现代数学基础

13 数论 II

——岩泽理论和自守形式

■ 黑川信重　栗原将人　斎藤毅　著

■ 印林生　胥鸣伟　译

高等教育出版社
HIGHER EDUCATION PRESS

现代数学基础

13

数论 II

—— 岩泽理论和自守形式

高等教育出版社
HIGHER EDUCATION PRESS

图字：01–2009–1458 号

数論 II —— 岩澤理論と保型形式
黒川信重，栗原将人，斎藤毅

SURON, II: IWASAWA RIRON TO HOKEI KEISIKI
by Nobushige Kurokawa, Masato Kurihara, 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．2，岩泽理论和自守形式/（日）黑川信重，（日）栗原将人，（日）斋藤毅著；印林生，胥鸣伟译．—北京：高等教育出版社，2009．6
ISBN 978 – 7 – 04 – 026361 – 9

Ⅰ．数… Ⅱ．①黑…②栗…③斋…④印…⑤胥… Ⅲ．数论 Ⅳ．O156

中国版本图书馆 CIP 数据核字（2009）第 042794 号

策划编辑 赵天夫　责任编辑 李　鹏　封面设计 张　楠　责任绘图 尹文军
版式设计 余　杨　责任校对 杨凤玲　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	13.25	印　　次	2009 年 6 月第 1 次印刷
字　　数	280 000	定　　价	29.00 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　26361–00

内 容 提 要

本书在《数论 I》的基础上，进一步迈向现代数论的两大主题: 解析方面的自守形式和代数方面的岩泽理论, 以及二者之间的联系。在自守形式方面介绍了模形式、Eisenstein 级数、自守形式与表示论之间的关系以及 Langlands 猜想等。在岩泽理论方面介绍了分圆 $\mathbb{Z}_p$ 扩张、p 进 ζ 函数、岩泽主猜想及与自守形式的关系等。最后不予证明地介绍了 Wiles 对 Fermat 大定理的证明。这是读完本书后可进一步学习的主要方向之一。

本书适合于数论和相关专业研究生的学习, 也可以作为数论研究工作者的参考书。

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

数论魅力的源泉在于素数所具有的奇特性质。为了要弄清素数，研究数论的人们开发出了各式各样的手段和方法。对于 ζ 函数以及类域论，我们已在《数论 I》中见到过了。本书是《数论 I》的延续，对于构成现代数论基础的重要理论进行了阐述。现代数论的特征可以说成是，它的代数的方面与它的解析的方面相互缠绕在一起。所谓的代数方面是指数域、Galois 群还有代数几何的对象之类的，而解析方面则是指 ζ 函数、自守形式还有自守表示之类的。譬如，由高木贞治所完成的类域论的核心部分表现为 Galois 群的一维表示这个代数对象与伊代尔类群的一维表示 (Hecke 特征) 这个解析对象具有同一个 ζ 函数。因此在本书所处理的岩泽理论中，作为 ζ 函数的 p 进化身的 p 进 L 函数是作为解析对象出现的，它的代数的、数论的意义正在被弄清。

以将类域论推广到非交换 Galois 群的情形作为目标并正在建设之中的 "非交换类域论"，是现代数论的一个巨大的主题。其最初的例子是，有理数域上的椭圆曲线这个代数对象，与相关于模群的同余子群的自守形式这个解析对象之间的对应。根据所确立的这个对应，Wiles 解决了自问题提出已有 375 年之久的 Fermat 猜想的证明。这个伟大事件发生距今恰好 10 年了。

本书以这样的现代数论的动向为背景介绍了自守形式和岩泽理论的基础理论，另外还以对 Wiles 的 Fermat 猜想的证明概述为中心介绍了椭圆函数的算术。每章都借助于具体的计算以增进理解。无论如何，希望读者能动手来体验一下现代数论。还要说一句，这本书曾作为岩波讲座的现代数学基础发行的《数论 3》的单行本出版过。

