第42卷　第2期　Vol.42　No.2
山　东　大　学　学　报（理　学　版）
JOURNAL OF SHANDONG UNIVERSITY
2007年2月　Feb. 2007

文章编号:1671-9352(2007)02-0001-18

二次 Waring-Goldbach 问题

刘建亚，展　涛

（山东大学　数学与系统科学学院，山东　济南　250100）

摘要:本文简述二次 Waring-Goldbach 问题的最新进展,具体内容包括:Waring-Goldbach 问题,圆法,具有五个几乎相等变量的华罗庚定理,扩张主区间,四个素数平方之和的主区间,Dirichlet 多项式的均值定理,四个素数平方之和的余区间与例外集,素变数三角和的新估计,四个素数平方之和与筛法,殆素数变量的 Lagrange 定理,Linnik-Gallagher 问题,再论具有五个几乎相等变量的华罗庚定理,三个殆素数的平方和,Sarnak 猜想与三元二次型.

关键词: 二次 Waring-Goldbach 问题; 圆法; 筛法; 自守形式; Jacquet-Langlands 对应; Selberg 特征值猜想

中图分类号:O156　　　**文献标识码**:A

The quadratic Waring-Goldbach problem

LIU Jian-ya and ZHAN Tao

(School of Math. and System Sci., Shandong Univ., Jinan 250100, Shandong, China)

Abstract: The purpose of this paper is to briefly survey recent progress towards the quadratic Waring-Goldbach problem. Contents of the paper are as follows: the Waring-Goldbach problem, the circle method, Hua's theorem with five almost equal prime variables, treatment of the enlarged major arcs, the major arcs in the representation by four squares of primes, mean-value estimates for Dirichlet polynomials, the minor arcs and exceptional set in the representation by four squares of primes, estimates of exponential sums over primes, sieve methods in the representation by four squares of primes, Lagrange's theorem with almost prime variables, the Linnik-Gallagher problem, new results for Hua's theorem with five almost equal prime variables, sums of three squares of almost primes, Sarnak's conjecture and ternary quadratic forms.

Key words: quadratic Waring-Goldbach problem; circle method; sieve methods; automorphic form; Jacquet-Langlands correspondence; Selberg's eigenvalue conjecture

1　Waring-Goldbach 问题

Waring-Goldbach 问题旨在研究将满足必要条件的正整数 n 表为素数方幂之和的可能性,即

$$n = p_1^k + \cdots + p_s^k, \tag{1.1}$$

这里的 k 是事先给定的正整数,而 $s = s(k)$ 依赖于 k. 堆垒素数论的经典定理[72,28] 指出,对于每个 k 都存在充分大的 s, 使得(1.1) 可解. 但是对于固定的 k,我们希望 $s = s(k)$ 尽可能地小. 著名的 Goldbach 猜想只是线性的 Waring-Goldbach 问题. 本文介绍二次 Waring-Goldbach 问题及其最新进展; 关于 Goldbach 猜想,请参看潘承洞和潘承彪[59] 以及本文作者的综述文章[51];关于三次以上的 Waring-Goldbach 问题,请参看 Kumchev 和 Tolev 的综述文章[34].

收稿日期:2007-01-22
基金项目:国家自然科学基金重点项目(10531060);教育部科学技术重大项目资助(305009)

作者简介:刘建亚(1964-　),男,博士,教授,从事数论研究.
展　涛(1963-　),男,博士,教授,从事数论研究.

二次 Waring-Goldbach 问题的研究始于华罗庚 1938 年的经典论文[26]. 设 $\Lambda(n)$ 是 von Mangoldt 函数,定义

$$R_s(n) = \sum_{n = n_1^2 + \cdots + n_s^2} \Lambda(n_1) \cdots \Lambda(n_s). \tag{1.2}$$

这个 $R_s(n)$ 就是 n 表示为 s 个素数平方之和的加权表法个数. 应用 Hardy 和 Littlewood 提出的圆法,可以猜测 $R_s(n)$ 的阶. 一个非常乐观的猜想指出,若 $s \geqslant 3$,则

$$R_s(n) = C\mathfrak{S}_s(n) n^{s/2-1} + O\left(\frac{n^{s/2-1}}{\log^A n}\right), \tag{1.3}$$

这里 $C = C(s) > 0$ 是绝对常数, $\mathfrak{S}_s(n)$ 是奇异级数,而 $A > 0$ 是常数. 对固定的 $s \geqslant 4$,都可以定出关于 n 的同余条件,使得在这些同余条件下 $\mathfrak{S}_s(n) \gg 1$,从而(1.3) 指出

$$R_s(n) \gg n^{s/2-1}, \tag{1.4}$$

进而方程(1.1) 当 $k = 2$ 时有解. 华罗庚[26] 证明了,当 $s = 5$ 时(1.3) 成立,当 $s = 3$ 时(1.3) 对几乎所有的 n 成立;他还研究了 $\mathfrak{S}_s(n)$ 的性质,得到了相应的必要同余条件. 以下是华罗庚的经典定理.

定理 1.1 (1) 若 n 充分大且满足

$$n \equiv 5 \pmod{24}, \tag{1.5}$$

则 n 可以表示为五个素数的平方之和,

$$n = p_1^2 + \cdots + p_5^2. \tag{1.6}$$

(2) 几乎所有满足

$$n \equiv 3 \pmod{24},\ 5 \quad n \tag{1.7}$$

的 n 都可以表示为三个素数的平方之和,

$$n = p_1^2 + p_2^2 + p_3^2. \tag{1.8}$$

从定理 1.1(2) 可以推出

推论 1.2 几乎所有满足

$$n \equiv 4 \pmod{24} \tag{1.9}$$

的 n 都可以表示为四个素数的平方之和

$$n = p_1^2 + \cdots + p_4^2. \tag{1.10}$$

著名的 Lagrange 定理指出,每个正整数都可以表示为四个整数的平方之和. 定理 1.1 和推论 1.2 可以和 Lagrange 定理相比较. 特别地,可以提出如下猜想.

猜想 1.3 对所有满足必要条件(1.9) 的充分大的 n,表示式(1.10) 都成立.

这个猜想比三个素数平方之和的相应猜想要弱,但是仍然比偶数的 Goldbach 猜想强. 为了看出后半句的断言合理,我们回忆 Rieger 定理[63].

定理 1.4 若 f 能表示为 $f = p_1^2 + p_2^2$,则

$$\sum_{f \leqslant x} 1 \sim \frac{\pi}{2} \frac{x}{\log^2 x}. \tag{1.11}$$

Rieger 定理 1.4 指出,序列 $\{f : f = p_1^2 + p_2^2\}$ 的密度低于素数序列的密度. 猜想 1.3 相当于加法问题

$$n = f_1 + f_2,$$

故其难度大于偶数的 Goldbach 猜想. 有鉴于此,猜想 1.3 引起了很大关注,在此方向上的研究也取得了很多进展,而且这里产生的新思想也被广泛地应用于其他加法问题.

2 圆法

圆法是用来解决众多数论问题的一个强有力的思想,而不是一个一成不变的方法. 其出发点是将定义在整数集合上的 Dirac 函数 $\delta(n)$ 表示为加法特征;这是一个天才的思想.

取定一个大实数 Q. 设 $a'/q' < a/q < a''/q''$ 是三个相邻的 Farey 分数,其分母都 $\leqslant Q$. 定义

$$\mathfrak{M}\left(\frac{a}{q}\right)=\left(\frac{a+a'}{q+q'},\frac{a+a''}{q+q''}\right].$$

所以$(0,1]$就是这些 $\mathfrak{M}(a/q)$ 的非交并

$$(0,1]=\bigcup_{q\leqslant Q}\ \bigcup_{a \bmod q}{}^{*}\ \mathfrak{M}\left(\frac{a}{q}\right),$$

Hardy 和 Littlewood[18] 考虑了恒等式

$$\delta(n)=\sum_{q\leqslant Q}\sum_{a \bmod q}{}^{*}\int_{\mathfrak{M}(a/q)}e(n\alpha)\mathrm{d}\alpha,\tag{2.1}$$

其中 $e(x)=\mathrm{e}^{2\pi\mathrm{i}x}$,并由此出发实施圆法.设

$$S(\alpha)=\sum_{\sqrt{x}<m\leqslant x}\Lambda(m)e(m^2\alpha),\tag{2.2}$$

这里的 x 是一个参数;在本节中 $x=\sqrt{n}$. 这样,(2.1) 指出

$$R_s(n)=\sum_{q\leqslant Q}\sum_{a \bmod q}{}^{*}\int_{\mathfrak{M}(a/q)}S^s(\alpha)e(n\alpha)\mathrm{d}\alpha.\tag{2.3}$$

按照圆法的思路估计(2.3), 需要取另外一个参数 P, $1\leqslant P\leqslant Q$, 并将所有 $\mathfrak{M}(a/q)$ 按照分母 q 的大小分成两类:第一类 $1\leqslant q\leqslant P$, 称为主区间;第二类 $P<q\leqslant Q$,称为余区间. 所有主区间的并记为 $\mathfrak{M}$,所有余区间的并记为 $\mathfrak{m}$.

$$R_s(n)=\left\{\int_{\mathfrak{M}}+\int_{\mathfrak{m}}\right\}S^s(\alpha)e(-n\alpha)\mathrm{d}\alpha.\tag{2.4}$$

为了证明定理 1.1(1),华罗庚在(2.4) 中取

$$P=\log^B n,\ Q=\frac{n}{P\log^C n},\tag{2.5}$$

其中 B,C 是依赖于 A 的正常数. 因为 P 只是 $\log n$ 的方幂,所以在每个主区间 $\mathfrak{M}(a/q)$ 上可以直接利用 Siegel-Walfisz 定理,从而得到 $S(\alpha)$ 的渐近公式

$$S(\alpha)=\frac{C(q,a)}{\varphi(q)}\sum_{m\leqslant x}e(m^2\alpha)+O(x\log^{-A}x),\tag{2.6}$$

其中 $\varphi(q)$ 是 Euler 函数,而

$$C(q,a)=C(\chi^0,a),\ C(\chi,a)=\sum_{m=1}^{q}\bar{\chi}(h)e\left(\frac{ah^2}{q}\right),\tag{2.7}$$

这里 $\chi \bmod q$ 是 Dirichlet 特征. 利用(2.6) 和(2.7),容易得到主区间上积分的渐近公式,即

$$\int_{\mathfrak{M}}S^5(\alpha)\mathrm{d}\alpha=C\mathfrak{S}_5(n)n^{3/2}+O\left(\frac{n^{3/2}}{\log^A n}\right),\tag{2.8}$$

这里的 $C>0$ 是绝对常数. 为了估计余区间上的积分,需要华罗庚不等式

$$\int_0^1|S(\alpha)|^4\mathrm{d}\alpha\ll n\log n\tag{2.9}$$

和 Vinogradov[71] 关于素变数三角和的估计

$$\sup_{\alpha\in\mathfrak{m}}|S(\alpha)|\ll x\log^{-2A}x.\tag{2.10}$$

综合(2.9) 和(2.10),得

$$\int_{\mathfrak{m}}S^5(\alpha)\mathrm{d}\alpha\ll(\sup_{\alpha\in\mathfrak{m}}|S(\alpha)|)\int_0^1|S(\alpha)|^4\mathrm{d}\alpha\ll n^{3/2}\log^{-A}n.\tag{2.11}$$

最后,结合(2.11) 和(2.8),就证明了(1.3) 当 $s=5$ 时成立.

