丘成桐主编

数学翻译丛书

数论教程

A Course in Arithmetic

Jean-Pierre Serre 著

冯克勤 译

丁石孙 校

高等教育出版社

Higher Education Press

数论教程

A Course in Arithmetic

Jean-Pierre Serre 著

[redacted] 译

[redacted] 校

丘成桐主编
数学翻译丛书

数论教程
A Course in Arithmetic

■ Jean-Pierre Serre 著
■ 冯克勤 译
■ 丁石孙 校

高等教育出版社
Higher Education Press

International Press

图字: 01-2007-1421

图书在版编目 (CIP) 数据

数论教程 / (法) 塞尔 (Serre J. -P.) 著; 冯克勤译.
北京: 高等教育出版社, 2007.4
(数学翻译丛书 / 丘成桐主编)
书名原文: A Course in Arithmetic
ISBN 978-7-04-021584-7

I. 数… II. ①塞…②冯… III. 数论-高等学校-教材
IV.0156

中国版本图书馆 CIP 数据核字 (2007) 第 039639 号

策划编辑 王丽萍 **责任编辑** 王丽萍 **封面设计** 于 涛
责任校对 胡晓琪 **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**	800 - 810 - 0598
邮政编码	100011	**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	煤炭工业出版社印刷厂	**畅想教育**	http://www.widedu.com
开 本	787 × 960 1/16	**版 次**	2007 年 4 月第 1 版
印 张	9.75	**印 次**	2007 年 4 月第 1 次印刷
字 数	150 000	**定 价**	25.00 元

物料号 21584 - 00

《数学翻译丛书》序

改革开放以后, 国内大学逐渐与国外的大学增加交流. 无论到国外留学或邀请外地学者到中国访问的学者每年都有增长, 对中国的科学现代化都大有帮助. 但是在翻译外国文献方面的工作尚不能算多. 基本上所有中国的教科书都还是由本国教授撰写, 有些已经比较陈旧, 追不上时代了. 很多国家, 例如俄罗斯、日本等, 都大量翻译外文书本来增长本国国民的阅读内容, 对数学的研究都大有裨益. 高等教育出版社和海外的国际出版社有见及此, 开始计划做有系统的翻译, 由王元院士领导, 北京的晨兴数学中心和杭州的浙江大学数学科学研究中心共同组织数学教授进行这个工作. 参与的教授很多, 有杨乐院士, 刘克峰教授等等. 我们希望这套翻译书能够使我们的大学生有更多的角度来看数学, 丰富他们的知识. 海外的出版公司如美国数学学会等多有帮助, 我们谨此鸣谢.

丘成桐 (Shing-Tung Yau)
2005 年 1 月

前　言

本书分两部分.

第一部分是纯代数的. 它的目标是有理数域上二次型的分类 (Hasse-Minkowski 定理), 这工作在第四章完成. 前三章叙述某些预备知识: 二次互反律, p-adic 域, Hilbert 符号. 第五章是将上述结果用于判别式为 ± 1 的整二次型. 这种二次型出现在模函数、微分拓扑和有限群等各种问题中.

第二部分 (第六章和第七章) 采用 "解析" 方法 (全纯函数). 第六章给出 Dirichlet"算术级数中的素数定理" 的证明; 在前一部分 (第三章 §2.2) 的一个关键地方曾经用过这一定理. 第七章处理模形式, 特别是 theta 函数. 这里再次出现第五章中的某些二次型.

这两部分的材料来源于 1962 年和 1964 年巴黎高等师范学院 (Ecole Normale Supérieure) 大学二年级讲义. J.-J.Sansuc (第一到四章) 和 J.-P.Ramis 与 G.Ruget (第六、七章) 将这些讲义作了修订, 写成了笔记. 这些笔记对我是很有益处的, 在这里我谨向这些笔记的作者表示谢意.

J.-P.Serre

目　录

第一部分

代 数 方 法

第一章　有限域

下面所考虑的域全是可交换的.

