維 諾 格 拉 多 夫

維諾格拉多夫，И. (Виногорадов，Иван，英文名 Ivan Matveevich Vinogradov) 1891 年 9 月 14 日生於俄國西部普斯科夫省大盧基縣的米洛留勃村 (Milolyub，Velikie Luki，Pskov Province)；1983 年 3 月 20 日卒於莫斯科。數學。

維諾格拉多夫之圖像請參閱 The MacTutor History of Mathematics archive 網站

http://turnbull.mcs.st-and.ac.uk/history/PictDisplay/Vinogradov.html

維 諾 格 拉 多 夫

張 明 堯

(中國科學技術大學)

維諾格拉多夫，И. (Виноградов，Иван，英文名 Ivan Matveevich Vinogradov) 1891 年 9 月 14 日生於俄國西部普斯科夫省大盧基縣的米洛留勃村 (Milolyub，Velikie Luki，Pskov Province)；1983 年 3 月 20 日卒於莫斯科。數學。

維諾格拉多夫的父親是米洛留勃村墓地教堂的一名牧師，母親是一名教師。維諾格拉多夫從小就表現出繪畫的才能。當時牧師的孩子通常是進教會學校讀書，而他的父母卻一反慣例，於 1903 年送他到大盧基城的一所主要是講授自然科學、現代語言及繪畫的實科中學去就讀。1910 年他中學畢業後，進入首都聖彼得堡 (Петербург；1914－1924 年間改稱彼得格勒：Петроград；後又更名爲列寧格勒：Ленинград) 的聖彼得堡大學物理數學系學習，1914 年畢業。在該系著名學者 Я. В. 烏斯賓斯基 (Успéнский) 等人的影響下，維諾格拉多夫對數論產生了濃厚的興趣。1915 年，由於他關於二次剩餘及非剩餘分佈問題所獲得的研究成果，經 В. А. 斯捷克洛夫 (Стеклов) 推薦，授予他一項獎學金，此後他成功地通過了碩士學位。1918－1920 年，維諾格拉多夫先後在國立彼爾姆大學及蘇聯東歐部分的莫洛托夫大學任教，先任副教授，後擔任教授。1920 年底，他回到彼得格勒，任彼得格勒工學院教授及彼得格勒大學副教授。在彼得格勒工學院他開設高等數學課，在彼得格勒大學他開設數論課，這門課就成了他後來所著《數論基礎》(Основы теории чисел，1936) 一書的基礎。1925 年他升任列寧格勒大學教授，並擔任該校數論及概率論教研室主

任。

1929 年 1 月他當選爲蘇聯科學院院士，這標誌著他開始進入國家級的科學活動組織者及管理人才的行列中。他與 С. И. 瓦維洛夫 (Вавилов) 共同制訂了對科學院物理－數學研究所進行重大改組的計劃。1930－1932 年他出任人口統計研究所所長，1930－1934 年任物理－數學研究所數學部主任。1934 年，物理－數學研究所分爲兩個所：列別捷夫 (Лебедев) 物理研究所與斯捷克洛夫數學研究所。維諾格拉多夫被任命爲斯捷克洛夫數學研究所第一任所長，直到去世前，他一直擔任這一職務。其間，蘇聯科學院從列寧格勒遷往莫斯科，斯捷克洛夫數學研究所即建在瓦維洛夫大街上。1950 年起，他任《蘇聯科學院通報》(ИАН СССР) 數學組主編，1958 年起任全蘇數學家委員會主席。他始終對數學教育有極大的興趣，直到去世前一直任全蘇中學數學改革委員會主席。

維諾格拉多夫中等身材，體格異常健壯，即便到九十高齡，他也從不坐電梯去辦公室，且步履十分矯健。他與人談話常用俄語，他能說一口相當熟練的英語。他一生中只有很少幾次出國參加活動。其中有兩次出訪英國，一次是 1946 年參加英國皇家協會主辦的牛頓紀念活動，另一次是參加 1958 年的愛丁堡國際數學家大會。維諾格拉多夫十分好客，待人誠摯體貼。1971 年藉慶祝維諾格拉多夫八十壽辰之機，在莫斯科舉行了一次學術討論會。維諾格拉多夫自費主辦了一次宴會，邀請與會的國內外數學家參加，他親筆填寫了每份請帖，對每位客人都給予了熱情的款待。

維諾格拉多夫一生中被二十多個外國科學院及科學協會等機構授予院士、名譽院士、會員、名譽會員等稱號。1939 年被授予倫敦數學會名譽會員稱號，1942 年當選爲英國皇家學會外籍會員。他一生還多次榮獲蘇聯政府及蘇聯科學院等頒發的勳章及榮譽稱號。其中計有：社會主義勞動英雄 (二次)、列寧勳章 (五

次)、 錘子與鐮刀勳章 (二次)、 十月革命勳章 、 斯大林獎金 (現改稱國家獎金)、 列寧獎金 、 羅蒙諾索夫金質獎章 ， 其中羅蒙諾索夫金質獎章是蘇聯科學院的最高獎 。

波利亞 − 維諾格拉多夫不等式

設 $m \geq 1$ 爲給定的整數 ， a 、 b 爲兩個整數 。 若 $a-b$ 可被 m 整除 ， 則記 $m|(a-b)$ ， 稱 m 爲模 ， 並稱 a 與 b 對模 m 同餘 ， 記爲 $a \equiv b(\mathrm{mod}\, m)$ 。 對固定的模 m ， 同餘關係是一個等價關係 。 把對模 m 同餘的所有整數歸爲一類 ， 稱爲模 m 的一個剩餘類 ， 則全體整數恰可分成 m 個不同的剩餘類 。 從每一類中取一代表元組成的集合稱爲模 m 的一個完全剩餘類 。 對剩餘類可以很自然地定義類的加 、 減 、 乘法 ， 它們與整數的加 、 減 、 乘法有完全類似的性質 。