这就是定理 1.1(1) 的证明概要.定理 1.1(2) 的证明类似.

3　具有五个几乎相等变量的华罗庚定理

1996 年,本文作者[49] 深化了华罗庚的五素数平方定理,证明了定理 1.1(1) 中的五个素数可以几乎相等.

定理 3.1　假设广义 Riemann 猜想.若 n 充分大且满足(1.5),则 n 可以表示为五个几乎相等的素数的平

方之和

$$\begin{cases} n = p_1^2 + \cdots + p_5^2, \\ | p_j - \sqrt{n/5} | \leqslant U, \end{cases} \tag{3.1}$$

其中 $U = n^{9/20+\varepsilon}$.

这里,我们使用广义 Riemann 猜想是迫不得已.为了看出这一点,我们注意,方程(3.1)的解数 $R_5(n, U)$ 的阶应该是

$$R_5(n, U) \asymp \frac{U^4}{n^{1/2}}. \tag{3.2}$$

为了应用圆法证明定理 3.1,必须证明余区间上的积分的阶低于 $U^4 n^{-1/2}$. 现在应用本文作者[49] 的估计,有

$$S(\alpha, U) := \sum_{n_1 < m \leqslant n_2} \Lambda(m) e(m^2 \alpha) \ll U^{1+\varepsilon} \left(\frac{1}{q} + \frac{n^{1/4}}{U} + \frac{n^{2/3}}{U^2} + \frac{qn^{1/2}}{U^3} \right)^{1/4}, \tag{3.3}$$

其中 $n_1 = \sqrt{n/5} - U$, $n_2 = \sqrt{n/5} + U$. 从而得到

$$\sup_{\alpha \in \mathfrak{m}} | S(\alpha, U) | \ll U^{1+\varepsilon} P^{-1/4},$$

进而,类似于(2.11)有

$$\int_{\mathfrak{m}} S^5(\alpha, U) \mathrm{d}\alpha \ll \left(\sup_{\alpha \in \mathfrak{m}} | S(\alpha, U) |\right) \int_0^1 | S(\alpha, U) |^4 \mathrm{d}\alpha \ll \frac{U^{1+\varepsilon}}{P^{1/4}} \cdot U^{2+\varepsilon} \ll \frac{U^{3+\varepsilon}}{P^{1/4}}. \tag{3.4}$$

比较(3.2)和(3.4), 现在必须证明

$$\frac{U^{3+\varepsilon}}{P^{1/4}} \ll \frac{U^4}{n^{1/2}},$$

也就是 $P \gg (\sqrt{n}/U)^{4+\varepsilon}$.注意到 U 的阶必须低于$\sqrt{n}$,因此 P 必须取 n 的某个正方幂.当 q 接近 P 达到 n 的某个正方幂时,Siegel-Walfisz 定理和(2.6)都不再成立,从而导致主区间上的积分无法计算.为了计算主区间上的积分,我们利用了广义 Riemann 猜想,从而 P 可以大到 n 的方幂.

简言之,假设广义 Riemann 猜想是因为我们当时不会处理增大了的主区间.

当然,人们可以使用 Montgomery 和 Vaughan[58] 扩张主区间的办法.这个办法依赖于 Deuring-Heilbronn 现象[36],计算非常繁琐,结果却极不美观. 比如,Bauer[1] 用这个办法证明了可以无条件地将 P 扩大到 n 的一个非常小的方幂,从而推出定理 3.1 对 $U = n^{1/2-\delta}$ 成立,这里的 δ 是一个小正数,其具体数值难以确定.

4 扩张主区间

不使用广义 Riemann 猜想或者 Deuring-Heilbronn 现象处理增大了的主区间就成为了我们后续工作的主题.这个计划的首次实现是在本文作者的[50]中.

定理 4.1 不用广义 Riemann 猜想,定理 3.1 中的 U 可以取为 $n^{12/25+\varepsilon}$.

我们的基本思路是:当 q 大到 n 的方幂时,虽然对单个的 q 公式(2.6)不成立,但是通过对 q 求和,公式(2.6)平均起来是可能成立的.这个对 q 的求和来自(2.3). 上述思路的精神与 Bombieri-Vinogradov 定理相仿.

为此,命 $\alpha = a/q + \lambda$,并把 $S(\alpha, U)$ 表示成

$$S(\alpha, U) = S_1 + S_2 + E, \tag{4.1}$$

其中

$$S_1 = \frac{C(q, a)}{2\varphi(q)} \int_{n_1^2}^{n_2^2} v^{-1/2} e(\lambda v) \mathrm{d}\lambda,$$

$$S_2 = -\frac{1}{2\varphi(q)}\sum_{\chi \bmod q} C(\chi,a)\sum_{|\gamma|\le T}\int_{n_1^2}^{n_2^2} v^{\rho/2-1}e(\lambda v)\mathrm{d}\lambda,$$

而 E 是一个不复杂的余项. 这里的 $C(\chi,a)$ 由(2.7)定义,$\rho=\beta+\mathrm{i}\gamma$ 表示 $L(s,\chi)$ 的非显然零点,而 T 是依赖于 n 和 U 的参数. 这样,主区间的积分可以写成

$$\int_{\mathfrak{M}} S^5(\alpha,U)\mathrm{d}\alpha = I_0+\cdots+I_5+o(U^4 n^{-1/2}),$$

其中

$$I_j = \int_{\mathfrak{M}} S_1^j S_2^{5-j}\mathrm{d}\alpha.$$

容易证明 I_0 产生圆法的主项;剩下是要验证 $I_1,\cdots,I_5$ 都产生余项.

以 I_5 的估计为例. 对 $\psi_j \bmod q$,定义

$$B(q,\psi_1,\cdots,\psi_5) = \sum_{a \bmod q}{}^{*} e\left(-\frac{an}{q}\right)\prod_{j=1}^{5} C(\psi_j,a). \tag{4.2}$$

展开计算 I_5,得

$$\begin{aligned} I_5 = -\frac{1}{2^5}&\sum_{r_1\le P}\cdots\sum_{r_5\le P}\sum_{\chi_1 \bmod r_1}{}^{*}\cdots\sum_{\chi_5 \bmod r_5}{}^{*}\sum_{|\gamma_1|\le T}\cdots\sum_{|\gamma_5|\le T}\times \\ &\int_D v_1^{\rho_1/2-1}\cdots v_4^{\rho_4/2-1}(n-v_1-\cdots-v_4)^{\rho_5/2-1}\mathrm{d}v_1\cdots\mathrm{d}v_4\times \\ &\sum_{\substack{q\le P\\ r_j|q}}\frac{1}{\varphi^5(q)}B(q,\chi_1\chi^0,\cdots,\chi_5\chi^0), \end{aligned} \tag{4.3}$$

其中 D 是某个区域,$\chi_j \bmod r_j$, 而 $\chi^0 \bmod q$ 是主特征. 下面引理提供了关键的节约.

引理 4.2　设 $r_0=[r_1,\cdots,r_5]$. 则

$$\sum_{\substack{q\le P\\ r_0|q}}\frac{1}{\varphi^5(q)}B(q,\chi_1\chi^0,\cdots,\chi_5\chi^0)\ll r_0^{-3/2+\varepsilon}\log^{50}P.$$

用一阶和二阶导数检验法估计(4.3)里面的积分,再用引理 4.2 估计(4.3)最后的和式,并注意到

$$r_0 \ge r_1^{1/4}\cdots r_4^{1/4}, \tag{4.4}$$

得

$$I_5 \ll \frac{U^4}{n^{1/2}}\Big\{\sum_{r\le P} r^{-3/8+\varepsilon}\sum_{\chi \bmod r}{}^{*}\sum_{|\gamma|\le T} n^{(\beta-1)/2}\Big\}^4\log^{61} n. \tag{4.5}$$

上式花括号中的和式可以用大筛法型的零点密度定理来估计,从而当 P 取 n 的适当方幂时,花括号中的和式 $\ll \log^{-A}n$,这里的 $A>0$ 是任意的常数. 进而,

$$I_5 \ll U^4 n^{-1/2}\log^{-A}n, \tag{4.6}$$

如所欲证.

分析从(4.3)到(4.6)的论证过程,可以发现(4.5)中的 $r^{-3/8+\varepsilon}$ 起着决定性的作用;如果没有 r 的这个负幂,那么无论 P 取 n 的什么正方幂,(4.5)花括号中的和式都不是可控的. 我们注意,(4.5)中的 $r^{-3/8+\varepsilon}$ 来自(4.4)和引理 4.2 的 $r_0^{-3/2+\varepsilon}$. 因此,只要能改进引理 4.2 的 3/2,或者能找到比(4.4)更有效的方法,就能最终改进定理 4.1.

定理 4.1 是有效利用了 r_0 的负方次,从而首次不用广义 Riemann 猜想或 Deuring-Heilbronn 现象扩大了主区间. 这个思路有着深刻的意义,且在很多堆垒素数论的问题中有实质性的应用. 定理 4.1 的证明表明,只要 r_0 的方次是负的,就可以使用上述思想扩大主区间,且避免使用 Deuring-Heilbronn 现象. 假设我们有一个加法问题

$$n = p_1^{\nu_1}+\cdots+p_s^{\nu_s}, \tag{4.7}$$

其中次数 $\nu_1,\cdots,\nu_s$ 可以是任意给定的正整数,未必是二次. 容易证明, 对该加法问题有

$$\sum_{\substack{q\le P\\ r_0|q}}\frac{1}{\varphi^s(q)}B(q,\chi_1\chi^0,\cdots,\chi_s\chi^0)\ll r_0^{-s/2+1}\log^c P. \tag{4.8}$$

这个结果可以和引理4.2相比较. 我们指出,估计式(4.8)的上界仅依赖于加法问题(4.7)的变量个数 s,而与方程的次数 $\nu_1,\cdots,\nu_s$ 无关.