黑川信重，栗原将人，斋藤毅
2004 年 11 月 11 日

理论的概要与目标

本书是在《数论 I》(原来的 1,2) 的基础之上, 迈步走向了现代数论的两个代表性的主题。所说的两个主题就是在解析方面的自守形式论和在代数方面的岩泽理论。

自守形式分为第九章和第十一章。第九章以 Ramanujan 所发现的几个漂亮的等式的证明为目标, 考察了相对于模群的自守形式。特别地, 研究了 Eisenstein 级数与尖点形式。另外还引进了在现代数论中常常用到的 ζ 正规化积, 并证明了 Kronecker 极限公式。在这里本质性的内容是自守性。如其名字所示, 自守形式的要点是自守性. 所谓自守性就是满足某种形式的函数方程, 由于这是个特别强的条件, 故自守形式要依据具体情况而决定。其结果是使用自守性以及 Kronecker 极限公式, 就得到了 Ramanujan 的等式。在第十一章中, 为了从更广的观点眺望自守形式, 我们对群上的自守形式以及 Selberg 迹公式进行了展望。

第十章处理了岩泽理论。我们尽可能以容易理解的方式以岩泽主猜想为中心讲解了经典的岩泽理论。ζ 函数在整数的值中间有着 p 进的联系, 而这个现象由于 p 进 L 函数的存在变得可以得到清楚的理解。我们先对 p 进 L 函数进行讲解 (§10.1), 而后则叙述了所谓的岩泽 $\mathbb{Z}_p$ 扩张理论 (§10.2)。在这里, 我们研究了数论中的重要研究对象理想类群, 包括 Galois 群的作用, 特别地以 $\mathbb{Z}_p$ 扩域上的理想类群 (按照类域论, 这也可以说是最大非分歧 Abel 扩域的 Galois 群) 作为研究的目标。而且, §10.1 与 §10.2 的结果按照岩泽主猜想被联结了起来 (§10.3)。第十二章中, 在花了不少篇幅讲解了有关椭圆曲线的算术的基本事实后, 我们便来到了 Wiles 所给出的 Fermat 猜想证明的路线上了, 从而简洁地讲解了他的证明思想。

通过本书, 希望读者能品味到现代数论的乐趣。更希望能将本书作为基础深入钻研, 从而进入到数论研究的第一线。

目　　录

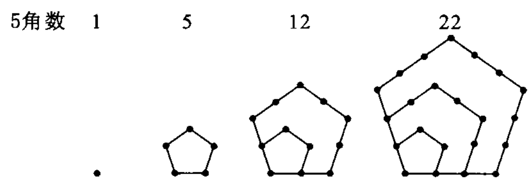
数论 I 的内容

第九章 何谓自守形式

自守形式最早出现在 1750 年 Euler 的五角数定理中:

$$\prod_{n=1}^{\infty}(1-q^n)=\sum_{m=-\infty}^{\infty}(-1)^m q^{\frac{3m^2-m}{2}}.$$

这里右端出现的 $\dfrac{3m^2-m}{2}=1,5,12,\cdots$ 为 5 角数 (《数论 I》§0.5).



称 Euler 等式的左端为 η 函数, 右端为 ϑ 函数, 这些便是 Euler 给出的自守形式的原型. 在其后的 1859 年, Riemann 研究了自守形式 ϑ, 它出现在 $\zeta(s)$ 的积分表示 (第七章) 中, 从而迎来了自守形式的 ζ 研究的新局面. 按照 Riemann 的积分表示, ϑ 的自守性转移到了 $\zeta(s)$ 的函数方程上.

在这种背景之下, 是 Ramanujan 发现了作为现代自守形式理论基础的新型的 ζ (1916 年). Ramanujan 研究了函数

$$\Delta(z)=q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

的 Fourier 展开

$$\Delta(z)=\sum_{n=1}^{\infty}\tau(n)q^n$$

中出现的系数 $\tau(n)$. 在这里 $q=e^{2\pi iz}$, 其中 z 为**上半平面** (upper half plane)

$$H=\{z\in\mathbb{C}\mid \mathrm{Im}(z)>0\}$$

中的变量. 因此 q 的绝对值小于 1, 从而 $\Delta(z)$ 的无限积表示和它的 Fourier 展开都绝对收敛. 这个 $\Delta(z)$ 在自守形式中显得尤其漂亮.

