圆法与筛法

以 Goldbach 猜想为例

QED

2026 年 10 月 27 日

目录

1 圆法 **3**

1.1 圆法的想法 . . . 3

1.1.1 Hardy-Ramanujan-Littlewood 的原始形式圆法 . . . 3

1.1.2 Vinogradov 形式的圆法 . . . 4

1.1.3 Farey 分割 . . . 5

1.2 三素数定理 . . . 6

1.2.1 圆的分割 . . . 6

1.2.2 优弧 . . . 7

1.2.3 劣弧 . . . 14

1.2.4 Vinogradov 定理的证明 . . . 25

1.3 强 Goldbach 猜想中的圆法 . . . 27

2 筛法 **34**

2.1 筛法的想法 . . . 34

2.1.1 筛法的一般框架 . . . 37

2.2 Brun 筛法 . . . 42

2.2.1 Brun 筛法的构造 . . . 42

2.2.2 孪生素数倒数和 . . . 44

2.2.3 命题 9+9 . . . 48

2.3 Rosser-Iwaniec 筛法 . . . 50

2.3.1 Rosser-Iwaniec 筛法的构造 . . . 50

2.3.2 微分-差分方程 . . . 54

2.4 线性筛法与 Jurkat-Richert 定理 . . . 59

2.5 Selberg 筛法 . . . 64

2.6 大筛法 . . . 72

2.6.1 大筛法的分析形式 . . . 74

2.6.2 大筛法的算术形式 79
2.7 陈景润定理 88
2.7.1 加权筛的构造 88
2.7.2 线性筛的应用 90
2.7.3 三个筛函数的估计 94
2.7.4 陈景润定理的证明 105
2.8 奇偶障碍 106

附录 A Siegel-Walfisz 定理 **108**

附录 B Bombieri-Vinogradov 定理 **109**

参考文献 **118**

本文的目的是介绍圆法和筛法, 并证明关于 Goldbach 猜想的两个著名定理, 即三素数定理和陈景润定理, 此外还包含一些其他相关内容.

- 弱 Goldbach 猜想: 每个大于 5 的奇数都可以表示为三个素数的和.
- 强 Goldbach 猜想: 每个大于 2 的偶数都可以表示为两个素数的和.

1 圆法

1.1 圆法的想法

圆法由 Hardy, Ramanujan 和 Littlewood 发明, 最初用于研究整数分拆问题, 后由 Vinogradov 提出另一形式, 并证明了三素数定理, 这里我们分别介绍这两种圆法.

1.1.1 Hardy-Ramanujan-Littlewood 的原始形式圆法

设 $a(n)$ 是一个定义在非负整数上的整数列, 设

$$F(z)=\sum_{n=0}^{\infty}a(n)z^n$$

为 $a(n)$ 的生成函数, 这里暂且不考虑收敛性问题, 由柯西积分公式可知

$$a(n)=\frac{1}{2\pi i}\int_{\gamma}\frac{F(z)}{z^{n+1}}\,\mathrm{d}z,$$

其中 γ 是复平面上包含原点的围道. 对于一些好的 $a(n)$, 收敛性不成问题, 例如分拆函数 $p(n)$, 有 Euler 公式

$$F(z)=\sum_{n=0}^{\infty}p(n)z^n=\prod_{k=1}^{\infty}\frac{1}{(1-z^k)},$$

收敛域为 $|z|<1$, 取 γ 为半径为 R 的圆, 其中 $0<R<1$, 则

$$p(n)=\frac{1}{2\pi i}\int_{\gamma}\frac{F(z)}{z^{n+1}}\,\mathrm{d}z=R^{-n}\int_0^1 F\left(Re^{2\pi i\theta}\right)e^{-2\pi in\theta}\,\mathrm{d}\theta,$$

研究该积分就是研究分拆函数本身, 围道 γ 就是圆法这个名字的来源. 通过对 γ 或 $[0,1]$ 的分割, Hardy 和 Ramanujan 得到了渐进估计

$$p(n)=\frac{1}{4\sqrt{3}}\frac{e^{\lambda\sqrt{m}}}{m}\left(1+O\left(\frac{1}{\sqrt{m}}\right)\right),$$

其中 $\lambda=\pi\sqrt{2/3}$, $m=n-1/24$, 通过更精细的分割, Rademacher 证明了精确的级数展开式

$$p(n)=\frac{1}{\pi\sqrt{2}}\sum_{k=1}^{\infty}\left(\sqrt{k}\left(\sum_{\substack{h=0\\(h,k)=1}}^{k-1}e^{\pi is(h,k)-2\pi inh/k}\right)\left[\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{1}{\sqrt{x}}\sinh\left(\frac{\pi}{k}\sqrt{\frac{2x}{3}}\right)\right)\right]_{x=n-1/24}\right),$$

其中 $s(h,k)$ 是 Dedekind 和, 证明见 [12] 第 36 章.

1.1.2 Vinogradov 形式的圆法

接下来叙述 Vinogradov 版本的圆法.

设 A 是一些正整数组成的集合, 定义 $r_{A,s}(N)$ 为将正整数 N 表示为 A 中 s 个数的和的方法数, 设

$$F_A(z,N)=\sum_{\substack{a\in A\\ a\leq N}}e(az),$$

由熟知的积分

$$\int_0^1 e(nz)\,\mathrm{d}z=\begin{cases}1, & n=0,\\ 0, & n\neq 0,\end{cases}$$

得

$$r_{A,s}(N)=\int_0^1 F_A(z,N)^s e(-Nz)\,\mathrm{d}z,$$

因为将被积函数展开后, 只有 $a_1+\cdots+a_s-N=0$ 时 $e((a_1+\cdots+a_s-N)z)$ 项的积分才非零, 总共 $r_{A,s}(N)$ 项非零, 其中每一项对积分的贡献为 1.

例 1 (Goldbach 猜想)**.** 取 A 为所有素数组成的集合, 设

$$F(z,N)=\sum_{p\leq N}e(pz),$$

强 *Goldbach* 猜想就是要证

$$\int_0^1 F(z,N)^2 e(-Nz)\,\mathrm{d}z>0,$$

弱 *Goldbach* 猜想就是要证

$$\int_0^1 F(z,N)^3 e(-Nz)\,\mathrm{d}z>0.$$

例 2 (Waring 问题)**.** 取 A 为所有 k 次方数组成的集合 $\left\{n^k\right\}_{n=1}^{\infty}$, 设

$$F_k(z,N)=\sum_{0\leq n\leq N^{1/k}}e\left(n^k z\right),$$

这里求和从 0 开始是为了将积分结果由[将 N 表示为精确的 s 个 k 次方数的和的方法数]变为[将 N 表示为至多 s 个 k 次方数的和的方法数], *Waring* 问题就是求使得

$$\int_0^1 F_k(z,N)^s e(-Nz)\,\mathrm{d}z>0$$

对任意正整数 N 均成立的最小 s, 记为 $g(k)$, 还有另一种 *Waring* 问题是求

$$\int_0^1 F_k(z,N)^s e(-Nz)\,\mathrm{d}z>0$$

对除至多有限个正整数 N 外均成立的最小 s, 记为 $G(k)$, 显然 $G(k)\leq g(k)$, 猜想

$$g(k)=2^k+\left[\left(\frac{3}{2}\right)^k\right]-2.$$

1.1.3 Farey 分割

对区间 $[0,1]$ 的分割最常见的方法称为 Farey 分割, 因为它基于所谓的 Farey 数列.

对于固定的正整数 Q, Q 阶 Farey 数列定义为 0 到 1 之间分母不超过 Q 的所有既约分数, 即

$$\left\{\frac{a}{q} : 0 \le a \le q \le Q, (a,q) = 1\right\},$$

Farey 分割的想法是, 将距离 Farey 数列较近的数组成的集合看做主要部分, 其余数组成的集合看做次要部分, 我们想办法估计主要部分上的积分, 并控制次要部分上的积分, 使得次要部分上的积分相对较小, 可以忽略.

具体来说, 要找到一个数 ε, 定义

$$\mathfrak{M}(q,a) = \left\{\alpha \in [0,1] : \left|\alpha - \frac{a}{q}\right| \le \varepsilon\right\},$$

$$\mathfrak{M} = \bigcup_{q=1}^{Q} \bigcup_{\substack{0\le a\le q\\(a,q)=1}} \mathfrak{M}(q,a),$$

并且我们希望诸 $\mathfrak{M}(q,a)$ 互不相交, 称 $\mathfrak{M}$ 为优弧或主区间, 定义

$$\mathfrak{m} = [0,1] - \mathfrak{M},$$

称 $\mathfrak{m}$ 为劣弧或余区间, 则

$$\int_0^1 F_A(z,N)^s e(-Nz)\,\mathrm{d}z = \int_{\mathfrak{M}} F_A(z,N)^s e(-Nz)\,\mathrm{d}z + \int_{\mathfrak{m}} F_A(z,N)^s e(-Nz)\,\mathrm{d}z,$$

其中第一项称为主项, 第二项称为误差项, 我们希望当 N 足够大时, 误差项相对于主项是可以忽略的.

以下定理在圆法中经常用到.

定理 1 (Dirichlet 逼近定理)**.** *对任意实数 α 和实数 $Q \ge 1$, 存在整数 a 和 q, 满足 $(a,q) = 1$, $1 \le q \le Q$, 且*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

证明. 以下 $[Q]+2$ 个数

$$0\alpha - [0\alpha], 1\alpha - [1\alpha], 2\alpha - [2\alpha], \ldots, [Q]\alpha - [[Q]\alpha], 1$$

均位于区间 $[0,1]$ 中, 因此必有其中两个的距离不超过 $1/([Q]+1)$, 首先假设这两个数中没有 1, 即设为 $k_1\alpha - [k_1\alpha]$ 和 $k_2\alpha - [k_2\alpha]$, $0 \le k_1 < k_2 \le [Q]$, 再设 $m = k_2 - k_1$, $n = [k_2\alpha] - [k_1\alpha]$, 取

$$q = \frac{m}{(m,n)}, \quad a = \frac{n}{(m,n)},$$

显然 $1 \le q \le Q$, 且

$$\left|\alpha - \frac{a}{q}\right| = \frac{|k_2\alpha - k_1\alpha - ([k_2\alpha] - [k_1\alpha])|}{m} \le \frac{1}{q([Q]+1)} < \frac{1}{qQ},$$

若这两个数中有 1, 不妨设另一个是 $k\alpha-[k\alpha]$, $k>0$, 再设 $m'=k$, $n'=[k\alpha]+1$, 取

$$q=\frac{m'}{(m',n')},\quad a=\frac{n'}{(m',n')},$$

显然 $1\leq q\leq Q$, 且

$$\left|\alpha-\frac{a}{q}\right|=\frac{|k\alpha-[k\alpha]-1|}{m'}\leq\frac{1}{q([Q]+1)}<\frac{1}{qQ},$$

因此不管是哪种情况, 所选的 q 和 a 都满足定理要求. □

1.2 三素数定理

定理 2 (三素数定理)**.** *存在一个正常数 C, 使得任意正奇数 N, 若 $N>C$, 则 N 可以表示为三个素数的和.*

三素数定理的证明方法一般可以分为两种, 分别为非实效方法和实效方法, 使用非实效方法的证明无法具体计算出定理中的常数 C, 但可以得到较好的渐进公式, 实效方法可以具体计算出常数 C, 但得到的渐进公式可能较弱, 本文中使用的是 Vaughan 改进的非实效方法.

需要说明三素数定理并不意味着弱 Goldbach 猜想得证, 因为常数 C 可能十分巨大以至于小于 C 的情形无法验证, 直至 2013 年, Helfgott 使用圆法结合筛法将该常数降至 10^{27}, 并使用计算机验证了小于 10^{27} 的所有奇数均满足弱 Goldbach 猜想, 这才完全证明了弱 Goldbach 猜想.

以下设

$$r(N)=\sum_{p_1+p_2+p_3=N}1,$$

我们将证明以下定理.

定理 3 (Vinogradov 定理)**.** *对足够大的奇数 N, 有*

$$r(N)=\mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\left(1+O\left(\frac{\log\log N}{\log N}\right)\right),$$

其中 $\mathfrak{S}(N)$ 是算术函数, 当 N 是偶数时, $\mathfrak{S}(N)=0$, 当 N 是奇数时,

$$\frac{1}{2}<\mathfrak{S}(N)<e^{\zeta(3)}.$$

$\mathfrak{S}(N)$ 称为弱 Goldbach 猜想中的奇异级数, 尽管该级数的行为十分正常, 奇异这个名字可能与生成函数在单位圆上的奇点相关.

