数论的方法

（下　册）

闵嗣鹤

科学出版社

数论的方法

（下册）

闵嗣鹤

科学出版社

1981

内 容 简 介

本书是《数论的方法》一书的下册．上册介绍了数论中几种重要的初等方法以及解析数论的一些基本理论与方法．下册系统地论述了三角和方法，包括有理型三角和、李变数三角和及二维三角和方法等．三角和方法是数论中最重要的方法之一．作者以较少的篇幅，阐明了三角和方法的基本内容，并且给出了在哥德巴赫问题、除数问题等方面的应用．本书可作为大学数论专门化的教学参考书，并供有关的数学工作者参考．

数 论 的 方 法

（下 册）

闵 嗣 鹤

责任编辑 张鸿林 杜小杨

科学出版社出版

北京朝阳门内大街 137 号

中国科学院印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1981 年 7 月第 一 版 开本：850×1168 1/32

1981 年 7 月第一次印刷 印张：5 3/8

印数：0001—6,700 字数：139,000

统一书号：13031·1603

本社书号：2203·13—1

定价：1.00 元

目　　录

第三篇　三角和的方法

第三篇　三角和的方法

引　论

三角和在数论中的作用

§1. 格点与三角和

在 n 维欧几里德空间 E 中引进直角坐标，每一点 M 就可以用它的坐标 $(x_1, x_2, \cdots, x_n)$ 来决定. 我们把坐标都是整数的点叫作格点. 在 E 内取定一个区域（开或闭都可以）或者是任意的集合，记作 R. 在数论里面，一个重要的问题就是估计 R 所包含的格点数：

$$N_R = \sum_{\substack{x_1 \\ (x_1, \cdots, x_n) \in R}} \cdots \sum_{x_n} 1 = \sum_{M \in R} 1. \tag{1.1}$$

这种问题常称为格点问题. 更普遍的问题是这样：设 $f(M) \equiv F(x_1, \cdots, x_n)$ 是定义在 R 上的函数，我们要估计和数：

$$N_R(f) = \sum_{\substack{x_1 \\ (x_1, \cdots, x_n) \in R}} \cdots \sum_{x_n} F(x_1, \cdots, x_n) = \sum_{M \in R} F(M). \tag{1.2}$$

特别是当 $F(M) = e^{2\pi i f(M)}$ 时，和数 (1.2) 就变成

$$\sum_{\substack{x_1 \\ (x_1, \cdots, x_n) \in R}} \cdots \sum_{x_n} e^{2\pi i f(x_1, \cdots, x_n)} = \sum_{M \in R} e^{2\pi i f(M)}. \tag{1.3}$$

这就是所谓三角和.

在数论里面，有许多问题都和三角和有着极其密切的关系. 一个重要问题的解决常常依赖于一种三角和的估计. 因此，各类型的三角和的估计，常常变成数论的中心问题. 一种估计方法的改

进，一种估计结果的精密化，对于数论中一些重要问题的研究与解决时常起着关键性的作用. 为了使读者比较确切地体会这些话，我们将在以下数节里，通过一些有代表性的例子，给以简单的说明.

§2. 同余式的解数与三角和

我们容易看出，当 a 是整数而 m 是正整数时，

$$\sum_{x=0}^{m-1} e^{\frac{2\pi iax}{m}} = \begin{cases} m & m \mid a, \\ 0 & m \nmid a, \end{cases} \tag{2.1}$$

式中 $m \mid a$ 表示 m 除尽 a，$m \nmid a$ 表示 m 除不尽 a. 这个结果虽然简单，但却是三角和的一个基本的性质. 利用这个性质，就可以表出同余式

$$f(x) \equiv 0 (\mathrm{mod}\, m), \quad f(x) = a_0 x^k + \cdots + a_k \tag{2.2}$$

(其中 $a_0, \cdots, a_k$ 是整数)的解答个数：

$$\begin{aligned} T_m(f(x)) &= \frac{1}{m} \sum_{x=0}^{m-1} \sum_{a=0}^{m-1} e^{\frac{2\pi iaf(x)}{m}} \\ &= \frac{1}{m} \sum_{a=0}^{m-1} \sum_{x=0}^{m-1} e^{\frac{2\pi iaf(x)}{m}}. \end{aligned} \tag{2.3}$$