自守形式 (automorphic form) 的名字意味着 " 保持形式不变", 在 $\Delta(z)$ 的情形, 这种自守性表示为

$$\Delta\left(\frac{az+b}{cz+d}\right)=(cz+d)^{12}\Delta(z)$$

对于所有

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\mathbb{Z})$$

(就是说, $a,b,c,d\in\mathbb{Z}$ 且满足 $ad-bc=1$) 成立. 称 $(cz+d)^{12}$ 里的 12 为**权** (weight), 因此说 $\Delta(z)$ 是权为 12 的自守形式.

Ramanujan 发现的新型 ζ 是

$$L(s,\Delta)=\sum_{n=1}^{\infty}\tau(n)n^{-s},$$

并猜测 $L(s,\Delta)$ 具有 Euler 积表示

$$L(s,\Delta)=\prod_{p:\text{素数}}(1-\tau(p)p^{-s}+p^{11-2s})^{-1}.$$

到这里为止我们见到的 Euler 积有 Riemann ζ 函数

$$\zeta(s)=\sum_{n=1}n^{-s}=\prod_{p:\text{素数}}(1-p^{-s})^{-1}$$

以及 Dirichlet L 函数

$$L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}=\prod_{p:\text{素数}}(1-\chi(p)p^{-s})^{-1},$$

它们的每个局部因子都仅仅是 p^{-s} 的一次式 (这是本质性的). Ramanujan 发现了 2 次的 Euler 积, 同时提出了猜想, 即被称做 **Ramanujan 猜想** (Ramanujan conjecture) 的

$$|\tau(p)|<2p^{\frac{11}{2}}$$

(这等价于在 Euler 积中出现的二次式的判别式为负). 这给出了 20 世纪数论发展的一个原动力. 而且, 具有这样的 2 次 Euler 积的 ζ 终究是成就 Fermat 大定理解决的关键, 它的解决是与装点 20 世纪闭幕仪式相匹配的令人惊喜的事件, 这是 Ramanujan 肯定没有想到的.

现代数论进一步地把目标指向更高次 Euler 积的研究. 在这一章中我们一方面追寻 Ramanujan 所发现事实的证明, 另一方面则要进行具体的处理, 并要引进自守形式.

那么, 自守形式理论的特点是由自守性这一强的条件可以推导出非常多的不只是像猜想中那样的等式. 这大概是它特别吸引 Ramanujan 的理由吧. 在这一章中, 我们应用自守形式证明, 譬如, 下面这样的等式:

$$\sum_{n=1}^{\infty} \frac{n^5}{e^{2\pi n}-1} = \frac{1}{504}$$
$$\sum_{n=1}^{\infty} \frac{n}{e^{2\pi n}-1} = \frac{1}{24} - \frac{1}{8\pi}$$
$$\sum_{n=1}^{\infty} \frac{n^3}{e^{2\pi n}-1} = \frac{1}{80}\left(\frac{\varpi}{\pi}\right)^4 - \frac{1}{240}$$
$$\sum_{n=1}^{\infty} \frac{1}{n(e^{2\pi n}-1)} = -\frac{\pi}{12} - \frac{1}{2}\log\left(\frac{\varpi}{\sqrt{2}\pi}\right).$$

这里, π 是通常的圆周率

$$\pi = 2\int_0^1 \frac{dx}{\sqrt{1-x^2}} = 3.14159\cdots,$$

而

$$\varpi = 2\int_0^1 \frac{dx}{\sqrt{1-x^4}} = \frac{\Gamma\left(\frac{1}{4}\right)^2}{2^{\frac{3}{2}}\pi^{\frac{1}{2}}} = 2.62205\cdots$$

则是距今 (2004 年) 正好 200 年前 Gauss 所考虑的与圆周率类似的叫做 “双纽线 (lemniscate) 周率” 的数. 由于这些等式的难度在缓慢地加深, 希望读者能边读边品味.