从(4.8)看出,只要 $s \geqslant 3$,公式(4.8)右端 r_0 的指数就是负的,从而以上方法有效. 有趣的是,以上方法正好不能应用于偶数的 Goldbach 猜想.

5 四个素数的平方之和:主区间

有了 §4 扩展主区间的方法,就可以改进华罗庚的四素数平方定理,即推论1.2.

定理 5.1 设 N 是大实数,

$$P = N^{1/5-\varepsilon}, \tag{5.1}$$

而 $\mathfrak{M}$ 由(2.4)中定义,则对 $N/2 < n \leqslant N$ 有

$$\int_{\mathfrak{M}} S^4(\alpha)e(-n\alpha)\mathrm{d}\alpha = \frac{\pi^2}{16}\mathfrak{S}_4(n)n + O\left(\frac{N}{\log^A N}\right). \tag{5.2}$$

1999年,廖明哲和本文作者[43] 将 §3的方法用于四素数平方问题,证明了定理5.1对 $P = N^{1/25}$ 成立. 2000年,廖明哲和本文作者之一[41] 进一步将 P 推进为 $P = N^{13/15+\varepsilon}$. 目前最大的主区间是定理5.1中的(5.1),这是本文作者之一[40] 在2003年得到的.

文[40]引进了一个迭代方法处理主区间上的积分,从哲学上说,这个方法相当于避免了(4.4)形式的浪费.这个迭代方法将在下文叙述.

现在令

$$x = \sqrt{N}.$$

若 $q \leqslant P$ 且 $\sqrt{x} < p \leqslant x$,则 $(q,p) = 1$. 因此 $S(\alpha)$ 可以变形为

$$S\left(\frac{a}{q} + \lambda\right) = \frac{C(q,a)}{\varphi(q)}V(\lambda) + \frac{1}{\varphi(q)}\sum_{\chi \bmod q} C(\chi,a)W(\chi,\lambda),$$

其中 $C(\chi,a)$ 由(2.7)定义,而

$$V(\lambda) = \sum_{\sqrt{x} < m \leqslant x} e(m^2\lambda),\ W(\chi,\lambda) = \sum_{\sqrt{x} < m \leqslant x} (\log p)\chi(p)e(p^2\lambda) - \delta_\chi V(\lambda).$$

这里 δ_χ 是主特征的特征函数. 从而

$$\int_{\mathfrak{M}} S^4(\alpha)e(-n\alpha)\mathrm{d}\alpha = I_0 + \cdots + I_4, \tag{5.3}$$

其中

$$\begin{aligned} I_j = &\sum_{q \leqslant P} \frac{1}{\varphi^4(q)} \sum_{a \bmod q}{}^{*} C^{4-j}(q,a)e\left(-\frac{an}{q}\right) \times \\ &\int_{\mathfrak{M}(a/q)} V^{4-j}(\lambda)\Big\{\sum_{\chi \bmod q} C(\chi,a)W(\chi,\lambda)\Big\}^j e(-n\lambda)\mathrm{d}\lambda. \end{aligned}$$

同样可以证明 I_0 给出主项,剩下是要证明 $I_1,\cdots,I_4$ 给出余项.

我们以 I_4 为例. 像在(4.2)那样可以类似定义 $B(q,\psi_1,\cdots,\psi_4)$,有

$$\begin{aligned} |I_4| = &\left|\sum_{q \leqslant P}\frac{1}{\varphi^4(q)}\sum_{\chi_1 \bmod q}\cdots\sum_{\chi_4 \bmod q} B(n,q,\chi_1,\cdots,\chi_4) \times \int_{\mathfrak{M}(a/q)} W(\chi_1,\lambda)\cdots W(\chi_4,\lambda)e(-n\lambda)\mathrm{d}\lambda\right| \leqslant \\ &\sum_{r_1 \leqslant P}\cdots\sum_{r_4 \leqslant P}\sum_{\chi_1 \bmod r_1}{}^{*}\cdots\sum_{\chi_4 \bmod r_4}{}^{*}\sum_{\substack{q \leqslant P\\ r_0 \mid q}} \frac{|B(q,\chi_1\chi^0,\cdots,\chi_4\chi^0)|}{\varphi^4(q)} \times \\ &\int_{-1/qQ}^{1/qQ} |W(\chi_1\chi^0,\lambda)|\cdots|W(\chi_4\chi^0,\lambda)|\mathrm{d}\lambda, \end{aligned}$$

其中 χ^0 是模 q 的主特征,$r_0 = [r_1,\cdots,r_4]$. 可以证明当 α 属于主区间时 $W(\chi_j\chi^0,\lambda) = W(\chi_j,\lambda)$,因此

$$|I_4| \leqslant \sum_{r_1 \leqslant P}\cdots\sum_{r_4 \leqslant P}\sum_{\chi_1 \bmod r_1}{}^{*}\cdots\sum_{\chi_4 \bmod r_4}{}^{*}\int_{-1/r_0 Q}^{1/r_0 Q}|W(\chi_1,\lambda)|\cdots|W(\chi_4,\lambda)|\mathrm{d}\lambda \times$$

$$\sum_{\substack{q \leqslant P \\ r_0 \mid q}} \frac{| B(n, q, \chi_1 \chi^0, \cdots, \chi_4 \chi^0) |}{\varphi^4(q)}.$$

像引理 4.2 一样,可以证明上式中关于 q 的和

$$\ll r_0^{-1+\varepsilon} \log^{17} N, \tag{5.4}$$

从而

$$| I_4 | \ll \log^{17} x \sum_{r_1 \leqslant P} \cdots \sum_{r_4 \leqslant P} r_0^{-1+\varepsilon} \sum_{\chi_1 \bmod r_1}{}^{*} \cdots \sum_{\chi_4 \bmod r_4}{}^{*} \times \int_{-1/r_0 Q}^{1/r_0 Q} | W(\chi_1, \lambda) | \cdots | W(\chi_4, \lambda) | \mathrm{d}\lambda. \tag{5.5}$$

公式(5.4) 中的 $r_0^{-1+\varepsilon}$ 相当于引理 4.2 里的 $r_0^{-3/2+\varepsilon}$. 所谓迭代法的要点就是要充分利用这个 $r_0^{-1+\varepsilon}$,而不是像(4.4) 那样浪费了 r_0 的方次.

在(5.5) 最后的积分中,提出 $| W(\chi_1, \lambda) |$ 和 $| W(\chi_2, \lambda) |$,然后利用 Cauchy 不等式,得

$$\begin{aligned} | I_4 | \ll \log^{17} x & \sum_{r_1 \leqslant P} \sum_{\chi_1 \bmod r_1}{}^{*} \max_{|\lambda| \leqslant 1/r_1 Q} | W(\chi_1, \lambda) | \times \\ & \sum_{r_2 \leqslant P} \sum_{\chi_2 \bmod r_2}{}^{*} \max_{|\lambda| \leqslant 1/r_2 Q} | W(\chi_2, \lambda) | \times \\ & \sum_{r_3 \leqslant P} \sum_{\chi_3 \bmod r_3}{}^{*} \left(\int_{-1/r_3 Q}^{1/r_3 Q} | W(\chi_3, \lambda) |^2 \mathrm{d}\lambda \right)^{1/2} \times \\ & \sum_{r_4 \leqslant P} r_0^{-1+\varepsilon} \sum_{\chi_4 \bmod r_4}{}^{*} \left(\int_{-1/r_4 Q}^{1/r_4 Q} | W(r_4, \lambda) |^2 \mathrm{d}\lambda \right)^{1/2}. \end{aligned} \tag{5.6}$$

定义

$$J(g) = \sum_{r \leqslant P} [g, r]^{-1+\varepsilon} \sum_{\chi \bmod r}{}^{*} \max_{|\lambda| \leqslant 1/rQ} | W(\chi, \lambda) |,$$

且

$$K(g) = \sum_{r \leqslant P} [g, r]^{-1+\varepsilon} \sum_{\chi \bmod r}{}^{*} \left(\int_{-1/rQ}^{1/rQ} | W(\chi, \lambda) |^2 \mathrm{d}\lambda \right)^{1/2}.$$

文[40] 证明了下面结果.

引理 5.2 (1) 若 P 由(5.1) 确定, 则

$$J(g) \ll g^{-1+\varepsilon} x \log^c x,$$

这里 $c > 0$ 是某个常数.若 $g = 1$,则上述估计可以改进为

$$J(1) \ll x \log^{-A} x,$$

此处 $A > 0$ 是任意常数.

(2) 若 P 由(5.1) 确定, 则

$$K(g) \ll g^{-1+\varepsilon} \log^c x,$$

这里 $c > 0$ 是某个常数.

应用引理 5.2,我们可以逐个估计(5.6) 中关于 $r_4, \cdots, r_1$ 的和式. 这个过程就是所谓的迭代. 因为 $r_0 = [r_1, r_2, r_3, r_4] = [[r_1, r_2, r_3], r_4]$, 所以(5.6) 中关于 r_4 的和式

$$= \sum_{r_4 \leqslant P} [[r_1, r_2, r_3], r_4]^{-1+\varepsilon} \sum_{\chi_4 \bmod r_4}{}^{*} \left(\int_{-1/r_4 Q}^{1/r_4 Q} | W(\chi_4, \lambda) |^2 \mathrm{d}\lambda \right)^{1/2} = K([r_1, r_2, r_3]) \ll [r_1, r_2, r_3]^{-1+\varepsilon} \log^c x.$$

再次利用引理 5.2(2),上面的量对(5.6) 中关于 r_3 的和式的贡献为

$$\ll \log^c x \sum_{r_3 \leqslant P} [r_1, r_2, r_3]^{-1+\varepsilon} \sum_{\chi_3 \bmod r_3}{}^{*} \left(\int_{-1/r_3 Q}^{1/r_3 Q} | W(\chi_3, \lambda) |^2 \mathrm{d}\lambda \right)^{1/2} = K([r_1, r_2]) \log^c x \ll [r_1, r_2]^{-1+\varepsilon} \log^c x,$$

而后者对(5.6) 中关于 r_2 的和式的贡献为

$$\ll \log^c x \sum_{r_2 \leqslant P} [r_1, r_2]^{-1+\varepsilon} \sum_{\chi_2 \bmod r_2}^{*} \max_{|\lambda| \leqslant 1/r_2 Q} |W(\chi_2, \lambda)| =$$
$$J(r_1) \log^c x \ll r_1^{-1+\varepsilon} x \log^c x,$$

这里我们用到引理 5.2(1). 上式代入(5.6) 并利用应用引理 5.2(1),得

$$|I_4| \ll x \log^c x \sum_{r_1 \leqslant P} r_1^{-1+\varepsilon} \sum_{\chi_1 \bmod r_1}^{*} \max_{|\lambda| \leqslant 1/r_1 Q} |W(\chi_1, \lambda)| =$$
$$xJ(1) \log^c x \ll x^2 \log^{-A} x. \tag{5.7}$$

注意 $x = \sqrt{N}$,这就证明了定理 5.1.