更普遍一些，设 $f(x_1, \cdots, x_n)$ 是整系数多项式，则同余式

$$f(x_1, \cdots, x_n) \equiv 0 (\mathrm{mod}\, m) \tag{2.4}$$

的解数是

$$T_m(f(x_1, \cdots, x_n)) = \frac{1}{m} \sum_{a=0}^{m-1} \sum_{x_1=0}^{m-1} \cdots \sum_{x_n=0}^{m-1} e^{\frac{2\pi iaf(x_1, \cdots, x_n)}{m}}. \tag{2.5}$$

对于同余式组

$$\begin{aligned} &f_1(x_1, \cdots, x_n) \equiv 0 (\mathrm{mod}\, m), \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &f_s(x_1, \cdots, x_n) \equiv 0 (\mathrm{mod}\, m) \end{aligned} \tag{2.6}$$

(其中 $f_r(x_1, \cdots, x_n)$, $r = 1, \cdots, s$, 都是整系数多项式) 也可以用相仿的方法来表出解数，即

$$T_m(f_1, \cdots, f_s)$$
$$= \frac{1}{m^s} \sum_{a_1=0}^{m-1} \cdots \sum_{a_s=0}^{m-1} \sum_{x_1=0}^{m-1} \cdots \sum_{x_n=0}^{m-1} e_m(a_1 f_1 + \cdots + a_s f_s), \tag{2.7}$$

式中

$$e_m(x) = e^{\frac{2\pi i x}{m}}. \tag{2.8}$$

以上这些例子足够说明下面类型的三角和的用处：

$$\sum_{x_1} \cdots \sum_{x_n} e_m(f(x_1, \cdots, x_n)), \tag{2.9}$$

式中 $f(x_1, \cdots, x_n)$ 表示整系数多项式，而 $(x_1, \cdots, x_n)$ 的变化范围常受种种限制. 为方便起见，本书称形如(2.9)的三角和为有理型三角和. 它们的用处还不只是帮助确定同余式的解数，事实上，在以下的数节里面，所谈到问题的解法中也经常碰到这一类的三角和. 因此，它们的用处远比我们所想像的为大. 另一方面，在各类型的三角和中，有理型三角和是比较容易估计的，因此，我们对于这种三角和的估计，所能得到的结果也比较精密和完善.

§3. 丢番图方程的解数与三角和

与(2.1)相当的是下面的公式：当 α 是整数时

$$\int_0^1 e^{2\pi i \alpha x} dx = \begin{cases} 1 & \alpha = 0, \\ 0 & \alpha \neq 0. \end{cases} \tag{3.1}$$

设 $f(x_1, \cdots, x_n)$ 是整系数多项式，而 R 是某一区域或更普遍的集合，则丢番图方程(就是不定方程，我们所要求出的是它的整数解)

$$f(x_1, \cdots, x_n) = 0, \quad (x_1, \cdots, x_n) \in R \tag{3.2}$$

的解数是

$$T(f) = \sum_{(x_1, \cdots, x_n) \in R} \cdots \sum \int_0^1 e^{2\pi i \alpha f(x_1, \cdots, x_n)} d\alpha$$
$$= \int_0^1 \left(\sum_{(x_1, \cdots, x_n) \in R} \cdots \sum e^{2\pi i \alpha f(x_1, \cdots, x_n)} \right) d\alpha. \tag{3.3}$$

我们很容易推广到方程组的情形：设$f_\nu(x_1, \cdots, x_n)$, $\nu = 1, \cdots, s$是整系数多项式而R是某一区域或更普遍的集合，则方程组

$$\begin{aligned} &f_1(x_1, \cdots, x_n) = 0, \\ &\cdots\cdots\cdots\cdots \qquad (x_1, \cdots, x_n) \in R \\ &f_s(x_1, \cdots, x_n) = 0 \end{aligned} \tag{3.4}$$

