest for the generalization of quadratic, cubic, and biquadratic reciprocity laws to higher powers, and the explication of Gauss's difficult theory of composition of forms. Moreover, Kummer's amazingly rapid development of his class number formula and his discovery of the striking relationship between Fermat's Last Theorem for the exponent p and the Bernoulli numbers mod p, were, as he says, made possible by Dirichlet's solution of the analogous problem in the quadratic case. The genetic method suggests—almost demands—that these other issues be exploited in motivating the difficult but enormously fruitful idea of "ideal prime factors" that is so essential to an understanding of Kummer's work on Fermat's Last Theorem. Moreover, the material of these final three chapters provides a necessary background for the study of the higher reciprocity laws and class field theory which, in turn, are the context of the later work on Fermat's Last Theorem to be studied in the second volume.

In this book there is a good deal of emphasis, both in the text and in the exercises, on *computation*. This is a natural concomitant of the genetic method because, as even a superficial glance at history shows, Kummer and the other great innovators in number theory did vast amounts of computation and gained much of their insight in this way. I deplore the fact that contemporary mathematical education tends to give students the idea that computation is demeaning drudgery to be avoided at all costs. If you follow the computations of the text attentively and if you regard the more computational exercises not only as time-consuming (which they will inevitably be) but also as challenging, enjoyable, and enlightening, then I believe you can come to appreciate both the power and the ultimate simplicity of the theory.

I believe that there is no such thing as a passive understanding of mathematics. It is only in actively lecturing, writing, or solving problems that one can achieve a thorough grasp of mathematical ideas. This is the reason that the book contains so many exercises and the reason that I suggest that the serious reader do as many of them as he can. Some of my colleagues have suggested that by including so many exercises I will deter readers who want to read the book merely for the fun of it. To this I reply that the exercises are offered, they are not assigned. Do with them what you will, but you might in fact find that they can be fun too.

A famous prize for the proof of Fermat's Last Theorem was established by P. Wolfskehl in 1908. One of the conditions of the prize is that the proof must appear in print, and the primary result of the offer of the prize seems to have been a plague of nonsense proofs being submitted for publication and being published privately. It was with obvious satisfaction that Mordell and other number theorists announced that the post-World War I inflation in Germany had reduced the originally munificient prize to almost nothing. However, the economic recovery of Germany after World War II has reversed this situation to some extent. The Wolfskehl prize is at the present time worth about 10,000 DM or 4,000 American dollars. In order to win the prize, a proof must be published and must be judged to be correct, no sooner than two years after publication, by the Academy of Sciences in Gottingen.

If you are inclined to try to win the prize, you have my best wishes. I would be truly delighted if the problem were solved, and especially so if the solver had found my book useful. Although it might be argued that a book full of ideas that *haven't* worked couldn't possibly be of any use to someone hoping to solve the problem, I think that the unsuccessful efforts of so many first-rate mathematicians—not to mention many not-so-first-rate ones—are enough to render a naive approach to the problem completely hopeless. The ideas in this book *do* solve the problem for all exponents less than 37, which is more than can be said of any approach to the problem which does not use Kummer's theory of ideal factorization. But before you set out to win the Wolfskehl prize there is one further fact which you should take into account: there seems to me to be no reason at all to assume that Fermat's Last Theorem is true, but the prize does not offer a single *pfennig* for a disproof of the theorem.

Note added in the fifth printing

The Annals of Mathematics for May, 1995, contains a proof of Fermat's last theorem by Andrew Wiles of Princeton University, which, in all probability, will receive the Wolfskehl prize once the requisite two years have elapsed. This great achievement, which has been celebrated by scholars and the general public all over the world, will probably enhance rather than end interest in the topic. Not surprisingly, Wiles's proof uses very sophisticated modern concepts that could not possibly have been used by Fermat. We now know that Fermat's last theorem is true, but whether Fermat himself could prove it is still unresolved. The quest for a proof that might have been accessible to Fermat will surely continue.

Acknowledgments

Merely to say that work on this book was supported by a grant from the Vaughn Foundation would give a very inadequate notion of the extent of my indebtedness to the Foundation and to Mr. James M. Vaughn, Jr. Without their invitation for proposals related to Fermat's Last Theorem, I would never have conceived of this book, let alone written it. I am profoundly grateful to Mr. Vaughn and to the Foundation for involving me in what has been an extremely stimulating, enlightening, and enjoyable project.

I would also like to thank Bruce Chandler for his friendly encouragement and for his wise counsel. Bruce's Seminar on the History of Mathematical Sciences at NYU has been a meeting place for historians of mathematics which I and many others have found to be enormously useful and inspiring.