在以上论证中,r_0 的 -1 次方从头至尾都被保留了下来,而这正是迭代法的有力之处.

6 Dirichlet 多项式的均值定理

证明引理 5.2 的要点是下述 Dirichlet 多项式的均值定理,引理 6.1.

设 $X^{2/5} < Y \leqslant X$,而 $M_1, \cdots, M_{10}$ 是正整数且满足

$$2^{-10} Y \leqslant M_1 \cdots M_{10} < X,\ 2M_6, \cdots, 2M_{10} \leqslant X^{1/5}.$$

对于 $j = 1, \cdots, 10$ 定义

$$a_j(m) = \begin{cases} \log m & 若\quad j = 1, \\ 1 & 若\quad j = 2, \cdots, 5, \\ \mu(m) & 若\quad j = 6, \cdots, 10, \end{cases}$$

这里的 $\mu(n)$ 是 Möbius 函数. 定义

$$f_j(s, \chi) = \sum_{m \sim M_j} \frac{a_j(m) \chi(m)}{m^s}$$

以及

$$F(s, \chi) = f_1(s, \chi) \cdots f_{10}(s, \chi),$$

其中 $\chi \bmod q$ 是 Dirichlet 特征, 而 s 是复变量. 下面关于 $F(s, \chi)$ 的均值定理是在[40] 中建立的,其详细证明亦见[54].

引理 6.1 若 $1 \leqslant R \leqslant X^2$ 且 $T \geqslant 1$,则

$$\sum_{\substack{r \sim R \\ d | r}} \sum_{\chi \bmod r}^{*} \int_T^{2T} \left| F\left(\frac{1}{2} + \mathrm{i}t, \chi\right) \right| \mathrm{d}t \ll \left(\frac{R^2}{d} T + \frac{R}{d^{1/2}} T^{1/2} X^{3/10} + X^{1/2} \right) \log^c X.$$

引理 6.1 中的参数 d 对于 §5 中的迭代方法的实现起着至关重要的作用. 当 $d = 1$ 时,引理 6.1 是廖明哲和本文作者之一[41] 证明的. 我们注意,若直接取绝对值,则 $|F(1/2 + \mathrm{i}t, \chi)|$ 的平凡上界是 $O(X^{1/2} \log^c X)$,其中 $c > 0$ 是某个常数. 从而引理 6.1 中公式左端的平凡上界是

$$\ll \sum_{\substack{r \sim R \\ d | r}} \sum_{\chi \bmod r} \int_T^{2T} X^{1/2} \log^c X \mathrm{d}t \ll \frac{R^2}{d} T X^{1/2} \log^c X. \tag{6.1}$$

与(6.1) 相比较,引理 6.1 中公式的右边第一项节约了 X 的幂,第二项节约了 R, T 和 X 的幂, 而第三项节约了 R 和 T 的幂.

下面的均值定理是任秀敏[61] 证明的;利用这个这个引理,她得到了素变数三角和的一个新上界估计,见定理 8.1.

引理 6.2 设 $F(s, \chi)$ 定义如上. 若常数 $\beta \geqslant 1$,而 $2 \leqslant T \leqslant X^\beta$, 且 $2 \leqslant q \leqslant X^{2\beta}$,则

$$\sum_{\chi \bmod q} \int_T^{2T} \left| F\left(\frac{1}{2} + \mathrm{i}t, \chi\right) \right| \mathrm{d}t \ll (qT)^\varepsilon \{ qT + q^{1/2} T^{1/2} X^{3/10} + X^{1/2} \}.$$

7 四个素数的平方之和:余区间和例外集

设 $E_4(N)$ 表示这样的 n 的个数: $n \leqslant N$, 且 n 满足必要条件(1.9),但是 n 不能表示成(1.10). 则 $E_4(N)$

就是华罗庚的四素数平方定理的例外集合的计数函数. 从华罗庚[26] 和 Schwarz[65] 关于三个素数的平方之和的例外集的估计可以直接推出

$$E_4(N) \ll N\log^{-A}N, \tag{7.1}$$

其中 $A>0$ 是任意正数;参见下文(13.1). 2000 年,文[41] 证明了定理 5.1 对 $P=N^{2/15-\varepsilon}$ 成立,并由此推出

$$E_4(N) \ll N^{13/15+\varepsilon}. \tag{7.2}$$

使用文[41] 的 $P=N^{2/15-\varepsilon}$, Wooley[74] 将(7.2) 中的 13/15 降低为 13/30. Wooley 的节约来自他对余区间的有效处理. 粗略地说,他能够有效地利用加法问题中多余的变量.在目前的问题中,有一个变量是多余的,因为三个素数的平方和就已经有例外集形式的结果了,见定理 1.1(2). 稍后,[40] 得到了目前最大的主区间,见定理 5.1,并将 13/30 推进为 2/5. 2004 年,Wooley, 余刚和本文作者之一[48] 证明了下面定理.

定理 7.1　我们有 $E_4(N)\ll N^{3/8+\varepsilon}$.

为了说明 Wooley 处理余区间的想法,也为了说明迭代方法如何用于余区间,我们简述定理 7.1 的证明思路如下.

设 $P,\mathfrak{M},\mathfrak{m}$ 由定理 5.1 定义,而 $\mathfrak{F}(N)$ 是满足下述条件的自然数 n 的集合: $N/2<n\leqslant N$, n 满足(1.9) 但是不能表示成(1.10). 记

$$T(\alpha)=\sum_{n\in\mathfrak{F}(N)}e(n\alpha),$$

而且 $f(N)=|\mathfrak{F}(N)|$. 显然

$$0=\int_0^1 S^4(\alpha)T(-\alpha)\mathrm{d}\alpha=\int_{\mathfrak{M}}+\int_{\mathfrak{m}}. \tag{7.3}$$

应用定理 5.1 并对 $n\in\mathfrak{F}(N)$ 求和,得

$$\int_{\mathfrak{M}}S^4(\alpha)T(-\alpha)\mathrm{d}\alpha=\sum_{n\in\mathfrak{F}(N)}\int_{\mathfrak{M}}S^4(\alpha)e(-n\alpha)\mathrm{d}\alpha\gg fN,$$

从而(7.3) 给出

$$\left|\int_{\mathfrak{m}}S^4(\alpha)T(-\alpha)\mathrm{d}\alpha\right|\gg fN. \tag{7.4}$$

下面我们推导(7.4) 左端的上界,从而得出 f 的上界. 我们注意,所有 $\alpha\in\mathfrak{m}$ 都可以写成 $\alpha=a/q+\lambda$, 其中 $P<q\leqslant Q$ 而 $|\lambda|\leqslant 1/qQ$. 这样,Ghosh[14] 的估计就给出

$$\sup_{\alpha\in\mathfrak{m}}|S(\alpha)|\ll x^{1+\varepsilon}(P^{-1}+x^{-1/2}+Qx^{-2})^{1/4}\ll N^{1/2+\varepsilon}(P^{-1}+N^{-1/4}+QN^{-1})^{1/4}\ll N^{1/2+\varepsilon}P^{-1/4}. \tag{7.5}$$

应用 Hölder 不等式,得

$$\int_{\mathfrak{m}}S^4(\alpha)T(-\alpha)\mathrm{d}\alpha\ll N^{1+\varepsilon}P^{-1/4}(N^{1/2}f+f^2)^{1/2}. \tag{7.6}$$

结合(7.4) 与(7.6), 有

$$f\ll N^{1/2+\varepsilon}P^{-1/2}.$$

利用 $P=N^{1/5-\varepsilon}$ 得 $f=f(N)\ll N^{2/5+\varepsilon}$,从而 $E_4(N)\ll N^{2/5+\varepsilon}$. 这就是[40] 的证明概要.

上面论述表明,为了证明定理 7.1,我们必须证明更强的不等式

$$\int_{\mathfrak{m}}S^4(\alpha)T(-\alpha)\mathrm{d}\alpha\ll N^{15/16+\varepsilon}(N^{1/2}f+f^2)^{1/2}, \tag{7.7}$$

仅有(7.6) 是不够的. 为此,定义 $\mathfrak{n}\subset\mathfrak{m}$,使得在 $\mathfrak{n}$ 上 Ghosh 的估计给出 $S(\alpha)\ll N^{7/16+\varepsilon}$,从而

$$\int_{\mathfrak{n}}S^4(\alpha)T(-\alpha)\mathrm{d}\alpha\ll N^{15/16+\varepsilon}(N^{1/2}f+f^2)^{1/2}. \tag{7.8}$$

记 $\mathfrak{k}=\mathfrak{m}\setminus\mathfrak{n}$; 则有 $\mathfrak{m}=\mathfrak{n}\cup\mathfrak{k}$.若能证明

$$\int_{\mathfrak{k}}|S(\alpha)|^6\mathrm{d}\alpha\ll N^{15/8+\varepsilon}, \tag{7.9}$$

则 Hölder 不等式给出

$$\int_{\mathfrak{k}}S^4(\alpha)T(-\alpha)\mathrm{d}\alpha\ll N^{15/16+\varepsilon}(N^{1/2}f+f^2)^{1/2}.$$

这个估计结合(7.8) 就给出(7.7),即定理 7.1.

现在介绍证明(7.9) 的思路. [48] 给出了两个办法证明(7.9),这里我们只介绍其中的迭代方法. 集合 $\mathfrak{k}$ 可以剖分为 $\mathfrak{k}_1 \cup \mathfrak{k}_2$,其中 $\mathfrak{k}_1$ 上的积分可以直接由 Kawada 和 Wooley[30] 的一个引理来处理. $\mathfrak{k}_2$ 上的积分可以由 §5 介绍的迭代法处理. 现在我们有六个变量,所以

$$\sum_{\substack{q \leqslant P \\ r_0 \mid q}} \frac{1}{\varphi^6(q)} \mid B(q, \chi_1 \chi^0, \cdots, \chi_6 \chi^0) \mid \ll r_0^{-2+\varepsilon} \log^{70} P,$$

其中 r_0 和 $B(\cdot)$ 定义与前面类似,但是来自六个变量. 我们注意,此时 r_0 的方次比(5.4) 节约更多,而这些多余的节约正是证明(7.9) 的关键. 证明细节不再赘述.

8 素变数三角和的新估计

利用引理 6.2 和 Heath-Brown 恒等式[23],任秀敏[61] 得到了素变数三角和的一个新估计,并将其用于 Waring-Goldbach 问题.