1.2.1 圆的分割

按后见之明, 相比于研究指数和

$$\sum_{p\leq N}e(p\alpha),$$

研究以下形式的加权指数和

$$F(\alpha)=\sum_{p\leq N}e(p\alpha)\log p$$

会更容易, 则积分计算的就是

$$R(N)=\sum_{p_1+p_2+p_3=N}\log p_1\log p_2\log p_3=\int_0^1 F(\alpha)^3e(-N\alpha)\,\mathrm{d}\alpha,$$

当然使用原来的指数和也是可以的, 例如 [12].

对任意正实数 $B>0$, 令 $Q=(\log N)^B$, 优弧取

$$\mathfrak{M}(q,a)=\left\{\alpha\in[0,1]:\left|\alpha-\frac{a}{q}\right|\le\frac{Q}{N},0\le a\le q\le Q,(a,q)=1\right\},$$

$$\mathfrak{M}=\bigcup_{q=1}^{[Q]}\bigcup_{\substack{0\le a\le q\\(a,q)=1}}\mathfrak{M}(q,a),$$

若 $x\in\mathfrak{M}(q,a)\cap\mathfrak{M}(q',a')$, $a/q\ne a'/q'$, 则

$$\frac{1}{Q^2}\le\frac{1}{qq'}\le\frac{|aq'-a'q|}{qq'}=\left|\frac{a}{q}-\frac{a'}{q'}\right|\le\left|\frac{a}{q}-x\right|+\left|x-\frac{a'}{q'}\right|\le\frac{2Q}{N},$$

即

$$N\le 2Q^3=2(\log N)^{3B},$$

这在 N 足够大的时候是不可能的, 因此当 N 足够大时, 诸 $\mathfrak{M}(q,a)$ 互不相交. 再取劣弧为

$$\mathfrak{m}=[0,1]-\mathfrak{M},$$

则

$$\int_0^1 F(\alpha)^3e(-N\alpha)\,\mathrm{d}\alpha=\int_{\mathfrak{M}}F(\alpha)^3e(-N\alpha)\,\mathrm{d}\alpha+\int_{\mathfrak{m}}F(\alpha)^3e(-N\alpha)\,\mathrm{d}\alpha.$$

1.2.2 优弧

我们需要以下形式的 Siegel-Walfisz 定理, 证明见附录.

定理 4 (Siegel-Walfisz 定理)**.** *对任意实数 $B>1$, 若 $0\le a\le q\le(\log N)^B$, $(a,q)=1$, 则对任意 $1\le x\le N$, 任意实数 $C>0$, 有*

$$\pi(x;q,a)=\sum_{\substack{p\le x\\p\equiv a\pmod q}}1=\frac{\mathrm{Li}(x)}{\varphi(q)}+O\left(\frac{N}{(\log N)^C}\right),$$

$$\theta(x;q,a)=\sum_{\substack{p\le x\\p\equiv a\pmod q}}\log p=\frac{x}{\varphi(q)}+O\left(\frac{N}{(\log N)^C}\right),$$

其中大 O 常数只与 C 有关.

我们先来估计指数和

$$F_x(\alpha)=\sum_{p\le x}e(p\alpha)\log p.$$

引理 1. 对任意实数 $C>0$, $B>1$, 若 $0\le a\le q\le(\log N)^B=Q$, $(a,q)=1$, 则

$$F_x\left(\frac{a}{q}\right)=\frac{\mu(q)}{\varphi(q)}x+O\left(\frac{QN}{(\log N)^C}\right)$$

对任意 $1\le x\le N$ 一致的成立, 其中大 O 常数只与 B 和 C 有关.

证明. 将 p 按模 q 分类, 则

$$\begin{aligned}F_x\left(\frac{a}{q}\right)&=\sum_{p\le x}e\left(\frac{pa}{q}\right)\log p\\&=\sum_{r=1}^{q}\sum_{\substack{p\le x\\ p\equiv r\pmod q}}e\left(\frac{pa}{q}\right)\log p\\&=\sum_{\substack{r=1\\(r,q)=1}}^{q}\sum_{\substack{p\le x\\ p\equiv r\pmod q}}e\left(\frac{pa}{q}\right)\log p+\sum_{\substack{r=1\\(r,q)>1}}^{q}\sum_{\substack{p\le x\\ p\equiv r\pmod q}}e\left(\frac{pa}{q}\right)\log p,\end{aligned}$$

不妨设 $p=r+kq$, 则 $(r,q)|p$, 因此 $(r,q)>1$ 当且仅当 $(r,q)=(p,q)=p$ 当且仅当 $p|q$, 上式中第二项有估计

$$\sum_{\substack{r=1\\(r,q)>1}}^{q}\sum_{\substack{p\le x\\ p\equiv r\pmod q}}e\left(\frac{pa}{q}\right)\log p=\sum_{\substack{p\le x\\ p|q}}e\left(\frac{pa}{q}\right)\log p\ll\sum_{p|q}\log p\le\log q<\log Q,$$

故

$$\begin{aligned}F_x\left(\frac{a}{q}\right)&=\sum_{\substack{r=1\\(r,q)=1}}^{q}\sum_{\substack{p\le x\\ p\equiv r\pmod q}}e\left(\frac{pa}{q}\right)\log p+O(\log Q)\\&=\sum_{\substack{r=1\\(r,q)=1}}^{q}e\left(\frac{ra}{q}\right)\sum_{\substack{p\le x\\ p\equiv r\pmod q}}\log p+O(\log Q)\\&=\sum_{\substack{r=1\\(r,q)=1}}^{q}e\left(\frac{ra}{q}\right)\theta(x;q,r)+O(\log Q),\end{aligned}$$

由 Siegel-Walfisz 定理得

$$F_x\left(\frac{a}{q}\right)=\sum_{\substack{r=1\\(r,q)=1}}^{q}e\left(\frac{ra}{q}\right)\left(\frac{x}{\varphi(q)}+O\left(\frac{N}{(\log N)^C}\right)\right)+O(\log Q),$$

再记

$$c_q(a)=\sum_{\substack{r=1\\(r,q)=1}}^{q}e\left(\frac{ra}{q}\right)$$

为 Ramanujan 和, 由显然的估计 $|c_q(a)| < q$ 得

$$F_x\left(\frac{a}{q}\right) = \frac{c_q(a)}{\varphi(q)}x + O\left(\frac{qN}{(\log N)^C}\right) + O(\log Q),$$

因为在 $(q,a)=1$ 时, 有 $c_q(a)=\mu(q)$, 故

$$F_x\left(\frac{a}{q}\right) = \frac{\mu(q)}{\varphi(q)}x + O\left(\frac{qN}{(\log N)^C}\right) + O(\log Q) = \frac{\mu(q)}{\varphi(q)}x + O\left(\frac{QN}{(\log N)^C}\right)$$

成立. □

引理 2. 对任意实数 C 和 B, 满足 $C > 2B$ 和 $B > 1$, 若 $\alpha \in \mathfrak{M}(q,a)$, 设 $\beta = \alpha - a/q$,

$$u(\beta) = \sum_{m=1}^{N} e(m\beta),$$

则有

$$F(\alpha) = \frac{\mu(q)}{\varphi(q)}u(\beta) + O\left(\frac{Q^2N}{(\log N)^C}\right),$$
$$F(\alpha)^3 = \frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + O\left(\frac{Q^2N^3}{(\log N)^C}\right),$$

其中大 O 常数只与 B 和 C 有关.

证明. 令

$$\lambda(m) = \begin{cases} \log m, & m\text{是素数}, \\ 0, & \text{其他}, \end{cases}$$

则

$$\begin{aligned} F(\alpha) - \frac{\mu(q)}{\varphi(q)}u(\beta) &= \sum_{p\le N} e(p\alpha)\log p - \frac{\mu(q)}{\varphi(q)}\sum_{m=1}^{N} e(m\beta) \\ &= \sum_{m=1}^{N} \lambda(m)e(m\alpha) - \frac{\mu(q)}{\varphi(q)}\sum_{m=1}^{N} e(m\beta) \\ &= \sum_{m=1}^{N} \lambda(m)e\left(\frac{ma}{q} + m\beta\right) - \sum_{m=1}^{N}\frac{\mu(q)}{\varphi(q)}e(m\beta) \\ &= \sum_{m=1}^{N}\left(\lambda(m)e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\varphi(q)}\right)e(m\beta). \end{aligned}$$

设

$$A(x) = \sum_{1\le m\le x}\left(\lambda(m)e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\varphi(q)}\right),$$

则由 Abel 求和公式得

$$F(\alpha) - \frac{\mu(q)}{\varphi(q)}u(\beta) = A(N)e(N\beta) - 2\pi i\beta\int_1^N A(x)e(x\beta)dx$$

$$\ll |A(N)| + |\beta| N \max\{|A(x)| : 1 \le x \le N\}$$
$$\le |A(N)| + Q \max\{|A(x)| : 1 \le x \le N\},$$

最后一个不等式是因为 $|\beta| \le Q/N$, 而当 $1 \le x \le N$ 时一致的有

$$\begin{aligned} A(x) &= \sum_{1 \le m \le x} \left(\lambda(m) e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\varphi(q)} \right) \\ &= \sum_{1 \le m \le x} \lambda(m) e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\varphi(q)} x + O\left(1\right) \\ &= F_x\left(\frac{a}{q}\right) - \frac{\mu(q)}{\varphi(q)} x + O(1) \\ &= O\left(\frac{QN}{(\log N)^C}\right), \end{aligned}$$

于是

$$F(\alpha) - \frac{\mu(q)}{\varphi(q)} u(\beta) \ll \frac{Q^2 N}{(\log N)^C},$$

即

$$F(\alpha) = \frac{\mu(q)}{\varphi(q)} u(\beta) + O\left(\frac{Q^2 N}{(\log N)^C}\right).$$

又因 $C > 2B$, 有

$$\frac{Q^2 N}{(\log N)^C} = \frac{N}{(\log N)^{C-2B}} < N,$$

假设 $E = O\left(Q^2 N/(\log N)^C\right)$, 则 $|E| \ll N$, 并且显然 $|u(\beta)| \le N$, 因此

$$\begin{aligned} F(\alpha)^3 &= \frac{\mu(q)^3}{\varphi(q)^3} u(\beta)^3 + 3\frac{\mu(q)}{\varphi(q)} u(\beta) E^2 + 3\frac{\mu(q)^2}{\varphi(q)^2} u(\beta)^2 E + E^3 \\ &= \frac{\mu(q)}{\varphi(q)^3} u(\beta)^3 + O(N^2 |E|) \\ &= \frac{\mu(q)}{\varphi(q)^3} u(\beta)^3 + O\left(\frac{Q^2 N^3}{(\log N)^C}\right), \end{aligned}$$

引理得证. □

引理 3. 级数

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \frac{\mu(q) c_q(N)}{\varphi(q)^3}$$

绝对收敛, 并且部分和

$$\mathfrak{S}(N, Q) = \sum_{1 \le q \le Q} \frac{\mu(q) c_q(N)}{\varphi(q)^3} = \mathfrak{S}(N) + O\left(\frac{1}{Q^{1-\varepsilon}}\right)$$

对任意 $\varepsilon > 0$ 都成立. 该级数有 *Euler* 乘积

$$\mathfrak{S}(N) = \prod_{p | N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \nmid N} \left(1 + \frac{1}{(p-1)^3}\right),$$

且不等式

$$\frac{1}{2} < \mathfrak{S}(N) < e^{\zeta(3)}$$

对所有正奇数 N 成立.