設 $m = p \geq 3$ 爲質數 ， $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 是一個 $n \geq 1$ 次整係數多項式 。 若 x_0 滿足同餘方程

$$f(x) \equiv 0 \,(\mathrm{mod}\, p)\ , \tag{1}$$

易見一切滿足 $t \equiv x_0 \,(\mathrm{mod}\, p)$ 的 t 皆滿足 (1)， 它們稱爲 (1) 的一個解 。 與代數基本定理對應 ， 我們有如下定理 。

定理 (拉格朗日)　若 $a_n \not\equiv 0 \,(\mathrm{mod}\, p)$ ， 則 (1) 至多有 n 個解 。

當 $n = 2$ 時 ， 求解 (1) 可以歸結爲求解特殊形式的二次同餘方程

$$x^2 \equiv a \,(\mathrm{mod}\, p)\ 。 \tag{2}$$

A.M. 勒讓德 (Legendre) 首先定義了如下的符號 ， 此即初等數論中著名的勒讓德符號 ：

$$\left(\frac{a}{p}\right) = \begin{cases} 1\ ， & \text{當 } p \nmid a \text{ 且 (2) 有解 ，} \\ 0\ ， & \text{若 } p \mid a\ ， \\ -1\ ， & \text{若 } p \nmid a \text{ 且 (2) 無解 。} \end{cases} \tag{3}$$

根據 $\left(\frac{a}{p}\right) = 1$ 或 -1，我們稱 a 是模 p 的一個二次剩餘 (即平方剩餘) 或二次非剩餘 (即平方非剩餘)。在模 p 的一個完全剩餘系 $\{1, 2, \cdots, p\}$ 中，易見除 p 外，二次剩餘與非剩餘各佔一半，故

$$\sum_{a=1}^{p} \left(\frac{a}{p}\right) = 0 \text{。} \tag{4}$$

實際上，對任何整數 N 均有

$$\sum_{a=N+1}^{N+p} \left(\frac{a}{p}\right) = 0 \text{。} \tag{5}$$

這表明在模 p 的一個完全剩餘系裡，二次剩餘與非剩餘個數總是相等。一個自然的問題是：對任意整數 N 及任給正整數 M，當 a 取遍區間 $[N+1, N+M]$ 中的整數時，其中二次剩餘及非剩餘的分佈情況如何? (3) 表明其中二次剩餘與非剩餘的個數之差爲

$$\left| \sum_{a=N+1}^{M+N} \left(\frac{a}{p}\right) \right| \text{。}$$

由 (5) 知不妨可設 $1 \leq M < \frac{p}{2}$。維諾格拉多夫證明了

$$\left| \sum_{a=N+1}^{M+N} \left(\frac{a}{p}\right) \right| < \sqrt{p} \ln p \text{。} \tag{6}$$

上式表明，當區間長度 M 適當大時，其中二次剩餘與非剩餘的個數相差甚少。正是由於這項研究成果，1915 年他被授予一項獎學金，並被批准留校攻讀學位。

勒讓德符號實際上是以 p 爲模的一種實原特徵，它是更爲廣泛的狄利克雷 (Dirichlet) 特徵 $\chi_q(a)$ 的特例，這裡 q 是特徵的模。1918 年，維諾格拉多夫與波利亞互相獨立地證明了：若

$\chi_q(a)$ 是以 q 爲模的一個原特徵， 則對任何整數 $N \geq 1$ 皆有

$$\left|\sum_{a\leq N}\chi_q(a)\right| < \sqrt{q}\ln q\ 。 \tag{7}$$

若 $\chi_q(a)$ 爲非主特徵， 則有

$$\left|\sum_{a\leq N}\chi_q(a)\right| \ll \sqrt{q}\ln q\ 。 \tag{7*}$$

這些不等式統稱爲波利亞－維諾格拉多夫不等式 。

1977 年， H.L. 蒙哥馬利 (Montgomery) 與 R.C. 沃恩 (Vaughan) 在假設廣義黎曼猜想 (簡記爲 GRH) 成立的條件下證明了： 對非主特徵有

$$\left|\sum_{a\leq N}\chi_q(a)\right| \ll \sqrt{q}\ln\ln q\ , \tag{7.1}$$

而 R.E.A.C. 佩利 (Paley) 於 1932 年就構造出一列無窮多個不同的二次特徵 χ_{q_j} $(j = 1、2、\cdots)$， 使得

$$\max_N\left|\sum_{a\leq N}\chi_{q_j}(a)\right| \geq \frac{1}{7}\sqrt{q}_j\ln\ln q_j,$$

因此， (7*) 與最好可能的結果 (7.1) 相比已經相當接近 。

設 $n_2(p) > 1$ 爲模的 p 最小二次非剩餘 。 1919 年， 維諾格拉多夫利用 (7) 及質數分佈的簡單性質證明

$$n_2(p) \leq p^{\frac{1}{2\sqrt{e}}}(\ln p)^2\ ,$$

他猜想對任給 $\varepsilon > 0$ 有 $n_2(p) = O(p^\varepsilon)$， 他還猜想對任給 $\varepsilon > 0$ 有 $r_2^*(p) = O(p^\varepsilon)$， 這裡 $r_2^*(p)$ 表示 p 的二次剩餘中的最小質數 。 1952 年 N.C. 安克尼 (Ankeny) 證明了： 若 GRH 成立， 則有 $n_2(p) = O(\ln^2 p)$ 。 對於後一猜想， 1967 年 P.D.T.A. 埃利奧特