定理 8.1 设正整数 $k \geqslant 1$, 而 $\alpha = a/q + \lambda$ 满足 $1 \leqslant a \leqslant q$ 及 $(a, q) = 1$. 若

$$S_k(\alpha) = \sum_{\sqrt{x} < m \leqslant x} \Lambda(m) e(m^k \alpha),$$

则有

$$S_k(\alpha) \ll (qx)^{\varepsilon} \left(x^{1/2} \sqrt{q(\mid \lambda \mid x^k + 1)} + x^{4/5} + \frac{x}{\sqrt{q(\mid \lambda \mid x^k + 1)}} \right). \tag{8.1}$$

任秀敏[62] 研究了更一般的情形,比如 k 可以不是整数. 定理 8.1 可以和下面 Kumchev[33] 的结果相对照. 这两个定理互不包含,各有优势.

定理 8.2 设 k, α 如定理 8.1,且

$$1 \leqslant q \leqslant P, \mid \lambda \mid \leqslant \frac{P}{qx^k}.$$

若 $P \leqslant x$,则

$$S_k(\alpha) \ll P^{1/2} x^{11/20+\varepsilon} + \frac{q^{\varepsilon} x \log^c x}{\sqrt{q(\mid \lambda \mid x^k + 1)}}. \tag{8.2}$$

若 $k = 1$, 定理 8.1 和 8.2 化归 Vinogradov[72] 的经典结果(亦见 Vaughan[69] 或 Davenport[8], §§24 ~ 25)

$$S_1(\alpha) \ll \log^c(qx) \left(\frac{x}{q^{1/2}} + x^{4/5} + x^{1/2} q^{1/2} \right), \tag{8.3}$$

这个定理此前都是用初等方法证明的. 若 $k \geqslant 2$, 则定理 8.1 和 8.2 给出的估计是新的,而且结合 Ghosh[14] 或 Harman[19] 的定理可以推进 Waring-Goldbach 问题的很多结果.

现在利用定理 8.1 或 8.2,给出定理 7.1 的一个新证明. 定义 $\mathfrak{M}$ 和 $\mathfrak{m}$ 如 §7. 主区间 $\mathfrak{M}$ 上的积分可由定理 5.1 处理. 为了处理余区间,令

$$P^* = N^{1/4-\varepsilon}, \ Q^* = \frac{N}{P^* \log^B N}.$$

则每个 $\alpha \in \mathfrak{m}$ 都可以写成 $\alpha = a/q + \lambda$,其中

$$1 \leqslant q \leqslant Q^*, \mid \lambda \mid \leqslant \frac{1}{qQ^*}.$$

用 $\mathfrak{n}$ 表示 $\mathfrak{m}$ 中满足

$$P^* < q \leqslant Q^*, \mid \lambda \mid \leqslant \frac{1}{qQ^*}$$

的那些 α 构成的子集. 则在 $\mathfrak{n}$ 上可以应用 Ghosh 的估计,给出

$$\sup_{\alpha \in \mathfrak{n}} \mid S(\alpha) \mid \ll N^{7/16+\varepsilon}. \tag{8.4}$$

设 $\mathfrak{k}$ 是 $\mathfrak{n}$ 在 $\mathfrak{m}$ 中的补集,则 $\mathfrak{m} = \mathfrak{k} \cup \mathfrak{n}$. 若 $\alpha \in \mathfrak{k}$,则或者

$$P < q \leqslant P^*, \mid \lambda \mid \leqslant \frac{1}{qQ^*},$$

或者

$$q \leqslant P,\ \frac{1}{qQ} < |\lambda| \leqslant \frac{1}{qQ^*}.$$

无论上述情况哪个发生,都有

$$N^{1/10-\varepsilon} \ll \sqrt{\min\left(P, \frac{N}{Q}\right)} \ll \sqrt{q(1+|\lambda|N)} \ll \sqrt{P^* + \frac{N}{Q^*}} \ll N^{1/8+\varepsilon}.$$

从而定理 8.1 或 8.2 指出

$$\sup_{\alpha\in\mathfrak{k}} |S(\alpha)| \ll N^{2/5+\varepsilon}. \tag{8.5}$$

结合(8.5) 和(8.4) 得

$$\sup_{\alpha\in\mathfrak{m}} |S(\alpha)| \ll N^{7/16+\varepsilon}.$$

定理 7.1 随之成立.

9　四个素数的平方之和:筛法的引进

通过将筛法引进定理 7.1 的论证,Harman 和 Kumchev[21] 证明了目前最好的结果.

定理 9.1　我们有 $E_4(N) \ll N^{5/14+\varepsilon}$.

我们注意,定理 7.1 的指数 3/8 来自 Ghosh 的估计(7.5) 中的 $x^{7/8+\varepsilon}$. 要证明定理 9.1 必须改进(7.5) 中的 $x^{7/8+\varepsilon}$. 这种改进对素变数三角和 $S(\alpha)$ 不易实现;但是若适当地选取 $\rho(m)$,这个改进对指数和

$$H(\alpha) = \sum_{m\leqslant x}\rho(m)e(m^2\alpha) \tag{9.1}$$

可以实现. 例如 Harman[19] 证明,若 $\rho(m)$ 满足适当的乘法性质,则

$$\sup_{\alpha\in\mathfrak{m}} |H(\alpha)| \ll x^{6/7+\varepsilon}. \tag{9.2}$$

这些乘法性质与筛法相关,相当复杂,故不赘述;和我们姑且称之为性质(*),详见[21] 的引理 1.

余区间上的积分可以像 §7 一样处理. 可以证明,对于满足性质(*) 的 $\rho(m)$,主区间的积分

$$\int_{\mathfrak{M}} S^3(\alpha)H(\alpha)e(-n\alpha)\mathrm{d}\alpha$$

可以按照定理 5.1 的证明方法来估计. 最后,从(9.2) 推出定理 9.1.

10　殆素数变量的 Lagrange 定理

作为对猜想 1.3 的另一个近似,1976 年 Greaves[15] 证明了下述定理.

定理 10.1　每个大整数 n 都可以表示为两个整数的平方与两个素数的平方之和,即

$$n = m_1^2 + m_2^2 + p_1^2 + p_2^2. \tag{10.1}$$

实际上,Greaves 用筛法导出了方程(10.1) 解数的下界. 后来 Shields[67], Plaksin[60] 和 Kovalchik[32] 先后证明了方程(10.1) 解数的渐近公式; 推导解数的渐近公式用到了 Linnik 的方差法(dispersion method).

为了介绍方差法思想,假设我们要证明,对于几乎所有的 $n \in [1, N]$,都有

$$r(n) \sim R(n), \tag{10.2}$$

这里的 $r(n)$ 是我们感兴趣的研究对象,可以是一个与 n 有关的方程的解数,例如是方程(1.10) 的解数; $R(n)$ 是圆法所预料的主项,在方程(1.10) 的情形,应用定理 5.1,我们有

$$R(n) = \frac{\pi^2}{16}\mathfrak{S}_4(n)n.$$

方差法的出发点是

$$\sum_{n\leqslant N}(r(n) - R(n))^2 = \sum_{n\leqslant N}r^2(n) - 2\sum_{n\leqslant N}r(n)R(n) + \sum_{n\leqslant N}R^2(n), \tag{10.3}$$

以上诸和式的 n 还须满足必要条件(1.9). 公式(10.3) 右边第三项可以简单计算;右边第二项的计算也不复杂,其难度基本相当于 $\sum r(n)$; 右边第一项是最复杂的. 但是,注意到

$$\sum_{n\leqslant N} r^2(n) = \sum_{n\leqslant N}\Big\{\sum_{n=p_1^2+\cdots+p_4^2} 1\Big\}^2 = \sum_{p_1^2+\cdots+p_4^2=p_5^2+\cdots+p_8^2\leqslant N} 1.$$

最后的和式是八元素变量方程 $p_1{}^2+\cdots+p_4{}^2=p_5{}^2+\cdots+p_8{}^2$ 满足 $p_j\leqslant\sqrt{N}$ 的解数. 因为此方程的变量个数大于5,所以可以利用 §2 中的方法得到这个方程解数的渐近公式

$$\sum_{n\leqslant N} r^2(n) = CN^3 + O(N^\theta),$$

其中 $\theta\geqslant 2$ 是某个正常数. 简单计算得

$$\sum_{n\leqslant N} r(n)R(n) = CN^3 + O(N^\theta),$$

以及

$$\sum_{n\leqslant N} R^2(n) = CN^3 + O(N^\theta).$$

以上三个估计式代入(10.3)得

$$\sum_{n\leqslant N}(r(n)-R(n))^2 \ll N^\theta, \tag{10.4}$$

此处回忆以上诸和式的 n 还须满足必要条件(1.9). 现在以 $\mathfrak{F}(N)$ 记区间$[1,N]$中满足必要条件(1.9)但不能表示成(1.10)的 n 的集合,且 $f(N)=|\mathfrak{F}(N)|$. 若 $n\in\mathfrak{F}(N)$,则 $r(n)=0$,从而

$$\sum_{n\leqslant N}(r(n)-R(n))^2 \geqslant \sum_{n\in\mathfrak{F}(N)} R^2(n) \gg f(N)N^2.$$

此式结合(10.4),得 $f(N)\ll N^{\theta-2}$, 从而

$$E_4(N)\ll N^{\theta-2}\log N. \tag{10.5}$$

公式(10.5)可以与定理7.1等结果比较.

Linnik 自己相信,他的方差法至少与圆法同样有力[39]. 我们认为,应该更加深入地研究方差法.

1994年,Brüdern 和 Fouvry[6] 证明了满足条件(1.9)的 n 可以写成四个殆素数的平方之和. 值得注意的是,[6]提出了一个向量筛法,可以同时筛选问题中的四个变量.

定理 10.2 每个满足条件(1.9)的大整数 n 都可以表示为

$$n = m_1^2+m_2^2+m_3^2+m_4^2, \tag{10.6}$$

其中每个 m_j 都是 P_{34},即最多有34个素因子.

定理10.2还依赖于下面的均值定理[6]. 这个均值定理给出了均匀分布的水平,为应用向量筛法提供了基础.

