



# 王元文集

湖南教育出版社

WANG YUAN  
SELECTED PAPERS

# 王文集

湖南教育出版社

WANG WENJI

SELECTED PAPERS

王元文集  
WANG YUAN  
SELECTED PAPERS

责任编辑：孟实华

湖南教育出版社出版发行  
湖南省新华书店经销 湖南省新华印刷二厂印刷

242×160 16开 印张：29.5 字数：530000

1999年10月第1版 1999年10月第1次印刷

印数：1—1000

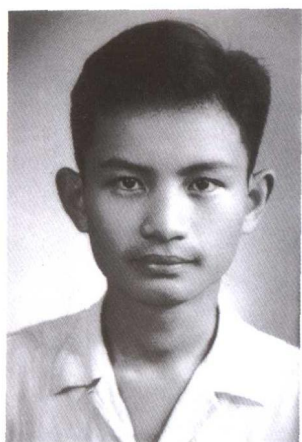
ISBN 7—5355—3047—8/G·3042

定价：44.50元

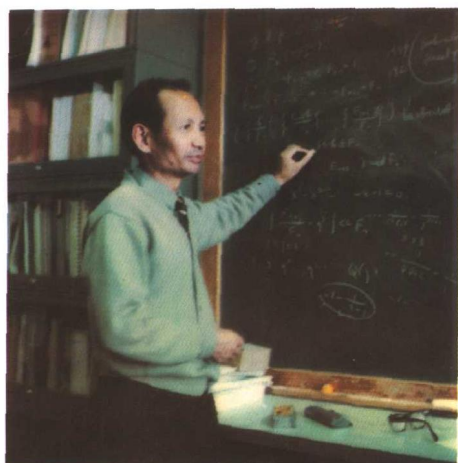
本书若有印刷、装订错误，可向承印厂调换



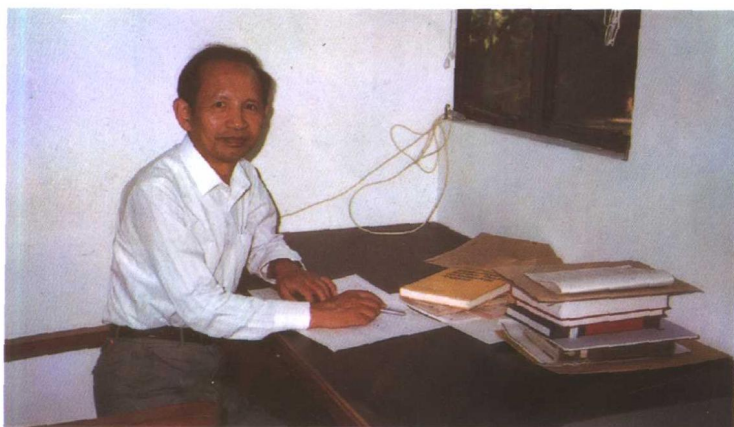
王元院士



大学毕业（1952年）



1980年在美国



1987年在香港



1992年在俄国



与华罗庚先生在一起



华罗庚先生与他的学生  
(左5王元, 左7华罗庚)



与苏步青先生一起在日本 (左起: 胡和生, 苏步青,  
村上信吾, 王元)



1981年与年轻学部委员在一起



1995年在台湾  
(中立者为合作者  
方源)



1992年在香港



1989年与肖文杰夫妇在北京

## 出版说明

王元先生是我国著名的数学家，他毕生从事数学研究，为我国的数学事业作出了重要的贡献。2000年是王元先生70华诞，我们出版了这本《王元文集》，以向王元先生祝贺。

这本文集收集的40篇文章，是王元先生从1956年～1998年间在国内外各种杂志上发表的主要论文，我们按内容分三大部分进行编排。对这些跨度几十年的文章，按照国际惯例，在形式上并不强求统一，以保持文章的原貌。这些论文较完整地体现了我国数论的发展历程，读完之后，就可对我国解放后数论的发展脉络有一个较全面的了解。