的解数是

$$\begin{aligned} &T(f_1, \cdots, f_s) \\ &= \int_0^1 \cdots \int_0^1 \sum_{(x_1, \cdots, x_n) \in R} \cdots \sum e(\alpha_1 f_1 + \cdots \\ &+ \alpha_s f_s) d\alpha_1 \cdots d\alpha_s, \end{aligned} \tag{3.5}$$

式中

$$e(x) = e^{2\pi i x}. \tag{3.6}$$

以上的例子足够说明形如

$$\sum_{\substack{x_1 \\ (x_1, \cdots, x_n) \in R}} \cdots \sum_{x_n} e(\alpha f(x_1, \cdots, x_n))$$

的三角和的重要性. 事实上，在数论里面，有很多重要问题的研究与解决都要用到这种三角和. 像华林（Waring）问题、哥德巴赫（Goldbach）问题、圆内格点问题及除数问题都是典型的例子. 对于这些问题，有的还要在以后详细讨论.

第 一 章

有理型三角和

§ 1. 有理型三角和的平均值

设

$$S_q(f(x)) = \sum_{x=0}^{q-1} e_q(f(x)), \tag{1.1}$$

其中 $e_q(f(x)) = e^{\frac{2\pi i f(x)}{q}}$，$f(x)$ 是一个整系数多项式：

$$f(x) = a_k x^k + \cdots + a_0.$$

我们要考虑两种平均值，即 $\{M_q(f(x))/q\}^{\frac{1}{2}}$ 及 $\{M_q/q^k\}^{\frac{1}{2k}}$，其中

$$M_q(f(x)) = \sum_{a=0}^{q-1} \left| \sum_{x=0}^{q-1} e_q(af(x)) \right|^2, \tag{1.2}$$

$$M_q = \sum_{a_k=0}^{q-1} \cdots \sum_{a_1=0}^{q-1} \left| \sum_{x=0}^{q-1} e_q(a_k x^k + \cdots + a_1 x) \right|^{2k}. \tag{1.3}$$

估计一种和数的平均值一般要比估计个别的和数来得容易，而从平均值的估计常常能够推测到和数本身绝对值的大小. 因此本章要从估计平均值开始. 在以上两种平均值的定义里面，并未限制 q 是素数，但下面仅讨论 $q = p$ 是素数的情形.

定理 1.1 当 $k \geqslant 1$ 而素数 $p \nmid a_k$ 时，

$$M_p(f(x)) \leqslant kp^2. \tag{1.4}$$

证

$$M_p(f(x)) = \sum_{a=0}^{p-1} \sum_{x=0}^{p-1} e_p(af(x)) \sum_{y=0}^{p-1} e_p(-af(y))$$

$$= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\sum_{a=0}^{p-1} e_p(a(f(x)-f(y))).$$

因当 A 与 m 是整数时，

$$\sum_{x=0}^{m-1} e_m(Ax) = \begin{cases} m & 当 \quad m \mid A, \\ 0 & 当 \quad m \nmid A. \end{cases} \tag{1.5}$$

故

$$M_p(f(x)) = \sum_{\substack{x=0 \\ f(x)\equiv f(y)(\mathrm{mod}\,p)}}^{p-1}\ \sum_{y=0}^{p-1} p \leqslant kp^2.$$

最后一步的成立是因为当 y 一定时，$f(x) \equiv f(y)(\mathrm{mod}\,p)$ 至多有 k 个解

定理 1.2 当 $k < p$ 时，

$$M_p \leqslant k!\,p^{2k}. \tag{1.6}$$

证

$$M_p = \sum_{a_k=0}^{p-1}\cdots\sum_{a_1=0}^{p-1}\sum_{x_1=0}^{p-1}\cdots\sum_{x_k=0}^{p-1}\sum_{y_1=0}^{p-1}\cdots\sum_{y_k=0}^{p-1} e_p\Big(\sum_{\nu=1}^{k} a_\nu \times (x_1^\nu + \cdots + x_k^\nu - y_1^\nu - \cdots - y_k^\nu)\Big)$$

$$= \sum_{x_1=0}^{p-1}\cdots\sum_{x_k=0}^{p-1}\sum_{y_1=0}^{p-1}\cdots\sum_{y_k=0}^{p-1}\sum_{a_k=0}^{p-1}\cdots\sum_{a_1=0}^{p-1} e_p\Big(\sum_{\nu=1}^{k} a_\nu \times (x_1^\nu + \cdots + x_k^\nu - y_1^\nu - \cdots - y_k^\nu)\Big).$$

