中国科学院数学研究所专刊

第 1 号

堆垒素数论

华罗庚

科学出版社

中国科学院数学研究所专刊

堆垒素数论

华罗庚

中国科学院数学研究所編輯
科学出版社出版
1957年北京

內 容 提 要

本書是關於堆壘素數論方面蘇聯維諾格拉陀夫院士的研究方法和本書作者自己的研究方法的總結性論著．在本書中給予維諾格拉陀夫院士的中值定理以顯著的中心地位，並且改進了它．作者把華林問題與古特拔黑問題的研究方法結合起來，並把華林問題一方面推廣到每一加數是整係數多項式的情形，一方面限制變數僅取素數值．作者把塔銳問題也加上了變數只取素數值的限制，同時又討論到更廣的素未知數的不定方程組．

本書是作者的早期的著作，最初於 1946 年在蘇聯用俄文第一次出版．解放後於 1953 年由中國科學院出版了中文版．現在作者又重新將這部書從頭到尾加以修改補充，內容變動很大，如第四章第五節，第五章第六節和第八節，及第九章全部，都是完全重寫的；還有一些節也近於重寫；此外並增加了一個附錄．

中國科學院數學研究所專刊

堆壘素數論（修訂本）

著者　華羅庚

出版者　科學出版社
北京朝陽門大街 117 號
北京市書刊出版業營業許可證出字第 061 號

印刷者　中國科學院印刷廠

總經售　新華書店

1957 年 9 月第一版　書號：0841　字數：182,000
1962 年 10 月第三次印刷　開本：787×1092 1/16
(京) 4,177—5,176　印張：10 1/4　插頁：2

定價：2.20 元

再　版　序

作者利用這一次再版的機會對本書做了一些修改和補充. 第四章第五節、第五章第六和第八節及第九章全部都是經過重寫的,此外還有不少章節做了部份改寫工作.

讀者讀了本書後,再參閱不多的近代文獻,就可以了解近代堆壘數論的中心部份,並且可以進入研究工作的領域. 但不要忘記,本書祇是一個專著,僅僅是敘述了數論中的一個分支,在深入的同時,也應當去了解數論的寬廣園地(請參閱科學出版社出版的拙著"數論導引").

作者乘此機會向越民義、王元、吳方、魏道政、陳景潤諸同志表示謝意,他們或指出錯誤或給以幫助,不是他們的協同工作,再版是不會這樣快就問世的.

華羅庚　1957年7月7日於北京

序

這一本小書能够用本國文字出版是和人民民主政權分不開的. 回憶一下離初稿完成的日子已經過了十二個年頭了,離俄文版刊出的日子也已隔了六年了. 在解放以前漫長的歲月中, 這書在我國刊出的問題, 由卽將出版、等待出版一直演變到把原稿搞得無影無蹤, 以致於到了今天, 在中國科學院敦促之下我還得從俄文本翻譯出來付印. 這些事實, 有力地說明了, 舊政權是怎樣腐化怎樣地不關心科學, 而人民民主政權又是怎樣地寶愛科學成果.

十二個年頭不算短暫, 科學工作又有了不少的進展, 所以僅把俄文本翻譯付印, 是不合當前的情況的. 我改寫了幾章, 特別是第五章我把維諾格拉陀夫院士在 1942 到 1947 年進一步的創造性的工作及著者 1947 年的工作包括進去.

在工作完成的時候, 心情是異常愉快的. 不但由於我的小書得以在祖國出版, 而特別是從前所渴望着的中蘇兩國的友誼今天是實現了——已經牢不可破了! 沒有中國科學院的鼓勵, 這本書是不可能再出版的, 所以我由衷地表示感謝. 數學研究所的同人分頭負責核閱及訂正, 人數之多使我不能在這兒一一列舉. 祇有在集體主義的今天才會出現這樣的友愛團結的精神. 而這又證明了人民民主政權的優越性.

華羅庚

北京, 1953 年 5 月

俄文版原序*

本文中敍述了關於堆壘素數論的新結果，這一學科的基礎是由 И. М. 維諾格拉陀夫院士所奠立的，而由著者發展的. 在第五、六兩章把開拓了新途徑的維諾格拉陀夫院士的工作加以簡化與改變而重述出來. 閱讀本文，除了引理 7·14 之外，並不要求有任何其他較專門化的知識.