证明. 由定义立得 $|c_q(N)| \leq \varphi(q)$, 因此

$$\left|\frac{\mu(q)c_q(N)}{\varphi(q)^3}\right| \leq \frac{1}{\varphi(q)^2},$$

接下来证明 $1/\varphi(n) = O(1/n^{1-\varepsilon})$ 对任意 $\varepsilon > 0$ 成立, 事实上有更强的

$$\lim_{n\to\infty} \frac{n^{1-\varepsilon}}{\varphi(n)} = 0,$$

当 n 是素数幂 p^m 时,

$$\frac{p^{m(1-\varepsilon)}}{\varphi(p^m)} = \frac{p^{m(1-\varepsilon)}}{p^m - p^{m-1}} = \frac{p}{p-1}\frac{p^{m(1-\varepsilon)}}{p^m} \leq \frac{2}{p^{m\varepsilon}} \to 0,$$

由 Euler 函数的乘性知也有 $n^{1-\varepsilon}/\varphi(n) \to 0$, 所以

$$\left|\frac{\mu(q)c_q(N)}{\varphi(q)^3}\right| \leq \frac{1}{\varphi(q)^2} \ll \frac{1}{q^{2-\varepsilon}},$$

因此级数绝对收敛, 并且

$$\mathfrak{S}(N) - \mathfrak{S}(N,Q) \ll \sum_{q>Q} \frac{1}{\varphi(q)^2} \ll \sum_{q>Q} \frac{1}{q^{2-\varepsilon}} \ll \frac{1}{Q^{1-\varepsilon}},$$

即

$$\mathfrak{S}(N,Q) = \sum_{q\leq Q} \frac{\mu(q)c_q(N)}{\varphi(q)^3} = \mathfrak{S}(N) + O\left(\frac{1}{Q^{1-\varepsilon}}\right).$$

由于 $\mu(q)c_q(N)/\varphi(q)^3$ 是关于 q 的乘性函数, 则有 Euler 乘积

$$\mathfrak{S}(N) = \prod_p \left(1 + \sum_{j=1}^{\infty} \frac{\mu(p^j)c_{p^j}(N)}{\varphi(p^j)^3}\right) = \prod_p \left(1 - \frac{c_p(N)}{(p-1)^3}\right),$$

因为

$$c_p(N) = \begin{cases} p-1 & p \mid N, \\ -1 & p \nmid N, \end{cases}$$

故有

$$\mathfrak{S}(N) = \prod_{p\mid N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right),$$

显然 N 是偶数时 $\mathfrak{S}(N) = 0$, N 是奇数时,

$$\mathfrak{S}(N) > \prod_{p\mid N} \left(1 - \frac{1}{(p-1)^2}\right) > \prod_{k=2}^{\infty} \left(1 - \frac{1}{k^2}\right) = \frac{1}{2},$$

$$\mathfrak{S}(N) < \prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right) < \exp\left(\sum_p \frac{1}{(p-1)^3}\right) < e^{\zeta(3)},$$

引理得证. □

引理 4. 设

$$u(\beta) = \sum_{m=1}^{N} e(m\beta),$$

则

$$J(N) = \int_{-1/2}^{1/2} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta = \binom{N-1}{2} = \frac{N^2}{2} + O(N).$$

证明. 显然该积分计算的是将 N 表示为三个正整数的方法数, 即在 $N-1$ 个空位插入 2 个竖线的方法数, 即

$$J(N) = \binom{N-1}{2} = \frac{N^2}{2} - \frac{3N}{2} + 1 = \frac{N^2}{2} + O(N),$$

引理得证. □

级数 $\mathfrak{S}(N)$ 称为奇异级数, 积分 $J(N)$ 称为奇异积分.

引理 5. 设 $x \geq 1$, β 是实数, 则

$$\left|\sum_{n\leq x} e(n\beta)\right| \leq \min\left\{x, \frac{1}{2\|\beta\|}\right\},$$

其中当 $\|\beta\| = 0$ 时出现的 $1/0$ 理解为无穷大.

证明. 当 β 不是整数时, $\|\beta\| \neq 0$, 有

$$\begin{aligned}\left|\sum_{n\leq x} e(n\beta)\right| &= \left|\frac{e(([x]+1)\beta) - e(\beta)}{e(\beta)-1}\right| \\ &\leq \frac{2}{|e(\beta)-1|} = \frac{2}{|e(\beta/2) - e(-\beta/2)|} = \frac{2}{|2i\sin\pi\beta|} \\ &= \frac{1}{|\sin\pi\beta|} = \frac{1}{\sin(\pi\|\beta\|)} \\ &\leq \frac{1}{2\|\beta\|},\end{aligned}$$

结合显然的估计

$$\left|\sum_{n\leq x} e(n\beta)\right| \leq \sum_{n\leq x} 1 \leq x$$

便得到了引理的结果. □

定理 5. 对任意正数 $\varepsilon>0$, $B>1$ 和 $C>2B$, 有

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)\,\mathrm{d}\alpha = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^{(1-\varepsilon)B}}\right) + O\left(\frac{N^2}{(\log N)^{C-5B}}\right),$$

其中大 O 常数只与 ε, B 和 C 有关.

证明. 由 $|\mathfrak{M}(q,a)| \le 2Q/N$,

$$\begin{aligned}
&\int_{\mathfrak{M}} \left(F(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha-\frac{a}{q}\right)^3\right) e(-N\alpha)\,\mathrm{d}\alpha \\
&= \sum_{q\le Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \left(F(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha-\frac{a}{q}\right)^3\right) e(-N\alpha)\,\mathrm{d}\alpha \\
&\ll \sum_{q\le Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \frac{Q^2N^3}{(\log N)^C}\,\mathrm{d}\alpha \\
&\ll \sum_{q\le Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} \frac{Q^3N^2}{(\log N)^C} \\
&\le \frac{Q^5N^2}{(\log N)^C} = \frac{N^2}{(\log N)^{C-5B}},
\end{aligned}$$

设 $\beta = \alpha - a/q \in [-Q/N, Q/N]$, 则

$$\begin{aligned}
&\sum_{q\le Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)^3} \int_{\mathfrak{M}(q,a)} u\left(\alpha-\frac{a}{q}\right)^3 e(-N\alpha)\,\mathrm{d}\alpha \\
&= \sum_{q\le Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)^3} \int_{a/q-Q/N}^{a/q+Q/N} u\left(\alpha-\frac{a}{q}\right)^3 e(-N\alpha)\,\mathrm{d}\alpha \\
&= \sum_{q\le Q} \frac{\mu(q)}{\varphi(q)^3} \sum_{\substack{a=1\\(a,q)=1}}^{q} e(-Na/q) \int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta \\
&= \sum_{q\le Q} \frac{\mu(q)c_q(-N)}{\varphi(q)^3} \int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta \\
&= \mathfrak{S}(N,Q) \int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta,
\end{aligned}$$

而当 $Q/N \le |\beta| \le 1/2$ 时, $u(\beta) < 1/(2\|\beta\|) \ll 1/|\beta|$, 因此有

$$\begin{aligned}
\int_{Q/N}^{1/2} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta &\ll \int_{Q/N}^{1/2} |u(\beta)|^3\,\mathrm{d}\beta \\
&\ll \int_{Q/N}^{1/2} \beta^{-3}\,\mathrm{d}\beta \\
&< \frac{N^2}{Q^2},
\end{aligned}$$

同理

$$\int_{-1/2}^{-Q/N} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta \ll \frac{N^2}{Q^2},$$

所以有

$$\begin{aligned}\int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta &= \int_{-1/2}^{1/2} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta + O(N^2Q^{-2}) \\ &= \frac{N^2}{2} + O(N) + O\left(\frac{N^2}{Q^2}\right) \\ &= \frac{N^2}{2} + O\left(\frac{N^2}{Q^2}\right),\end{aligned}$$

综上可得

$$\begin{aligned}\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)\,\mathrm{d}\alpha &= \mathfrak{S}(N,Q)\int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta + O\left(\frac{N^2}{(\log N)^{C-5B}}\right) \\ &= \left(\mathfrak{S}(N) + O\left(\frac{1}{Q^{1-\varepsilon}}\right)\right)\left(\frac{N^2}{2} + O\left(\frac{N^2}{Q^2}\right)\right) + O\left(\frac{N^2}{(\log N)^{C-5B}}\right) \\ &= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{Q^{1-\varepsilon}}\right) + O\left(\frac{N^2}{(\log N)^{C-5B}}\right) \\ &= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^{(1-\varepsilon)B}}\right) + O\left(\frac{N^2}{(\log N)^{C-5B}}\right),\end{aligned}$$

定理得证. □

1.2.3 劣弧

我们先来估计劣弧上线性指数和

$$\sum_{1\le m\le x} e(m\alpha),$$

这是 Weyl 不等式的最简单情形. 本节几乎处处都用到 Dirichlet 逼近定理.

引理 6. *令 α 是实数, a 和 q 是使得*

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q^2}$$

成立的整数, 其中 $(a,q)=1$, $q\ge 1$, 则

$$\sum_{1\le r\le q/2} \frac{1}{\|\alpha r\|} \ll q\log q.$$

证明. 当 $q=1$ 时, 不等式显然成立, 左边右边均为 0, 现设 $q\ge 2$. 设

$$\alpha = \frac{a}{q} + \frac{\theta}{q^2},$$

其中 $-1\le\theta\le 1$, 则

$$\|\alpha r\| = \left\|\frac{ar}{q} + \frac{\theta r}{q^2}\right\| = \left\|\left\{\frac{ar}{q}\right\} + \frac{\theta r}{q^2}\right\| = \left\|\left\{\frac{ar}{q}\right\} \pm \frac{|\theta| r}{q^2}\right\|,$$

无论 θ 正负, 由 $\|\cdot\|$ 的三角不等式有

$$\|\alpha r\| \geq \left\| \left\{ \frac{ar}{q} \right\} \right\| - \left\| \frac{\theta r}{q^2} \right\| \geq \left\| \frac{ar}{q} \right\| - \frac{1}{2q},$$

最后一个不等式是因为 $|\theta| \leq 1$ 和 $r \leq q/2$.

接下来证明 $r \mapsto \|ar/q\|$ 是单射, 若不然, 设 $1 \leq r_1 < r_2 \leq q/2$ 且 $\|ar_1/q\| = \|ar_2/q\|$, 则必有 $ar_1/q + ar_2/q$ 是整数或 $ar_1/q - ar_2/q$ 是整数, 即 $ar_1 \equiv ar_2 \pmod q$ 或 $ar_1 \equiv -ar_2 \pmod q$, 由 $(a,q) = 1$ 得 $r_1 \equiv r_2 \pmod q$ 或 $r_1 \equiv -r_2 \pmod q$, 又因 r_1 和 r_2 都不超过 $q/2$, 其和也不超过 q, 不论是哪种情况, 都必须有 $r_1 = r_2$, 矛盾, 因此 $r \mapsto \|ar/q\|$ 是单射, 因此当 r 跑遍 1 到 $q/2$ 时, $\|ar/q\|$ 跑遍 $\{b/q : 1 \leq b \leq q/2\}$, 故有

$$\sum_{1 \leq r \leq q/2} \frac{1}{\|\alpha r\|} \leq \sum_{1 \leq r \leq q/2} \frac{1}{\left\| \frac{ar}{q} \right\| - \frac{1}{2q}} = \sum_{1 \leq b \leq q/2} \frac{1}{\frac{b}{q} - \frac{1}{2q}} = 2q \sum_{1 \leq b \leq q/2} \frac{1}{2b-1} \leq 2q \sum_{1 \leq b \leq q/2} \frac{1}{b} \ll q \log q,$$

引理得证. □

引理 7. 令 α 是实数, a 和 q 是使得

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{q^2}$$

成立的整数, 其中 $(a,q) = 1$, $q \geq 1$, 则对任意非负实数 V 和非负整数 h, 有

$$\sum_{r=1}^{q} \min \left\{ V, \frac{1}{\|\alpha(hq+r)\|} \right\} \ll V + q \log q.$$

证明. 由于 $0 \leq \|\alpha(hq+r)\| \leq 1/2$, 将 $[0, 1/2]$ 分割为

$$J(s) = \left[\frac{s}{q}, \frac{s+1}{q} \right], \quad s \in \mathbb{Z}, 0 \leq s < \frac{q}{2},$$

对每个 r, 必存在某个 s 使得 $\|\alpha(hq+r)\| \in J(s)$.

现设

$$\alpha = \frac{a}{q} + \frac{\theta}{q^2}, \quad \theta \in [-1, 1],$$

则

$$\begin{aligned} \alpha(hq+r) &= ah + \frac{ar}{q} + \frac{\theta h}{q} + \frac{\theta r}{q^2} \\ &= ah + \frac{ar}{q} + \frac{[\theta h] + \{\theta h\}}{q} + \frac{\theta r}{q^2} \\ &= ah + \frac{ar + [\theta h] + \delta(r)}{q}, \end{aligned}$$

其中

$$-1 \leq \delta(r) = \{\theta h\} + \frac{\theta r}{q} < 2,$$

对每个 r, 都存在整数 r' 使得

$$\{\alpha(hq+r)\} = \frac{ar + [\theta h] + \delta(r)}{q} - r'.$$

取 $0 \le t \le 1 - 1/q$, 若

$$t \le \{\alpha(hq + r)\} \le t + \frac{1}{q},$$

则

$$qt \le ar - qr' + [\theta h] + \delta(r) \le qt + 1,$$

所以有

$$qt - [\theta h] - 2 < qt - [\theta h] - \delta(r) \le ar - qr' \le qt - [\theta h] + 1 - \delta(r) \le qt - [\theta h] + 2,$$

即 $ar - qr'$ 位于区间 $(qt - [\theta h] - 2, qt - [\theta h] + 2]$ 中, 而该区间中有恰好 4 个整数. 若 $1 \le r_1 \le r_2 \le q$, 且 $ar_1 - qr_1' = ar_2 - qr_2',$, 则有 $ar_1 \equiv ar_2 \pmod q$, 又由于 $(a, q) = 1$, 则有 $r_1 \equiv r_2 \pmod q$, 因此必有 $r_1 = r_2$, 所以映射 $r \mapsto ar - qr'$ 是从 $\mathbb{Z} \cap [1, q]$ 到 $\mathbb{Z}$ 的单射, 故区间 $(qt - [\theta h] - 2, qt - [\theta h] + 2]$ 的原像中至多只有 4 个数, 即至多只有 4 个 r 使得 $t \le \{\alpha(hq + r)\} \le t + 1/q$.