由 (1.5)

$$M_p = p^k N,$$

其中 N 是下列同余式组的解答个数：

$$x_1^\nu + \cdots + x_k^\nu \equiv y_1^\nu + \cdots + y_k^\nu (\mathrm{mod}\ p),$$
$$\nu = 1, \cdots, k. \tag{1.7}$$

根据对称函数的一个定理(牛顿公式[1]),由(1.7)知道 $x_1,\cdots,x_k$ 的初等对称函数一定与对应的 $y_1,\cdots,y_k$ 的初等对称函数彼此同余(这里用到 $k<p$).

因此,

$$(x-x_1)\cdots(x-x_k)\equiv(x-y_1)\cdots(x-y_k)(\mathrm{mod}\,p)$$

对每一个 x 的值都成立. 令 $x\equiv x_1(\mathrm{mod}\,p)$, 即知 $y_1,\cdots,y_k$ 之中一定有一个与 x_1 同余 $(\mathrm{mod}\,p)$,设为 y_1. 于是当 $x\not\equiv x_1(\mathrm{mod}\,p)$ 时有

$$(x-x_2)\cdots(x-x_k)\equiv(x-y_2)\cdots(x-y_k)(\mathrm{mod}\,p).$$

因 $k-1<p-1$, 上式对于所有的 x 的值都成立. 这样,就可以仿前进行直到证出 $y_1,\cdots,y_k$ 不过是 $x_1,\cdots,x_k$ 的另一排列(对模 p 而言). 因此

$$N\leqslant k!p^k.$$

定理遂之成立. [证完]

由定理 1.1 及定理 1.2 知道

$$\left(\frac{M_pf(x)}{p}\right)^{\frac{1}{2}}\leqslant k^{\frac{1}{2}}p^{\frac{1}{2}},$$

---

1) 设 $x_1,\cdots,x_n$ 是方程

$$x^n+p_1x^{n-1}+\cdots+p_n=0$$

的根而

$$S_\nu=x_1^\nu+\cdots+x_n^\nu,\qquad \nu=1,2,\cdots,$$

则所谓牛顿公式就是下列公式

$$\begin{cases}S_1+p_1=0,\\ S_2+p_1S_1+2p_2=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ S_{n-1}+p_1S_{n-2}+\cdots+(n-1)p_{n-1}=0;\end{cases}$$

$$\begin{cases}S_n+p_1S_{n-1}+\cdots+np_n=0,\\ S_{n+1}+p_1S_n+\cdots+p_nS_1=0,\\ S_{n+2}+p_1S_{n+1}+\cdots+p_nS_2=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\end{cases}$$

虽然牛顿公式是关于方程的根的公式,对于素数模同余式的解而言这些公式仍然成立. 当然从域论的眼光看来,解同余式的问题其实就是解特征是某一素数 p 的域内的方程的问题.

$$\left(\frac{M_p}{p^k}\right)^{\frac{1}{2k}} \leqslant (k!)^{\frac{1}{2k}} p^{\frac{1}{2}},$$

这两种平均值的阶都是 $p^{\frac{1}{2}}$. 因此,我们可以猜想到当 $p\nmid a_k$, $k>1$ 时, $S_p(f(x))$ 的阶是 $\sqrt{p}$. 这个猜想的正确性已由 L. Carlitz 与 S. Uchiyama 予以证明. 更确切地说,他们证明了

定理 1.3 $|S_p(f(x))| \leqslant (k-1)p^{\frac{1}{2}}$. (1.8)

他们的证明用到 Andre Weil 所证明的类似黎曼假设. 由于超出本书范围,这里从略.