本文中大部份是著者所獲得並在這裏首次發表的結果的系統敍述.

無論著者如何地感謝維諾格拉陀夫院士都不會是過份的.

閔嗣鶴、鍾開萊兩位先生對於本文手稿之準備都曾給予幫助.

最後，著者對蘇聯科學院對他的著作的好評價願表示深切的謝意. 在這些困難的日子裏，我們的科學研究的成果能獲得最友好的人民的最高權威方面的贊助，這特別給予我們很大的鼓舞. 這種文化的合作是永遠寶貴的，而在現在的時刻，這更具有特殊的意義. 謹祝此書的出版將會加強我們兩偉大人民間的眞誠友誼與相互親善.

華 羅 庚

中國昆明國立清華大學

1941 年 2 月 18 日

在幾年的戰爭之後，承維諾格拉陀夫院士給予我訪問蘇聯的機會. 我非常高興地獲悉我在 1940—1941 年所寫的這篇論文已在付印. 在 1942 年維諾格拉陀夫院士已把他的方法更精密化，而著者在到莫斯科之前還完全不知道. 他的精密化加強了關於平均值的定理（本文中的定理 7）. 藉助這一定理我們可以改進定理 8, 9, 11, 13, 17 等等. 例如定理 11 對於 $s \geqslant 10\, k^2 \log k$ 也眞實，而定理 13 對於 $s \geqslant s_0 \sim 4\, k \log k$ 也正確，等等.

最後，我謹向翻譯此文的 Б. И. Сегал 與 Д. А. Васильков 兩位教授致謝.

華 羅 庚

莫斯科，1946 年 4 月 17 日

---

* 編者(指斯切克洛夫數學研究所專刊的編者)識：本書於 1941 年交數學研究所專刊編輯部，但由於 1941—1945 年的戰時條件，現在纔能出版.

說　　明

本文並無一般的引言．各章的第一段有主要結果的敍述．本文中常引用下列符號：

對於實數 x，$[x]$ 表示不大於 x 的最大整數，而 $\{x\}$ 表示由 x 到最近整數的距離．

$$e(z) = e^{2\pi iz}. \qquad e_q(x) = e^{2\pi ix/q}.$$

k 表示一正整數；P 是充分大的正數，而 $L = \log P$.

$\max(a, b, \cdots, g)$ 表示 $a, b, \cdots, g$ 中最大的一個，而 $\min(a, b, \cdots, g)$ 表示其中最小的一個．

如習常所用：$a|b$ 表示 a 整除 b，$a \nmid b$ 表示 a 不整除 b．本文中常用 p 表示素數，$p^l \| n$ 表示 $p^l | n$ 而 $p^{l+1} \nmid n$.

$c(a, b, \cdots, g)$ 表示某一依存於 $a, b, \cdots, g$ 的正數；ε 是任意小正數，但不一定在每次出現時都是一樣的．

$f(x) = O(\varphi(x))$ 或 $f(x) \ll \varphi(x)$ 表示

$$|f(x)| \leqslant c(a, b, \cdots, g)\varphi(x).$$

在陳述定理時我們不用符號 $\ll$ 及 O，而用如以上形式的不等式．在證明中或引理中如果用到符號 $\ll$ 或 O，則其所包有的常數僅依賴於定理敍述中所涉及的 $a, b, \cdots, g$.