(Elliott) 證明了它是 GRH 的一個推論。這兩個猜想迄今仍未獲得證明。他關於二次及高次剩餘分佈、原根與指數分佈等問題的許多結果已被 D.A. 伯吉斯 (Burgess) 等人加以改進。有關結果請見 W. 納基耶維奇 (Narkiewicz) 所寫專著第 II 章及其它文獻。

類數均值公式及格點問題

設 a、b、c 爲取定的整數，稱二次齊次式

$$f(x,y)=ax^2+bxy+cy^2$$

爲一個二元二次型，簡記爲 $\{a,b,c\}$，稱 $d=b^2-4ac$ 爲其判別式。若 $(a,b,c)=1$，則稱 $\{a,b,c\}$ 爲本原二次型，簡稱原型，這裡 (a,b,c) 表 a、b、c 三數的最大公約數。

設給定兩個型 $\{a_1,b_1,c_1\}$ 與 $\{a_2,b_2,c_2\}$，其變量分別爲 x、y 及 u、v。若有一個整係數變換

$$\begin{cases} x &= ru+sv\,, \\ y &= tu+wv\,, \end{cases} \qquad rw-st=1\,,$$

使 $\{a_1,b_1,c_1\}$ 變爲 $\{a_2,b_2,c_2\}$，則稱它們是相似型。易證相似是二次型的一種等價關係。利用它可將判別式爲 d 的所有本原二次型分成兩兩不相交的等價類。用 $h(d)$ 表示把判別式 d 的本原二次型所分成的等價類的個數。容易證明，對每個判別式 d，$h(d)$ 皆有限。

對判別式爲 $-d<0$ 的正定型，F. 高斯 (Gauss) 在其所著《算術研究》(*Disquisitiones arithmeticae*，1801) 一書第 302 篇中不加證明地給出一個漸近公式

$$\sum_{d=1}^{n}h(-d)=\frac{4\pi}{21\xi(s)}n^{\frac{3}{2}}-\frac{2}{\pi^2}n+R(n)\,, \tag{8}$$

這裡對 $s>1$ 定義 $\xi(s)=\sum\limits_{m=1}^{\infty}\dfrac{1}{m^s}$。高斯也沒有給出餘項 $R(n)$ 的估計。1865 及 1874 年，R. 李普希茨 (Lipschitz) 與 F. 默滕斯

(Mertens) 先後得到 (8) 式的第一項 (參見 P. 巴赫曼 (Bachmann) 著《解析數論》(*Die analytische Zahlentheorie*，1894) 二卷十三章 §16，但他們的方法均未能得到第二項主項。

1917 年，維諾格拉多夫給出了研究算術函數漸近表示中餘項估計這一難題的一個新方法，它比 Г. 沃羅諾伊 (Вороной) 於 1903 年提出的方法簡單，且能獲得幾乎相同的結果。維諾格拉多夫新方法的重點在於如下的所謂“第一基本公式”：

設 $k \geq 1$、$A > 29$、$R > Q$ 皆爲實數，函數 $f(x)$ 在區間 $[Q, R]$ 中二階可微且滿足

$$\frac{1}{kA} \leq f''(x) \leq \frac{1}{A}\ , \tag{9}$$

則有

$$\sum_{Q<x<R} \{f(x)\} = \frac{1}{2}(R-Q) + G\ , \tag{10}$$

其中 $\{y\}$ 表示實數 y 的小數部分，而

$$|G| < 2k\left(\frac{R-Q}{A}+1\right)(A\ln A)^{\frac{2}{3}}\ 。 \tag{11}$$

由此並利用上述李普希茨文章中的一個恆等式

$$\sum_{d=1}^{n} h(-d) = \sum_{r=1}^{\infty} \mu(2r-1) F\left(\frac{n}{(2r-1)^2}\right)\ , \tag{12}$$

即證得 (8) 式，並得到

$$R(n) = O(n^{\frac{5}{6}}(\ln n)^{\frac{2}{3}})\ , \tag{13}$$

其中 $\mu(m)$ 爲莫比爾斯 (Möbius) 函數，$F(m)$ 爲滿足某些不等式組的整值解組數。1963 年他得到

$$R(n) = O(n^{\frac{2}{3}}(\ln n)^{6})\ , \tag{14}$$

這一紀錄至今未被打破。

維諾格拉多夫的第一基本公式可以解釋成爲關於由

$$x = Q \text{ 、 } x = R \text{ 、 } y = f(x) \text{ 、 } y = 0$$

所圍成的平面區域內的整點個數的一個命題。1925 年 V. 雅尼克 (Jarnik) 證明了，(11) 已是基本上最好可能的結果。由是可知，維諾格拉多夫方法可用於處理域內整點問題。設 $P(x)$ 表示落在球

$$u^2 + v^2 + w^2 \leq x$$

中的整點個數。1963 年維諾格拉多夫證明了

$$P(x) = \frac{4}{3}\pi x^{\frac{3}{2}} + O(x^{\frac{2}{3}}(\ln x)^6)\text{，} \tag{15}$$

這仍是目前已知最好的結果。

華林問題

1770 年，E. 華林 (Waring) 在《代數沉思錄》(*Meditationes algebraicae*) 第 204 − 205 頁上發表了如下的猜想：

每個正整數皆可表爲四個整數的平方和，皆可表爲九個非負整數的立方和，皆可表爲十九個整數的四次方之和 $\cdots$ 等等。

綜觀其言，他實質上提出了如下的問題：對每個給定的整數 $k \geq 2$，是否存在一個只與 k 有關的正整數 $s = s(k)$，使每個正整數皆可表爲至多 s 個非負整數的 k 次方之和? 求最小正整數 $s(k) = g(k)$，使每個正整數皆可表爲 $g(k)$ 個非負整數的 k 次方之和，此即著名的關於 $g(k)$ 的華林問題。若不要求這種表示對每個正整數成立，改爲要求對充分大的正整數皆成立，又以 $G(k)$ 表示滿足這種要求的最小的 $s(k)$，估計 $G(k)$ 的上界即著名的關於 $G(k)$ 的華林問題。