出版者



# 序

杨 乐 潘承洞

王元院士是我国著名的数学家。他长期从事数论及其应用的研究，取得优良成果。他为人谦虚随和，受到大家的尊敬与爱戴。

王元院士，籍贯江苏镇江，1930年4月29日出生于浙江省兰溪县。其父王懋勤当时任兰溪县长，40年代时任中央研究院总务主任，主任秘书等职；其母汪纫秋，忠厚老实，料理家务。

王元院士在数学上的聪明才智，在浙江大学学习时已有所表现。他不仅各门功课成绩优秀，而且在著名数学家陈建功、苏步青教授倡导的讨论班上报告 A. E. Ingham 的名著“素数分布论”，得到陈、苏等教授的赞赏。

1952年，王元院士由浙江大学毕业，陈建功、苏步青教授推荐他到中国科学院数学研究所工作，在数学大师华罗庚教授的指导下，研究数论及其应用。1956年升任助理研究员，1963年任副研究员，1978年任研究员，1980年当选为中国科学院数学物理学部委员（院士）。他历任中国科学院数学研究所所长（1984—1987），中国数学会理事长（1988—1992），中国科学院数理学部常委（1992—1996）、副主任（1994—1996）等职。他还担任中国科学技术协会常务委员会委员（1986—1991），全国政治协商委员会委员（1986— ）。

王元院士在我国长期倡导数论研究，在国内开拓了一些研究领域。早在1953年，即从事筛法与哥德巴赫猜想的研究。1957年，他证明了每个充分大的偶数都是一个不超过2个素数的乘积及一个不超过3个素数的乘积之和，简记为 $(2, 3)$ 。以后，潘承洞证明了 $(1, 5)$ 与 $(1, 4)$ 。最后，陈景润证明了 $(1, 2)$ ，被称为“陈氏定理”。30年过去了，陈景润的结果仍为这方面的最佳记录。陈景润、王元与潘承洞关于哥德巴赫猜想的研究获得1981年的国家自然科学一等奖。他们的这项研究受到国际数论界的重视。

此外，王元在区间中殆素数分布、圆法与哥德巴赫猜想、最小原根估计、算术函数的分布等方面的研究，也有建树。

从1959年开始，王元与华罗庚合作，在近似分析中用代数数论与丢番图逼近论的方法取代统计实验的蒙特卡罗方法，证明了用分圆域的独立单位系构造高维单位立方体的一致分布点序列的一般定理。这一方法用于重积分的近似计算十分有效，国外将它称为“华—王方法”，于1990年荣获陈嘉庚物质科学奖。

1980年以后，王元从事了代数解析数论的研究。他将有理数域上的关于丢番图方程与不等式的结果，推广到代数数域上去，得到同等精密的结果。这方面的研究工作，已总结在其专著“代数数域上的丢番图方程与不等式”里，由德国施普林格出版社于1989年出版。

与此同时，王元与数理统计专家方开泰教授合作。他们研究如何利用数论方法来合理安排试验的问题，提出了“均匀设计”的方法，在实际工作中取得了广泛应用。

此外，王元院士还于1994年荣获何梁何利数学奖。

王元院士除了在研究工作上的贡献，还十分热心地培养青年数论学者。我国年轻一辈的数论学者，几乎都直接得到他的指导和帮助。

王元院士关心国内数学界的活动与中国数学会的工作，支持与鼓励奥林匹克数学竞赛活动。他成功地在北京参与主持了1990年第31届国际奥林匹克数学竞赛的工作。他注重我国现代数学史料的搜集与研究，撰写了《华罗庚》传，用丰富的材料、严谨的叙述，流畅的文笔展现了近代数学在我国发展的过程。