如有特別聲明，符號的含義可能有局部性的改變．

目　　錄

說　明

第　一　章　三角和… … … … … … … … … … … … … … … … 1

第　二　章　包含除數函數的和的估值… … … … … … … … … … 10

第　三　章　某些三角和的中值定理（I） … … … … … … … … … 16

第　四　章　Виноградов 的中值定理及其推論… … … … … … … … 22

第　五　章　某些三角和的中值定理（II） … … … … … … … … … 34

第　六　章　含有素數變數的三角和 … … … … … … … … … … 56

第　七　章　華林 - 古特拔黑問題的解數的漸近式 … … … … … … … 66

第　八　章　奇異級數 … … … … … … … … … … … … … … 85

第　九　章　華林 - 古特拔黑問題進一步的研究… … … … … … … … 93

第　十　章　素數未知數的不定方程組… … … … … … … … … … 105

第十一章　前章問題進一步的研究 … … … … … … … … … … 132

第十二章　其他的結果… … … … … … … … … … … … … … 147

附　錄… … … … … … … … … … … … … … … … … … … 151

第 一 章

三 角 和

§1. 定理及基本引理的叙述

定理 1. 命 $f(x)$ 代表一個有整數係數的多項式

$$f(x) = a_k x^k + \cdots + a_1 x + a_0 .$$

若 $(a_k, \cdots, a_1, q) = 1$, 則

$$\left| \sum_{x=1}^{q} e^{2\pi i f(x)/q} \right| \leqslant c_1(k, \varepsilon) q^{1-\frac{1}{k}+\varepsilon},$$

此處 ε 是一任與的正數.

爲了簡單起見,我們引用下面的符號:

$$a = \frac{1}{k}, \quad e_q(x) = e^{2\pi i x/q}$$

及

$$S(q, f(x)) = \sum_{x=1}^{q} e_q(f(x)) .$$

基本引理 (引理 1·1). 若 $p \nmid (a_k, \cdots, a_1)$, 則

$$|S(p^l, f(x))| \leqslant c_2(k) p^{l(1-a)} .$$

§2. 由基本引理推出定理

引理 1·2. 用 $\nu(q)$ 表示 q 的不同的素數因子的個數. 用 $d(q)$ 表 q 的正除數的個數. 則

$$2^{\nu(q)} \leqslant d(q) \leqslant c_3(\varepsilon) q^{\varepsilon} .$$

證: 若素數 $p > 2^{1/\varepsilon}$, 則

$$\frac{d(p^l)}{p^{l\varepsilon}} = \frac{l+1}{p^{l\varepsilon}} \leqslant \frac{l+1}{2^l} = \frac{l+1}{(1+1)^l} \leqslant \frac{l+1}{l+1} = 1.$$

又若素數 $p \leqslant 2^{1/\varepsilon}$ 及 $l \geqslant 1$, 則

$$\frac{d(p^l)}{p^{l\varepsilon}} = \frac{l+1}{p^{l\varepsilon}} \leqslant \frac{l+1}{2^{l\varepsilon}} \leqslant \frac{l+1}{l\varepsilon \log 2} \leqslant \frac{2}{\varepsilon \log 2} .$$

命 $q = p_1^{l_1} \cdots p_s^{l_s}$, 此處 $p_1, \cdots, p_s$ 是 q 所有的不同的素因子,則

$$\frac{d(q)}{q^{\varepsilon}}=\prod_{p|q}\frac{d(p^{l})}{p^{l\varepsilon}}\leqslant\prod_{p\leqslant 2^{1/\varepsilon}}\frac{2}{\varepsilon\log 2}=c_3(\varepsilon).$$

引理中第一不等式顯然眞實.

引理 1·3. 若 $(q_1, q_2)=1$ 及 $f(0)=0$, 則

$$S(q_1q_2, f(x))=S(q_1, f(q_2x)/q_2)\,S(q_2, f(q_1x)/q_1).$$

證: 命 $x=q_1y+q_2z$. 當 y 及 z 各經過以 q_2 及 q_1 爲模的完全剩餘系, 則 x 經過以 q_1q_2 爲模的完全剩餘系. 顯然得出

$$e_{q_1q_2}(f(q_1y+q_2z))=e_{q_2}(f(q_1y)/q_1)e_{q_1}(f(q_2z)/q_2),$$

及

$$\begin{aligned}S(q_1q_2, f(x))&=\sum_{x=1}^{q_1q_2}e_{q_1q_2}(f(x))=\\&=\sum_{y=1}^{q_2}\sum_{z=1}^{q_1}e_{q_2}(f(q_1y)/q_1)e_{q_1}(f(q_2z)/q_2)=\\&=S(q_1, f(q_2x)/q_2)\,S(q_2, f(q_1x)/q_1).\end{aligned}$$