§1. 一般结果

1.1 有限域

设 K 是一个域, $\mathbb{Z}$ 在 K 中的像是一个整环, 从而同构于 $\mathbb{Z}$ 或者 $\mathbb{Z}/p\mathbb{Z}$, 其中 p 为素数; 它的商域同构于 $\mathbb{Q}$ 或者

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

在第一种情形下, 称 K 为特征零域; 在第二种情形下, 称 K 为特征 p 域.

K 的特征记成 $\mathrm{char}(K)$. 如果 $\mathrm{char}(K) = p \neq 0$, 那么 p 也是满足 $n \cdot 1 = 0$ 的最小正整数 n.

引理 如果 $\mathrm{char}(K) = p$, 则映射 $\sigma : x \mapsto x^p$ 是 K 到其子域 K^p 上的同构.

证 我们有 $\sigma(xy) = \sigma(x)\sigma(y)$. 进而, 如果 $0 < k < p$, 则二项式系

数 $\binom{p}{k} \equiv 0 \pmod{p}$. 由此得到

$$\sigma(x+y) = \sigma(x) + \sigma(y);$$

从而 σ 是一个同态. 此外, σ 显然是单射.

定理 1 i) 有限域 K 的特征是素数 $p \neq 0$. 如果

$$f = [K : \mathbb{F}_p],$$

则 K 的元素个数为 $q = p^f$.

ii) 设 p 为素数, 且 $q = p^f (f \geqslant 1)$ 为 p 的方幂. 令 Ω 为特征 p 的代数封闭域. 则 Ω 存在唯一的 q 元子域 $\mathbb{F}_q$, 它就是多项式 $X^q - X$ 的根所构成的集合.

iii) 每个 $q = p^f$ 元有限域均同构于 $\mathbb{F}_q$.

证 如果 K 是有限的, 它不能包含域 $\mathbb{Q}$, 从而它的特征是素数 p. 如果 f 为扩张 $K/\mathbb{F}_p$ 的次数, 显然 $\operatorname{card}(K) = p^f$, 这就得到 i).

另一方面, 如果 Ω 是特征 p 的代数封闭域, 上面的引理表明映射 $x \mapsto x^q (q = p^f, f \geqslant 1)$ 是 Ω 的自同构, 这是因为此映射是自同构 $\sigma : x \mapsto x^p$ 重复 f 次 (注意由于 Ω 代数封闭, 从而 σ 是满射). 因此对于 $x \mapsto x^q$ 不变的元素 $x \in \Omega$ 形成 Ω 的一个子域 $\mathbb{F}_q$. 多项式 $X^q - X$ 的微商是

$$qX^{q-1} - 1 = p \cdot p^{f-1} X^{q-1} - 1 = -1,$$

即不为零. 由于 Ω 代数封闭, 这导致 $X^q - X$ 有 q 个不同的根, 于是 $\operatorname{card}(\mathbb{F}_q) = q$. 反之, 如果 K 是 Ω 的 q 元子域, 则 K 内非零元素组成的乘法群 K^* 有 $q-1$ 个元素. 于是若 $x \in K^*$, 则 $x^{q-1} = 1$; 若 $x \in K$, 则 $x^q = x$. 这表明 K 包含在 $\mathbb{F}_q$ 之中. 由于 $\operatorname{card}(K) = \operatorname{card}(\mathbb{F}_q)$, 我们有 $K = \mathbb{F}_q$, 这就完成了 ii) 的证明.

由 ii) 及每个 p^f 元域均可嵌到 Ω 中 (因为 Ω 代数封闭) 这一事实即可得到 iii).

1.2 有限域的乘法群

设 p 为素数, f 为大于等于 1 的整数, $q = p^f$.

定理 2 有限域 $\mathbb{F}_q$ 的乘法群 $\mathbb{F}_q^*$ 是 $q-1$ 阶循环群.

证 如果 $d \geqslant 1$ 为整数, 以 $\phi(d)$ 表示 Euler ϕ– 函数, 即满足 $1 \leqslant x \leqslant d$ 并且与 d 互素的整数 x 的个数 (换句话说, 即在 $\mathbb{Z}/d\mathbb{Z}$ 中的像为该群生成元的 x 的个数, $1 \leqslant x \leqslant d$). 显然 d 阶循环群的生成元个数为 $\phi(d)$.

