现代数学基础

12 数论 I

——Fermat 的梦想和类域论

■ 加藤和也　黑川信重　斎藤毅　著

■ 胥鸣伟　印林生　译

高等教育出版社
HIGHER EDUCATION PRESS

12 数论 I

—— Fermat 的梦想和类域论

高等教育出版社
HIGHER EDUCATION PRESS

图字：01-2009-1457 号

数論 I —— Fermat の夢と類体論
加藤和也，黒川信重，斎藤毅

SURON, I: FERMAT NO YUME TO RUITAIRON
by Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito

Originally published in Japanese by Iwanami Shoten, Publishers, Tokyo, 2005.
This simplified Chinese language edition published in 2009
by the Higher Education Press, Beijing
by arrangement with the proprietor c/o Iwanami Shoten, Publishers, Tokyo

图书在版编目（CIP）数据

数论．1，Fermat 的梦想和类域论/（日）加藤和也，（日）黑川信重，（日）斋藤毅著；胥鸣伟，印林生译．—北京：高等教育出版社，2009.6
ISBN 978-7-04-026360-2

Ⅰ.数… Ⅱ.①加…②黑…③斋…④胥…⑤印… Ⅲ.数论 Ⅳ.O156

中国版本图书馆 CIP 数据核字（2009）第 042791 号

策划编辑 赵天夫　责任编辑 蒋　青　封面设计 张　楠　责任绘图 尹文军
版式设计 余　杨　责任校对 王　超　责任印制 朱学忠

出版发行	高等教育出版社	购书热线	010-58581118
社　址	北京市西城区德外大街 4 号	免费咨询	400-810-0598
邮政编码	100120	网　址	http://www.hep.edu.cn
总　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　刷	北京新丰印刷厂	畅想教育	http://www.widedu.com
开　本	787×1092　1/16	版　次	2009 年 6 月第 1 版
印　张	21.75	印　次	2009 年 6 月第 1 次印刷
字　数	450 000	定　价	39.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　26360-00

内 容 提 要

本书起点低, 但内容丰富, 包括了现代数论的基本知识, 如: 椭圆曲线、p 进数、代数数域、局部–整体方法等。该书的主要目标是证明数论的顶峰之一: 类域论。在以往的数论书籍中, 代数数论、椭圆曲线、类域论是分开的三本书, 但本书在有限的篇幅内, 将三者巧妙地融为一体, 使读者能很快地达到数论的一个顶峰。开篇通过介绍 Fermat 的工作, 给出了现代数论的一些定理的背景和意义。对于初学者难以掌握的类域论, 专门有一章介绍类域论的背景和主要定理的意义。类域论的主要定理通过应用 ζ 函数计算 Brauer 群而得到证明。本书的另一特点是先承认一些结论, 然后推导出一些进一步的结果, 而将它们的证明放在一起一个一个地进行。

本书的第零章通过介绍 Fermat 的工作和结果, 从而窥见丰富的、深奥的数的世界。第一章以 Fermat 的工作为起点, 介绍椭圆曲线的基本知识。第二章介绍 p 进数及二次曲线的 Hasse 原理。第三章介绍了 ζ 函数在整点的特殊值。这几章适合于仅知道群、环、域概念的低年级本科生。后面几章关于代数数论和类域论的内容适合于高年级本科生和研究生学习。

中文版序言

我们非常高兴看到我们的日文著作《数论》的中文版。我们十分感谢译者、编辑和出版者。

希望本书的中译本能吸引更多的中国读者探索数的奥妙，并进一步促进日中的学术交流。

全体作者代表
斋藤毅
2009 年 4 月

前　言

在本书出版的 1996 年前的 200 年, 即 1796 年, Gauss 将现代数论大大地向前推进了一步, 这距今实在是有些年头了。当时正值十几岁年龄段最后一年的 Gauss, 在是年的 3 月 30 日, 发现了正十七边形的作图法, 4 月 8 日又证明了被 Gauss 自己称为 "瑰宝" 的 "二次剩余互反律" (参看本书的 §2.2), 5 月 31 日则提出了关于素数分布的 "素数定理" 的猜想, 7 月 10 日又证明了所有自然数可表示为不多于三个的三角数之和 (参看本书的 §0.5), 到了 10 月 1 日则得到了对以后年代产生极大影响的关于有限域系数的方程的解的个数的结果, 等等许多的研究。所有这些都写在了《数论 I》及后续的《数论 II》中。