假设 $\|\alpha(hq + r)\| \in J(s)$, 则要么 $s/q \le \{\alpha(hq + r)\} \le s/q + 1/q$, 要么 $s/q \le 1 - \{\alpha(hq + r)\} \le s/q + 1/q$, 后者等价于 $1 - s/q - 1/q \le \{\alpha(hq + r)\} \le 1 - s/q$, 在此前的讨论中取 t 为 s/q 或 $1 - s/q - 1/q$ 便知道, 至多只有 8 个 r 使得 $\|\alpha(hq + r)\| \in J(s)$.

因此, 有

$$\begin{aligned}
&\sum_{r=1}^{q} \min\left\{V, \frac{1}{\|\alpha(hq + r)\|}\right\} \\
&= \sum_{0 \le s < q/2} \sum_{\|\alpha(hq+r)\| \in J(s)} \min\left\{V, \frac{1}{\|\alpha(hq + r)\|}\right\} \\
&= \sum_{\|\alpha(hq+r)\| \in J(0)} \min\left\{V, \frac{1}{\|\alpha(hq + r)\|}\right\} + \sum_{1 \le s < q/2} \sum_{\|\alpha(hq+r)\| \in J(s)} \min\left\{V, \frac{1}{\|\alpha(hq + r)\|}\right\} \\
&\le 8V + 8 \sum_{1 \le s < q/2} \frac{q}{s} \\
&\ll V + q \log q,
\end{aligned}$$

引理得证. □

定理 6. *令 α 是实数, a 和 q 是使得*

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q^2}$$

成立的整数, 其中 $(a, q) = 1$, $q \ge 1$, 则对任意实数 $u \ge 2$ 和正数 N, 有

$$\sum_{1 \le k \le u} \min\left(\frac{N}{k}, \frac{1}{\|\alpha k\|}\right) \ll q \log q + u \log q + \frac{N}{q} \log u.$$

证明. 对 k 模 q 分类,

$$\sum_{1 \le k \le u} \min\left(\frac{N}{k}, \frac{1}{\|\alpha k\|}\right) \le \sum_{0 \le h < u/q} \sum_{1 \le r \le q} \min\left(\frac{N}{hq + r}, \frac{1}{\|\alpha(hq + r)\|}\right),$$

当 $h=0$ 且 $1\le r\le q/2$ 时,

$$\sum_{1\le r\le q/2}\min\left(\frac{N}{r},\frac{1}{\|\alpha r\|}\right)\le\sum_{1\le r\le q/2}\frac{1}{\|\alpha r\|}\ll q\log q,$$

当 $h=0$ 且 $r>q/2$ 时, 显然 $hq+r>(h+1)q/2$ 成立, 当 $h\ge 1$ 时, $hq+r>(h+1)q/2$ 当且仅当 $hq+2r>q$ 显然成立, 故

$$\sum_{0\le h<u/q}\sum_{1\le r\le q}\min\left(\frac{N}{hq+r},\frac{1}{\|\alpha(hq+r)\|}\right)\ll q\log q+\sum_{0\le h<u/q}\sum_{1\le r\le q}\min\left(\frac{2N}{hq+q},\frac{1}{\|\alpha(hq+r)\|}\right),$$

而 $2N/(hq+q)$ 与 r 无关, 因此由前一个引理即得

$$\sum_{1\le r\le q}\min\left(\frac{2N}{hq+q},\frac{1}{\|\alpha(hq+r)\|}\right)\ll\frac{2N}{hq+q}+q\log q,$$

于是

$$\sum_{0\le h<u/q}\sum_{1\le r\le q}\min\left(\frac{2N}{hq+q},\frac{1}{\|\alpha(hq+r)\|}\right)\ll\sum_{0\le h<u/q}\left(\frac{2N}{hq+q}+q\log q\right)\ll\frac{N}{q}\log\left(1+\frac{u}{q}\right)+u\log q,$$

再结合当 $u\ge 2$ 时 $\log(1+u/q)<\log(1+u)\ll\log u$ 得

$$\sum_{1\le k\le u}\min\left(\frac{N}{k},\frac{1}{\|\alpha k\|}\right)\ll q\log q+u\log q+\frac{N}{q}\log u,$$

定理成立. □

接下来使用这些结果来估计劣弧上的指数和

$$F(\alpha)=\sum_{p\le N}e(p\alpha)\log p,$$

这里我们采取的是 Vaughan 的方法. 对于 $u\ge 1$, 下记

$$M_u(k)=\sum_{\substack{d\mid k\\ d\le u}}\mu(d),$$

由于

$$\sum_{d\mid k}\mu(d)=\begin{cases}1, & k=1,\\ 0, & \text{其他},\end{cases}$$

因此当 $k=1$ 时, $M_u(k)=1$, 当 $1<k\le u$ 时, $M_u(k)=0$, 当 $k>u$ 时则比较复杂.

引理 8 (Vaughan 恒等式)**.** 令 $\Phi(m,n)$ 是双变量算术函数, 则对任意 $u\in[1,N)$, 有

$$\sum_{u<\ell\le N}\Phi(1,\ell)=\sum_{d\le u}\sum_{u<\ell\le N/d}\sum_{m\le N/(\ell d)}\mu(d)\Phi(dm,\ell)-\sum_{u<k\le N}\sum_{u<\ell\le N/k}M_u(k)\Phi(k,\ell).$$

证明. 考虑和式

$$\sum_{k=1}^{N}\sum_{u<\ell\le N/k} M_u(k)\Phi(k,\ell),$$

一方面, 由 M_u 的定义得

$$\sum_{k=1}^{N}\sum_{u<\ell\le N/k} M_u(k)\Phi(k,\ell)=\sum_{u<\ell\le N}\Phi(1,\ell)+\sum_{u<k\le N}\sum_{u<\ell\le N/k} M_u(k)\Phi(k,\ell).$$

另一方面, 交换求和顺序并令 $k=dm$ 得

$$\begin{aligned}\sum_{k=1}^{N}\sum_{u<\ell\le N/k} M_u(k)\Phi(k,\ell)&=\sum_{k=1}^{N}\sum_{u<\ell\le N/k}\sum_{\substack{d\mid k\\ d\le u}}\mu(d)\Phi(k,\ell)\\&=\sum_{d\le u}\sum_{\substack{k=1\\ d\mid k}}^{N}\sum_{u<\ell\le N/k}\mu(d)\Phi(k,\ell)\\&=\sum_{d\le u}\sum_{m\le N/d}\sum_{u<\ell\le N/(dm)}\mu(d)\Phi(dm,\ell)\\&=\sum_{d\le u}\sum_{u<\ell\le N/d}\sum_{m\le N/(\ell d)}\mu(d)\Phi(dm,\ell),\end{aligned}$$

两式结合并移项即得定理. □

引理 9. 设

$$\begin{aligned}S_1(\alpha)&=\sum_{d\le u}\sum_{\ell\le N/d}\sum_{m\le N/(\ell d)}\mu(d)\Lambda(\ell)e(\alpha d\ell m),\\S_2(\alpha)&=\sum_{d\le u}\sum_{\ell\le u}\sum_{m\le N/(\ell d)}\mu(d)\Lambda(\ell)e(\alpha d\ell m),\\S_3(\alpha)&=\sum_{u<k\le N}\sum_{u<\ell\le N/k}M_u(k)\Lambda(\ell)e(\alpha k\ell),\end{aligned}$$

则

$$F(\alpha)=S_1(\alpha)-S_2(\alpha)-S_3(\alpha)+O\left(N^{1/2}\right)+O\left(u\right)$$

对任意 $u\in[1,N)$ 成立.

证明. 在 Vaughan 恒等式中取

$$\Phi(k,\ell)=\Lambda(\ell)e(\alpha k\ell),$$

则等式左边为

$$\begin{aligned}\sum_{u<\ell\le N}\Phi(1,\ell)&=\sum_{u<\ell\le N}\Lambda(\ell)e(\alpha\ell)\\&=\sum_{\ell=1}^{N}\Lambda(\ell)e(\alpha\ell)-\sum_{\ell\le u}\Lambda(\ell)e(\alpha\ell)\end{aligned}$$

$$
\begin{aligned}
&= \sum_{p^k \le N} (\log p) e(\alpha p^k) + O(u) \\
&= \sum_{p \le N} (\log p) e(\alpha p) + \sum_{\substack{p^k \le N \\ k \ge 2}} (\log p) e(\alpha p^k) + O(u) \\
&= F(\alpha) + O\left(\sum_{\substack{p^k \le N \\ k \ge 2}} \log p \right) + O(u) \\
&= F(\alpha) + O\left(\sum_{p^2 \le N} \left[\frac{\log N}{\log p} \right] \log p \right) + O(u) \\
&= F(\alpha) + O\left(\pi(N^{1/2}) \log N \right) + O(u) \\
&= F(\alpha) + O\left(N^{1/2} \right) + O(u),
\end{aligned}
$$

其中使用了 Chebyshev 界 $\sum_{\ell \le u} \Lambda(\ell) = O(u)$ 和 $\pi(N^{1/2}) \ll N^{1/2}/\log N$.

Vaughan 恒等式中右边第一项为

$$
\begin{aligned}
&\sum_{d \le u} \sum_{u < \ell \le N/d} \sum_{m \le N/(\ell d)} \mu(d) \Lambda(\ell) e(\alpha d \ell m) \\
=& \sum_{d \le u} \sum_{\ell \le N/d} \sum_{m \le N/(\ell d)} \mu(d) \Lambda(\ell) e(\alpha d \ell m) - \sum_{d \le u} \sum_{\ell \le u} \sum_{m \le N/(\ell d)} \mu(d) \Lambda(\ell) e(\alpha d \ell m) \\
=& S_1(\alpha) - S_2(\alpha).
\end{aligned}
$$

右边第二项为

$$
\sum_{u < k \le N} \sum_{u < \ell \le N/k} M_u(k) \Lambda(\ell) e(\alpha k \ell) = S_3(\alpha),
$$

故

$$
F(\alpha) + O\left(N^{1/2} \right) + O(u) = S_1(\alpha) - S_2(\alpha) - S_3(\alpha),
$$

移项即得引理. □

因此要估计 $F(\alpha)$ 就是要估计 $S_1(\alpha)$, $S_2(\alpha)$ 和 $S_3(\alpha)$.

引理 10. *令 α 是实数, a 和 q 是使得*

$$
\left| \alpha - \frac{a}{q} \right| \le \frac{1}{q^2}
$$

成立的整数, 其中 $(a, q) = 1$, $1 \le q \le N$, 则

$$
S_1(\alpha) \ll \left(\frac{N}{q} + u + q \right) (\log N)^2
$$

对任意 $u \in [1, N)$ 成立.

证明. 令 $r=\ell m$ 得

$$\begin{aligned}S_1(\alpha)&=\sum_{d\le u}\sum_{\ell\le N/d}\sum_{m\le N/(\ell d)}\mu(d)\Lambda(\ell)e(\alpha d\ell m)\\&=\sum_{d\le u}\sum_{\ell m\le N/d}\mu(d)\Lambda(\ell)e(\alpha d\ell m)\\&=\sum_{d\le u}\sum_{r\le N/d}\mu(d)e(\alpha dr)\sum_{\ell\mid r}\Lambda(\ell)\\&=\sum_{d\le u}\mu(d)\sum_{r\le N/d}e(\alpha dr)\log r\\&\ll\sum_{d\le u}\left|\sum_{r\le N/d}e(\alpha dr)\log r\right|,\end{aligned}$$

设部分和

$$A(t)=\sum_{r\le t}e(\alpha dr),$$

则由 Abel 求和公式得

$$\left|\sum_{r\le N/d}e(\alpha dr)\log r\right|\le\left|A\left(\frac{N}{d}\right)\log\frac{N}{d}\right|+\int_1^{N/d}\left|A(t)t^{-1}\right|\,\mathrm{d}t\ll\log N\sup_{1\le t\le N/d}|A(t)|,$$

又因 $t\le N/d$ 时,

$$A\left(t\right)=\sum_{r\le t}e(\alpha dr)\ll\min\left\{t,\frac{1}{\|\alpha d\|}\right\}\le\min\left\{\frac{N}{d},\frac{1}{\|\alpha d\|}\right\},$$

故

$$\begin{aligned}S_1(\alpha)&\ll\log N\sum_{d\le u}\min\left\{\frac{N}{d},\frac{1}{\|\alpha d\|}\right\}\\&\ll\left(q\log q+u\log q+\frac{N}{q}\log u\right)\log N\\&\ll\left(\frac{N}{q}+u+q\right)(\log N)^2,\end{aligned}$$

引理成立. □

引理 11. 令 α 是实数, a 和 q 是使得

$$\left|\alpha-\frac{a}{q}\right|\le\frac{1}{q^2}$$

成立的整数, 其中 $(a,q)=1$, $1\le q\le N$, 则

$$S_2(\alpha)\ll\left(\frac{N}{q}+u^2+q\right)(\log N)^2$$

对任意 $u\in[1,N)$ 成立.