定理的證明. 我們可以假定 $a_0=0$ 而不失其普遍性. 命 $q=p_1^{l_1}\cdots p_s^{l_s}$, 此處 $p_1, \cdots, p_s$ 是 q 所有的不同的素因子. 由引理 1·3

$$S(q, f(x))=\prod_{p|q}S\left(p^{l}, \frac{f(qx/p^{l})}{q/p^{l}}\right),$$

及由引理 1·1 可得

$$\left|S(q, f(x))\right|\leqslant c_2^{\nu(q)}q^{1-a}.$$

再由引理 1·2 (我們可設 $c_2>1$),

$$c_2^{\nu(q)}=(2^{\nu(q)})^{\log c_2/\log 2}\leqslant c_1(k, \varepsilon)q^{\varepsilon}.$$

由此卽得出本定理.

§3. 當 $l=1$ 時基本引理的證明 (Mordell*)

並不失去普遍性,我們可以假定 $p>k$ 及 $a_0=0$. 爲了簡單起見,我們用 $\sum_x$ 代表 $\sum_{x=1}^{p}$. 如是得到

$$\sum_{a_k}\cdots\sum_{a_1}\left|\sum_x e_p(a_kx^k+\cdots+a_1x)\right|^{2k}=$$

* *Quarterly Jour. of Math.*, 3 (1932), 161—167.

$$= \sum_{x_1} \cdots \sum_{x_k} \sum_{y_1} \cdots \sum_{y_k} \sum_{a_k} \cdots \sum_{a_1} e_p(a_k(x_1^k + \cdots + x_k^k - y_1^k - \cdots - y_k^k) +$$

$$+ \cdots + a_1(x_1 + \cdots + x_k - y_1 - \cdots - y_k)) = p^k N,$$

此處 N 表示下列相合式組的解答的個數:

$$x_1^h + \cdots + x_k^h \equiv y_1^h + \cdots + y_k^h \pmod{p}, \quad 1 \leqslant h \leqslant k, \quad 1 \leqslant x, \ y \leqslant p. \tag{1}$$

注意,獲得此結論時,引用了下面的公式

$$\sum_{x=1}^{q} e_q(hx) = \begin{cases} q & \text{若 } q \mid h, \\ 0 & \text{若 } q \nmid h. \end{cases}$$

由對稱函數中一習知的定理,由(1)可以引出

$$(x - x_1) \cdots (x - x_k) \equiv (x - y_1) \cdots (x - y_k) \pmod{p}.$$

由此可知 $y_1, \cdots, y_k$ 乃由 $x_1, \cdots, x_k$ 轉換次序而得出的 (mod p). 所以

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

由此得出

$$\sum_{a_k} \cdots \sum_{a_1} \left| S(p, a_k x^k + \cdots + a_1 x) \right|^{2k} \leqslant k! p^{2k}. \tag{2}$$

顯然,對任一 λ($\not\equiv 0 \pmod{p}$) 及任一 μ 常有

$$|S(p, f(x))|^k = |S(p, f(\lambda x + \mu) - f(\mu))|.$$

所有這種形式的和都在(2)式的左邊出現. 今往求出由所有不同的多項式 $f(\lambda x + \mu) - f(\mu)$ 所得的和 $S(p, f(\lambda x + \mu) - f(\mu))$ 的個數. 若二多項式的係數各各相合 (mod p), 則此二多項式算爲全同, mod p. 我們可以假定 $p \nmid a_k$ 而不失其普遍性. 若 $f(\lambda x + \mu) - f(\mu)$ 與 $f(x)$ 全同, mod p, 則得

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

適合 $\lambda^k \equiv 1 \pmod{p}$ 的 λ 的個數 $\leqslant k$. 對一固定的 λ, μ 就唯一決定. 所以形如 $f(\lambda x + \mu) - f(\mu)$ 的多項式中最多有 k 個與 $f(x)$ 全同, mod p.