In addition, I am grateful to many scholars for comments on the manuscript. In particular I would like to mention John Brillhart, Ed Curtis, Pierre Dugac, J. M. Gandhi, Lynette Ganim, Paul Halmos, Jean Itard, Walter Kaufmann-Bühler, Morris Kline, Carlos Moreno, Al Novikoff, Harold Shapiro, Gabriel Stolzenberg, James Vaughn, and André Weil.

Finally, I am grateful to the Courant Institute of Mathematical Sciences here at NYU for providing a good place to work, an excellent library, and the superb typing services of Helen Samoraj and her staff.

April 1977
New York City

Harold M. Edwards

Contents

Fermat 1

1.1 Fermat and his "Last Theorem"

When Pierre de Fermat died in 1665 he was one of the most famous mathematicians in Europe. Today Fermat's name is almost synonymous with number theory, but in his own time his work in number theory was so revolutionary and so much ahead of its time that its value was poorly understood and his fame rested much more on his contributions in other fields. These included important work in analytic geometry—which he invented independently of Descartes—in the theory of tangents, quadrature, and maxima and minima—which were the beginning of calculus—and in mathematical optics—which he enriched with the discovery that the law of refraction can be derived from the principle of least time.

There are two surprising facts about Fermat's fame as a mathematician. The first is that he was not a mathematician at all, but a jurist. Throughout his mature life he held rather important judicial positions in Toulouse, and his mathematical work was done as an avocation. The second is that he never published a single* mathematical work. His reputation grew out of his correspondence with other scholars and out of a number of treatises which circulated in manuscript form. Fermat was frequently urged to publish his work, but for unexplained reasons he refused to allow his treatises to be published and many of his discoveries—particularly his discoveries in number theory—were never put in publishable form.

This fact that Fermat refused to publish his work caused his many admirers to fear that he would soon be forgotten if an effort weren't made to collect his letters and unpublished treatises and to publish them posthumously. The task was undertaken by his son, Samuel. In addition to

*There is one slight exception. He did allow a minor work to be published in 1660 as an appendix to a book written by a colleague. However, it is an exception which proves the rule: it was published anonymously.

soliciting letters and treatises from his father's correspondents, Samuel de Fermat went through his father's own papers and books, and it was in this way that Fermat's famous "Last Theorem" came to be published.

Diophantus' *Arithmetic*, one of the great classics of ancient Greek mathematics which had been rediscovered and translated into Latin shortly before Fermat's time, was the book which had originally inspired Fermat's study of the theory of numbers. Samuel found that his father had made a number of notes in the margins of his copy of Bachet's translation of Diophantus, and as a first step in publishing his father's works he published a new edition of Bachet's Diophantus [D3] which included Fermat's marginal notes as an appendix. The second of these 48 "Observations on Diophantus" was written in the margin next to Diophantus' problem 8 in Book II which asks "given a number which is a square, write it as a sum of two other squares." Fermat's note states, in Latin, that "On the other hand, it is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as a sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers. I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain." This simple statement, which can be written in symbols as "for any integer $n > 2$ the equation $x^n + y^n = z^n$ is impossible" is now known as *Fermat's Last Theorem*. If Fermat did indeed have a demonstration of it, it was truly "marvelous," because no one else has been able to find a demonstration of it in the three hundred and more years since Fermat's time. It is a problem that many great mathematicians have tried unsuccessfully to solve, although sufficient progress has been made to prove Fermat's assertion for all exponents n well up into the thousands. To this date it is unknown whether the assertion is true or false.

The origin of the name "Fermat's Last Theorem" is obscure. It is not known at what time in his life Fermat wrote this marginal note, but it is usually assumed that he wrote it during the period when he was first studying Diophantus' book, in the late 1630s, three decades before his death, and in this case it surely was not his last theorem. Very possibly the name stems from the fact that of the many unproved theorems that Fermat stated, this is the last one which remains unproved. It is perhaps worth considering that Fermat may have thought better of his "marvelous proof," especially if he did write of it in the 1630s, because his other theorems are stated and restated in letters and in challenge problems to other mathematicians—and the special cases $x^3 + y^3 \neq z^3$, $x^4 + y^4 \neq z^4$ of the Last Theorem are also stated elsewhere—whereas this theorem occurs just once, as observation number 2 on Diophantus, a sphinx to mystify posterity.

Since the *Arithmetic* of Diophantus deals exclusively with rational numbers, it goes without saying that Fermat meant that there are no *rational* numbers x, y, z such that $x^n + y^n = z^n$ $(n > 2)$. If irrational