证明. 令 $k=d\ell$, 则

$$\begin{aligned}S_2(\alpha)&=\sum_{d\le u}\sum_{\ell\le u}\sum_{m\le N/(d\ell)}\mu(d)\Lambda(\ell)e(\alpha d\ell m)\\&=\sum_{k\le u^2}\left(\left(\sum_{m\le N/k}e(\alpha km)\right)\left(\sum_{\substack{d\ell=k\\ d\le u,\,\ell\le u}}\mu(d)\Lambda(\ell)\right)\right),\end{aligned}$$

而

$$\sum_{\substack{d\ell=k\\ d\le u,\,\ell\le u}}\mu(d)\Lambda(\ell)\ll\sum_{\substack{d\ell=k\\ d\le u,\,\ell\le u}}\Lambda(\ell)\le\sum_{\ell\mid k}\Lambda(\ell)=\log k\ll\log u\le\log N,$$

故

$$\begin{aligned}S_2(\alpha)&\ll\log N\sum_{k\le u^2}\sum_{m\le N/k}e(\alpha km)\\&\ll\log N\sum_{k\le u^2}\min\left\{\frac{N}{k},\frac{1}{\|\alpha k\|}\right\}\\&\ll\left(\frac{N}{q}+u^2+q\right)(\log N)^2,\end{aligned}$$

引理成立. □

引理 12. 令 α 是实数, a 和 q 是使得

$$\left|\alpha-\frac{a}{q}\right|\le\frac{1}{q^2}$$

成立的整数, 其中 $(a,q)=1$, $1\le q\le N$, 则

$$S_3(\alpha)\ll\left(\frac{N}{q^{1/2}}+u^{-1/2}N+N^{1/2}q^{1/2}\right)(\log N)^4$$

对任意 $u\in[1,N)$ 成立.

证明. 在 S_3 中要使得满足 $u<\ell\le N/k$ 的 ℓ 存在, 至少要 $k\le N/u$, 即第一个求和下标可以由 $u<k\le N$ 改为 $u<k\le N/u$, 当 $u\ge\sqrt{N}$ 时, $S_3(\alpha)=0$, 引理显然成立, 以下设 $u<\sqrt{N}$, 令

$$h=\left[\frac{\log(N/u^2)}{\log 2}\right]+1,$$

而 $2^hu\ge2^{\log_2(N/u^2)}u=N/u\ge k$ 且 h 是满足该式的最小正整数, 即 $2^{h-1}u<N/u\le2^hu$, 所以

$$\begin{aligned}S_3(\alpha)&=\sum_{u<k\le N/u}\sum_{u<\ell\le N/k}M_u(k)\Lambda(\ell)e(\alpha k\ell)\\&=\sum_{i=1}^{h}\sum_{2^{i-1}u<k\le2^iu}M_u(k)\sum_{u<\ell\le N/k}\Lambda(\ell)e(\alpha k\ell)\\&=\sum_{i=1}^{h}S_{3,i}(\alpha)\end{aligned}$$

$$\leq h \max_{1\leq i\leq h} S_{3,i}(\alpha)$$
$$\ll \log N \max_{1\leq i\leq h} S_{3,i}(\alpha),$$

其中

$$S_{3,i}(\alpha) = \sum_{2^{i-1}u<k\leq 2^i u} M_u(k) \sum_{u<\ell\leq N/k} \Lambda(\ell) e(\alpha k\ell).$$

由 Cauchy-Schwarz 不等式得

$$|S_{3,i}(\alpha)|^2 \leq \left(\sum_{2^{i-1}u<k\leq 2^i u} |M_u(k)|^2\right)\left(\sum_{2^{i-1}u<k\leq 2^i u}\left|\sum_{u<\ell\leq N/k}\Lambda(\ell)e(\alpha k\ell)\right|^2\right),$$

对于第一个和式, 由

$$|M_u(k)| = \left|\sum_{\substack{d|k\\ d\leq u}}\mu(d)\right| \leq \sum_{\substack{d|k\\ d\leq u}} 1 \leq d(k)$$

和估计

$$\sum_{k\leq y} d(k)^2 \ll y(\log y)^3$$

得

$$\sum_{2^{i-1}u<k\leq 2^i u} |M_u(k)|^2 \leq \sum_{2^{i-1}u<k\leq 2^i u} d(k)^2 \ll 2^i u(\log 2^i u)^3 \ll 2^i u(\log N)^3.$$

对于第二个和式,

$$\begin{aligned}\sum_{2^{i-1}u<k\leq 2^i u}\left|\sum_{u<\ell\leq N/k}\Lambda(\ell)e(\alpha k\ell)\right|^2 &= \sum_{2^{i-1}u<k\leq 2^i u}\sum_{u<\ell\leq N/k}\sum_{u<m\leq N/k}\Lambda(\ell)\overline{\Lambda(m)}e(\alpha k(\ell-m))\\ &= \sum_{u<\ell<N/(2^{i-1}u)}\sum_{u<m<N/(2^{i-1}u)}\Lambda(\ell)\Lambda(m)\sum_{2^{i-1}u<k\leq b} e(\alpha k(\ell-m)),\end{aligned}$$

其中

$$b = \min\left\{2^i u, \frac{N}{\ell}, \frac{N}{m}\right\},$$

由 $b - 2^{i-1}u \leq 2^i u - 2^{i-1}u = 2^{i-1}u$ 知

$$\sum_{2^{i-1}u<k\leq b} e(\alpha k(\ell-m)) = e(\alpha 2^{i-1}u(\ell-m)) \sum_{0<k\leq b-2^{i-1}u} e(\alpha k(\ell-m)) \ll \min\left\{2^{i-1}u, \frac{1}{\|\alpha(\ell-m)\|}\right\},$$

故

$$\begin{aligned}\sum_{2^{i-1}u<k\leq 2^i u}\left|\sum_{u<\ell\leq N/k}\Lambda(\ell)e(\alpha k\ell)\right|^2 &\ll \sum_{u<\ell<N/(2^{i-1}u)}\sum_{u<m<N/(2^{i-1}u)}\Lambda(\ell)\Lambda(m)\min\left\{2^{i-1}u, \frac{1}{\|\alpha(\ell-m)\|}\right\}\\ &\ll (\log N)^2 \sum_{u<m<N/(2^{i-1}u)}\sum_{u<\ell<N/(2^{i-1}u)}\min\left\{2^{i-1}u, \frac{1}{\|\alpha(\ell-m)\|}\right\},\end{aligned}$$

设 $j=\ell-m$, 则必有 $|j|<N/(2^{i-1}u)-u<N/(2^{i-1}u)$, 并且每个 j 至多取到 $N/(2^{i-1}u)-u<N/(2^{i-1}u)$ 次, 故

$$\begin{aligned}\sum_{2^{i-1}u<k\le 2^iu}\left|\sum_{u<\ell\le N/k}\Lambda(\ell)e(\alpha k\ell)\right|^2 &\ll \frac{N}{2^{i-1}u}(\log N)^2\left(2^{i-1}u+\sum_{1\le j<N/(2^{i-1}u)}\min\left\{2^{i-1}u,\frac{1}{\|\alpha j\|}\right\}\right)\\ &\ll \frac{N}{2^{i-1}u}(\log N)^2\left(2^{i-1}u+\sum_{1\le j\le N/(2^{i-1}u)}\min\left\{\frac{N}{j},\frac{1}{\|\alpha j\|}\right\}\right)\\ &\ll \frac{N}{2^{i-1}u}(\log N)^2\left(2^{i-1}u+\log N\left(q+\frac{N}{2^{i-1}u}+\frac{N}{q}\right)\right)\\ &\ll \frac{N}{2^{i-1}u}(\log N)^3\left(2^{i-1}u+q+\frac{N}{2^{i-1}u}+\frac{N}{q}\right),\end{aligned}$$

由 $2^{i-1}u\le 2^{h-1}u\le N/u$ 知

$$\sum_{2^{i-1}u<k\le 2^iu}\left|\sum_{u<\ell\le N/k}\Lambda(\ell)e(\alpha k\ell)\right|^2\ll\frac{N}{2^{i-1}u}(\log N)^3\left(q+\frac{N}{u}+\frac{N}{q}\right),$$

因此

$$|S_{3,i}(\alpha)|^2\ll 2^iu(\log N)^3\frac{N}{2^{i-1}u}(\log N)^3\left(q+\frac{N}{u}+\frac{N}{q}\right)\ll N^2(\log N)^6\left(\frac{q}{N}+\frac{1}{u}+\frac{1}{q}\right),$$

故

$$|S_{3,i}(\alpha)|\ll N(\log N)^3\left(\frac{q^{1/2}}{N^{1/2}}+\frac{1}{u^{1/2}}+\frac{1}{q^{1/2}}\right),$$

$$S_3(\alpha)\ll\log N\max_{1\le i\le h}|S_{3,i}(\alpha)|\ll\left(\frac{N}{q^{1/2}}+u^{-1/2}N+N^{1/2}q^{1/2}\right)(\log N)^4,$$

引理得证. □

当 u 较大时, S_1 和 S_2 的上界较大, 而 S_3 的上界较小, 当 u 较小时, 则 S_1 和 S_2 的上界较小, S_3 的上界较大, 我们要选取一个合适的 u, 来获得一个较平衡的上界. 假设 $u=N^\delta$, 则应该有 $u^2=u^{-1/2}N$, 解得 $\delta=2/5$, 即 $u=N^{2/5}$.

定理 7. *令 α 是实数, a 和 q 是使得*

$$\left|\alpha-\frac{a}{q}\right|\le\frac{1}{q^2}$$

成立的整数, 其中 $(a,q)=1$, $1\le q\le N$, 则

$$F(\alpha)\ll\left(\frac{N}{q^{1/2}}+N^{4/5}+N^{1/2}q^{1/2}\right)(\log N)^4.$$

证明. 在以上三个引理中取 $u=N^{2/5}$, 则

$$S_1(\alpha)\ll\left(\frac{N}{q}+N^{2/5}+q\right)(\log N)^2,$$

$$S_2(\alpha) \ll \left(\frac{N}{q} + N^{4/5} + q\right)(\log N)^2,$$

$$S_3(\alpha) \ll \left(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2}q^{1/2}\right)(\log N)^4,$$

代入

$$F(\alpha) = S_1(\alpha) - S_2(\alpha) - S_3(\alpha) + O(N^{1/2}) + O(N^{2/5})$$

即得

$$F(\alpha) \ll \left(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2}q^{1/2}\right)(\log N)^4$$

成立. □

定理 8. 对任意实数 $B > 0$, 有

$$\int_{\mathfrak{m}} F(\alpha)^3 e(-\alpha N)\,\mathrm{d}\alpha \ll \frac{N^2}{(\log N)^{B/2-5}},$$

其中 $\ll$ 常数只依赖于 B.

证明. 设 $\alpha \in \mathfrak{m}$, 由 Dirichlet 逼近定理知, 存在整数 a 和 q, 满足 $(a,q) = 1$, $1 \le q \le N/Q$, 且

$$\left|\alpha - \frac{a}{q}\right| \le \frac{Q}{qN} \le \frac{1}{q^2},$$

若 $q \le Q$, 则 $\alpha \in \mathfrak{M}(q,a)$, 与 $\alpha \in \mathfrak{m}$ 矛盾, 故 $Q < q \le N/Q$. 于是

$$\begin{aligned} F(\alpha) &\ll \left(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2}q^{1/2}\right)(\log N)^4 \\ &\ll \left(\frac{N}{Q^{1/2}} + N^{4/5} + N^{1/2}\frac{N^{1/2}}{Q^{1/2}}\right)(\log N)^4 \\ &\ll \frac{N}{(\log N)^{B/2-4}}, \end{aligned}$$

再由

$$\int_0^1 |F(\alpha)|^2 d\alpha = \sum_{p\le N} (\log p)^2 \le \log N \sum_{p\le N} \log p \ll N \log N$$

得

$$\begin{aligned} \int_{\mathfrak{m}} F(\alpha)^3 e(-\alpha N)\,\mathrm{d}\alpha &\ll \int_{\mathfrak{m}} |F(\alpha)|^3 d\alpha \\ &\ll \sup\{|F(\alpha)| : \alpha \in \mathfrak{m}\} \int_{\mathfrak{m}} |F(\alpha)|^2 d\alpha \\ &\ll \frac{N}{(\log N)^{(B/2)-4}} \int_0^1 |F(\alpha)|^2 d\alpha \\ &\ll \frac{N^2}{(\log N)^{(B/2)-5}}, \end{aligned}$$

定理得证. □

1.2.4 Vinogradov 定理的证明

定理 9. 设 $\mathfrak{S}(N)$ 是奇异级数, 则对足够大的奇数 N 和任意正实数 $A>0$, 有

$$R(N)=\mathfrak{S}(N)\frac{N^2}{2}+O\left(\frac{N^2}{(\log N)^A}\right),$$

其中大 O 常数只依赖于 A.