由此可得,在所有的 $p(p-1)$ 個多項式

$$f(\lambda x + \mu) - f(\mu), \qquad 1 \leqslant \lambda \leqslant p - 1, \qquad 1 \leqslant \mu \leqslant p,$$

中,至少有 $p(p-1)/k$ 個是互不相同的. 所以

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

即

$$|S(p, f(x))| \leqslant \left(\frac{k \cdot k!}{p(p-1)} \right)^{\frac{1}{2a}} p \leqslant (2k \cdot k!)^{\frac{1}{2a}} p^{1-a} \leqslant k p^{1-a}. \tag{3}$$

§4. 幾 條 引 理

引理 1·4. 假定 $s(x)$ 是一整數係數的多項式,mod p. α 是 $s(x)\equiv 0 \pmod p$ 的 m 重根. $p^u \| s(px+\alpha)$*. 命 $t(x)=p^{-u}s(px+\alpha)$, 則相合式

$$t(x)\equiv 0 \pmod p$$

至多有 m 個根.

證: 並不失其普遍性,可以假定 $\alpha=0$. 如此則

$$s(x)=x^m s_1(x)+p s_2(x),$$

此處 $s_1(0)\not\equiv 0 \pmod p$, $s_2(x)$ 的次數低於 m. $s_1(x)$ 及 $s_2(x)$ 都是整係數多項式. 由此得出

$$s(px)=p^m x^m s_1(px)+p s_2(px).$$

因爲 x^m 的係數 $p^m s_1(0)$ 不能爲 p^{m+1} 所整除,所以 $u\leqslant m$. 又因爲 $p^{-u}s(px)$ 的次數 $\leqslant m \pmod p$,所以證明了本引理.

引理 1·5. 假定

$$f(x)=a_k x^k+\cdots+a_1 x,$$

$p\nmid(a_k,\cdots,a_1)$. 如果 p^σ 恰能整除 $f(\mu+py)-f(\mu)$ 所有的係數,則

$$1\leqslant\sigma\leqslant k.$$

證: 假定 $\sigma\geqslant k+1$, 則由於 p^σ 能整除 $f(\mu+py)-f(\mu)$ 所有的係數,可知

$$p^\sigma \Big| \frac{p^h}{h!}f^{(h)}(\mu), \qquad 1\leqslant h\leqslant k.$$

即對任一 h 常有

$$p^{k+1}\Big|\frac{p^h}{h!}f^{(h)}(\mu),$$

由此得出

$$p\Big|\frac{1}{h!}f^{(h)}(\mu).$$

因而得出 $p\mid a_k, p\mid a_{k-1},\cdots, p\mid a_1$. 此與假定 $p\nmid(a_k,\cdots,a_1)$ 相違背.

§5. 基本引理的證明

基本引理可以由以下的更明確的引理來概括.

引理 1·6. 命 $f(x)=a_k x^k+\cdots+a_1 x+a_0$, $p\nmid(a_k,\cdots,a_1)$. 則

$$|S(p^l,f(x))|\leqslant k^3 p^{(1-\alpha)l}.$$

---

* $p^u\|g(x)$ 表示 p^u 整除 $g(x)$ 的所有的係數,但 p^{u+1} 不能.

證：命 t 是能整除 $(ka_k, \cdots, 2a_2, a_1)$ 的 p 的最高方次．又設 $\mu_1, \cdots, \mu_r$ 是相合式

$$f'(x) \equiv 0 \pmod{p^{t+1}}, \qquad 0 \leqslant x < p,$$

的相異的根．其重數分別爲 $m_1, \cdots, m_r$．命 $m_1 + \cdots + m_r = m$，易見 $m \leqslant k-1$．此引理顯然是不等式

$$|S(p^l, f(x))| \leqslant k^2 \max(1, m) p^{(1-a)l} \tag{4}$$

的直接推理．現在用數學歸納法來證明上式．

由於 $p \nmid (a_k, \cdots, a_1)$ 及 $p^t \parallel (ka_k, \cdots, 2a_2, a_1)$，所以一定有 $p^t \leqslant k$．

1）假定 $l < 2(t+1)$．如果 $t = 0$，則得 $l = 1$．這是已經討論過的情況．若 $t \geqslant 1$，則顯然可見

$$|S(p^l, f(x))| \leqslant p^l \leqslant p^{l(1-a)} \cdot p^{(2t+1)a} \leqslant p^{l(1-a)} k^{(2+1/t)a} \leqslant k^2 p^{l(1-a)},$$