定理 10.3 设 $\boldsymbol{d}=(d_1,\cdots,d_4)$ 表示四维向量,而 $A_{\boldsymbol{d}}$ 表示方程

$$n = d_1^2x_1^2+\cdots+d_4^2x_4^2$$

的解数. 定义

$$A_{\boldsymbol{d}} = \frac{\omega(\boldsymbol{d})}{d_1\cdots d_4}\frac{\pi^2}{16}\mathfrak{S}_4(n)n + R(\boldsymbol{d}),$$

其中 $\omega(\boldsymbol{d})$ 是某个算术函数,其具体形式从略. 令 $D=n^{1/22-\varepsilon}$,则有

$$\sum_{\|\boldsymbol{d}\|\leqslant D} |\mu(\boldsymbol{d})||R(\boldsymbol{d})| \ll n^{1-\varepsilon}.$$

2003年, Heath-Brown 和 Tolev[25] 将定理10.2中的34推进为25.他们还证明了这四个变量中有一个可以取素数,而其它每个 m_j 都是 P_{101}.

最近,吕广世[57] 不用向量筛法,而是用四维加权筛法[17,9,10] 得到了下面定理.

定理 10.4 每个满足条件(1.9)的大整数 n 都可以表示为(10.6),使得四个变量的乘积 $m_1\cdots m_4$ 是 P_{53}.

这个结果虽然没有改进单个 m_j 作为殆素数的质量,但是改进了四个变量的乘积 $m_1\cdots m_4$ 的质量.

此外,Wooley[74] 的下述例外集合形式的结果,可以和以上几个定理比较.

定理 10.5 表示式

$$n = p_1^2+p_2^2+p_3^2+m^2$$

的例外集合的计数函数是 $O(\log^{6+\varepsilon}N)$,这里的 m 是整数.

最近,Tolev[68] 证明了在定理 10.5 中可以取 m 为 P_{11}.

11　Linnik-Gallagher 问题

1951 年,Linnik[37,38] 证明了一个几乎 Goldbach 定理,即存在一个非负整数 k,使得每个大偶数 n 都可以表示为

$$n = p_1 + p_2 + 2^{\nu_1} + \cdots + 2^{\nu_k}. \tag{11.1}$$

定理的简化证明见 A. I. Vinogradov[73] 和 Gallagher[13]. 表达式(11.1) 之所以叫做几乎 Goldbach 定理,是因为序列

$$\{2^{\nu_1} + \cdots + 2^{\nu_k} : \nu_j \geqslant 0\}$$

非常稀疏. 事实上,区间[1, x] 中这类整数的个数是 $O(\log^k x)$. 几乎 Goldbach 定理的意义在于,虽然我们目前还不能证明偶数的 Goldbach 猜想,但是可以证明偶数的 Goldbach 猜想再贴上一个稀疏的数列后成立.

受 Linnik 几乎 Goldbach 定理的启发,作为对猜想 1.3 的近似,Gallagher 提出了如下猜想.

猜想 11.1　存在常数 $k \geqslant 0$,使得每个大偶数 n 都可以表示为四个素数的平方与 k 个 2 的方幂之和,

$$n = p_1^2 + p_2^2 + p_3^2 + p_4^2 + 2^{\nu_1} + \cdots + 2^{\nu_k}. \tag{11.2}$$

显然, $k = 0$ 时猜想 11.1 就强化为猜想 1.3. 1999 年,廖明哲和本文作者[43,44] 证明了上述 Gallagher 猜想.

定理 11.2　猜想 11.1 成立.

下面简述定理 11.2 的证明思路. 设 P 由(5.1) 定义,令

$$G(\alpha) = \sum_{2^\nu \leqslant n} e(2^\nu \alpha) = \sum_{\nu \leqslant L} e(2^\nu \alpha),$$

其中 $L = \log_2 n$. 则(11.2) 的解数 $r_k(N)$ 可以表示为

$$r_k(N) = \int_0^1 S^4(\alpha) G^k(\alpha) e(-n\alpha)\mathrm{d}\alpha = \left\{\int_{\mathfrak{M}} + \int_{\mathfrak{m}}\right\} S^4(\alpha) G^k(\alpha) e(-n\alpha)\mathrm{d}\alpha. \tag{11.3}$$

主区间上的积分可以用类似定理 5.1 的证明方法处理. 在余区间上,我们需要 Linnik 关于 $G(\alpha)$ 的上界估计[37,38],还需要方程

$$m = p_1^2 + p_2^2 - p_3^2 - p_4^2,\ |m| \leqslant n,\ p_j^2 \leqslant n. \tag{11.4}$$

解数的精确上界. 精确上界的意思是说,其阶必须完全正确,不能有一点浪费. 这样要求是因为,Linnik 关于 $G(\alpha)$ 的上界估计只是节约了常数因子,不能节约 $\log n$,更不能节约 n 的幂.

引理 11.3　设 $m \neq 0$ 满足 $m \equiv 0(\bmod 24)$, 并以 $r_-(m)$ 表示方程(11.4) 的解数. 则

$$r_-(m) \leqslant c\mathfrak{S}_-(m)\frac{\pi^2}{16}\frac{n}{\log^4 n}.$$

这里的 c 是可以计算的常数,

$$\mathfrak{S}_-(m) = \left(2 - \frac{1}{2^{\beta_0 - 1}} - \frac{1}{2^{\beta_0}}\right) \cdot \prod_{\substack{p^\beta \| m \\ p \geqslant 3 \\ \beta \geqslant 0}} \left(1 + \frac{1}{p} - \frac{1}{p^{\beta+1}} - \frac{1}{p^{\beta+2}}\right),$$

而 β_0 满足 $2^{\beta_0} \| m$.

这就是定理 11.2 的证明思路.

定理 11.2 给出了表达式(11.2) 里 k 的存在性, k 的可允许数值是一个值得关心的问题. 2000 年,廖明哲和本文作者之一[42] 定出了 $k = 8\,330$ 是可以允许的. 最近,吕广世和本文作者之一[45] 改进了这个数值.

定理 11.4　表达式(11.2) 对 $k = 165$ 成立.

定理 11.4 的证明在主区间上用到定理 5.1,在余区间上还用到任秀敏的定理 8.1, 以及 Heath-Brown 与 Puchta[24] 关于 2 的方幂的指数和估计.

12　再论具有五个几乎相等变量的华罗庚定理

正如 §§3 ~ 4 指出的那样,要想推进定理 4.1 的结果,必须做两件事:第一,在尽可能大的主区间上建

立积分的渐近公式;第二,改进余区间上素变数三角和的估计. 沿着第一个思路,2000 年本文作者[52] 将定理 4.1 里面 U 的指数缩小为 11/23, 2005 年 Bauer[2] 得到 203/425. 利用证明定理 5.1 所用的迭代方法,吕广世[55,56] 在目前最大的主区间上得到了积分的渐近公式,从而将 U 的指数缩减为 17/35 和 13/28.

最近,吕广世和本文作者[46] 无条件地证明了定理 3.1.

定理 12.1 不用广义 Riemann 猜想,定理 3.1 也成立.

为了证明定理 12.1,我们[46] 必须同时注重上述主区间和余区间两个方面: 在目前最大的主区间上,利用[55] 的渐近公式;在余区间上,先证明小区间素变数三角和的一个新估计,见下文定理 12.2,然后利用这个估计处理余区间上的积分.

定理 12.2 设 k, α 如定理 8.1,而实数 x, y 满足 $2 \leqslant y \leqslant x$. 定义

$$S_k(x, y; \alpha) = \sum_{x < m \leqslant x+y} \Lambda(m) e(m^k \alpha).$$

若

$$\xi = |\lambda| x^k + x^2 y^{-2},$$

则

$$S_k(x, y; \alpha) \ll (qx)^{\varepsilon} \left(\frac{q^{1/2} y \xi^{1/2}}{x^{1/2}} + q^{1/2} x^{1/2} \xi^{1/6} + y^{1/2} x^{3/10} + \frac{x^{4/5}}{\xi^{1/6}} + \frac{x}{q^{1/2} \xi^{1/2}} \right).$$

我们注意,在 $y = x$ 的特殊情形, 定理 12.2 退化成为定理 8.1. 定理 12.2 的证明依赖于下面引理[46].

引理 12.3 设 $F(s, \chi)$, β, T, q 同引理 6.2. 若 $1 \leqslant H \leqslant T$,则

$$\sum_{\chi \bmod q} \int_T^{T+H} \left| F\left(\frac{1}{2} + \mathrm{i}t, \chi\right) \right| \mathrm{d}t \ll (qT)^{\varepsilon} \{ q(H + T^{2/3}) + q^{1/2}(H + T^{2/3})^{1/2} X^{3/10} + X^{1/2} \}.$$

引理 12.3 的证明要用到 Dirichlet L- 函数在小区间$[T, T + H]$上的四次均值估计. 细节从略.

13 三个素数的平方之和

以 $E_3(N)$ 记区间$[1, N]$中满足条件(1.7) 但是不能表示为(1.8) 的整数 n 的个数. 则 $E_3(N)$ 就是定理 1.1(2) 的例外集合的计数函数. 华罗庚[26] 实际上证明了

$$E_3(N) \ll N \log^{-A} N, \tag{13.1}$$

其中 $A > 0$是某个常数. Schwarz[65] 证明了(13.1) 里的 A 可以取成任意正数. 后来,梁敏翔和廖明哲[35] 将此推进为

$$E_3(N) \ll N^{1-\delta}, \tag{13.2}$$

这里的 $\delta > 0$ 是一个很小的常数,其具体数值依赖于 Deuring-Heilbronn 现象中的常数,而且计算相当繁复. 公式(13.2) 是用 Deuring-Heilbronn 现象解决堆垒素数论问题所能得到的典型结果. 2000 年,Bauer,廖明哲以及本文作者之一[3] 发展了[50] 中的思想(见 §3),既不用 Deuring-Heilbronn 现象也不用零点密度,而是用均值定理证明了

$$E_3(N) \ll N^{77/80+\varepsilon}. \tag{13.3}$$

必须指出,[3] 成文在[41] 之前;[41] 及后续文章借鉴和发展了[3] 的思想. 特别地,本文作者[53,54] 先后把 77/80 缩减成 47/50 和 11/12. 最近,任秀敏[61] 和 Kumchev[33] 相互独立地证明了更好的结果,他们的证明需要各自指数和估计的新上界,见定理 8.1 和 8.2.

定理 13.1 我们有 $E_3(N) \ll N^{7/8+\varepsilon}$.

Harman 和 Kumchev[21] 证明了下面结果,所用方法和证明定理 9.1 的方法一致.

定理 13.2 我们有 $E_3(N) \ll N^{6/7+\varepsilon}$.

14 三个殆素数的平方之和

Blomer 和 Brüdern[4] 研究了表正整数 n 为三个殆素数之和的问题,得到如下结果.

定理 14.1　每个满足(1.7)的充分大的 n 都可以写成

$$n = m_1^2 + m_2^2 + m_3^2,$$

其中每个 m_j 都是 P_{521}.