在由简单地列举 $1, 2, 3, 4, \cdots$ 而数出来的数世界里, 隐藏着许多使得年轻的 Gauss 着迷的奇特东西, 而一个时代的发现呼唤出下一个时代的更为深刻的发现。100 年后的 1896 年, 上述的素数定理得到了证明, 大约 120 年后, 二次剩余互反律在 "类域论" 中得到了发展, 大约 150 年后,Weil 在考察了上述 10 月 1 日的 Gauss 的结果后, 提出了对于 20 世纪的代数几何给予极大影响的 Weil 猜想。Gauss 所琢磨过的瑰宝经后来人们的琢磨更增添了光彩。即便在声称地球的秘境几乎已探索穷尽了的现代, 在数的世界里所充满的谜还远未被探索清楚, 使我们感到我们所有的并非是一个浅底的自然界, 而是显示出她的无限丰厚。

在本书中, 我们不仅重视数所具有的奇特性质, 而且也在探索现代的数论, 想要描绘出在它的深处的丰富多彩的世界。由于作者们才疏学浅, 有许多力所不能及之处, 如果读者们只要能因此而感受到数的不可思议之处, 以及自然界的丰富多彩, 我们就颇感荣幸了。

加藤和也, 黑川信重, 斋藤毅

1996 年 8 月

写在单行本发行之际

本书是将岩波讲座 “现代数学基础” 的《数论 1》、《数论 2》、《数论 3》中的《数论 1》和《数论 2》合成一卷改版而成的。作者们的意图及愿望在前版的《数论 1》开篇的 “前言” 中已经阐明, 故将该 “前言” 再录于此。主要修改的是 “附录 §C 素数的威力”, 补充了关于考虑局部域的好处。在本书中, 包含了作为现代整数理论核心的 “代数数论” 以及 “类域论”。在这本《数论 I》中没有包含 “岩泽 (Iwasawa) 理论” 和 “自守形式理论”, 对于它们请阅读本书的续篇《数论 II》(其前身是岩波讲座 “现代数学基础” 的《数论 3》), 如能那样, 我们将深感荣幸。

作者记识

2004 年 10 月 8 日

理论的概要及目标

讲讲本书的构成。

数论的基本点在于, 与数所具有的奇特性质相对照的, 竟是令人吃惊的简单和朴素。因为数的这种奇特性质在被称做现代数论鼻祖的 Fermat 的工作中已很好地表现出来了, 所以我们首先在第零章里介绍 Fermat 在数论方面的有关工作。能否清楚知道在 Fermat 所发现的每一个事实的背后究竟潜藏着怎样的世界, 请读者在以后的各章中去寻找答案吧。在第零章之后, 是现代数论中重要的对象。讲解了椭圆曲线 (第一章)、p 进数 (第二章和第六章), ζ 函数 (第三章和第七章)、数域 (第四章和第六章)、类域论 (第五章和第八章)。我们把同一个主题分成两章来讲, 在前一章中从易于接近之处着手而直奔其主题的核心, 后一章则进行全面的讲解, 这便是我们这样做的意图。譬如, 就类域论的理论而言, 我们以为按第八章那样的叙述是最完善的, 但要说起容易理解还要数第五章最为完善。在第一章中讲解了椭圆曲线, 就是说, 引进了在现代数论中越来越具重要性的数论的代数几何方向。由于从第一章到第四章能相当独立地进行阅读 (即非不懂前一章便读不了后一章, 也不是后面的章节比起前面的更不容易懂), 那么请从你认为容易读的地方开始读吧。

我们所讨论的许多重要的对象, 因实际可书写的篇幅不足, 许多只能忍痛割爱了。我们也不能叙述关于所见到的最新进展 "Diophantus 逼近论"、"超越数论" 了。

作为本卷的续篇的《数论 II》讲述了岩泽理论, 自守形式理论。另外, 丛书 "现代数学入门" 中的山本芳彦著的《数论入门》(岩波书店, 2003) 和本书合起来读的话, 我们认为可以补充本书的不足。

为了阅读本书, 作为预备知识希望读者掌握群、环、域的基础知识。对于在第四章中使用的 Dedekind 环理论我们在附录 §A 中有所概括。而在第五章及以后所用到的 Galois 理论, 则在附录 §B 中安排了 Galois 理论的一个概要。

建议读者实际地拿起笔和纸, 试着写下简单而质朴的例子。像在天文学中进行天文观测是重要的那样, 在数论中进行这样的 “观测” 也是重要的, 试着观测一下, 那么奇特的景象就搁在那里了。还有, 数论具有悠久的历史, 从历史中大有可学之处, 建议读者也关心一下数论的历史。

数学记号与用语

在本书中使用下列记号.