1909 年，D. 希爾伯特 (Hilbert) 首次用多重積分證明了 A. 胡爾維茨 (Hurwitz) 提出而未能證明的一個恆等式，由此即得：對形如 $k = 2^c$ 的冪 k，華林問題中的 $s(k)$ 是存在的。由此再用初等方

法可對一般性的 k 證明 $s(k)$ 的存在性。但希爾伯特方法所得 $s(k)$ 之數值太大，方法也相當複雜，在近代數論的發展中沒有找到進一步的應用。

1920－1928 年間，G.H. 哈代 (Hardy) 與 J.E. 李特爾伍德 (Littlewood) 在總標題爲 "'Partitio numerorum' 的若干問題" (*Some problems of"Partitio numerorum"*) 的七篇論文中，系統地開創並發展了解析數論中一個新方法，此即當今著稱的哈代與李特爾伍德的圓法。而在哈代與 S. 拉馬努金 (Ramanujan) 1918 年發表的一篇論文中已經有了圓法的思想。

1924 年，維諾格拉多夫對希爾伯特關於華林問題的結果給出一個新證明，它相當初等，只用到傅里葉 (Fourier) 級數及外爾 (Weyl) 估計三角和的方法，而沒有用圓法。E. 朗道 (Landau) 在《數論導引》(*Vorlesungen Über Zahlentheorie*，1927) 第一卷第六部分第五章指出，維諾格拉多夫的方法可用於求 $g(k)$ 的相當滿意的上界。1936 年 L.E. 迪克森 (Dickson) 與 S.S. 皮萊 (Pillai) 相互獨立地得到 $g(k)$ 問題近乎最後的解決，其中證明的關鍵部分有賴於對維諾格拉多夫方法的應用。

在哈代與李特爾伍德上述系列文章的 IV 中證明了：若 $s \geq (k-2)2^{k-1}+5$、$k \geq 3$、$R_s(n)$ 是 n 表爲 s 個 k 次方之和的表法數，則對充分大的 n 有

$$R_s(n) \sim \mathcal{S}(n) n^{\frac{s}{k}-1} \frac{\left(\Gamma(1+\frac{1}{k})\right)^s}{\Gamma(\frac{s}{k})} \text{。} \tag{16}$$

其中 $\mathcal{S}(n)$ 大於某個正常數。由此他們首次得出顯式上界

$$G(k) \leq (k-2)2^{k-1}+5 \text{。} \tag{17}$$

在 1925 年發表的 VI 中，他們糾正了上文中一個引理證明中的錯誤

並得到：對 $k \geq 4$ 有

$$G(k) \leq (k-2)2^{k-2} + k + 5 + \left[\frac{(k-2)\ln 2 + \ln(1 - \frac{2}{k})}{\ln(1 + \frac{1}{k-1})} \right] 。 \tag{18}$$

他們的方法是考慮無限和

$$f(z) = \sum_{m=1}^{\infty} z^{m^k}$$

及其 s 次冪

$$f(z)^s = \sum_{n=0}^{\infty} R_s(n) z^n 。$$

由柯西積分公式有

$$R_s(n) = \frac{1}{2\pi i} \int_C f(z)^s z^{-n-1} dz ， \tag{19}$$

C 是以原點爲圓心，半徑爲 ρ $(0 < \rho < 1)$ 的圓周，他們在 $s \geq s_0(k)$ 且 n 充分大時找到一種漸近計算積分 (19) 的方法。

1928 年，維諾格拉多夫改爲考慮有限和

$$S(\alpha) = \sum_{m=1}^{N} e(\alpha m^k) \tag{20}$$

及其 s 次冪

$$S(\alpha)^s = \sum_{m=1}^{sn} R_s(m,n) e(\alpha m) ， \tag{21}$$

這裡 $e(x) = e^{2\pi i x}$ 、$N = [n^{\frac{1}{k}}]$，而 $R_s(m,n)$ 是 m 表爲 s 個不超過 N 的非負整數 k 次冪和的表法個數。易見

$$R_s(n) = \int_0^1 S(\alpha)^s e(-\alpha n) d\alpha 。 \tag{22}$$

由此他也導出了 (16)，並證明了 (17)。這大大簡化了哈代與李特爾伍德的方法，也爲解決數論中各種困難的的問題開闢了一條更爲廣闊的道路。此後，他多次回到這一問題。他關於漸近公式成立時 $G(k)$ 上界的最後結果是

$$G(k) \leq 2k^2(2\ln k + \ln\ln k + 5) \quad (k \geq 4)。 \tag{23}$$

如果放棄漸近公式 (16) 而只證 $R_s(n) > 0$，則可得到 $G(k)$ 的好得多的上界。1934 年，維諾格拉多夫第一個獲得階爲 $k\ln k$ 的上界

$$G(k) < 6k\ln k + (\ln 216 + 4)k \quad (k \geq 4)。 \tag{24}$$

顯然可證有

$$G(k) > k，\tag{25}$$

故 (24) 中的階 $k\ln k$ 已基本上是最好可能的了。1959 年他得到：對 $k > 170000$ 有

$$G(k) < k(2\ln k + 4\ln\ln k + 2\ln\ln\ln k + 13)，\tag{26}$$

並且得到

$$\overline{\lim_{k\to\infty}}\frac{G(k)}{k\ln k} \leq 2。 \tag{27}$$

1985 年 A. A. 卡拉楚巴 (Карачуба) 用 $p-$adic 方法證明了，對 $k \geq 4000$ 有

$$G(k) < 2k(\ln k + \ln\ln k + 6)，\tag{28}$$

這是目前 $G(k)$ 上界的最好結果。對較小的 k，更好的結果請見所列文獻及專著。

哥德巴赫猜想

1742 年，德國數學家 C. 哥德巴赫 (Goldbach) 在與 L. 歐拉 (Euler) 的幾次通信中提出了整數表爲質數和的兩個猜想，用現代語言來說，就是：