定理的证明思路和定理 10.2 很接近,也是用向量筛法和一个类似于定理 10.3 的均值定理. 但是现在这个均值定理的证明却与定理 10.3 大不相同. 定理 10.3 的证明是利用 Kloosterman 的圆法,而这里要用半整权模形式的理论. 细节从略.

值得指出的是,下节定理 15.2 的殆素数的质量远高于上面结果. 原因之一是, 定理 15.2 使用的不是半整权模形式,而是整权模形式,见定理 15.3;而对于整权模形式,相应的特征值问题的估计比半整权模形式要好.

15　Sarnak 猜想与三元二次型

2006 年,Sarnak[64] 以及 Bourgain, Gamburd, Sarnak[5] 提出了几个意义深远的纲领性猜想,这些猜想涉及素数分布的各个方面,并将素数分布的所有问题纳入到一个统一框架中. 例如,Sarnak 猜想包含:Dirichlet 算术级数中的素数定理, Hardy 和 Littlewood[18] 的 k 生素数猜想,Vinogradov 的三素数定理[70], Green 和 Tao[16] 关于素数集合中存在任意长算术级数的著名定理,Schinzel 假设,以及所有的 Waring-Goldbach 问题. 我们相信,Sarnak 猜想的研究会成为以后素数分布理论的主流. 详细解释 Sarnak 的猜想必将超出本文的范围,因此我们仅满足于介绍下面的猜想 15.1,它是 Sarnak 猜想的简单推论,其内容与本节中问题相关.

设 $f(\boldsymbol{x})$ 是非确定的三元整二次型,其判别式无平方因子. 本节里,$\boldsymbol{x}$ 表示向量(x_1, x_2, x_3). 对非零整数 t,定义

$$V = \{\boldsymbol{x} : f(\boldsymbol{x}) = t\},$$

根据 Siegel 公式以及这种 f 的特性[7],有

$$V(\mathbb{Z}) := \{\boldsymbol{x} \in (\mathbb{Z} : f(\boldsymbol{x}) = t\} \neq \varnothing \tag{15.1}$$

当且仅当 $f(\boldsymbol{x}) = t(\bmod d)$ 对每个 $d \geqslant 1$ 可解. 本节恒假设(15.1).

设 $d \geqslant 2$,定义

$$V(\mathbb{Z}/d\,\mathbb{Z}) = \{\boldsymbol{x} \in (\mathbb{Z}/d\,\mathbb{Z})^3 : f(\boldsymbol{x}) \equiv t(\bmod d)\}, \tag{15.2}$$

以及

$$V^0(\mathbb{Z}/d\,\mathbb{Z}) = \{\boldsymbol{x} \in V(\mathbb{Z}/d\,\mathbb{Z}) : x_1 x_2\ x_3 \equiv 0(\bmod d)\}. \tag{15.3}$$

一个素数 p 被称为坏素数,若此 p 使得(15.2)与(15.3)相等,

$$V^0(\mathbb{Z}/p\,\mathbb{Z}) = V(\mathbb{Z}/p\,\mathbb{Z}). \tag{15.4}$$

此时任何 $\boldsymbol{x} \in V^0(\mathbb{Z})$ 都满足 $p \mid x_1 x_2 x_3$, 从而至少一个 x_j 可以被 p 整除. 因此,当计算 V 中的殆素数所含的素因子个数时,我们不计入这样的坏素数 p.幸好,只可能有有限个坏素数,见下文引理 15.4.

这些坏素数将给出 Sarnak 猜想局部障碍. 定义

$$P = \{\boldsymbol{x} \in V(\mathbb{Z}) : x_j \text{ 都是素数}\} \subset V(\mathbb{Z}).$$

若希望集合 P 在 $V(\mathbb{Z})$ 中 Zariski 稠密,就必须逾越这些局部障碍.Zariski 稠密是代数几何中的一个简单概念,可以参看 Hartshorne[22,第一章].

Sarnak 猜想的一个简单推论如下.

猜想 15.1　若没有局部障碍,则 P 在 $V(\mathbb{Z})$ 中 Zariski 稠密.

若以

$$x_1^2 + x_2^2 - 7x_1^2 = -5$$

定义 V,则此时没有坏素数,因为(1,1,1)是方程的解. 从而猜想 15.1 指出,对于这个方程,P 在 $V(\mathbb{Z})$ 中 Zariski 稠密.

我们必须区别考虑 f 在$\mathbb{Q}$上是 isotropic 或 anisotropic 这两种情况. 第一种情形下,f 可以参数化,即存在 $g = (g_1, g_2, g_3)$ 其中 g_j 是单变量的整多项式,使得对所有 $y \in \mathbb{Z}$ 都有 $g(y) \in V(\mathbb{Z})$. 此时可以用标准的

Abel 型的筛法[10] 寻找殆素数. 例如

$$f(\boldsymbol{x}) = x_1^2 + x_2^2 - x_3^2 = 0 \tag{15.5}$$

就可以参数化. 利用这一点,Diamond 与 Halberstam[9] 证明了(15.5)有无穷多个解,使得 $x_1x_2x_3$ 是 P_{17}. 当 f 是一般的 isotropic 二次型时,同样的方法也有效.

Sarnak 和本文作者之一[47] 处理 f 是 anisotropic 的情形. 此时,f 不可以参数化,因此我们利用[5]提出的非 Abel 轨道方法与加权筛法. 为了在 $V(\mathbb{Z})$ 上实施筛法,我们利用 Kim 与 Sarnak[31] 关于 Selberg 特征值猜想[66] 的最好上界,还要用到目前最有效的三维加权筛法[17,9,10].

定理 15.2 设 $f(\boldsymbol{x})$ 是非确定的 anisotropic 三元整二次型,其判别式无平方因子, 而 t 是非零整数. 则方程 $f(\boldsymbol{x}) = t$ 满足 $x_1x_2x_3$ 是 P_{26} 的解集合在 V 中 Zariski 稠密. 假设 Selberg 特征值猜想,上述 26 可以改进为 22.

设 $SO_f(\mathbb{R})$ 是固定 f 的实 3×3 正交矩阵群. 而 K 是 $SL_f(\mathbb{R})$ 的最大紧子群. 设 $\|\cdot\|$ 是$\mathbb{R}^3$上的 K 不变 Euclid 范数. 构造一组函数 $F_T:[0,\infty)^3\to\mathbb{R}$,满足

$$\begin{cases} 0 \leqslant F_T(\boldsymbol{x}) \leqslant 1, \\ 0 \leqslant F_T(\boldsymbol{x}) = 1 & 若\ \|\boldsymbol{x}\| \leqslant T/e, \\ 0 \leqslant F_T(\boldsymbol{x}) = 0 & 若\ \|\boldsymbol{x}\| \geqslant Te. \end{cases}$$

设 Γ 是 $SL_2(\mathbb{Z})$ 的同余子群, λ_1 是 $X_\Gamma = \Gamma\backslash\mathbb{H}$ 的第一个 Laplace 特征值. 设 $0 \leqslant \theta < 1/4$ 满足

$$\lambda_1(X_\Gamma) \geqslant \frac{1}{4} - \theta^2. \tag{15.6}$$

则 $\theta = 7/64$ 就是目前最好的估计,由 Kim 与 Sarnak[31] 得到. Selberg 特征值猜想断言 $\theta = 0$. 设 $1 \leqslant n \ll T^3$,定义

$$a_n(T) = \sum_{\substack{\boldsymbol{x}\in V(\mathbb{Z}) \\ x_1x_2x_3 = \pm n}} F_T(\boldsymbol{x}),\ X = \sum_{n\geqslant1} a_n(T).$$

可以证明,当 $T\to\infty$ 时 $X \sim cT$,其中 $c = c(V)$ 是常数.

下面定理[47] 给出了均匀分布的水平,是证明定理 15.2 的关键.

定理 15.3 设 $f(\boldsymbol{x})$ 是非确定的 anisotropic 三元整二次型,其判别式无平方因子, 而 t 是非零整数. 若 $1 \leqslant d \leqslant T$,则

$$\sum_{n\equiv0(\mathrm{mod}\,d)} a_n(T) = \frac{|V^0(\mathbb{Z}/d\mathbb{Z})|}{|V(\mathbb{Z}/d\mathbb{Z})|}X + O_\varepsilon(d^{1+\varepsilon}T^{1/2+\theta}).$$

比较上式的主项和余项可以看出,定理 15.3 相当强. 我们注意,这个定理没有对 d 求和,所以它不是 Bombieri-Vinogradov 型定理. 让我们指出,即使对 d 求和,也只是相当于在余项里面取 $\theta = 0$,即假设 Selberg 特征值猜想,从而不会带来大的节约. 这是因为 $\theta = 7/64$ 已经相当接近猜测的 $\theta = 0$.

定理 15.3 的证明要用到强逼近定理[7], 还有 Duke, Rudnick 和 Sarnak[11] 的技术, 最后用到 Jacquet-Langlands 对应[29]. 细节从略.

上文提到,对于固定的 f,只可能有有限个坏素数. 下面引理[47] 给出了更加具体的信息.

引理 15.4 设 $f(\boldsymbol{x})$ 是三元整二次型, 其判别式 Δ 无平方因子, 而 t 是整数, 未必非零. 设 $|V(\mathbb{Z}/p\mathbb{Z})|$ 及 $|V^0(\mathbb{Z}/p\mathbb{Z})|$ 由(15.2)及(15.3)定义. 若 $|V(\mathbb{Z}/p\mathbb{Z})| = |V^0(\mathbb{Z}/p\mathbb{Z})|$,则 $p\mid(\Delta,t)$ 或者 $p = 2,3,5$. 也就是说,方程的 $f(x_1,x_2,x_3) = t$ 的坏素数构成

$$\{2,3,5\}\cup\{p:\ p\mid(\Delta,t)\}$$

的子集.

引理的证明并不复杂,主要涉及 Gauss 和的计算.

后记 今年是我们的导师潘承洞院士逝世十周年. 潘老师以其对 Goldbach 猜想研究的震惊世界的工作而闻名于世. 潘老师的学术观点和著作深深影响了我们. 本文介绍的作者自己的工作就是在潘老师这些影响之下取得的. 在潘老师离开我们十周年之际,谨以此文记载我们对他的深切敬仰与怀念.

参考文献:

[1] C Bauer. A note on sums of five almost equal prime squares[J]. Arch Math, 1997, 69:20 ~ 30.

[2] C Bauer. Sums of five almost equal prime squares[J]. Acta Math Sin, 2005, 21:833 ~ 840.

[3] C Bauer, M C Liu, T Zhan. On sums of three prime squares[J]. J Number Theory, 2000, 85:336 ~ 359.