§9.1 Ramanujan 的发现

1916 年 Ramanujan 对于在

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} \quad (q = e^{2\pi iz})$$

的 Fourier 展开

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n)q^n$$

中出现的系数 $\tau(n)$ 进行了大量的计算:

$$\begin{array}{llll}\tau(1)=1, & \tau(2)=-24, & \tau(3)=252, & \tau(4)=-1472,\\ \tau(5)=4830, & \tau(6)=-6048, & \tau(7)=-16744, & \\ \tau(8)=84480, & \tau(9)=-113643, & \tau(10)=-115920, & \cdots.\end{array}$$

凝视着这些得到的数, Ramanujan 提出了下面的猜想 ①, ②, 并进行了 ③ 的证明:

① 令 $L(s,\Delta)=\sum_{n=1}^{\infty}\tau(n)n^{-s}$,则 $L(s,\Delta)=\prod_{p:\text{素数}}(1-\tau(p)p^{-s}+p^{11-2s})^{-1}$.

② 对于素数 p 有 $|\tau(p)|<2p^{\frac{11}{2}}$.

③ 对于素数 p 有 $\tau(p)\equiv 1+p^{11} \mod 691$.

它们之中的 ① 在次年即 1917 年由 Mordell 利用算子 $T(p)$ 予以证明. ② 则在近 60 年后的 1974 年由 Deligne 利用代数几何的手段予以证明. 猜想 ②(单称为 Ramanujan 猜想) 被归结到了作为 Riemann 猜想的代数几何类比的 Weil 猜想, 而 ③ 则给出了思考 l 进表示的一个启示 (691 是个素数). Deligne 的方法是以 Grothendieck 对代数几何的创新为基础的, 对此, 现代数学进展的岩波讲座"Weil 猜想与 Etale 上同调" 有所叙述.

本节要进行对 ① 与 ③ 的证明. 但是, 为此利用 $\Delta(z)$ 的作为自守形式的性质是必需的, 为了使证明的推理易于理解, 这些事实将放在 §9.2 给予证明.

(a) Mordell 的证明

现在来证明 Ramanujan 猜想, 而 Mordell 给出了证明的结果.

定理 9.1 (Mordell, 1917 年)

$$\sum_{n=1}^{\infty}\tau(n)n^{-s}=\prod_{p:\text{素数}}(1-\tau(p)p^{-s}+p^{11-2s})^{-1}.$$

[证明] Mordell 对于每个素数 p 构造了 **Mordell 算子**(Mordell operator)

$$(T(p)\Delta)(z)=\frac{1}{p}\sum_{l=0}^{p-1}\Delta\left(\frac{z+l}{p}\right)+p^{11}\Delta(pz). \tag{9.1}$$

并证明了

$$T(p)\Delta=\tau(p)\Delta$$

(即 Δ 为 $T(p)$ 的特征函数而 $\tau(p)$ 为其特征值). 我们首先来看由此等式如何得到定理 9.1(Ramanujan 的 ①). 现将

$$\Delta(z)=\sum_{n=1}^{\infty}\tau(n)q^{n}$$

代入 $(T(p)\Delta)(z)$ 的表达式中, 于是

$$(T(p)\Delta)(z) = \frac{1}{p}\sum_{l=0}^{p-1}\sum_{n=1}^{\infty}\tau(n)\exp\left(2\pi in\frac{z+l}{p}\right) + p^{11}\sum_{n=1}^{\infty}\tau(n)q^{pn}$$
$$= \sum_{n=1}^{\infty}\left(\frac{1}{p}\sum_{l=0}^{p-1}e^{2\pi in\frac{l}{p}}\right)\tau(n)q^{\frac{n}{p}} + p^{11}\sum_{n=1}^{\infty}\tau(n)q^{pn},$$

其中

$$\frac{1}{p}\sum_{l=0}^{p-1}e^{2\pi in\frac{l}{p}} = \begin{cases}1 & p|n\\ 0 & p\nmid n.\end{cases}$$

因此有

$$(9.2)\qquad \begin{aligned}(T(p)\Delta)(z) &= \sum_{n=1}^{\infty}\tau(pn)q^n + p^{11}\sum_{n=1}^{\infty}\tau(n)q^{pn}\\ &= \sum_{n=1}^{\infty}\left(\tau(pn) + p^{11}\tau\left(\frac{n}{p}\right)\right)q^n.\end{aligned}$$

但是, 一般地如果 $x \notin \mathbb{Z}$ 则令 $\tau(x) = 0$. 特别地当 $p \nmid n$ 时有 $\tau\left(\frac{n}{p}\right) = 0$.