引理 1 *若 $n \geqslant 1$ 为整数, 则 $n = \sum_{d|n} \phi(d)$(注意符号 $d|n$ 表示 d 整除 n).*

证 如果 $d|n$, 令 C_d 表示 $\mathbb{Z}/n\mathbb{Z}$ 中唯一的 d 阶子群, 而以 Φ_d 表示 C_d 的生成元集合. 由于 $\mathbb{Z}/n\mathbb{Z}$ 中每个元素均生成某个 C_d, 从而群 $\mathbb{Z}/n\mathbb{Z}$ 是所有 Φ_d 的非交并集, 于是我们有

$$n = \operatorname{card}(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \operatorname{card}(\Phi_d) = \sum_{d|n} \phi(d).$$

引理 2 *令 H 为 n 阶有限群. 假设对 n 的每个因子 d, 集合 $\{x \in H | x^d = 1\}$ 至多有 d 个元素. 则 H 必为循环群.*

证 设 d 为 n 的因子. 如果存在 d 阶元素 $x \in H$, 则由 x 生成的子群 $(x) = \{1, x, \cdots, x^{d-1}\}$ 是 d 阶循环群. 按照假设, 使 $y^d = 1$ 的每个元素 $y \in H$ 均属于 (x) (特别地, H 中所有 d 阶元素都是 (x) 的生成元), 而它们共有 $\phi(d)$ 个. 从而 H 中 d 阶元素的个数或者为零或者为 $\phi(d)$. 如果对某个 d 的值该数是零, 则公式 $n = \sum_{d|n} \phi(d)$ 表明 H 中元素的个数小于 n, 这与假设相矛盾. 特别地, H 中存在着 n 阶元素 x, 因而 H 即为循环群 (x).

将引理 2 用于 $H = \mathbb{F}_q^*$ 和 $n = q - 1$ 即得定理 2, 因为次数为 d 的方程 $x^d = 1$ 在 $\mathbb{F}_q$ 中至多有 d 个解.

注 由上述证明可知更一般地, 一个域的乘法群的每个有限子群都是循环群.

§2. 有限域上的方程

设 q 为素数 p 的方幂, 而 K 为 q 元域.

2.1 方幂和

引理 设 $u>0$ 为整数, 则和式

$$S(X^u)=\sum_{x\in K}x^u=\begin{cases}-1, \text{当 } u\geqslant 1 \text{ 且 } (q-1)|u \text{ 时},\\ 0, \quad \text{在相反情况下}.\end{cases}$$

(当 $u=0$ 时, 即使 $x=0$, 也都规定 $x^u=1$.)

证 如果 $u=0$, 和式中每项均为 1, 由于 K 的特征为 p, 从而 $S(X^u)=q\cdot 1=0$.

如果 $u\geqslant 1$, 并且 $(q-1)|u$, 则 $0^u=0$, 而当 $x\neq 0$ 时 $x^u=1$, 从而 $S(X^u)=(q-1)\cdot 1=-1$.

最后, 如果 $u\geqslant 1$, 且 $(q-1)\nmid u$, 根据定理 2, K^* 是 $q-1$ 阶循环群, 从而存在 $y\in K^*$, 使 $y^u\neq 1$, 于是有

$$S(X^u)=\sum_{x\in K^*}x^u=\sum_{x\in K^*}y^ux^u=y^uS(X^u),$$

即 $(1-y^u)S(X^u)=0$, 从而推得 $S(X^u)=0$.

(**另证** 利用如下事实: 如果 $d\geqslant 2, d$ 与 p 互素, 则 d 次单位根之和为零.)