§ 2. Mordell 的结果

本节要证明的是下面比定理 1.3 较弱的定理:

定理 2.1 (Mordell) 设 $f(x) = a_k x^k + \cdots + a_1 x + a_0$ 而 $(a_k, \cdots, a_1, p) = 1$,

则

$$S_p(f(x)) = O(p^{1-\frac{1}{k}}), \tag{2.1}$$

式中 O 所隐含的常数只与 k 有关.

证 显然不妨假定 $p > k$, $a_0 = 0$ 及 $p\nmid a_k$. 由定理 1.2,

$$\sum_{a_k=0}^{p-1} \cdots \sum_{a_1=0}^{p-1} |S_p(a_k x^k + \cdots + a_1 x)|^{2k} \leqslant k! p^{2k}. \tag{2.2}$$

我们要证明在 (2.2) 的左边至少有 $\frac{p(p-1)}{k}$ 项与 $|S_p(f(x))|^{2k}$ 相等. 实际上,当 $\lambda \not\equiv 0 \pmod p$ 而 μ 任意时都有

$$|S_p(f(\lambda x + \mu) - f(\mu))| = |S_p(f(x))|. \tag{2.3}$$

对于不同的组合 λ, μ 及 λ_0, μ_0 是否所得的项 (即 (2.3) 的左端) 也是不同的, 就要看 $f(\lambda x + \mu) - f(\mu)$ 与 $f(\lambda_0 x + \mu_0) - f(\mu_0)$ 是否不全同 (mod p) 而定. 这里所谓全同 (mod p) 就是相当项的系数彼此同余 (mod p).

若 $f(\lambda x + \mu) - f(\mu)$ 与 $f(x)$ 全同 (mod p), 则

$$a_k \lambda^k \equiv a_k,\ k a_k \lambda^{k-1}\mu + a_{k-1}\lambda^{k-1} \equiv a_{k-1} \pmod p.$$

由假定 $a_k \not\equiv 0 \pmod p$, 故第一个同余式至多有 k 个解. 又当 λ

一定对，易知 μ 即由上面第二个同余式唯一地决定. 因此，至多有 k 个多项式 $f(\lambda x+\mu)-f(\mu)$ 与 $f(x)$ 全同 $(\mathrm{mod}\ p)$. 上面的讨论实际上并不是局限于 $f(x)$ 的. 一般地说，在 $p(p-1)$ 个多项式 $f(\lambda x+\mu)-f(\mu)(\lambda\not\equiv 0\ (\mathrm{mod}\ p))$ 之中，与其中任意指定的一个多项式 $f(\lambda_0 x+\mu_0)-f(\mu_0)$ 全同的，至多有 k 个. 因此，其中互不全同的多项式的个数至少有 $\frac{p(p-1)}{k}$ 个. 这就是说，在 (2.2) 左边至少有 $\frac{p(p-1)}{k}$ 个不同的项与 $|S_p(f(x))|^{2k}$ 相等. 故由 (2.2)

$$\frac{p(p-1)}{k}|S_p(f(x))|^{2k}\leqslant k!p^{2k},$$

即

$$|S_p(f(x))|\leqslant\left(\frac{k\cdot k!}{p(p-1)}p^{2k}\right)^{\frac{1}{2k}}=O(p^{1-\frac{1}{k}}),$$

式中 O 所隐含的常数显然只与 k 有关. [证完]

§3. Mordell 结果的 n 维推广

(一) 华罗庚与著者曾得到 Mordell 定理的一个二维类似定理，后来又由著者推广到 n 维. 设 $f(x_1,\cdots,x_n)$ 是一个整系数 n 元多项式，我们所要估计的是

$$S\{f(x_1,\cdots,x_n)\}=\sum_{x_1=1}^{p}\cdots\sum_{x_n=1}^{p}e_p\{f(x_1,\cdots,x_n)\},\quad(3.1)$$

其中 p 表素数.