(A)　每個 ≥ 6 的偶數都是兩個奇質數之和，

(B)　每個 ≥ 9 的奇數都是三個奇質數之和。

這就是當今著稱的哥德巴赫猜想，(A) 通常稱爲關於偶數的哥德巴赫猜想，(B) 稱爲關於奇數的哥德巴赫猜想。直到 1900 年希爾伯特在巴黎召開的第二屆國際數學家大會上的著名演講發表之前，有關這個猜想的研究尚未取得任何實質性的進展。

哈代與李特爾伍德在他們上述系列論文的 III 與 V (發表於 1923 年) 中，用圓法對哥德巴赫猜想進行了研究。鑒於圓法與維諾格拉多夫方法對哥德巴赫猜想的主要貢獻在於解決了猜想 (B)，而對猜想 (A) 只能得到 “幾乎全體偶數皆可表爲二奇質數之和” 這樣的結果，本文中只對涉及猜想 (B) 的結果加以討論。

在 III 中，哈代與李特爾伍德考慮了函數

$$f(x) = \sum_{p} x^p \ln p \tag{29}$$

及其 r 次冪

$$f(x)^r = \sum_{n=1}^{\infty} v_r(n) x^n \ ， \tag{30}$$

這裡

$$v_r(n) = \sum_{p_1+\cdots+p_r=n} \ln p_1 \cdots \ln p_r \ 。 \tag{31}$$

於是

$$v_r(n) = \frac{1}{2\pi i} \int_{C_1} (f(z))^r z^{-n-1} dz \ ， \tag{32}$$

這裡 C_1 是以原點爲中心、半徑爲 $e^{-\frac{1}{n}}$ 的圓周。與前類似地將積分 (32) 分成主項與餘項，他們在餘項的估計中遇到對狄利克雷 L 函數的零點分佈缺乏了解這一重大困難。不得已假設下面的猜想 (R) 成立：

(R)　存在實數 θ、$\frac{1}{2} \le \theta < \frac{3}{4}$，使得所有狄利克雷 L 函數的全部零點皆位於半平面 $\mathrm{Re} z \le \theta$ 中。

在此假設下，他們證明了：充分大的奇數 n 表爲三個奇質數之和的表法個數 $N_3(n)$ 有漸近式

$$N_3(n) \sim C_3 \frac{n^2}{(\ln n)^3} \prod_{p|n} \left(\frac{(p-1)(p-2)}{p^2 - 3p + 3} \right) , \tag{33}$$

其中

$$C_3 = \prod_{p>2} \left(1 + \frac{1}{(p-1)^3} \right) 。 \tag{34}$$

特別地，當 (R) 成立時，每個充分大的奇數 n 皆可表爲三個奇質數之和。

維諾格拉多夫在他於 1937 年發表的著名論文中改爲考慮過質數值求和的有限三角和

$$S(\alpha, n) = \sum_{p \le n} e(\alpha p) 。 \tag{35}$$

用 I_n 記 n 表爲三個奇質數和的表法個數，則與 (22) 式同法有

$$I_n = \int_0^1 S(\alpha, n)^3 e(-\alpha n) d\alpha 。 \tag{36}$$

適當將 $[0, 1]$ 劃分成基本區間 (也稱優弧) 與餘區間 (也稱劣弧) 兩部分，相應的積分分別記爲 $I_n(1)$ 與 $I_n(2)$。

對 $I_n(1)$ 用西格爾 (Siegel) − 瓦爾菲茨 (Walfisz) 定理不難給出其主項及餘項估計。爲估計 $I_n(2)$，維諾格拉多夫對形如 (35) 的質變數三角和給出了非平凡的上界估計，從而不用任何假設證明了：存在常數 B_0 (現在稱爲維諾格拉多夫常數)，每個奇數 $n \ge B_0$ 皆可表爲三個奇質數之和。

應用上面的證法，常數 B_0 無法算出來，這是因爲上面證明中用到的西格爾－瓦爾菲茨定理涉及的常數不能有效地算出。爲具體求出 B_0 的上界，可用較弱的佩奇 (Page) 定理代替西格爾－瓦爾菲茨定理。1956 年，K. Г. 博羅茲德基 (Бороздкий) 求得

$$B_0 \leq \exp(\exp 16.038)\ , \tag{37}$$

這個值現在完全可以得到較大的改進。

同年，維諾格拉多夫對形如

$$\sum_{p\leq n} e(f(p)) \tag{38}$$

的更一般的質變數三角和得到非平凡的上界估計，這裡 $f(x)$ 爲實係數多項式。特別當 $f(x)=x^k$ 時他對華林－哥德巴赫問題得到如下結果：

設 I_n^* 是 n 表爲 s 個質數的 k 次冪之和的表法個數，$k\geq 5$、$s\geq [2k^2(2\ln k+\ln\ln k+5)]$，則 $n\to\infty$ 時有

$$I_n^* \sim \mathcal{S}(n)\frac{\left(\Gamma(\frac{1}{k})\right)^s}{\Gamma(\frac{s}{k})}\frac{n^{\frac{s}{k}-1}}{(\ln n)^s}\ , \tag{39}$$