$\mathbb{Z}$ 全体整数

$\mathbb{Q}$ 全体有理数

$\mathbb{R}$ 全体实数

$\mathbb{C}$ 全体复数

所谓环是指具有乘法单位元 (记为 1) 的环, 而环同态则将 1 变到 1.

对于环 A, 用 $A^\times$ 表示 A 的可逆元 (具有关于乘法逆元的元) 全体所构成的乘法群. 特别地, 在 A 为域的情形, $A^\times$ 为 0 以外的所有元构成的乘法群.

目　　录

数论 II 的内容

第零章　序 —— Fermat 和数论

350 多年来没有得到证明的 Fermat 大定理 (Fermat's last theorem)

"当 n 不小于 3 时, 不存在满足

$$x^n + y^n = z^n$$

的自然数 x, y, z"

却由 Wiles 在 1994 年 9 月所证明. Fermat 大定理是 Fermat(1601—1665) 于大约 1630 年在自己读的一本书的空白边上写下的, Fermat 在此写了 "对此我发现了令人惊叹的证明, 但由于这里的空白太小记不下来" 这样的话. 以后尽管经过许多人的努力, 一直也没有能给出它的证明.

在此序章中, 我们将集中关注被称作 "近代数论开创者" 的 Fermat, 回顾 Fermat 的有关数论方面的论述, 以及它们在后来的数论里是如何发展的, 而且在本书中还要谈及如何用现代数学方法来处理这些论述.

§0.1　Fermat 以前

Fermat 大定理被写在古代数学家 Diophantus 所著的书《数论》中讨论方程式 $x^2 + y^2 = z^2$ 的有理数解部分的空白边上. Fermat 试着去做把方程式的 2 次改为 3 次, 4 次, 5 次的情形.

方程式 $x^2 + y^2 = z^2$ 的自然数解有

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2, \quad 8^2 + 15^2 = 17^2$$

等等许多 (参照 §2.1). 因为这些自然数是按照三平方定理 (Pythagoras 定理) 形成如图 0.1 上的直角三角形的三条边的长度, 所以从古以来都对其重视有加. 在从近 4000

年以前的古巴比伦王国遗址出土的黏土板上, 写了许多满足这个方程 $x^2+y^2=z^2$ 的自然数, 如

$$119^2+120^2=169^2$$

等等. 这些是在 20 世纪中期被解读出来的. 想必写这些黏土板的人当初已经知道了找出这些 x,y,z 的方法了.

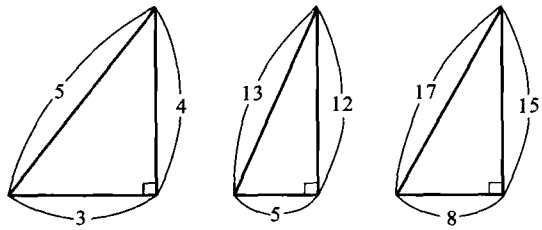

图 0.1 三平方定理 (Pythagoras 定理)

在古希腊, 出现了以被称为首先证明了三平方定理的 Pythagoras (公元前 6 世纪) 为首的许多卓越的数学家. Pythagoras 也被称为数论的鼻祖, 他强烈地感觉到数所具有的神秘性, 留下了 "万物皆数" 的话. Pythagoras 考察了音阶, 知道由具有漂亮的整数长度比的弦能产生出美妙的和声, 因而整数的比得到重视, 另一方面, 据说这时不是整数比的实数, 即无理数, 也开始被发现.

表现为整数比的数是有理数, 我们看到它们在由实数构成的数直线上没有空隙地满满地排列着, 但实际上却存在像 $\sqrt{5}$ 这样的不是有理数的实数. 这个事实用我们的肉眼难于判断, 而虽然只有经古希腊数学所得到的所谓 "证明" 方法之后才认知了这个事实, 但据说 Pythagoras 本人对于亲自证明了无理数存在这件事则深感惊恐, 因不知对此该如何解释而苦恼. (Pythagoras 把无理数存在这件事看成是神的失败, 从而禁止弟子们向外人说出此事, 据传说, 有破坏了禁令的弟子因冒犯神灵罪被乘船抛海而丧命.)