王元院士在数学园地里45年的辛勤耕耘，取得了累累硕果。在他行将进入古稀之年，湖南教育出版社决定出版他的这本选集，这是一件有价值的事情。从这本选集里，我们可以看到王元院士一生主要的研究工作，这对我国数学界，尤其是数论及其应用方面，具有参考价值。

最后，让我们与广大读者共同祝愿王元院士健康长寿，家庭幸福。

# 目 录

## 1. 数论

- [1] 表大偶数为一个不超过三个素数的乘积及一个不超过四个素数的乘积之和..... ( 1 )
- [2] 整值多项式的某些性质..... ( 15 )
- [3] 论筛法及其有关的若干问题..... ( 23 )
- [4] 论筛法及其若干应用..... ( 26 )
- [5] 表大偶数为两个殆素数之和..... ( 30 )
- [6] 关于函数  $\varphi(n)$ ,  $\sigma(n)$  与  $\theta(n)$  某些性质的一个注记 ..... ( 34 )
- [7] 论数论函数  $\varphi(n)$ ,  $\sigma(n)$  与  $d(n)$  的一些性质 ..... ( 47 )
- [8] 论筛法及其有关的若干应用..... ( 59 )
- [9] 论筛法及其有关的若干应用 (殆素数的分布问题) ..... ( 82 )
- [10] 论素数的最小正原根 ..... ( 98 )
- [11] 表大整数为素数及殆素数之和 ..... (110)
- [12] 关于特征和的估计及其应用 ..... (130)
- [13] 表每个大偶数为一个素数与一个殆素数之和 ..... (137)
- [14] 关于 Davenport 一个定理的注记 ..... (149)
- [15] 关于 Goldbach 数的 Linnik 方法 ..... (153)
- [16] 关于线性型的一个转换定理 ..... (170)
- [17] 关于线性型转换定理的一个注记 ..... (174)
- [18] 关于丢番图逼近某些测度定理的一个注记 ..... (179)
- [19] 代数数域中型的丢番图不等式 ..... (192)
- [20] 关于齐次加型同余式 ..... (209)
- [21] 同余式的最小解 ..... (221)
- [22] 有限域上二次型的最小零点( I ) ..... (237)

## 2. 近似分析与统计

- [23] 关于多重积分的近似计算的若干注记 ..... (246)
- [24] 某类函数插值公式的一个注记 ..... (250)
- [25] 丢番图逼近与数值积分( I ) ..... (255)
- [26] 丢番图逼近与数值积分( II ) ..... (259)

〔27〕 多维周期函数的数值积分 .....	(263)
〔28〕 关于一类函数的插入公式 .....	(277)
〔29〕 论一致分布与近似分析——数论方法(Ⅰ) .....	(281)
〔30〕 论一致分布与近似分析——数论方法(Ⅱ) .....	(304)
〔31〕 论一致分布与近似分析——数论方法(Ⅲ) .....	(323)
〔32〕 关于均匀分布与试验设计(数论方法) .....	(338)
〔33〕 丢番图逼近与近似分析(Ⅰ) .....	(345)
〔34〕 丢番图逼近与近似分析(Ⅱ) .....	(354)
〔35〕 应用统计中的数论方法 .....	(365)
〔36〕 应用统计中的数论方法(Ⅱ) .....	(381)
〔37〕 混料均匀设计 .....	(393)
<b>3. 其他工作</b>	
〔38〕 关于在等高线图上计算矿藏储量与坡地面积的问题 .....	(405)
〔39〕 关于 $s$ 阶的两两正交拉丁方的最大数目(筛法的应用) .....	(419)
〔40〕 华罗庚——生平与工作简介 .....	(432)
王元的生平与工作简介 李文林 袁向东 .....	(443)
王元著作目录 .....	(453)

# 表大偶数为一个不超过三个素数的乘积 及一个不超过四个素数的乘积之和\*

## 引 言

V. Brun<sup>[1]</sup>最初在 1920 年证明了:

每一充分大的偶数可表为两个各不超过 9 个素数的乘积之和, 简记之为 (9,9).