其中

$$\begin{aligned}
\mathcal{S}(n) &= \sum_{r=1}^{\infty} A_s(n,r)\ ,\\
A_s(n,r) &= \sum_{\substack{h=1\\(h,r)=1}}^{r}\left(\frac{W_{h,r}}{\varphi(r)}\right)^s e\left(\frac{-hn}{r}\right)\ ,\\
W_{h,r} &= \sum_{\substack{l=1\\(l,r)=1}}^{r} e\left(\frac{hl^k}{r}\right)\ 。
\end{aligned}$$

有關其它形狀的質變數三角和估計及應用請見的列專著及文獻。

模 1 均勻分佈

先考慮一個簡單問題。設 θ 爲一個實數，對任意給定的正整數 N，考慮區間 $[0,1)$ 中如下 $N+1$ 個實數

$$0、\{\theta\}、\cdots、\{N\theta\}。$$

如果將 $[0,1)$ 等分成 N 個長爲 $\frac{1}{N}$ 的子區間，則至少有兩個整數 a、b、$0 \le a < b \le N$，使 $\{a\theta\}$ 與 $\{b\theta\}$ 在同一子區間中，即

$$|\{b\theta\} - \{a\theta\}| < \frac{1}{N}。$$

定義 $k = b-a$、$h = [b\theta] - [a\theta]$，則有一對整數 h、k、$0 < k \le N$，使

$$|k\theta - h| < \frac{1}{N} \le \frac{1}{k}，$$

事實上可以要求 $(h,k)=1$，又在 θ 爲無理數時，滿足上述要求的數對 h、k 有無窮多對。完全類似地可證下述命題：設 θ 爲無理數，a 爲任一實數，則有無窮多對整數 h_n、$k_n(k_n>0)$ 使

$$|\theta k_n - h_n - a| < \frac{3}{k_n}。$$

由此立即推出，$[0,1)$ 中每一點都是點集 $\{m\theta\}$ $(m=1、2、\cdots)$ 的極限點。那麼，點集 $\{m\theta\}$ 在 $(0,1)$ 中是否“均勻分佈”呢?爲了使“均勻分佈”意義明確，我們給出如下的定義：設 $w = (x_n)$, $n=1、2、\cdots$ 是一個給定的實數列，我們稱 w 是模 1 均勻分佈的，如果對每對實數 a、b、$0 \le a < b \le 1$ 有

$$\lim_{N\to\infty} \frac{A([a,b)\ ;\ N\ ;\ w)}{N} = b-a，$$

這裡 $A([a,b)\ ;\ N\ ;\ w)$ 表示 $x_1、\cdots、x_N$ 中使小數部分 $\{x_n\}$ 落在 $[a,b)$ 中的項的個數。

對如何判別均勻分佈 (mod 1)，有如下重要的外爾判別法：數列 (x_n)，$n = 1、2、\cdots$ 爲均勻分佈 (mod 1) 的充分必要條件是，對所有整數 $h \neq 0$ 有

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(hx_n) = 0。$$

因此，能否對形如

$$\sum_{n=1}^{N} e(hx_n)$$

的三角和給出適當的估計，是判別數列是否均勻分佈的關鍵。在某些重要而又困難的情形，維諾格拉多夫方法是解決這一關鍵困難的基本工具。

設 α 爲一給定無理數，定義

$$x_n = \alpha p_n，n = 1、2、\cdots，$$

這裡 p_n 表示第 n 個質數，則由維諾格拉多夫估計 (35) 型和的方法易得

$$\begin{aligned} \sum_{n=1}^{N} e(h\alpha p_n) &= \sum_{p\le p_N} e(h\alpha p) \\ &= o(\pi(p_N)) = o(N)， \end{aligned}$$

故由外爾判別法立即證得 (αp_n) 是均勻分佈的。完全類似地可證：數列 $(f(p_n))$，$n = 1、2、\cdots$ 爲均勻分佈 (mod 1)，這裡 $f(x)$ 是首項係數爲無理數的實係數多項式。值得一提的是，1937 年 P. 屠阮 (Turán) 首次在假設 GRH 爲眞的條件下證明了 (αp_n) 的均勻分佈性。

帶誤差項的質數定理

令 $\pi(x)$ 表示不超過 x 的質數個數，尋求它當 x 充分大時的漸近表示是十九世紀近百年中數學家們的一項中心任務。$1848 - 1850$

年，俄國數學家 П. Л. 切比雪夫 (Чебышев) 首開記錄，證得

$$\begin{aligned} 0.92129 &\le \varliminf_{x\to\infty} \frac{\pi(x)}{\dfrac{x}{\ln x}} \le 1 \le \varlimsup_{x\to\infty} \frac{\pi(x)}{\dfrac{x}{\ln x}} \\ &\le (1.2)(0.92129) \end{aligned} \tag{40}$$

1859 年，黎曼在其著名論文中用新的解析方法揭示出 ζ 函數與質數分佈之間的深刻聯繫。1896 年，J. 阿達瑪 (Hadamard) 與 C.J. 德拉瓦萊－普桑 (de la Vallée Poussin) 相互獨立地證明了質數定理：

$$\lim_{x\to\infty} \frac{\pi(x)}{\dfrac{x}{\ln x}} = 1 \text{，} \tag{41}$$

這等價於

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{li}x} = 1 \text{，} \tag{42}$$