公元前 3 世纪左右写就的集古希腊数学之大成的 Euclid 的《几何原本》中, 关于数方面写了 "存在无限多个素数" 的证明以及关于最大公约数、最小公倍数等等 (《几何原本》全部 13 卷中的第 7 卷和第 9 卷) . 在《几何原本》中还谈及上述的无理数存在问题, 即关于 "以整数比 (有理数) 为出发点如何得出实数" 这样的问题, 从而展开了更高层次的实数理论的讨论 (《几何原本》第 5 卷). 这个使 Pythagoras 烦恼的, 而《几何原本》却讨论了很多的 "从有理数为出发点如何得出实数" 的问题, 在很远以后的 19 世纪才给出了完全的解答 (参看本书 §2.4) .

然而以 19 世纪所具有的实数理论还不足以给古希腊数学所提出的 "何为数" 的问题打上终止符. 到了 20 世纪, 用从有理数制造实数相近的方法, 在所有的素数 p, 人们以有理数为出发点给出了与实数世界完全不同的数的世界, 即 "p 进数的世界", 并且事实已证明 p 进数 (p-adic number) 世界跟实数一样的自然, 也是重要的数世

界. 有

$$\{p \text{ 进数}\} \supset \{\text{有理数}\} \subset \{\text{实数}\},$$

关于这种 p 进数我们将在第二章中讲解.

综合了古希腊数学流派的 3 世纪左右的数学家 Diophantus 写了叫做《数论》的书, 论述了关于方程式的有理数解问题. Diophantus 以后的数论到 Fermat 之前一直处在休眠状态. 由于在文艺复兴时代古希腊的自由精神活动受到高度重视, Diophantus 的《数论》被重新刻印, 从而使 Fermat 能阅读 Diophantus 的《数论》, 并受到激励, 研究起了数论.

Fermat 是法国图鲁兹地方的一个律师, 与 Descartes 同时独立地开创了用方程式来表示图形 (例如以方程式 $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$ 表示椭圆), 还用相近于微分法的思想去求函数的极大和极小, 从而得到了发现微分学的线索, 另一方面则在数论上留下了很大的业绩, 可以说他是 17 世纪前半叶最大的数学家.

下面介绍由 Fermat 发现并给出了证明的、与数相关的命题. 它们都或多或少地超越了古代的数学水平, 从而宣告了近代数论的诞生. Fermat 所写的证明几乎都没有流传下来, 但经过以后许多人的努力而成功地完成了对这些命题的证明. 这些命题是与方程的整数解和有理数解相关的一些命题. 初看起来, Fermat 的命题只是对各个相关方程的零星事实的罗列. 事实上, 与 Fermat 同时代的数学家们也都持有同样的看法.

然而, 像喜爱这些命题的 Fermat 大概也感觉到的那样, 考察方程的整数解或有理数解的许多问题都引导到数学的深处, 这些定理不过是深藏的数学矿脉的矿头罢了, 后来数学的发展证实了这点.

§0.2 素数与二平方和

Fermat 在他自己所持有的 Diophantus 的《数论》空白处, 对有关该书的他自己的研究成果写下了 48 条评注. 这些评注由 Fermat 的儿子在他死后整理出版."Fermat 大定理" 是这些评注中的第 2 条. (在足立恒雄所著《解读 Fermat》(日本评论社) 中对所有的评注都有介绍.)

在它们的第 7 条评注中, Fermat 得到了下面的命题 0.1, 0.2.

命题 0.1 *如果 p 为被 4 除余 1 的素数 (例如 5, 13, 17 等等), 则存在斜边长为 p 同样的, 三边为整数的直角三角形. 然而, 对于除以 4 余 3 的素数 (例如 3, 7, 11) 却不存在这样的直角三角形.* □

在前面的图 0.1 中, 我们注意到这些是三边长为整数而斜边长为被 4 除余 1 的素数 5, 13, 17. 同样是被 4 除余 1 的自然数 21 (它不是素数) 却不是三边为整数的直角三角形的斜边. 如前所述, 从古代以来人们一直在考虑三边为整数的直角三角形, 但首先看出与素数的这种关系的是 Fermat.