后来, 不少数学家改进与简化了 Brun 方法, 因此, Brun 的结果也得到相应的改进, 现在将其发展历史写于下:

- (9,9) (Brun 1920),
- (7,7) (Rademacher 1924)<sup>[2]</sup>,
- (6,6) (Estermann 1932)<sup>[3]</sup>,
- (5,7), (4,9), (3,15), (2,366)(Ricci 1937)<sup>[11]</sup>,
- (5,5) (Бухштраб 1938)<sup>[4]</sup>.
- (4,4) (Бухштраб 1940)<sup>[5]</sup>.

华罗庚教授指出用 Selberg<sup>[6]</sup>方法结合 Brun-Бухштраб 方法可以改进上述结果. 本文目的在于根据这一指示将上述结果改进为 (3,4), 即

**定理 1.** 每一充分大的偶数可表为一个不超过 3 个素数的乘积及一个不超过 4 个素数的乘积之和.

**定理 2.** 存在无限多个整数  $n$ ,  $n$  为不超过 3 个素数的乘积, 而  $n+2$  为不超过 4 个素数的乘积.

本文所用之  $p, p', p'', \dots; p_1, p_2, \dots$  均表示素数.

用本文的方法证明 (3,3) 的可能性看来是存在的, 但得涉及冗长而复杂的数值计算.

## § 1. 若干计算

引 1. 若  $x \geq 1, N \geq 1, \Omega(n)$  表示  $n$  的不同的素因子的个数, 则

$$\sum_{\substack{n \leq N \\ (n, x) = 1}} \frac{|\mu(n)| 2^{\Omega(n)}}{n} = \frac{1}{2} \prod_{p|x} \frac{p}{p+2} \prod_p \left(1 - \frac{1}{p}\right)^2 \left(1 + \frac{2}{p}\right) \log^2 N \\ + O(\log 2N \cdot \log \log 3xN) + O((\log \log 3x)^2),$$

此处  $\mu(n)$  表示熟知的 Möbius 函数.

证明见 [7].

引 2. 命

$$g(1) = 1; g(2) = \frac{1}{2}; g(p) = \frac{2}{p} (p > 2); \text{ 当 } n \text{ 无平方因子时, } g(n) =$$

$\prod_{p|n} g(p)$ . 则当  $z \geq 1$  时,

$$\sum_{\substack{n \leq N \\ 2 \nmid n}} |\mu(n)| g(n) \prod_{p|n} (1 - g(p))^{-1} \\ = \frac{1}{8} \prod_{p > 2} \frac{(p-1)^2}{p(p-2)} \log^2 z + O(\log 2z \cdot \log \log 3z).$$

证: 命  $\psi(q) = \prod_{p|q} (p-2)$ , 则

$$\sum_{\substack{2 \leq n \leq z \\ 2 \nmid n}} |\mu(n)| g(n) \prod_{p|n} (1 - g(p))^{-1} = \sum_{\substack{2 \leq n \leq z \\ 2 \nmid n}} |\mu(n)| \frac{2^{\Omega(n)}}{n} \prod_{p|n} \frac{p}{p-2} \\ = \sum_{\substack{n \leq z \\ 2 \nmid n}} |\mu(n)| \frac{2^{\Omega(n)}}{n} \prod_{p|n} \left(1 + \frac{2}{p-2}\right) \\ = \sum_{\substack{n \leq z \\ 2 \nmid n}} |\mu(n)| \frac{2^{\Omega(n)}}{n} \sum_{r|n} \frac{2^{\Omega(r)}}{\psi(r)} \\ = \sum_{\substack{r \leq z \\ 2 \nmid r}} |\mu(r)| \frac{2^{2\Omega(r)}}{\psi(r)r} \sum_{\substack{s \leq z/r \\ (s, 2r) = 1}} \frac{|\mu(s)| 2^{\Omega(s)}}{s} \\ = \sum_{\substack{r \leq z \\ 2 \nmid r}} |\mu(r)| \frac{2^{2\Omega(r)}}{\psi(r)r} \left\{ \frac{1}{2} \prod_p \frac{(p-1)^2 (p+2)}{p^3} \prod_{p|2r} \frac{p}{p+2} \right. \\ \left. \cdot \log^2 \frac{z}{r} + O(\log 2z \cdot \log \log 3z) \right\} \\ = \frac{1}{4} \prod_p \frac{(p-1)^2 (p+2)}{p^3} \log^2 z \cdot \sum_{\substack{r \leq z \\ 2 \nmid r}} \frac{4^{\Omega(r)} |\mu(r)|}{\prod_{p|r} (p^2 - 4)}$$