這裡 $\mathrm{li}x = \int_2^x \dfrac{du}{\ln u}$。

此後，數學家們一直致力於求 $\pi(x) - \mathrm{li}x$ 的最佳誤差。1901 年，H. 馮科克 (von Koch) 在黎曼猜想成立的假設下證明了有

$$\pi(x) = \mathrm{li}x + O(\sqrt{x}\ln x)\text{。} \tag{43}$$

熟知，只要對 ζ 函數在 $\sigma = 1$ 附近的值給出適當的估計，就可以得出 $\zeta(s)$ 無零點區域的對應結果，從而給出 $\pi(x) - \mathrm{li}x$ 的相應估計。而在估計 ζ 函數鄰近 $\sigma = 1$ 的階時，維諾格拉多夫的三角和方法是相當有效的。1958 年，維諾格拉多夫與 H. M. 科羅博夫 (Коробов) 相互獨立地得到

$$\pi(x) = \mathrm{li}x + O(xe^{-\alpha(\ln x)^{0.6+\varepsilon}}) \tag{44}$$

($a > 0$、$\varepsilon > 0$ 爲任意給定的實數)，相應的 ζ 函數無零點區域爲

$$\sigma \ge 1 - \frac{C}{(\ln(|t|+3))^{\frac{2}{3}+\varepsilon}} \text{，} \tag{45}$$

這些都是迄今已知的最好的結果。

本橋洋一 (Motohashi Yoichi) 曾用篩法對形如

$$\sigma \geq 1 - \frac{C}{(\ln(|t|+3))^{\frac{2}{3}}(\ln\ln(|t|+3))^{\frac{1}{3}}} \tag{46}$$

的無零點區域給出一個初等證明，而蒙哥馬利則用另外的方法給出 (46) 的另一證明，這些請見他們各自的專著。

主要著作評介及對中國數論界的影響

維諾格拉多夫一生發表過一百多篇論文，出版過四部專著及兩部選集。他的四部專著中，影響最大的是其中的三部：《數論基礎》(Основы теории чисел，1936)，以下簡稱《基礎》；《數論中的三角和方法》(Метод тригонометрических сумм в теории чисел，1947)，以下簡稱《方法》；《三角和方法的特殊變體》(Особые варианты метода тригонометрических сумм，1976)，以下簡稱《變體》。

《基礎》一書初版於 1936 年，先後譯成匈牙利文 (1952)、捷克文 (1953)、英文 (1954)、波蘭文 (1954)、德文 (1955)、日文 (1961)、西班牙文 (1971) 等多種文字。1952 年由上海商務印書館初次出中文版，1956 年由北京高等教育出版社出新一版，譯者裘光明。我國著名數學家、中國科學院數學研究所第一任所長華羅庚教授爲中譯本撰寫了一篇指導性的介紹，題爲“介紹《數論基礎》”，對書的內容、習題及維諾格拉多夫的研究成果，給了極高的評價。

《基礎》一書共分六章，介紹了初等數論的一些基本內容。每章後習題分兩部分，計算題強調了計算技巧的訓練；而通過理論性的習題向讀者介紹了許多著名的數論問題，如：有理數逼近實數、切比雪夫不等式、圓內整點問題、狄利克雷除數問題、V. 布龍 (Brun) 篩法、三角和估計、函數值的分數部分的估計、佩爾

(Pell) 方程 、 波利亞 − 維諾格拉多夫不等式 、 剩餘與非剩餘的分佈等 。 使初學者也能對近代解析數論的一些問題與方法 ， 特別是維諾格拉多夫方法的基本技巧有所了解 。 即使在今天 ， 它也不失爲一本好的參考書 。

《 方法 》一書是維諾格拉多夫方法的代表作 。 1947 年初版 ， 1954 年出了英文版 ， 次年在我國《 數學進展 》1 卷 1 期上印行了中文譯本 ， 譯者越民義 。 由於維諾格拉多夫在其科學研究最初十年中的重要成就 ， 朗道在他的前述專著中曾專闢一章對他的方法加以介紹 。 此後出版的許多重要數論專著中都有關於維諾格拉多夫方法的專門介紹 。

在《 方法 》一書的引言中 ， 維諾格拉多夫介紹了他本人自 1934 年以來所創立的三角和方法的要旨 、 應用及歷史 。 他指出 ， 這一方法的最基本結論是形如

$$I = \int_0^1 \cdots \int_0^1 |T|^{2b} d\alpha_n \cdots d\alpha_1$$

的積分之估計 ， 此即著名的維諾格拉多夫平均值定理 ， 這裡

$$T = \sum_{x=1}^{p} e(f(x)) \ ,$$

而

$$f(x) = \alpha_n x^n + \cdots + \alpha_1 x$$

爲實係數多項式 。 目前估計 I 上界的最滿意的方法係由卡拉楚巴於 1965 年給出的 ， 這方面的理論已推廣到多重三角和中 ， 這些發展均基於卡拉楚巴 1962 − 1966 年間提出的一種新的 p − adic 形式的維諾格拉多夫方法 (參見《 斯捷克洛夫數學研究所著作集 》英譯本 1986 年第 3 期 (*Proc. of the Steklov Institute of Math.* ， 1986 ， Issue 3 ， 3 − 30)) 。

維諾格拉多夫方法的關鍵技巧在於對形如

$$W=\sum_{x\le X}\sum_{y\le Y}\xi(x)\eta(y)e(\alpha xy)$$

的雙重三角和給出非平凡估計，這裡 $\xi(x)$、$\eta(y)$ 是任意的複值函數，α 爲實數且

$$\alpha=\frac{a}{q}+\frac{\theta}{q^2}\text{、}(a,q)=1\text{、}|\theta|\le 1\text{。}$$

由柯西不等式有

$$|W|^2\le\sum_{x\le X}|\xi(x)|^2\sum_{x\in X}\left|\sum_{y\le Y}\eta(y)e(\alpha xy)\right|^2\text{，}$$

右方的二重和可按幾何級數來計算，由此可得 W 的適當估計。當然，如何把一個數論問題與一個恰當的二重三角和聯繫起來，這是需要相當技巧的。在該書中作者對其方法的基本工具、技巧及在華林問題、多項式值的分數部分之分佈、華林－哥德巴赫問題中的應用作了較詳盡的介紹。