证明. 已知对任意正实数 $\varepsilon>0$, $B>1$, $C>2B$, 有

$$\begin{aligned}R(N)&=\int_0^1 F(\alpha)^3e(-N\alpha)d\alpha\\&=\int_{\mathfrak{M}}F(\alpha)^3e(-N\alpha)d\alpha+\int_{\mathfrak{m}}F(\alpha)^3e(-N\alpha)d\alpha\\&=\mathfrak{S}(N)\frac{N^2}{2}+O\left(\frac{N^2}{(\log N)^{(1-\varepsilon)B}}\right)+O\left(\frac{N^2}{(\log N)^{C-5B}}\right)+O\left(\frac{N^2}{(\log N)^{B/2-5}}\right),\end{aligned}$$

现对任意正数 $A>0$, 取 $B=2A+10$, $C=A+5B$, $\varepsilon=1/2$, 则 $C-5B=B/2-5=A$, $(1-\varepsilon)B=A+5>A$, 故

$$R(N)=\mathfrak{S}(N)\frac{N^2}{2}+O\left(\frac{N^2}{(\log N)^A}\right),$$

定理得证. □

实际上该定理已足够推出三素数定理, 因为由该渐进公式可知对于足够大的 N 一定有 $R(N)>0$, 只是这个足够大无法实效的计算出来. 但我们仍想直接求出 $r(N)$ 的渐进公式.

Vinogradov 定理的证明. 显然

$$R(N)=\sum_{p_1+p_2+p_3=N}\log p_1\log p_2\log p_3\le(\log N)^3\sum_{p_1+p_2+p_3=N}1=(\log N)^3r(N),$$

即 $(\log N)^3r(N)-R(N)\ge0$. 现取实数 $\delta\in(0,1/2)$, 定义 $r_\delta(N)$ 为将 N 表示为 $p_1+p_2+p_3$ 的形式的方法数, 其中至少有一个 p 满足 $p_i\le N^{1-\delta}$, 即

$$r_\delta(N)=\sum_{\substack{N=p_1+p_2+p_3\\p_1\le N^{1-\delta}\vee p_2\le N^{1-\delta}\vee p_3\le N^{1-\delta}}}1,$$

于是有

$$\begin{aligned}r_\delta(N)&\le\sum_{\substack{N=p_1+p_2+p_3\\p_1\le N^{1-\delta}}}1+\sum_{\substack{N=p_1+p_2+p_3\\p_2\le N^{1-\delta}}}1+\sum_{\substack{N=p_1+p_2+p_3\\p_3\le N^{1-\delta}}}1\\&=3\sum_{\substack{N=p_1+p_2+p_3\\p_1\le N^{1-\delta}}}1\\&\ll\sum_{p_1\le N^{1-\delta}}\sum_{p_2+p_3=N-p_1}1\end{aligned}$$

$$
\begin{aligned}
&\leq \sum_{p_1 \leq N^{1-\delta}} \sum_{p_2 < N} 1 \\
&\leq \pi(N^{1-\delta})\pi(N) \\
&\ll \frac{N^{2-\delta}}{(\log N)^2},
\end{aligned}
$$

也就是说, 存在常数 $C > 0$ 使得

$$
|r_\delta(N)| = r_\delta(N) \leq C\frac{N^{2-\delta}}{(\log N)^2},
$$

所以

$$
\begin{aligned}
R(N) &\geq \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3 > N^{1-\delta}}} \log p_1 \log p_2 \log p_3 \\
&\geq (1-\delta)^3 (\log N)^3 \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3 > N^{1-\delta}}} 1 \\
&\geq (1-\delta)^3 (\log N)^3 \left(r(N) - r_\delta(N)\right) \\
&\geq (1-\delta)^3 (\log N)^3 \left(r(N) - C\frac{N^{2-\delta}}{(\log N)^2}\right) \\
&= (1-\delta)^3 (\log N)^3 r(N) - C(1-\delta)^3 N^{2-\delta} \log N,
\end{aligned}
$$

移项得

$$
(\log N)^3 r(N) \leq (1-\delta)^{-3} R(N) + CN^{2-\delta} \log N,
$$

所以

$$
0 \leq (\log N)^3 r(N) - R(N) \leq \left((1-\delta)^{-3} - 1\right) R(N) + C(\log N) N^{2-\delta}.
$$

由于 $0 < \delta < 1/2$, $1/2 < 1-\delta < 1$, 所以

$$
0 < (1-\delta)^{-3} - 1 = \frac{1-(1-\delta)^3}{(1-\delta)^3} < 8\left(1-(1-\delta)^3\right) = 8(3\delta + \delta^2(\delta-3)) < 24\delta,
$$

再结合

$$
R(N) = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A}\right) \ll N^2
$$

得到

$$
\begin{aligned}
(\log N)^3 r(N) - R(N) &\ll \left((1-\delta)^{-3} - 1\right) R(N) + (\log N) N^{2-\delta} \\
&\ll \delta R(N) + (\log N) N^{2-\delta} \\
&\ll \delta N^2 + (\log N) N^{2-\delta} \\
&= N^2 \left(\delta + \frac{\log N}{N^\delta}\right),
\end{aligned}
$$

现取

$$\delta = \frac{2\log\log N}{\log N},$$

显然当 N 足够大的时候 $0 < \delta < 1/2$, 则

$$\delta + \frac{\log N}{N^\delta} = \frac{2\log\log N}{\log N} + \frac{\log N}{(\log N)^2} \ll \frac{\log\log N}{\log N},$$

于是

$$(\log N)^3 r(N) - R(N) \ll \frac{N^2 \log\log N}{\log N},$$

取 $A = 1$ 即得

$$\begin{aligned}(\log N)^3 r(N) &= R(N) + O\left(\frac{N^2\log\log N}{\log N}\right)\\ &= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A}\right) + O\left(\frac{N^2\log\log N}{\log N}\right)\\ &= \mathfrak{S}(N)\frac{N^2}{2}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right),\end{aligned}$$

即

$$r(N) = \mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right),$$

定理得证. □

1.3 强 Goldbach 猜想中的圆法

虽然目前使用圆法无法推出强 Goldbach 猜想, 但也有一些较好的结果, 即所谓的 “几乎所有偶数都可以表示为两个素数的和”.

定义 1. 对于 $x \in (2, +\infty)$, 定义 $E(x)$ 为 $(2, x]$ 中不能表示为两个素数的和的正偶数个数.

强 Goldbach 猜想显然等价于 $E(x) = 0$, 本节我们证明对足够大的实数 x 和任意正实数 $A > 0$ 有

$$E(x) \ll \frac{x}{(\log x)^A},$$

因为不大于 x 的偶数大约有 $x/2$ 个, 则例外占所有偶数的比例为

$$\frac{2E(x)}{x} \ll \frac{1}{(\log x)^A} \to 0, \quad x \to \infty,$$

所以这个定理描述的就是几乎所有偶数都满足 Goldbach 猜想. 该定理还可以改进到 x^δ 级别, 其中 δ 是一个小于 1 的正常数.

本节中的优弧 $\mathfrak{M}$ 和劣弧 $\mathfrak{m}$ 与之前相同, Q 依然为 $(\log N)^B$. 定义

$$r_2(N) = \sum_{N = p_1 + p_2} 1,$$

$$R_2(N)=\sum_{N=p_1+p_2}\log p_1\log p_2=\int_0^1 F(\alpha)^2e(-N\alpha)\,\mathrm{d}\alpha,$$

$$R_{\mathfrak{M}}(N)=\int_{\mathfrak{M}} F(\alpha)^2e(-N\alpha)\,\mathrm{d}\alpha,$$

$$R_{\mathfrak{m}}(N)=\int_{\mathfrak{m}} F(\alpha)^2e(-N\alpha)\,\mathrm{d}\alpha.$$

定理 10. 对任意正整数 $N>2$, $B>0$ 有

$$\sum_{m=1}^{N}|R_{\mathfrak{m}}(m)|^2\ll\frac{N^3}{(\log N)^{B-9}},$$

其中 $\ll$ 常数只与 B 有关.

证明. 定义

$$G(\alpha)=\begin{cases}F(\alpha)^2, & \alpha\in\mathfrak{m},\\ 0, & \alpha\in\mathfrak{M},\end{cases}$$

则 $G(\alpha)$ 的傅里叶系数即为

$$\int_0^1 G(\alpha)e(-m\alpha)\,\mathrm{d}\alpha=\int_{\mathfrak{m}}F(\alpha)^2e(-m\alpha)\,\mathrm{d}\alpha=R_{\mathfrak{m}}(m),\quad m\in\mathbb{Z},$$

由 Parseval 公式得

$$\begin{aligned}\sum_{m=1}^{N}|R_{\mathfrak{m}}(m)|^2&\le\sum_{m=-\infty}^{\infty}|R_{\mathfrak{m}}(m)|^2\\&=\int_0^1|G(\alpha)|^2\,\mathrm{d}\alpha\\&=\int_{\mathfrak{m}}|F(\alpha)|^4\,\mathrm{d}\alpha\\&\le\sup\{|F(\alpha)|^2:\alpha\in\mathfrak{m}\}\int_0^1|F(\alpha)|^2\,\mathrm{d}\alpha\\&\ll\left(\frac{N}{(\log N)^{(B/2)-4}}\right)^2N\log N\\&=\frac{N^3}{(\log N)^{B-9}},\end{aligned}$$

其中使用到了定理 8 的证明过程. □

引理 13. 设 $Z\ge1$, 则

$$\sum_{\nu>Z}\frac{1}{\varphi(\nu)^2}\ll\frac{1}{Z}.$$

证明. 对 $0\le x\le1$ 有 $(1+x)^2\le1+3x$, 故

$$\frac{n^2}{\varphi(n)^2}=\prod_{p\mid n}\left(1+\frac{1}{p-1}\right)^2\le\prod_{p\mid n}\left(1+\frac{3}{p-1}\right)=\sum_{d\mid n}\frac{\mu^2(d)\,3^{\omega(d)}}{\varphi(d)},$$

其中 $\omega(d)$ 表示 d 的素因子个数, 于是

$$\sum_{n\leq x}\frac{n^2}{\varphi(n)^2}\leq\sum_{d\leq x}\frac{\mu^2(d)\,3^{\omega(d)}}{\varphi(d)}\sum_{\substack{n\leq x\\ d\mid n}}1\leq x\sum_{d\leq x}\frac{\mu^2(d)\,3^{\omega(d)}}{d\varphi(d)}\leq x\prod_p\left(1+\frac{3}{p(p-1)}\right)\ll x,$$

其中 Euler 乘积收敛是因为 $\sum_p 1/p^2$ 收敛, 所以

$$\sum_{\nu>Z}\frac{1}{\varphi(\nu)^2}=\sum_{j=0}^{\infty}\sum_{2^jZ<\nu\leq 2^{j+1}Z}\frac{\nu^2/\varphi(\nu)^2}{\nu^2}\ll\sum_{j=0}^{\infty}\frac{2^{j+1}Z}{(2^jZ)^2}\ll\frac{1}{Z},$$

引理得证. □

引理 14. 级数

$$\mathfrak{S}_2(m)=\sum_{q=1}^{\infty}\frac{\mu(q)^2c_q(m)}{\varphi(q)^2}$$

绝对收敛, 并且部分和

$$\mathfrak{S}_2(m,Q)=\sum_{1\leq q\leq Q}\frac{\mu(q)^2c_q(m)}{\varphi(q)^2}=\mathfrak{S}_2(m)+O(\log 2m),$$

该级数有 *Euler* 乘积

$$\mathfrak{S}_2(m)=\prod_{p\mid m}\left(1+\frac{1}{p-1}\right)\prod_{p\nmid m}\left(1-\frac{1}{(p-1)^2}\right)=\frac{m}{\varphi(m)}\prod_{p\nmid m}\left(1-\frac{1}{(p-1)^2}\right),$$

当 m 是奇数时 $\mathfrak{S}_2(m)=0$, 当 m 是偶数时不等式

$$\mathfrak{S}_2(m)>1$$

恒成立.