$$\begin{aligned}
 & + O\left(\log 2z \cdot \sum_{\substack{n \leq z \\ 2 \nmid n}} \frac{4^{a(r)} |\mu(r)| \log r}{\prod_{p|r} (p^2 - 4)}\right) + O(\log 2z \cdot \log \log 3z) \\
 & = \frac{1}{8} \prod_{p>2} \frac{(p-1)^2}{p(p-2)} \cdot \log^2 z + O(\log 2z \cdot \log \log 3z).
 \end{aligned}$$

引 3. 当  $n$  无平方因子时, 命

$$f(n) = \sum_{d|n} \frac{\mu(d)}{g\left(\frac{n}{d}\right)} = \frac{1}{g(n)} \prod_{p|n} (1 - g(p)),$$

则当  $z \geq 1$  时, 有

$$\sum_{n \leq z} \frac{|\mu(n)|}{f(n)} = \frac{1}{4} \prod_{p>2} \frac{(p-1)^2}{p(p-2)} \log^2 z + O(\log 2z \cdot \log \log 3z).$$

证: 
$$\sum_{n \leq z} \frac{|\mu(n)|}{f(n)} = \sum_{\substack{n \leq z \\ 2 \nmid n}} \frac{|\mu(n)|}{f(n)} + \sum_{\substack{n \leq z \\ 2|n}} \frac{|\mu(n)|}{f(n)}$$

$$\begin{aligned}
 & = \sum_{\substack{n \leq z \\ 2 \nmid n}} |\mu(n)| g(n) \prod_{p|n} (1 - g(p))^{-1} + \frac{1}{f(2)} \\
 & \quad \times \sum_{\substack{n \leq z/2 \\ 2 \nmid n}} |\mu(n)| g(n) \prod_{p|n} (1 - g(p))^{-1} \\
 & = \frac{1}{8} \prod_{p>2} \frac{(p-1)^2}{p(p-2)} \log^2 z + \frac{1}{8f(2)} \prod_{p>2} \frac{(p-1)^2}{p(p-2)} \log^2 \frac{z}{2} \\
 & \quad + O(\log 2z \cdot \log \log 3z) \\
 & = \frac{1}{4} \prod_{p>2} \frac{(p-1)^2}{p(p-2)} \log^2 z + O(\log 2z \cdot \log \log 3z).
 \end{aligned}$$

引 4. 若  $\alpha$  和  $\beta$  是固定两数,  $2 < \alpha < \beta$ , 则

$$\begin{aligned}
 \sum_{x^{1/\beta} < p \leq x^{1/\alpha}} \frac{1}{p \log^2 \frac{x}{p}} & = \frac{1}{\log^2 x} \left\{ \log \frac{\beta-1}{\alpha-1} + \frac{1}{\alpha-1} - \frac{1}{\beta-1} \right\} \\
 & + O\left(\frac{1}{\log x}\right).
 \end{aligned}$$

证明见 [4], [8].