[4] V Blomer, J Brüdern. A three squares theorem with almost primes[J]. Bull London Math Soc, 2005, 37:507 ~ 513.

[5] J Bourgain, A Gamburd, P Sarnak. Sieving and expanders[J]. C R Math Acad Sci Paris, 2006, 343:155 ~ 159.

[6] J Brüdern, E Fouvry. Lagrange's four squares theorem with almost prime variables[J]. J Riene Angew Math, 1994, 454:59 ~ 96.

[7] J W S Cassels. Rational quadratic forms[A]. London Mathematical Society Monographs 13[C]. London-New York: Academic Press, 1978.

[8] H Davenport. Multiplicative Number Theory, 2nd ed[M]. Berlin: Springer, 1980.

[9] H Diamond, H Halberstam. Combinatorial sieves of dimension exceeding 1[J]. J Number Theory, 1988, 28:306 ~ 346.

[10] H Diamond, H Halberstam. Some applications of sieves of dimension exceeding 1, in Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), 101-107[A]. London Math Soc Lecture Note Ser, 237[C]. Cambridge: Cambridge Univ Press, 1997.

[11] W Duke, Z Rudnick, P Sarnak. Density of integer points on affine homogeneous varieties[J]. Duke Math J, 1993, 71:143 ~ 179.

[12] P X Gallagher. A large sieve density estimate near $\sigma = 1$[J]. Invent Math, 1970, 11:329 ~ 339.

[13] P X Gallagher. Primes and powers of 2[J]. Invent Math, 1975, 29:125 ~ 142.

[14] A Ghosh. The distribution of αp^2 modulo 1[J]. Proc London Math Soc, 1981, 42(3):252 ~ 269.

[15] G Greaves. On the representation of a number in the form $x^2 + y^2 + p^2 + q^2$ where p and q are odd primes[J]. Acta Arith, 1976, 29: 257 ~ 274.

[16] B Green, T Tao. The primes contain arbitrarily long arithmetic progressions[J]. To appear in Ann Math.

[17] H Halberstam, H E Richert. Sieve methods[M]. New York: Academic Press, 1974.

[18] G H Hardy, J E Littlewood. Some problem of "patitio numerorum" Ⅲ: On the expression of a number as a sum of primes[J]. Acta Math, 1923, 44:1 ~ 70.

[19] G Harman. Trigonometric sums over primes(Ⅰ)[J]. Mathematika, 1981, 28:249 ~ 254.

[20] G Harman. The values of ternary quadratic forms at prime arguments[J]. To appear in Mathematika.

[21] G Harman, A V Kumchev. On sums of squares of primes[J]. Math Proc Cambridge Philos Soc, 2006, 140:1 ~ 13.

[22] R Hartshorne. Algebraic Geomerty[M]. New York: Springer-Verlag, 1977.

[23] D R Heath-Brown. Prime numbers in short intervals and a generalized Vaughan's identity[J]. Can J Math, 1982, 34:1 365 ~ 1 377.

[24] D R Heath-Brown, J C Puchta. Integers represented as a sum of primes and powers of two[J]. Asian J Math, 2002, 6:535 ~ 565.

[25] D R Heath-Brown, D I Tolev. Lagrange's four squares theorem with one prime and three almost-prime variables[J]. J Riene Angew Math, 2003, 558:159 ~ 224.

[26] L K Hua. Some results in the additive prime number theory[J]. Quart J Math (Oxford), 1938, 9:68 ~ 80.

[27] L K Hua. On the representation of numbers as the sums of the powers of primes[J]. Math Z, 1938, 44:335 ~ 346.

[28] L K Hua. Additive theory of prime numbers(in Chinese)[M]. Beijing: Science Press, 1957; English Version, Rhode Island: Amer Math Soc, 1965.

[29] H Jacquet, R P Langlands. Automorphic forms on GL(2)[M]. Lecture Notes in Mathematics, Vol. 114. Berlin-New York: Springer-Verlag, 1970.

[30] K Kawada, T Wooley. On the Waring-Goldbach problem for fourth and fifth powers[J]. Proc London Math Soc, 2001, 83(3):1 ~ 50.

[31] H Kim, P Sarnak. Refined estimates towards the Ramanujan and Selberg conjectures[J]. J Amer Math Soc, 2003, 16:175 ~ 181.

[32] F B Kovalchik. Some analogies of the Hardy-Littlewood equation[J]. Zap Nauchn Sem Leningrad Otdel Mat Inst Steklov, 1982, 116: 86 ~ 95, 163.

[33] A V Kumchev. On Weyl sums over primes and almost primes[J]. Michigan Math J, 2006, 54:168 ~ 243.

[34] A V Kumchev, D I Tolev. An invitation to additive prime number theory[J]. Serdica Math J, 2005, 31:1 ~ 74.

[35] M C Leung, M C Liu. On generalized quadratic equations in three prime variables[J]. Mh Math, 1993, 115:133 ~ 169.

[36] Yu V Linnik. On the least prime in an arithmetic progression[J]. Mat Sb N S, 1944, 15:139 ~ 178; Ⅱ: The Deuring-Heilbronn phenomenon[J]. Mat Sb N S, 1944, 15:347 ~ 368.

[37] Yu V Linnik. Prime numbers and powers of two[J]. Trudy Mat Inst Steklov, 1951, 38:151 ~ 169.

[38] Yu V Linnik. Addition of prime numbers and powers of one and the same number[J]. Mat Sb N S, 1953, 32:3 ~ 60.
[39] Yu V Linnik. The dispersion method in binary additive problems[J]. Amer Math Soc, 1963.
[40] J Y Liu. On Lagrange's theorem with prime variables[J]. Quart J Math (Oxford), 2003, 54:453 ~ 462.
[41] J Y Liu, M C Liu. The exceptional set in the four prime squares problem[J]. Illinois J Math, 2000, 44:272 ~ 293.
[42] J Y Liu, M C Liu. Representations of even integers as squares of primes and powers of 2[J]. J Number Theory, 2000, 83:202 ~ 225.
[43] J Y Liu, M C Liu, T Zhan. Squares of primes and powers of two[J]. Mh Math, 1999, 128:283 ~ 313.
[44] J Y Liu, M C Liu, T Zhan. Squares of primes and powers of two (Ⅱ)[J]. J Number Theory, 2002, 92:99 ~ 116.
[45] J Y Liu, G S Lü. Four squares of primes and 165 powers of 2[J]. Acta Arith, 2004, 114:55 ~ 70.
[46] J Y Liu, G S Lü, T Zhan. Exponential sums over primes in short intervals[J]. Sci China Ser A, 2006, 49:611 ~ 619.
[47] J Y Liu, P Sarnak. Almost primes on 3-quadrics[J]. Preprint.
[48] J Y Liu, T D Wooley, G Yu. The quadratic Waring-Goldbach problem[J]. J Number Theory, 2004, 107:298 ~ 321.
[49] J Y Liu, T Zhan. On sums of five almost equal prime squares[J]. Acta Arith, 1996, 77:369 ~ 383.
[50] J Y Liu, T Zhan. Sums of five almost equal prime squares (Ⅱ)[J]. Sci China, 1998, 41:710 ~ 722.
[51] J Y Liu, T Zhan. The Goldbach-Vinogradov theorem[A]. Number theory in progress, Vol. 2(Zakopane-Koscielisko, 1997)[C]. Berlin: de Gruyter, 1999. 1 005 ~ 1 023.
[52] J Y Liu, T Zhan. Hua's theorem on prime squares in short intervals[J]. Acta Math Sin, 2000, 16:1 ~ 22.
[53] J Y Liu, T Zhan. Distribution of integers that are sums of three squares of primes[J]. Acta Arith, 2001, 98:207 ~ 228.
[54] J Y Liu, T Zhan. The exceptional set in Hua's theorem for three squares of primes[J]. Acta Math Sin, 2005, 21:335 ~ 350.
[55] G S Lü. Hua's theorem with five almost equal prime variables[J]. Chinese Ann Math Ser B, 2005, 26:291 ~ 304.
[56] G S Lü. Hua's theorem on five almost equal prime squares[J]. Acta Math Sin, 2006, 22:907 ~ 916.
[57] G S Lü. Lagrange's theorem with almost prime variables[J]. To appear in Acta Math Sin.
[58] H L Montgomery, R C Vaughan. The exceptional set in Goldbach's problem[J]. Acta Arith, 1975, 27:353 ~ 370.
[59] 潘承洞,潘承彪.哥德巴赫猜想[M].北京:科学出版社,1981; English edition: The Goldbach Conjecture[M]. Beijing: Science Press, 1992.
[60] V A Plaksin. An asymptotic formula for the number of solutions of a nonlinear equation for prime numbers[J]. Math USSR Izv, 1982, 18:275 ~ 348.
[61] X M Ren. On exponential sums over primes and application in Waring-Goldbach problem[J]. Sci China, Ser A, 2005, 48:785 ~ 797.
[62] X M Ren. Vinogradov's exponential sum over primes[J]. Acta Arith, 2006, 124:269 ~ 285.
[63] G J Rieger. Über die Summe aus einem Quadrat und einem Primzahlquadrat[J]. J Reine Angew Math, 1968, 251:89 ~ 100.
[64] P Sarnak. Equi-distribution and primes. The Rademarcher lecture series, available online.
[65] W Schwarz. Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen Ⅱ[J]. J Riene Angew Math, 1961, 206:78 ~ 112.
[66] A Selberg. On the estimation of Fourier coefficients of modular forms[J]. Proc Sympos Pure Math, Amer Math Soc, Providence, R I 1965, 8:1 ~ 15.
[67] P Shields. Some applications of sieve methods in number theory[M]. Thesis: University of Wales, 1979.
[68] D I Tolev. On the exceptional set of Lagrange's equation with three prime and one almost-prime variables[J]. J Thór Nombres Bordeaux, 2005, 17:925 ~ 948.
[69] R C Vaughan. Sommes trigonométriques sur les nombres primiers[J]. C R Acad Sci Paris, Sér A, 1977, 285:981 ~ 983.
[70] I M Vinogradov. Representation of an odd numberas the sum of three primes[J]. Dolk Akad Nauk SSSR, 1937, 15:291 ~ 294.
[71] I M Vinogradov. Some new problems in the theory of primes[J]. Dolk Akad Nauk SSSR, 1937, 16:131 ~ 132.
[72] I M Vinogradov. Selected works[M]. New York: Springer, 1980.
[73] A I Vinogradov. On an "almost binary" problem[J]. Izv Akad Nauk SSSR, Ser Mat, 1956, 20:713 ~ 750.
[74] T D Wooley. Slim exceptional sets for sums of four squares[J]. Proc London Math Soc, 2002, 85(3):1 ~ 21.

(编辑:冯保初)