证明. $m=1$ 时显然绝对收敛, 以下设 $m\geq 2$. 设 X 和 Y 为正实数, 且 $X<Y$, 由 Ramanujan 和

$$c_q(m)=\frac{\mu\left(q/(m,q)\right)\varphi(q)}{\varphi\left(q/(m,q)\right)},$$

当 $\mu(q)\neq 0$ 时 $(q/(q,m),(q,m))=1$, 并且必有 $\mu\left(q/(m,q)\right)\neq 0$, 则

$$\sum_{X<q\leq Y}\left|\frac{\mu(q)^2c_q(m)}{\varphi(q)^2}\right|=\sum_{X<q\leq Y}\frac{\mu(q)^2}{\varphi(q)^2}|c_q(m)|=\sum_{X<q\leq Y}\frac{\mu(q)^2}{\varphi(q)^2}\varphi((q,m))=\sum_{d\mid m}\varphi(d)\sum_{\substack{X<q\leq Y\\ (m,q)=d}}\frac{\mu^2(q)}{\varphi^2(q)},$$

由于 $(m,q)=d$, 可设 $q=\nu d$, 由于 $\mu(q)\neq 0$, 则必有 $(\nu,d)=1$, 由 μ 和 φ 的乘性可得

$$\sum_{X<q\leq Y}\left|\frac{\mu(q)^2c_q(m)}{\varphi(q)^2}\right|=\sum_{d\mid m}\frac{\mu^2(d)}{\varphi(d)}\sum_{\substack{X/d<v\leq Y/d\\ (v,m)=1}}\frac{\mu^2(v)}{\varphi^2(v)}\leq\sum_{d\mid m}\frac{\mu^2(d)}{\varphi(d)}\sum_{v=1}^{\infty}\frac{1}{\varphi^2(v)}\ll\sum_{d\mid m}\frac{\mu^2(d)}{\varphi(d)},$$

其中用到了级数 $\sum \varphi(\nu)^{-2}$ 收敛, 再由 Mertens 定理得

$$\sum_{d|m} \frac{\mu^2(d)}{\varphi(d)} = \prod_{p|m} \left(1 + \frac{1}{\varphi(p)}\right) = \prod_{p|m} \left(1 + \frac{1}{p-1}\right) = \prod_{p|m} \left(1 - \frac{1}{p}\right)^{-1} \leq \prod_{p \leq m} \left(1 - \frac{1}{p}\right)^{-1} \ll \log 2m,$$

即

$$\sum_{X < q \leq Y} \left| \frac{\mu(q)^2 c_q(m)}{\varphi(q)^2} \right| \ll \log 2m,$$

取 $0 < X < 1$, $Y \to \infty$ 即得 $\mathfrak{S}_2(m)$ 绝对收敛, 取 $X = Q$, $Y \to \infty$ 即得

$$|\mathfrak{S}_2(m, Q) - \mathfrak{S}_2(m)| \ll \log 2m.$$

由于 $\mu(q)^2 c_q(m)/\varphi(q)^2$ 是关于 q 的乘性函数, 与弱 Goldbach 猜想中相同, 有 Euler 乘积

$$\begin{aligned}
\mathfrak{S}_2(m) &= \prod_p \left(1 + \sum_{j=1}^{\infty} \frac{\mu(p^j)^2 c_{p^j}(m)}{\varphi(p^j)^2}\right) \\
&= \prod_p \left(1 + \frac{c_p(m)}{(p-1)^2}\right) \\
&= \prod_{p|m} \left(1 + \frac{1}{p-1}\right) \prod_{p \nmid m} \left(1 - \frac{1}{(p-1)^2}\right) \\
&= \frac{m}{\varphi(m)} \prod_{p \nmid m} \left(1 - \frac{1}{(p-1)^2}\right),
\end{aligned}$$

显然当 m 是奇数时 $\mathfrak{S}_2(m) = 0$, 当 m 是偶数时不等式

$$\mathfrak{S}_2(m) > \frac{m}{\varphi(m)} \prod_{k=2}^{\infty} \left(1 - \frac{1}{k^2}\right) = \frac{m}{2\varphi(m)} \geq 1$$

恒成立. □

引理 15. 设

$$u(\beta) = \sum_{k=1}^{N} e(k\beta),$$

则

$$J_2(m) = \int_{-1/2}^{1/2} u(\beta)^2 e(-m\beta) \, \mathrm{d}\beta = m - 1.$$

证明. 显然该积分计算的是将 m 表示为两个正整数的方法数, 即

$$J_2(m) = \binom{m-1}{1} = m - 1,$$

引理得证. □

$\mathfrak{S}_2$ 和 J_2 分别称为强 Goldbach 猜想的奇异级数和奇异积分.

引理 16. 对任意正整数 $m \le N$, 正实数 B 和 C 满足 $B > 1$, $C > 2B$, 则有

$$R_{\mathfrak{M}}(m) = m\mathfrak{S}_2(m, Q) + O\left(\frac{N}{(\log N)^{B-1}}\right) + O\left(\frac{N}{(\log N)^{C-5B}}\right),$$

其中大 O 常数只与 B 和 C 有关.

证明. 设 $\alpha \in \mathfrak{M}(q, a)$, $\beta = \alpha - a/q$, 由

$$F(\alpha) = \frac{\mu(q)}{\varphi(q)} u(\beta) + O\left(\frac{Q^2 N}{(\log N)^C}\right),$$

得

$$F(\alpha)^2 = \frac{\mu(q)^2}{\varphi(q)^2} u(\beta)^2 + O\left(\frac{Q^2 N^2}{(\log N)^C}\right),$$

所以有

$$\begin{aligned}
&\int_{\mathfrak{M}} \left(F(\alpha)^2 - \frac{\mu(q)^2}{\varphi(q)^2} u\left(\alpha - \frac{a}{q}\right)^2\right) e(-m\alpha)\,\mathrm{d}\alpha \\
&= \sum_{q \le Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \left(F(\alpha)^2 - \frac{\mu(q)^2}{\varphi(q)^2} u\left(\alpha - \frac{a}{q}\right)^2\right) e(-m\alpha)\,\mathrm{d}\alpha \\
&\ll \sum_{q \le Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \frac{Q^2 N^2}{(\log N)^C}\,\mathrm{d}\alpha \\
&\ll \sum_{q \le Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \frac{Q^3 N}{(\log N)^C} \\
&\le \frac{Q^5 N}{(\log N)^C} = \frac{N}{(\log N)^{C-5B}},
\end{aligned}$$

而

$$\begin{aligned}
&\sum_{q \le Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \frac{\mu(q)^2}{\varphi(q)^2} \int_{\mathfrak{M}(q,a)} u\left(\alpha - \frac{a}{q}\right)^2 e(-m\alpha)\,\mathrm{d}\alpha \\
&= \sum_{q \le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{\mu(q)^2}{\varphi(q)^2} \int_{a/q - Q/N}^{a/q + Q/N} u\left(\alpha - \frac{a}{q}\right)^2 e(-m\alpha)\,\mathrm{d}\alpha \\
&= \sum_{q \le Q} \frac{\mu(q)^2}{\varphi(q)^2} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(-ma/q) \int_{-Q/N}^{Q/N} u(\beta)^2 e(-m\beta)\,\mathrm{d}\beta \\
&= \sum_{q \le Q} \frac{\mu(q)^2 c_q(-m)}{\varphi(q)^2} \int_{-Q/N}^{Q/N} u(\beta)^2 e(-m\beta)\,\mathrm{d}\beta \\
&= \mathfrak{S}_2(m, Q) \int_{-Q/N}^{Q/N} u(\beta)^2 e(-m\beta)\,\mathrm{d}\beta,
\end{aligned}$$

当 $Q/N \le |\beta| \le 1/2$ 时, $u(\beta) < 1/(2\|\beta\|) \ll 1/|\beta|$, 因此有

$$\begin{aligned}\int_{Q/N}^{1/2} u(\beta)^2 e(-m\beta)\,\mathrm{d}\beta &\ll \int_{Q/N}^{1/2} |u(\beta)|^2\,\mathrm{d}\beta \\ &\ll \int_{Q/N}^{1/2} \beta^{-2}\,\mathrm{d}\beta \\ &< \frac{N}{Q},\end{aligned}$$

同理

$$\int_{-1/2}^{-Q/N} u(\beta)^2 e(-m\beta)\,\mathrm{d}\beta \ll \frac{N}{Q}.$$

所以有

$$\begin{aligned}\int_{-Q/N}^{Q/N} u(\beta)^2 e(-m\beta)\,\mathrm{d}\beta &= \int_{-1/2}^{1/2} u(\beta)^2 e(-m\beta)\,\mathrm{d}\beta + O\left(\frac{N}{Q}\right) \\ &= m - 1 + O\left(\frac{N}{Q}\right) \\ &= m + O\left(\frac{N}{Q}\right),\end{aligned}$$

综上可得

$$\begin{aligned}R_{\mathfrak{M}}(m) = \int_{\mathfrak{M}} F(\alpha)^2 e(-m\alpha)\,\mathrm{d}\alpha &= \mathfrak{S}_2(m,Q)\int_{-Q/N}^{Q/N} u(\beta)^2 e(-m\beta)\,\mathrm{d}\beta + O\left(\frac{N}{(\log N)^{C-5B}}\right) \\ &= \mathfrak{S}_2(m,Q)\left(m + O\left(\frac{N}{Q}\right)\right) + O\left(\frac{N}{(\log N)^{C-5B}}\right) \\ &= m\mathfrak{S}_2(m,Q) + O\left(\frac{N}{(\log N)^{B-1}}\right) + O\left(\frac{N}{(\log N)^{C-5B}}\right),\end{aligned}$$

其中最后一步使用了 $\mathfrak{S}_2(m,Q) \ll \log 2m \ll \log N$, 引理得证. □

引理 17. *对任意正数 $A > 0$, 有*

$$\sum_{m=1}^{N} |R_2(m) - m\mathfrak{S}_2(m)|^2 \ll \frac{N^3}{(\log N)^A},$$

其中 $\ll$ 常数只与 A 有关.

证明. 先前已经证明

$$\sum_{X<q\le Y}\left|\frac{\mu(q)^2 c_q(m)}{\varphi(q)^2}\right| = \sum_{d|m}\frac{\mu^2(d)}{\varphi(d)}\sum_{\substack{X/d<v\le Y/d\\(v,m)=1}}\frac{\mu^2(v)}{\varphi^2(v)} \le \sum_{d|m}\frac{\mu^2(d)}{\varphi(d)}\sum_{X/d<v}\frac{1}{\varphi^2(v)},$$

而

$$\sum_{\nu>Z}\frac{1}{\varphi(\nu)^2} \ll \frac{1}{Z},$$

所以

$$|\mathfrak{S}_2(m,Q)-\mathfrak{S}_2(m)|\le\sum_{Q<q}\left|\frac{\mu(q)^2c_q(m)}{\varphi(q)^2}\right|\ll\sum_{d|m}\frac{\mu^2(d)d}{\varphi(d)Q},$$

故

$$\begin{aligned}\sum_{m=1}^{N}|\mathfrak{S}_2(m,Q)-\mathfrak{S}_2(m)|^2&\ll\log N\sum_{m=1}^{N}|\mathfrak{S}_2(m,Q)-\mathfrak{S}_2(m)|\\&\ll\log N\sum_{m=1}^{N}\sum_{d|m}\frac{\mu^2(d)d}{\varphi(d)Q}\\&=\log N\sum_{d\le N}\frac{N}{d}\frac{\mu^2(d)d}{\varphi(d)Q}\\&=NQ^{-1}\log N\sum_{d\le N}\frac{\mu^2(d)}{\varphi(d)},\end{aligned}$$

依然使用 Mertens 定理得

$$\sum_{d\le N}\frac{\mu^2(d)}{\varphi(d)}\le\prod_{p\le N}\left(1+\frac{1}{\varphi(p)}\right)=\prod_{p\le N}\left(1-\frac{1}{p}\right)^{-1}\ll\log N,$$

于是

$$\sum_{m=1}^{N}|\mathfrak{S}_2(m,Q)-\mathfrak{S}_2(m)|^2\ll\frac{N}{(\log N)^{B-2}}.$$

由于对任意实数 $(a+b)^2\le2(a^2+b^2)$, 即 $(a+b)^2\ll a^2+b^2$, 取 $B=A+9$, $C=5B+A$, 结合前几个引理即得

$$\begin{aligned}\sum_{m=1}^{N}|R_2(m)-m\mathfrak{S}_2(m)|^2&\ll\sum_{m=1}^{N}\left(|R_{\mathfrak{m}}(m)|^2+|R_{\mathfrak{M}}(m)-m\mathfrak{S}_2(m,Q)|^2+|m\mathfrak{S}_2(m,Q)-m\mathfrak{S}_2(m)|^2\right)\\&\ll\frac{N^3}{(\log N)^A}+\frac{N^3}{(\log N)^A}+\frac{N^3}{(\log N)^{A+7}}\\&\ll\frac{N^3}{(\log N)^A},\end{aligned}$$

引理得证. □

定理 11. *对足够大的实数 x 和任意正实数 $A>0$, 有*

$$E(x)\ll\frac{x}{(\log x)^A},$$

其中 $\ll$ 常数只与 A 有关.