## § 2.

给出一组数列

$$(w)a = 0 \text{ 或 } 1, \quad 0 \leq a_i, b_i < p_i, \quad a_i \neq b_i, \quad (1 \leq i \leq r),$$

此处  $3 = p_1 < p_2 < \dots < p_r \leq \xi$  为不超过  $\xi$  的全部奇素数.

命  $P_w(x, \xi)$  为适合下面条件的整数  $n$  的个数

$$\begin{aligned} n \leq x, n \equiv a \pmod{2}, n \not\equiv a_i \pmod{p_i}, \\ n \not\equiv b_i \pmod{p_i} \quad (1 \leq i \leq r). \end{aligned} \tag{1}$$

由孙子定理可知下面的联立同余式

$$\begin{cases} y \equiv 1 + a \pmod{2}, \\ y \equiv a_i \pmod{p_i} (1 \leq i \leq r); \end{cases} \begin{cases} y \equiv 1 + a \pmod{2}, \\ y \equiv b_i \pmod{p_i} (1 \leq i \leq r), \end{cases}$$

在区间  $0 \leq y < 2p_1 \cdots p_r$  内均有唯一的解, 命其分别为  $a^*$ ,  $b^*$ .

现在来证明适合(1)式的整数  $n$  的个数与适合下式的整数个数相同:

$$\begin{aligned} n \leq x, (n - a^*)(n - b^*) \not\equiv 0 \pmod{p_i} (1 \leq i \leq r), \\ (n - a^*)(n - b^*) \not\equiv 0 \pmod{2}. \end{aligned} \tag{2}$$

实际上, 当  $n$  适合(1)式, 则

$$\begin{aligned} (n - a^*)(n - b^*) &\equiv (n - a_i)(n - b_i) \not\equiv 0 \pmod{p_i} (1 \leq i \leq r), \\ (n - a^*)(n - b^*) &\equiv (a - 1 - a)^2 \equiv 1 \pmod{2}, \end{aligned}$$

故  $n$  亦适合(2)式.

反之, 若  $n$  适合(2)式, 则

$$(n - a_i)(n - b_i) \equiv (n - a^*)(n - b^*) \not\equiv 0 \pmod{p_i} \quad (1 \leq i \leq r),$$

即  $n \not\equiv a_i \pmod{p_i}, n \not\equiv b_i \pmod{p_i} \quad (1 \leq i \leq r).$

又

$$(n - 1 - a)^2 \equiv (n - a^*)(n - b^*) \not\equiv 0 \pmod{2},$$

故  $n \not\equiv 1 + a \pmod{2}$ , 即  $n \equiv a \pmod{2}$ . 因此  $n$  又适合(1)式.

**定理 A.** 命  $c > 0$ ;  $P = \prod_{p \leq \xi} p$ . 则对于任何给予的整数列  $(w)$  皆有

$$P_w(x, \xi) \leq \frac{x}{\sum_{\substack{1 \leq k \leq \xi \\ k|P}} \frac{\mu^2(k)}{f(k)}} + O\left(\sum_{\substack{1 \leq k_1, k_2 \leq \xi \\ k_1|P \\ k_2|P}} |\lambda_{k_1} \lambda_{k_2}| 2^{\alpha(k_1)} 2^{\alpha(k_2)}\right),$$

此处  $g(1) = 1; g(2) = \frac{1}{2}; g(p) = \frac{2}{p} (p > 2)$ ; 当  $n$  无平方因子时  $g(n) =$

$$\prod_{p|n} g(p); f(n) = \sum_{d|n} \frac{\mu(d)}{g\left(\frac{n}{d}\right)}; \text{ 及}$$

$$\lambda_n = \frac{\mu(n)}{g(n)f(n)} \sum_{\substack{1 \leq m \leq \xi \\ (n,m)=1 \\ m|P}} \frac{\mu^2(m)}{f(m)} \Big/ \sum_{\substack{1 \leq l \leq \xi \\ l|P}} \frac{\mu^2(l)}{f(l)}.$$