2.2 Chevalley 定理

定理 3 (Chevalley-Warning) 设 $f_\alpha\in K[X_1,\cdots,X_n]$ 是 n 元多项式, $\sum\limits_\alpha \deg f_\alpha<n$, 而 V 是它们在 K^n 中的公共零点集合, 我们有

$$\operatorname{card}(V)\equiv 0 \pmod p.$$

证 令 $P=\prod\limits_\alpha(1-f_\alpha^{q-1}), x\in K^n$. 如果 $x\in V$, 则所有 $f_\alpha(x)$ 均为零, 从而 $P(x)=1$; 如果 $x\notin V$, 则必有某个 $f_\alpha(x)$ 不为零, 从而 $f_\alpha(x)^{q-1}=1$, 于是 $P(x)=0$. 因而 P 是集合 V 的特征函数. 如果对每个多项式 f, 记 $S(f)=\sum\limits_{x\in K^n}f(x)$, 我们有

$$\operatorname{card}(V)\equiv S(P) \pmod p,$$

于是将问题归结为证明 $S(P)=0$.

现在由假设 $\sum_{\alpha}\deg f_\alpha < n$ 可知: $\deg P < n(q-1)$. 从而 P 是单项式 $X^u = X_1^{u_1}\cdots X_n^{u_n}$ 的线性组合, 其中 $\sum u_i < n(q-1)$. 只需证明对于每个这样的单项式 X^u, 有 $S(X^u)=0$, 而这一点由引理即可推出, 因为至少有一个 $u_i < q-1$.

系 1 如果 $\sum_{\alpha}\deg f_\alpha < n$, 并且每个 f_α 都没有常数项, 则 f_α 有非平凡的公共零点.

证 这是因为若 V 只是 $\{0\}$, 则 $p\nmid \mathrm{card}(V)$.

系 1 可以用于当 f_α 都是齐次多项式的时候. 特别有

系 2 每个至少有 3 个变数的二次型在 K 上都有非平凡零点.

(用几何的话说, 就是有限域上的每个二次超曲面都有有理点.)

§3. 二次互反律

3.1 $\mathbb{F}_q$ 中平方元素

设 q 为素数 p 的方幂.

定理 4 (a) 如果 $p=2$, 则 $\mathbb{F}_q$ 中每个元素都是平方元素.

(b) 如果 $p\neq 2$, 则 $\mathbb{F}_q^*$ 的平方元素形成 $\mathbb{F}_q^*$ 的指数为 2 的子群, 这个子群是同态

$$x\mapsto x^{(q-1)/2},\quad \mathbb{F}_q^*\to\{\pm 1\}$$

的核. 换句话说, 我们有正合列

$$1\to\mathbb{F}_q^{*2}\to\mathbb{F}_q^*\to\{\pm1\}\to 1.$$

证 情形 (a) 从 $x\mapsto x^2$ 为 $\mathbb{F}_q$ 的自同构这一事实即可推出.

对于情形 (b), 令 Ω 为 $\mathbb{F}_q$ 的代数闭包. 如果 $x\in\mathbb{F}_q^*$, 令 $y\in\Omega$, 使 $y^2=x$. 我们有

$$y^{q-1}=x^{(q-1)/2}=\pm 1\quad (\text{因为 } x^{q-1}=1).$$

要使 x 是 $\mathbb{F}_q$ 中的平方元素, 其充要条件是 $y\in\mathbb{F}_q^*$, 即 $y^{q-1}=1$. 于是 $\mathbb{F}_q^{*2}$ 为 $x\mapsto x^{(q-1)/2}$ 的核. 进而, 由于 $\mathbb{F}_q^*$ 是 $q-1$ 阶循环群, 从而 $\mathbb{F}_q^{*2}$ 的指数是 2.

3.2 Legendre 符号 (基本情形)

定义 设 $p \neq 2$ 为素数, $x \in \mathbb{F}_p^*$. x 的 Legendre 符号 $\left(\frac{x}{p}\right)$ 是整数 $x^{(p-1)/2} = \pm 1$.