《變體》一書出版於 1976 年，它與《方法》的不同之處是在於，《變體》討論的是其方法的較爲簡單的變體 (指不需要平均值定理爲基礎) 所涉及的一些應用，如球內整點問題，$G(k)$ 上界估計，哥德巴赫奇數猜想及若干特殊的質變數三角和估計等，最後一章給出他的方法的某種初等形式維諾格拉多夫方法及其著作對中國及世界數學界產生了重大影響。華羅庚教授三十年代起的許多研究工作都受到維諾格拉多夫方法的深刻影響。1941 年，華羅庚教授將自己對維諾格拉多夫方法的研究成果寫成《堆壘素數論》一書，寄交蘇聯斯捷克洛夫數學研究所作爲專刊發表，得到維諾格拉多夫院士的讚賞和支持。時因二次大戰，該書俄文版推遲到 1946 年才正式出版。維諾格拉多夫院士還邀請華羅庚教授訪問蘇

聯。華羅庚教授在數學研究所培養的第一批研究人材中，就有相當數量的人深入學習過維諾格拉多夫方法，並在後來的研究工作中反覆運用這一方法取得過出色的成就。

1988 年夏天在北京舉行的“紀念華羅庚數論與分析國際會議”，就有卡拉楚巴等維諾格拉多夫學派傳人參加。這對加強中蘇兩國的學術交流，恢復並發展由維諾格拉多夫與華羅庚所建立的兩國數學界 (尤其是數論學界) 的傳統友誼，將起到良好的作用。

文　　獻

原始文獻

[1] И. Виноградов, Основы теории чисел, Единенное Наухно–Техническое издательство, 1936 (中譯本：И. 維諾格拉多夫，數論基礎，裘光明譯，商務印書館，1952；高等教育出版社 (新一版)，1956)。

[2] И. Виноградов, Метод тригонометрических сумм в теории чисел, Труды Матем. нн–та Им. В. А. Стеклова, т. 23(1947), 1－109 (中譯文：И. 維諾格拉多夫，數論中的三角和方法，越民義譯，數學進展，1(1955)，3－106)。

[3] И. Виноградов, Особые варианты метода тригонометрических сумм, Наука, 1976。

[4] И. Виноградов, Избранные труды, Изд. АН СССР, 1952。

[5] *Ivan Matveevic Vinogradov selected works*, Springer–Verlag, 1985。(由於選集中已收入其主要論文著作，且有他的論文詳細目錄，故其主要論文不再列出。)

研究文獻

[6] W. Narkiewicz, *Classical problems in number theory*, PWN–Polish Scientific Publishers, 1986。

[7] C.F. Gauss, *Disquisitiones arithmeticae*, Leipzig, Fleischer, 1801, reprinted in vol. 1 of Gauss's Werke, Yale Univ. Press, 1966。

[8] P. Bachmann, *Analytische Zahlentheorie*, Leipzig, 1894。

[9] E. Landau, *Vorlesungen Über Zahlentheorie*, Leipzig, 1927。

[10] R.C. Vaughan, *The Hardy–Littlewood method*, Cambridge, 1981

[11] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, fifth edition, The English Language Book Society and Oxford University Press, 1981 。

[12] A. Walfisz, *Weylsche Exponentialsummen in der Neueren Zahlentheorie*, VEB Deutscher Verlag der Wiss., 1963 。

[13] E.C. Titchmarsh, *The theory of the Riemann zeta-function*, second edition, Clarendon Press, 1986 。

[14] K. Prachar, *Primzahlverteilung*, Springer-Verlag, 1957 。

[15] H. Davenport, *Multiplicative number theory*, second edition, Springer–Verlag, 1980 。

[16] H.L. Montgomery, *Topics in multiplicative number theory*, Springer–Verlag, 1971 。

[17] A. Ivic, *The Riemann zeta–function*, Wiley–Interscience, 1985

[18] H. Halberstam and C. Hooley, *Recent progress in analytic number theory*, vol. I, Academic Press, 1981 。

[19] А. А. Карачуба, Основы аналитической теории чисел, Наука, 1975 (中譯本： A. A. 卡拉楚巴 ， 解析數論基礎 ， 潘承彪 、 張南岳譯 ， 科學出版社 ， 1984 年) 。

[20] L. Kuipers and H. Niederreiter, *Uniform Distribution of sequences*, John Wiley & Sons, 1974 。

[21] 華羅庚 ， 堆壘素數論 ， 科學出版社 ， 1953 。

[22] 華羅庚 ， 指數和的估計及其在數論中的應用 ， 科學出版社 ， 1963

[23] 華羅庚 ， 數論導引 ， 科學出版社 ， 1957 。

[24] 王元 ， 哥德巴赫猜想研究 ， 黑龍江教育出版社 ， 1987 。

[25] 閔嗣鶴 ， 數論的方法 ， 下册 ， 科學出版社 ， 1981 。

[26] 潘承洞與潘承彪 ， 哥德巴赫猜想 ， 科學出版社 ， 1981 。

[27] J.W.S. Cassels and R.C. Vaughan, *Ivan Matveevich Vinogradov (Obituary)*, Bull. London Math. Soc., 17(1985), 584－600 (中譯本 ： J.W.S. 卡斯爾斯和 R.C. 沃恩 ， 依萬 • 馬特維也維奇 • 維諾格拉朵多 ， 張明堯譯 ， 數學譯林 ， 6(1987) ， 2 ， 第 147－156 頁) 。

[28] Ю. В. Андропов и другие, Академик Иван Матвеевич Виног-

радов, Усиехц Матем. Наук. 38(1983), 6(234), 105－106 (原載 1983 年 3 月 23 日《眞理報》(Правда))。