在估计 (3.1) 之前，我们要考虑域 Π 中的代数方程组

$$f_i(x_1,\cdots,x_n)=0\quad(i=1,\cdots,n),\qquad(3.2)$$

其中 $f_i(x_1,\cdots,x_n)$ 是域 Π 中的多项式. 实际上，我们在本节中只需考虑 Π 的特征是 p 的情形，或者更狭一些，只需考虑一组对模 p 的同余式. 但是为了不损害下面定理 3.1 的一般性，我们还是就一般的域 Π 来讨论. 让我们先引进一个定义：

定义 能使函数行列式(或称 Jacobian)

$$J = J(f_1, \cdots, f_n) = \begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \cdots\cdots\cdots\cdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{vmatrix} \neq 0$$

的(3.2)的解称为非异解.

定理 3.1 方程组(3.2)的非异解数不超过一个只与 n 有关而与 k 无关的常数 $c = c(n)$.

证 当 $n = 1$ 时,定理显然正确. 设定理对 $n-1$ 个变数及 $n-1$ 个方程是成立的,现证明对 n 个变数 n 个方程也成立.

若 $f_1, \cdots, f_n$ 不含 x_n, 定理显然正确,因为这时 $J \equiv 0$, 故(3.2)没有非异解. 若其中只有一个包含 x_n, 设其为 f_n, 定理也成立,这是因为,若 $(x_1^{(0)}, \cdots, x_n^{(0)})$ 是(3.2)的非异解,则

$$J(f_1, \cdots, f_n) = \frac{\partial f_n}{\partial x_n} J(f_1, \cdots, f_{n-1}) \neq 0$$

$$(\text{当 } x_\nu = x_\nu^0,\ \nu = 1, \cdots, n).$$

这表明 $(x_1^{(0)}, \cdots, x_{n-1}^{(0)})$ 是方程组

$$f_1 = 0, \cdots, f_{n-1} = 0$$

的非异解,由归纳法的假定,这种非异解数 $\leqslant c$. 而 $f_n(x_1^{(0)}, \cdots, x_{n-1}^{(0)}, x_n)$ 不恒为 0,所以满足 $f_n(x_1^{(0)}, \cdots, x_{n-1}^{(0)}, x_n) = 0$ 的 $x_n^{(0)}$ 的个数不超过某常数.

设 f_i 对于 x_n 的次数是 λ_i, 则当 $\lambda_1 + \cdots + \lambda_n \leqslant 1$ 时定理成立,这是因为在此时,(3.2)内顶多有一个方程包含 x_n. 今设当

$$\lambda_1 + \cdots + \lambda_n \leqslant r$$

时定理成立,我们要证明当 $\lambda_1 + \cdots + \lambda_n \leqslant r + 1$ 时定理仍然成立.

不妨失去普遍性,我们假定

$$f_1 = f_{10}x_n^{\lambda_1} + \cdots + f_{1\lambda_1},\ f_2 = f_{20}x_n^{\lambda_2} + \cdots + f_{2\lambda_2}, \quad (3.3)$$

其中 $\lambda_1 \geqslant \lambda_2 \geqslant 1$ 而 f_{1i}, f_{2i} 是 $x_1, \cdots, x_{n-1}$ 的多项式.

考虑方程组

$$f_1' = f_{20}f_1 - f_{10}x_n^{\lambda_1-\lambda_2}f_2 = 0,\ f_i = 0 (i = 2, \cdots, n). \quad (3.4)$$

上面第一方程可能是恒等式，但在那种情形下（3.4）就没有非异解了(看下面(3.5),(3.5′)). 显然(3.2)的每一个解都是(3.4)的解，我们要证明(3.2)的每一个满足 $f_{20}\neq 0$ 的非异解 $(x_1^{(0)},\cdots,x_n^{(0)})$ 一定也是(3.4)的非异解.