为方便起见, 令 $\left(\frac{0}{p}\right) = 0$, 从而将 $\left(\frac{x}{p}\right)$ 扩充到 $\mathbb{F}_p$ 的全部元素上. 并且对于 $x \in \mathbb{Z}$, 若 x 有像元素 $x' \in \mathbb{F}_p$, 则记作

$$\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right).$$

我们有 $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$: Legendre 符号是 "特征" (见第六章 §1). 正如定理 4 中所表明的, $\left(\frac{x}{p}\right) = 1$ 等价于 $x \in \mathbb{F}_p^{*2}$. 如果 $x \in \mathbb{F}_p^*$, x 在 $\mathbb{F}_p$ 的代数闭包中有平方根 y, 则

$$\left(\frac{x}{p}\right) = y^{p-1}.$$

对于 $x = 1, -1, 2$, 计算 $\left(\frac{x}{p}\right)$:

若 n 为奇整数, 令 $\varepsilon(n), \omega(n)$ 为 $\mathbb{Z}/2\mathbb{Z}$ 中的元素, 定义为

$$\varepsilon(n) \equiv \frac{n-1}{2} (\mathrm{mod}\ 2) = \begin{cases} 0, \text{如果} n \equiv 1 (\mathrm{mod}\ 4), \\ 1, \text{如果} n \equiv -1 (\mathrm{mod}\ 4), \end{cases}$$

$$\omega(n) \equiv \frac{n^2-1}{8} (\mathrm{mod}\ 2) = \begin{cases} 0, \text{如果} n \equiv \pm 1 (\mathrm{mod}\ 8), \\ 1, \text{如果} n \equiv \pm 5 (\mathrm{mod}\ 8). \end{cases}$$

[函数 ε 是乘法群 $(\mathbb{Z}/4\mathbb{Z})^*$ 到 $\mathbb{Z}/2\mathbb{Z}$ 上的同态; 类似地 ω 是 $(\mathbb{Z}/8\mathbb{Z})^*$ 到 $\mathbb{Z}/2\mathbb{Z}$ 上的同态.]

定理 5 i) $\left(\frac{1}{p}\right) = 1$; ii) $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$; iii) $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$.

证 只有最后一个公式值得证明. 令 α 为 $\mathbb{F}_p$ 之代数闭包 Ω 中的一个 8 次本原单位根. 元素 $y = \alpha + \alpha^{-1}$, 满足 $y^2 = 2$ (因为由 $\alpha^4 = -1$ 可知 $\alpha^2 + \alpha^{-2} = 0$). 我们有

$$y^p = \alpha^p + \alpha^{-p}.$$

若 $p \equiv \pm 1(\mathrm{mod}\ 8)$, 这导致 $y^p = y$, 因此 $\left(\frac{2}{p}\right) = y^{p-1} = 1$. 如果 $p \equiv \pm 5(\mathrm{mod}\ 8)$, 我们发现

$$y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y.$$

(这又是从 $\alpha^4 = -1$ 推出来的.) 由此得到 $y^{p-1} = -1$, 从而证明了 iii).

注 定理 5 可以表达成下面的方式:

-1 是 mod p 平方数 $\Leftrightarrow p \equiv 1(\mathrm{mod}\ 4)$.

2 是 mod p 平方数 $\Leftrightarrow p \equiv \pm 1(\mathrm{mod}\ 8)$.

3.3 二次互反律

设 l 和 p 是两个不同的奇素数.

定理 6 (Gauss) $\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\varepsilon(l)\varepsilon(p)}$.

证 设 Ω 为 $\mathbb{F}_p$ 的代数闭包,$w \in \Omega$ 是 l 次本原单位根. 如果 $x \in \mathbb{F}_l$, 因为 $w^l = 1$, 从而元素 w^x 是可以定义的. 于是我们可以作成 Gauss 和:

$$y = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) w^x.$$

引理 1 $y^2 = (-1)^{\varepsilon(l)} l$.

(记号 l 也表示 l 在域 $\mathbb{F}_p$ 中的像.)

证 我们有

$$y^2 = \sum_{x,z} \left(\frac{xz}{l}\right) w^{x+z} = \sum_{u \in \mathbb{F}_l} w^u \left(\sum_{t \in \mathbb{F}_l} \left(\frac{t(u-t)}{l}\right)\right).$$

现在若 $t \neq 0$:

$$\left(\frac{t(u-t)}{l}\right) = \left(\frac{-t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right) = (-1)^{\varepsilon(l)}\left(\frac{1-ut^{-1}}{l}\right),$$

而

$$(-1)^{\varepsilon(l)} y^2 = \sum_{u \in \mathbb{F}_l} C_u w^u,$$