故引理成立．

2）假定 $l \geqslant 2(t+1)$．寫

$$S(p^l, f(x)) = \sum_{\nu=1}^{p} \sum_{\substack{0 \leqslant x \leqslant p^l - 1 \\ x \equiv \nu \pmod p}} e_{pl}(f(x)) = \sum_{\nu=1}^{p} S_\nu .$$

如果 ν 並非 μ_i 之一，則命

$$x = y + p^{l-t-1} z, \qquad 0 \leqslant y < p^{l-t-1}, \qquad 0 \leqslant z < p^{t+1},$$

即得

$$S_\nu = \sum_{\substack{0 \leqslant x < p^l \\ x \equiv \nu \pmod p}} e_{pl}(f(x)) = \sum_{\substack{0 \leqslant y < p^{l-t-1} \\ y \equiv \nu \pmod p}} \sum_{0 \leqslant z < p^{t+1}} e_{pl}(f(y) + y^{l-t-1} z f'(y)) =$$

$$= \sum_{\substack{0 \leqslant y < p^{l-t-1} \\ y \equiv \nu \pmod p}} e_{pl}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_{p^{t+1}}(z f'(y)) = 0, \tag{5}$$

最後等式是由於 $f'(y) \not\equiv 0 \pmod{p^{t+1}}$．

如果 $\nu = \mu_i$，則依引理 1·5 來定義 σ_i，如此則得

$$S_{\mu_i} = \sum_{\substack{x=1 \\ x \equiv \mu_i \pmod p}}^{p^l} e_{pl}(f(x)) = \sum_{y=1}^{p^{l-1}} e_{pl}(f(\mu_i + py)) =$$

$$= e_{pl}(f(\mu_i)) \sum_{y=1}^{p^{l-1}} e_{p^{l-\sigma_i}}(p^{-\sigma_i}(f(\mu_i + py) - f(\mu_i))).$$

命 $g_i(x) = p^{-\sigma_i}(f(\mu_i + px) - f(\mu_i))$．由引理 1·5 可知

$$|S_{\mu_i}| = p^{\sigma_i - 1} |S(p^{l-\sigma_i}, g_i(x))| \leqslant$$

$$\leqslant p^{\sigma_i(1-a)} |S(p^{l-\sigma_i}, g_i(x))|. \tag{6}$$

總括 (5),(6) 二式得出

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} p^{\sigma_i(1-a)} |S(p^{l-\sigma_i}, g_i(x))| . \tag{7}$$

如果 $l > \max(\sigma_1, \cdots, \sigma_r)$,則用歸納法並引理 1·4, 由 (7) 式可得

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} m_i p^{\sigma_i(1-a)} k^2 p^{(l-\sigma_i)(1-a)} < mk^2 p^{l(1-a)} .$$

若 $l \leqslant \max(\sigma_1, \cdots, \sigma_r)$,則 $l \leqslant k$

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} p^{\sigma_i - 1} p^{l-\sigma_i} \leqslant k p^{l(1-a)} .$$

由是基本引理卽已完全證明.

所以定理 1 也就已經完全證明.

§6. 推 論

在論述若干推理之前,我們先引入關於整值多項式的觀念.

定義. 如果對整數 x, 一多項式 $f(x)$ 的值也是整數,這多項式就稱爲整值多項式.

引理 1·7. 命

$$v! F_v(x) = x(x-1)\cdots(x-v+1) .$$

一多項式是整值多項式的必要且充分條件是它可以表成

$$a_k F_k(x) + \cdots + a_1 F_1(x) + a_0$$

的形式,此處 $a_k, \cdots, a_1, a_0$ 都是整數.

證: 顯然 $F_v(x)$ 是整值多項式,所以 $a_k F_k(x) + \cdots + a_1 F_1(x) + a_0$ 也是整值多項式.

反之,任一多項式常可表成

$$f(x) = b_k F_k(x) + \cdots + b_1 F_1(x) + b_0 .$$

連續以 $x = 0, 1, 2, \cdots, k$ 代入上式,若 $f(x)$ 爲整值多項式,則可知諸 b 一定是整數.