证: 当  $k|P$  时,

$$\sum_{\substack{k|(n-a^*)(n-b^*) \\ n \leq x}} 1 = 2^{\alpha(k) - \alpha((k,2))} \left[ \frac{x}{k} \right] + O(2^{\alpha(k)})$$



$$\begin{aligned}
 &= \frac{2^{\Omega(k)-\Omega(k,2)}}{k}x + O(2^{\Omega(k)}) \\
 &= g(k)x + O(2^{\Omega(k)}).
 \end{aligned}$$

由于满足条件(1)与条件(2)的整数个数相同, 以及  $\lambda_1=1$ ;  $\lambda_d=0$  ( $d>\xi^c$ ),

故

$$\begin{aligned}
 P_w(x, \xi) &= \sum_{\substack{n \leq x \\ ((n-a^*)(n-b^*), P)=1}} 1 = \sum_{n \leq x} \sum_{d | ((n-a^*)(n-b^*), P)} \mu(d) \\
 &\leq \sum_{n \leq x} \left( \sum_{d | ((n-a^*)(n-b^*), P)} \lambda_d \right)^2 \\
 &= \sum_{\substack{d_1 | P \\ d_1 \leq \xi}} \sum_{\substack{d_2 | P \\ d_2 \leq \xi}} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{d_1 d_2 | (n-a^*)(n-b^*) \\ n \leq x}} 1 \\
 &= x \sum_{\substack{d_1 | P \\ d_1 \leq \xi}} \sum_{\substack{d_2 | P \\ d_2 \leq \xi}} \lambda_{d_1} \lambda_{d_2} g\left(\frac{d_1 d_2}{(d_1, d_2)}\right) \\
 &\quad + O\left(\sum_{\substack{d_1 | P \\ d_1 \leq \xi}} \sum_{\substack{d_2 | P \\ d_2 \leq \xi}} |\lambda_{d_1} \lambda_{d_2}| 2^{\Omega(d_1)+\Omega(d_2)}\right) = xQ + R.
 \end{aligned}$$

当  $n$  无平方因子时

$$\begin{aligned}
 \frac{1}{g(n)} &= \sum_{\tau | n} \frac{1}{g(\tau)} \sum_{d | n/\tau} \mu(d) \\
 &= \sum_{d\tau | n} \frac{\mu(d)}{g(\tau)} = \sum_{k | n} \sum_{d | k} \frac{\mu(d)}{g\left(\frac{k}{d}\right)} = \sum_{k | n} f(k).
 \end{aligned}$$

故

$$\begin{aligned}
 Q &= \sum_{\substack{1 \leq d_1 \leq \xi \\ d_1 | P}} \sum_{\substack{1 \leq d_2 \leq \xi \\ d_2 | P}} \lambda_{d_1} \lambda_{d_2} \frac{g(d_1)g(d_2)}{g((d_1, d_2))} \\
 &= \sum_{\substack{1 \leq d_1 \leq \xi \\ d_1 | P}} \sum_{\substack{1 \leq d_2 \leq \xi \\ d_2 | P}} \lambda_{d_1} \lambda_{d_2} g(d_1)g(d_2) \sum_{d | (d_1, d_2)} f(d) \\
 &= \sum_{\substack{1 \leq d \leq \xi \\ d | P}} f(d) \left( \sum_{\substack{1 \leq k \leq \xi \\ d | k | P}} \lambda_k g(k) \right)^2.
 \end{aligned}$$

命

$$S = \sum_{\substack{1 \leq m \leq \xi \\ m | P}} \frac{\mu^2(m)}{f(m)},$$

则

$$\lambda_k g(k) = \frac{1}{S} \sum_{\substack{1 \leq m \leq \xi/k \\ (m, k)=1 \\ m | P}} \frac{\mu(k)\mu^2(m)}{f(k)f(m)}$$