对于 $x_i(i=1,\cdots,n)$ 微分(3.4)的第一个方程即得

$$\begin{aligned}\frac{\partial f_1'}{\partial x_i}&=f_{20}\frac{\partial f_1}{\partial x_i}-f_{10}x_n^{\lambda_1-\lambda_2}\frac{\partial f_2}{\partial x_i}+\frac{\partial f_{20}}{\partial x_i}f_1-\frac{\partial f_{10}}{\partial x_i}x_n^{\lambda_1-\lambda_2}f_2\\&=f_{20}\frac{\partial f_1}{\partial x_i}-f_{10}x_n^{\lambda_1-\lambda_2}\frac{\partial f_2}{\partial x_i},\quad \text{当}\quad x_\nu=x_\nu^{(0)}\qquad(3.5)\\&\qquad(i=1,2,\cdots,n-1),\end{aligned}$$

$$\begin{aligned}\frac{\partial f_1'}{\partial x_n}&=f_{20}\frac{\partial f_1}{\partial x_n}-f_{10}x_n^{\lambda_1-\lambda_2}\frac{\partial f_2}{\partial x_n}-(\lambda_1-\lambda_2)f_{10}x_n^{\lambda_1-\lambda_2-1}f_2\\&=f_{20}\frac{\partial f_1}{\partial x_n}-f_{10}x_n^{\lambda_1-\lambda_2}\frac{\partial f_2}{\partial x_n},\quad \text{当}\quad x_\nu=x_\nu^{(0)}.\qquad(3.5')\end{aligned}$$

故当 $x_\nu=x_\nu^{(0)}$ 时，

$$J(f_1',f_2,\cdots,f_n)=f_{20}J(f_1,\cdots,f_n)\neq 0.\qquad(3.6)$$

现在设 $(x_1^{(0)},\cdots,x_n^{(0)})$ 是(3.2)的一个满足 $f_{20}=0$ 的非异解，则此解同时满足

$$\begin{aligned}&f_1=0,\ f_2'=f_2-f_{20}x_n^{\lambda_2}=0,\\&f_i=0\quad(i=3,\cdots,n),\end{aligned}\qquad(3.7)$$

即

$$f_1=0,\ f_{20}=0,\ f_i=0(i=3,\cdots,n).\qquad(3.8)$$

由(3.7),

$$\begin{aligned}\frac{\partial f_2'}{\partial x_i}&=\frac{\partial f_2}{\partial x_i}-\frac{\partial f_{20}}{\partial x_i}x_n^{\lambda_2}\quad(i=1,\cdots,n-1),\\\frac{\partial f_2'}{\partial x_n}&=\frac{\partial f_2}{\partial x_n}-\lambda_2 f_{20}x_n^{\lambda_2-1}=\frac{\partial f_2}{\partial x_n},\quad \text{当}\quad x_\nu=x_\nu^{(0)}.\end{aligned}$$

故当 $x_\nu=x_\nu^{(0)}$ 时，

$$\begin{aligned}0\neq J(f_1,\cdots,f_n)&=J(f_1,f_2',f_3,\cdots,f_n)\\&\quad+x_n^{\lambda_2}J(f_1,f_{20},f_3,\cdots,f_n).\end{aligned}\qquad(3.9)$$

这表明 $J(f_1,f_2',f_3,\cdots,f_n)$ 与 $J(f_1,f_{20},f_3,\cdots,f_n)$ 不能同时

为零.

因此，从 (3.6) 与 (3.9) 可以看出 (3.2) 的每一个非异解必定是 (3.4)，(3.7) 与 (3.8) 三个方程组之一的非异解. 但它们各自对 x_n 的次数之和都不超过 r. 由数学归纳法立得本定理.

(二) 下面证明一个很简单的定理：

定理 3.2 设 $f(x_1, \cdots, x_n)$ 是域 II 内不恒等于 0 的多项式，并设 II 是特征为 P 而元素个数是 p^m 的有限域，则

$$f(x_1, \cdots, x_n) = 0 \tag{3.10}$$

的解数是 $O(p^{m(n-1)})$，其中 O 所隐含的常数与 p 及 m 无关.