現在可敍述本章的定理及基本引理的推論.

推論 1·1. 命 $f(x)$ 是一 k 次整值多項式,它的係數的最小公分母用 d 表示. 設 $p^t \| d$, 並且假定並非 $f(x)$ 的所有的非常數項的係數的分子都是 p 的倍數. 則

$$\left| \sum_{x=1}^{p^{l+t}} e_{pl}(f(x)) \right| \leqslant c_4(k) p^{l(1-a)} .$$

證: 由於 $d | k!$, 所以得此推論.

推論 1·2. 命 $f(x)$ 是一 k 次整值多項式，它的係數的最小公分母是 d. 假定對 q 的任一素因子 p，並非 $f(x)$ 的所有非常數項的係數的分子都是 p 的倍數. 則

$$\left|\sum_{x=1} e_q(f(x))\right| \leqslant c_5(k,\varepsilon)q^{1-a+\varepsilon},$$

此處 $\bar{q} = q \cdot \prod_{\substack{p \mid q \\ p^t \parallel d}} p^t$.

推論 1·3. 仍如推論 1·1 及 1·2 的假定，我們有

$$\left|\sum_{\substack{x=1 \\ p \nmid x}}^{p^{l+t}} e_{pl}(f(x))\right| \leqslant c_6(k)p^{(1-a)l}$$

及

$$\left|\sum_{\substack{x=1 \\ (x,q)=1}} e_q(f(x))\right| \leqslant c_7(k,\varepsilon)q^{1-a+\varepsilon}.$$

證：我們現在僅證明第一不等式，第二式可由第一式推得. 顯然有

$$\sum_{\substack{x=1 \\ p \nmid x}}^{p^{l+t}} e_{pl}(f(x)) = \sum_{x=1}^{p^{l+t}} e_{pl}(f(x)) - \sum_{x=1}^{p^{l+t-1}} e_{pl}(f(px)).$$

寫

$$df(x) = a_k x^k + \cdots + a_1 x + a_0, \quad p \nmid (a_k, \cdots, a_1).$$

命 p^μ 是 p 的最高方次可以整除 $(f(px)-f(0))\,d$ 的所有的係數者. 顯然 $1 \leqslant \mu \leqslant k$. 所以當 $l \geqslant \mu$ 時，

$$\left|\sum_{x=1}^{p^{l+t-1}} e_{pl}(f(px))\right| = \left|\sum_{x=1}^{p^{l+t-l}} e_{p^{l-\mu}}(p^{-\mu}(f(px)-f(0)))\right| \leqslant$$
$$\leqslant p^{\mu-1} \cdot c_4(k)p^{(l-\mu)(1-a)} \leqslant$$
$$\leqslant c_4(k)p^{l(1-a)-1+\mu a} \leqslant c_4(k)p^{l(1-a)}.$$

若 $l < \mu \leqslant k$，則顯然有

$$\left|\sum_{x=1}^{p^{l+t-1}} e_{pl}(f(px))\right| \leqslant p^{l+t-1} \leqslant k!\,p^{l-1} \leqslant k!\,p^{(1-a)l}.$$

§7. 有限的富利埃級數

引理 1·8. 命

$$S = \sum_{q' < n \leqslant q''} e(n\alpha), \qquad e(x) = e^{2\pi i x}.$$

則得

$$|S| \leqslant \min\left(q'' - q', \frac{1}{2\{\alpha\}}\right),$$

此處 $\{\alpha\}$ 代表從 α 到和它最接近的整數的距離. 換言之, $\{\alpha\} = \min\ (\alpha - [\alpha], [\alpha] + 1 - \alpha)$.

證: 顯然有不等式 $|S| \leqslant q'' - q'$. 若 $\alpha \neq [\alpha]$, 命 $Q = q'' - q'$, 則有

$$\left|\sum_{q' < n \leqslant q''} e(n\alpha)\right| = \left|\sum_{n=0}^{Q-1} e(n\alpha)\right| = \left|\frac{1 - e(Q\alpha)}{1 - e(\alpha)}\right| \leqslant \frac{2}{|1 - e(\alpha)|} =$$

$$= \frac{1}{|\sin \pi\alpha|} \leqslant \frac{1}{2\{\alpha\}}.$$

(當 $0 \leqslant \xi \leqslant \frac{1}{2}$ 時 $\sin \pi\xi > 2\xi$, 所以有 $|\sin \pi\xi| \geqslant 2\{\xi\}$).