因此应用 $T(p)\Delta = \tau(p)\Delta$ 便得到了

$$(9.3)\qquad \tau(pn) + p^{11}\tau\left(\frac{n}{p}\right) = \tau(p)\tau(n) \quad (n = 1, 2, \cdots;\ p \text{ 为素数}).$$

我们从这里便可以推出定理. 事实上, 在 (9.3) 中令 $n = p^k$, 则有

$$(9.4)\qquad \tau(p^{k+1}) = \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1}) \quad (k = 1, 2, \cdots)$$

因此得到

$$\sum_{k=0}^{\infty}(\tau(p^k) - \tau(p)\tau(p^{k-1}) + p^{11}\tau(p^{k-2}))u^k = 1,$$

于是

$$\text{左端} = \left(\sum_{k=0}^{\infty}\tau(p^k)u^k\right)(1 - \tau(p)u + p^{11}u^2).$$

从而

$$(9.5)\qquad \sum_{k=0}^{\infty}\tau(p^k)u^k = \frac{1}{1 - \tau(p)u + p^{11}u^2}.$$

特别地, $\tau(n)$ 具有乘性的性质 (即对于使得 $(m,n) = 1$ 的 m, n 有 $\tau(mn) = \tau(m)\tau(n)$) 可像下面那样由 (9.3) 得到. 为此只要证明

$$(9.6)\qquad \text{如果 } p \nmid m \text{则 } \tau(p^k m) = \tau(p^k)\tau(m)$$

就可以了. 这可由对 k 的归纳进行证明. 当 $k=0$ 时这是显然的, 而 $k=1$ 时则是在 (9.3) 中取 $n=m$ 的结果. 现在设直到 k 其都成立. 在 (9.3) 中取 $n=p^k m$ 则有

$$\tau(p^{k+1}m)=\tau(p)\tau(p^k m)-p^{11}\tau(p^{k-1}m)$$

再由归纳法假定, 便有

$$\begin{aligned}\tau(p^{k+1}m) &= \tau(p)\tau(p^k)\tau(m)-p^{11}\tau(p^{k-1})\tau(m)\\ &= (\tau(p)\tau(p^k)-p^{11}\tau(p^{k-1}))\tau(m)\\ &\underset{(9.4)}{=} \tau(p^{k+1})\tau(m),\end{aligned}$$

故在 $k+1$ 时也成立, 从而 $\tau(n)$ 为乘性函数. 因此

$$\begin{aligned}\sum_{n=1}^{\infty}\tau(n)n^{-s} &= \prod_p(\sum_{k=0}^{\infty}(\tau(p^k)p^{-ks})\\ &= \prod_p(1-\tau(p)p^{-s}+p^{11-2s})^{-1}.\end{aligned}$$

(由这个推导可知, 定理中的等式等价于 $\tau(n)$ 为乘性函数以及 $\tau(p^k)$ 的递推公式 (9.4) 这两个联合条件.)

如此一来, 对定理 9.1 的证明只要能证明 $T(p)\Delta=\tau(p)\Delta$ 就好了. 我们说 Δ 为特征函数, 这一等式表明对于函数

$$f(z)=\frac{(T(p)\Delta)(z)}{\Delta(z)}$$

下面的两个条件成立:

(1) $f(z)$ 为常数函数,

(2) 这个常数等于 $\tau(p)$.

先看 (1). 如果能证明 $f(z)$ 对于所有的 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})$ 满足

$$f\left(\frac{az+b}{cz+d}\right)=f(z)$$

即可. 知道了这一点以及 $SL_2(\mathbb{Z})\backslash H$ 的代表系(基本区域) 是如图 9.1 所示的阴影部分

$$\begin{aligned}D=&\left\{x+iy\,\middle|\,-\frac{1}{2}<x<\frac{1}{2},\ y>\sqrt{1-x^2}\right\}\\ &\sqcup\left\{-\frac{1}{2}+iy\,\middle|\,y>\frac{\sqrt{3}}{2}\right\}\sqcup\left\{x+i\sqrt{1-x^2}\,\middle|\,-\frac{1}{2}\leqslant x\leqslant 0\right\}\end{aligned}$$