证 定理当 $n = 1$ 时显然成立. 今设对 $n-1$ 个未知数也成立，令

$$f(x_1, \cdots, x_n) = g_0 x_n^k + \cdots + g_k,$$

式中 g_i 是 $x_1, \cdots, x_{n-1}$ 的多项式，并且 g_0 不恒为 0. 显然满足

$$f = 0, \qquad g_0 \neq 0$$

的解数是 $O(p^{m(n-1)})$，而满足

$$f = 0, \qquad g_0 = 0$$

的解数由归纳法的假设知道是 $O(p^{m(n-2)}p^m)$. 故 (3.10) 的解数是 $O(p^{m(n-1)})$. [证完]

(三) 在证明主要定理之前我们还需要先证明一个常常用到的不等式：

引理 3.1 (Hölder 不等式) 设 $\frac{1}{\lambda} + \frac{1}{\mu} = 1, \lambda > 0, \mu > 0$，又设 $a_k \geqslant 0$，$b_k \geqslant 0$，$k = 1, \cdots, n$，则

$$\sum_{k=1}^{n} a_k b_k \leqslant \left(\sum_{k=1}^{n} a_k^{\lambda}\right)^{\frac{1}{\lambda}} \left(\sum_{k=1}^{n} b_k^{\mu}\right)^{\frac{1}{\mu}}, \tag{3.11}$$

式中“=”号只在

$$\frac{a_1^{\lambda}}{b_1^{\mu}} = \frac{a_2^{\lambda}}{b_2^{\mu}} = \cdots = \frac{a_n^{\lambda}}{b_n^{\mu}} \tag{3.12}$$

时 $\frac{0}{0}$ 算作可以等于任何数，当 A 不是 0 时 $\frac{A}{0}$ 算作 ∞ 才成立.

证 1) 先证当 $x>1$，$0<m<1$ 时，

$$x^m-1<m(x-1). \tag{3.13}$$

实际上，

$$x^m-1=\int_1^x mx^{m-1}dx<m\int_1^x dx=m(x-1).$$

2) 其次证明当 $\alpha+\beta=1$，α，β 是正数，且 a，b 非负时，

$$a^\alpha b^\beta\leqslant \alpha a+\beta b, \tag{3.14}$$

式中的“=”号只有当 $a=b$ 时才成立.

显然当 $a=b$ 时 (3.14) 两边相等，又当 a，b 之一为 0 时 (3.14) 仍成立. 今设 $a>b>0$，则由 (3.13)

$$\left(\frac{a}{b}\right)^m-1<m\frac{(a-b)}{b}.$$

两边用 b 乘再移项得

$$a^m b^{1-m}<b+m(a-b)=ma+(1-m)b.$$

令 $m=\alpha$，$1-m=\beta$，即得

$$a^\alpha b^\beta<\alpha a+\beta b.$$

3) 当 (3.12) 成立时，(3.11) 的两边相等. 今设 (3.12) 不成立 则由 (3.14)

$$\sum_{\nu=1}^{n}\left\{\left(\frac{A_\nu}{\sum_{\nu=1}^{n}A_\nu}\right)^\alpha\left(\frac{B_\nu}{\sum_{\nu=1}^{n}B_\nu}\right)^\beta\right\}$$

$$<\sum_{\nu=1}^{n}\left(\alpha\frac{A_\nu}{\sum_{\nu=1}^{n}A_\nu}+\beta\frac{B_\nu}{\sum_{\nu=1}^{n}B_\nu}\right)=\alpha+\beta=1,$$

令式中 $A_\nu=a_\nu^{1/\alpha}$，$B_\nu=b_\nu^{1/\beta}$，$\alpha=\frac{1}{\lambda}$，$\beta=\frac{1}{\mu}$，即得

$$\sum_{\nu=1}^{n}a_\nu b_\nu<\left(\sum_{\nu=1}^{n}a_\nu^\lambda\right)^{1/\lambda}\left(\sum_{\nu=1}^{n}b_\nu^\mu\right)^{1/\mu}. \qquad \text{[证完]}$$

(四) 现在可以证明我们的主要定理：