引理 1·9. 命 $g(x)$ 表一週期是 q 的函數, 且

$$g(x) = \begin{cases} 1 & \text{當 } 0 < x \leqslant m, \\ 0 & \text{當 } m < x \leqslant q. \end{cases}$$

則

$$g(x) = \frac{m}{q} + \frac{1}{q}\sum_{n=1}^{q-1} e_q(nx)\sum_{t=1}^{m} e_q(-nt).$$

證: 顯然 $g(x)$ 可以表成

$$g(x) = \frac{1}{q}\sum_{n=1}^{q} e_q(nx)\sum_{t=1}^{m} e_q(-nt) =$$

$$= \frac{m}{q} + \frac{1}{q}\sum_{n=1}^{q-1} e_q(nx)\sum_{t=1}^{m} e_q(-nt).$$

§8.

定理 2. 設 $f(x) = a_k x^k + \cdots + a_1 x + a_0$ 是一整數係數多項式. 命 $(a_k, \cdots, a_2, q) = d$, 則

$$\left|\sum_{x=1}^{m} e_q(f(x)) - \frac{m}{q} S(q, f(x))\right| \leqslant c_8(k, \varepsilon) q^{1-a+\varepsilon} d^a.$$

又當 $1 \leqslant m \leqslant q$ 時

$$\left|\sum_{x=1}^{m} e_q(f(x))\right| \leqslant c_9(k, \varepsilon) q^{1-a+\varepsilon} d^a.$$

證: 由引理 1·9 已知

$$\sum_{x=1}^{m} e_q(f(x)) = \sum_{x=1}^{q} e_q(f(x))g(x) =$$

$$= \frac{m}{q} S(q, f(x)) + \frac{1}{q}\sum_{x=1}^{q} e_q(f(x))\sum_{n=1}^{q-1} e_q(nx)\sum_{t=1}^{m} e_q(-nt).$$

即得（由引理 1·8）

$$\left|\sum_{x=1}^{m} e_q(f(x)) - \frac{m}{q} S(q, f(x))\right| \leqslant \frac{1}{q} \sum_{n=1}^{q-1} \frac{1}{2\left\{\frac{n}{q}\right\}} \left|\sum_{x=1}^{q} e_q(f(x) + nx)\right|.$$

命 $(d, a_1 + n) = q'$，则由定理 1 可知

$$\frac{1}{q} \sum_{n=1}^{q-1} \frac{1}{2\left\{\frac{n}{q}\right\}} \left|\sum_{x=1}^{q} e_q(f(x) + nx)\right| \leqslant \frac{1}{q} \sum_{q'|d} \sum_{\substack{n=1 \\ a_1+n\equiv 0 (\mathrm{mod}\, q')}}^{q-1} \frac{1}{2\left\{\frac{n}{q}\right\}} \left|\sum_{x=1}^{q} e_{q/q'}\left(\frac{f(x)+nx}{q'}\right)\right| \ll$$

$$\ll \frac{1}{q} \sum_{q'|d} \sum_{\substack{n=1 \\ a_1+n\equiv 0 (\mathrm{mod}\, q')}}^{q-1} \frac{1}{\left\{\frac{n}{q}\right\}} q'\left(\frac{q}{q'}\right)^{1-a+\epsilon} \ll$$

$$\ll q^{1-a+\epsilon}\left(\sum_{q'|d} q'^{a}\left(\sum_{\substack{1\leqslant n\leqslant q/2 \\ a_1+n\equiv 0 (\mathrm{mod}\, q')}} \frac{1}{n} + \sum_{\substack{1\leqslant n\leqslant q/2 \\ a_1-n\equiv 0 (\mathrm{mod}\, q')}} \frac{1}{n}\right)\right) \ll$$

$$\ll q^{1-a+\epsilon} \sum_{q'|d} q' a \ll q^{1-a+\epsilon} d^{a}.$$