证明. 当 m 被 $E(x)$ 计数时, $R_2(m)=0$, 所以有

$$m^{-2}|R_2(m)-m\mathfrak{S}_2(m)|^2=\mathfrak{S}_2(m)^2\ge1,$$

由 Abel 求和公式即得

$$\begin{aligned}E(x) &= \sum_{\substack{2<m\le x\\ R_2(m)=0}} 1\\ &\le \sum_{\substack{2<m\le x\\ R_2(m)=0}} m^{-2}|R_2(m)-m\mathfrak{S}_2(m)|^2\\ &\le \sum_{2<m\le x} m^{-2}|R_2(m)-m\mathfrak{S}_2(m)|^2\\ &\ll \frac{x}{(\log x)^A},\end{aligned}$$

定理得证. □

此外, 由以上推导可以看出, 假如强 Goldbach 猜想得证, 则将偶数 N 表示为两个素数的方法数的主项应该是

$$\begin{aligned}r_2(N) &\sim \frac{N\mathfrak{S}_2(N)}{(\log N)^2},\\ R_2(N) &\sim N\mathfrak{S}_2(N).\end{aligned}$$

2 筛法

2.1 筛法的想法

筛法源于古希腊数学家 Eratosthenes 的 Eratosthenes 筛法, 但此时筛法只是一个算法, 并不能得到什么好的定理. 现代筛法则由 Brun 发明, 他使用他创造的新方法证明了孪生素数的倒数和收敛, 以及命题 "9+9" 成立.

设 $A\subseteq\mathbb{Z}_{\ge1}$ 是一个有限集, $|A|$ 是其元素个数, 筛法的想法就是, 假设 $P_1,\dots,P_n$ 是 n 个关于正整数的性质, 如果 A 中的元素 a 满足这些性质中的任意一个或多个, 则将 a 从 A 中去掉, 即这些性质 P_i 起到一个筛子的作用, 将剩余的元素组成的集合记为 A^*, 筛法的目标就是得到 $|A^*|$ 的上下界估计. 在实践中这些性质 P_i 通常为一些同余条件.

现设 $A=\{a(n)\}_{n=1}^{\infty}$ 是一个数列, 满足对所有的 n, 都有 $a(n)\ge0$, 并且

$$\sum_{n=1}^{\infty}a(n)<\infty$$

收敛, 记这个级数的值为 $|A|$. 设 $\mathcal{P}$ 是一些素数组成的集合, 可以是有限集也可以是无限集, 称为筛域, 定义

$$P(z)=\prod_{\substack{p\in\mathcal{P}\\ p<z}}p,\quad P(w,z)=\prod_{\substack{p\in\mathcal{P}\\ w\le p<z}}p,$$

显然 $P(z)=P(2,z)$.

定义 2 (筛函数)**.** 符号如上, 筛函数定义为

$$S(A,\mathcal{P},z)=\sum_{(n,P(z))=1}a(n).$$

显然 $S(A,\mathcal{P},2)=|A|$. 筛函数是关于 z 的递减函数.

当 $\{a(n)\}_{n=1}^{\infty}$ 是某个有限集的指示函数

$$a(n)=\begin{cases}1, & n\in A,\\ 0, & n\notin A,\end{cases}$$

时, $|A|$ 就是集合 A 的大小, 此时说这个筛法是不加权的, 否则称为加权筛法, 在不加权时我们不区分作为有限集合的 A 和作为指示函数列的 A. 将之前的那些性质取为 $n\equiv 0 \pmod p$, $p\in\mathcal{P}$, 则显然 $\lim_{z\to\infty}S(A,\mathcal{P},z)=|A^*|$.

定义

$$|A_d|=\sum_{d|n}a(n),$$

由 $|A|$ 收敛知对任意正整数 d, $|A_d|$ 也收敛.

引理 18 (Legendre)**.** 符号如上,

$$S(A,\mathcal{P},z)=\sum_{d|P(z)}\mu(d)|A_d|.$$

证明. 由

$$\sum_{d|n}\mu(d)=\begin{cases}1, & n=1,\\ 0, & n\neq 1,\end{cases}$$

得

$$\begin{aligned}S(A,\mathcal{P},z)&=\sum_{(n,P(z))=1}a(n)\\ &=\sum_{n=1}^{\infty}a(n)\sum_{d|(n,P(z))}\mu(d)\\ &=\sum_{d|P(z)}\mu(d)\sum_{d|n}a(n)\\ &=\sum_{d|P(z)}\mu(d)|A_d|,\end{aligned}$$

引理得证. □

引理 19 (Buchstab 恒等式)**.** 令 $2\le w<z$, 则有

$$S(A,\mathcal{P},z)=|A|-\sum_{\substack{p\in\mathcal{P}\\ p<z}}S(A_p,\mathcal{P},p),$$

$$S(A,\mathcal{P},z)=S(A,\mathcal{P},w)-\sum_{\substack{p\in\mathcal{P}\\ w\le p<z}}S(A_p,\mathcal{P},p),$$

其中 A_d 表示数列 $\{a(nd)\}_{n=1}^{\infty}$.

证明. 将正整数集 $\mathbb{Z}_{\ge1}$ 分类, 定义 Z_1 为 $\mathbb{Z}_{\ge1}$ 的子集, 若存在 $p\in\mathcal{P}$ 且 $p<z$, 使得 $p|n$, 则 $n\in Z_1$, 定义 $Z_0=\mathbb{Z}_{\ge1}-Z_1$, 即不存在 $\mathcal{P}$ 中小于 z 的素数作为素因子的所有正整数组成的集合, 也就是所有满足 $(n,P(z))=1$ 的正整数 n, 那么有

$$\sum_{n\in Z_0}a(n)=S(A,\mathcal{P},z),$$

而对于 Z_1, 将其按属于 $\mathcal{P}$ 的最小素因子分类, 对每个 $\mathcal{P}$ 中小于 z 的素数 p, 定义 Z_p 为 Z_1 中所有被 p 整除并且不被 $\mathcal{P}$ 中任何小于 p 的素数整除的数, 则由定义知

$$\sum_{n\in Z_p}a(n)=S(A_p,\mathcal{P},p),$$

由 Z_1 的定义知它是诸 Z_p 的无交并, 所以

$$|A|=\sum_{n\in\mathbb{Z}_{\ge1}}a(n)=\sum_{n\in Z_0}a(n)+\sum_{\substack{p\in\mathcal{P}\\ p<z}}\sum_{n\in Z_p}a(n)=S(A,\mathcal{P},z)+\sum_{\substack{p\in\mathcal{P}\\ p<z}}S(A_p,\mathcal{P},p),$$

因此

$$S(A,\mathcal{P},z)=|A|-\sum_{\substack{p\in\mathcal{P}\\ p<z}}S(A_p,\mathcal{P},p),$$

在该式中取 $z=w$ 得

$$S(A,\mathcal{P},w)=|A|-\sum_{\substack{p\in\mathcal{P}\\ p<w}}S(A_p,\mathcal{P},p),$$

故

$$S(A,\mathcal{P},z)=S(A,\mathcal{P},w)+\sum_{\substack{p\in\mathcal{P}\\ p<w}}S(A_p,\mathcal{P},p)-\sum_{\substack{p\in\mathcal{P}\\ p<z}}S(A_p,\mathcal{P},p)=S(A,\mathcal{P},w)-\sum_{\substack{p\in\mathcal{P}\\ w\le p<z}}S(A_p,\mathcal{P},p),$$

引理得证. □

例 3 (Legendre–Eratosthenes 筛法)**.** *Legendre* 首先将 *Eratosthenes* 筛法由算法升级为具体的公式. 设实数 $x>9$, $A=\{n:1\le n\le x\}$, $\mathcal{P}$ 为所有素数组成的集合, 则

$$S\left(A,\mathcal{P},[\sqrt{x}]+1\right)=\pi(x)-\pi\left(\sqrt{x}\right)+1,$$

其中最后加的 1 表示未被筛掉的整数 1, 而显然

$$|A_d|=\left[\frac{x}{d}\right],$$

于是由 *Legendre* 公式得

$$\pi(x)-\pi(\sqrt{x})+1=\sum_{d|P([\sqrt{x}]+1)}\mu(d)\left[\frac{x}{d}\right]$$

$$= [x] - \sum_{p_1 \le \sqrt{x}} \left[\frac{x}{p_1}\right] + \sum_{p_2 < p_1 \le \sqrt{x}} \left[\frac{x}{p_1 p_2}\right] - \sum_{p_3 < p_2 < p_1 \le \sqrt{x}} \left[\frac{x}{p_1 p_2 p_3}\right] + \cdots .$$

例 4 (孪生素数猜想)**.** 对实数 $x \ge 3$, 设 $A = \{n(n+2) : 1 \le n \le x\}$, $\mathcal{P}$ 为全体素数组成的集合, 再设 $\pi_2(x)$ 表示不超过 x 的素数 p 中, 满足 $p+2$ 也是素数的个数, 则

$$S(A, \mathcal{P}, \sqrt{x+2}) = \pi_2(x) - \pi_2(\sqrt{x+2}) + O(1).$$

例 5 (强 Goldbach 猜想)**.** 对偶数 $N \ge 2$, 设 $A = \{n(N-n) : 1 \le n < N\}$, $\mathcal{P}$ 为全体素数组成的集合 (计顺序), 再设 $r_2(N)$ 表示将 N 表示为两个素数的和的方法数, 则

$$S(A, \mathcal{P}, \sqrt{N}) - 2 \le r_2(N).$$

2.1.1 筛法的一般框架

由 Legendre 公式可知, 要估计筛函数就必须研究 $|A_d|$. 我们假设 $g_n(d)$ 是一个定义在正整数上的乘性函数, 并且要求 g_n 在任意素数 p 上满足

$$0 \le g_n(p) < 1.$$

显然, 若 d 是 $\mathcal{P}$ 中一些不同的素数的乘积, 则级数

$$\sum_{n=1}^{\infty} a(n) g_n(d)$$

收敛, 我们使用它来近似 $|A_d|$, 并且设余项为

$$r(d) = |A_d| - \sum_{n=1}^{\infty} a(n) g_n(d).$$

所以有

$$\begin{aligned}
S(A, \mathcal{P}, z) &= \sum_{d | P(z)} \mu(d) |A_d| \\
&= \sum_{d | P(z)} \mu(d) \left(\sum_{n=1}^{\infty} a(n) g_n(d) + r(d) \right) \\
&= \sum_{n=1}^{\infty} a(n) \sum_{d | P(z)} \mu(d) g_n(d) + \sum_{d | P(z)} \mu(d) r(d) \\
&= \sum_{n=1}^{\infty} a(n) \prod_{p | P(z)} (1 - g_n(p)) + \sum_{d | P(z)} \mu(d) r(d) \\
&= \sum_{n=1}^{\infty} a(n) V_n(z) + R(z),
\end{aligned}$$

其中

$$V_n(z) = \prod_{p | P(z)} (1 - g_n(p)),$$

$$R(z)=\sum_{d|P(z)}\mu(d)r(d).$$

初看这个方法可能莫名其妙, 为什么要添加一个函数 g_n 来替代 $|A_d|$? 事实上, 函数 g_n 经常是与 n 无关的, 取 A 为有限集合时, 并且想象诸 A_d 在 A 中的分布大致是均匀的, 即 A_d 大致占 A 的比例为 $1/d$, 取 $g_n(d)=1/d$, 则

$$|A_d|=\frac{1}{d}|A|+r(d),$$
$$S(A,\mathcal{P},z)=|A|V(z)+R(z),$$

其中

$$V(z)=\prod_{p|P(z)}\left(1-\frac{1}{p}\right).$$

也就是说, 函数 g_n 表示的其实是某种密度.

例 6 (失败的 Legendre–Eratosthenes 筛法)**.** *将以上方法应用于 Legendre–Eratosthenes 筛法, 则*

$$|r(d)|=\left|\frac{|A|}{d}-|A_d|\right|=\left|\frac{[x]}{d}-\left[\frac{x}{d}\right]\right|=O(1),$$

因此

$$|R(z)|\leq\sum_{d|P(z)}|\mu(d)r(d)|=O\left(\sum_{d|P(z)}1\right)=O\left(2^{\pi(z)}\right),$$

代入筛函数并由 Mertens 定理得到

$$S(A,\mathcal{P},z)=[x]\prod_{p<z}\left(1-\frac{1}{p}\right)+O\left(2^{\pi(z)}\right)=[x]\frac{e^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right)+O\left(2^{\pi(z)}\right),$$

当 z 相对于 x 较大时, 例如 $z=x^{1/2}$, 主项大约为 $x/\log x$ 级别, 而余项达到了 $2^{\sqrt{x}/\log x}$ 级别, 余项比主项更大, Legendre–Eratosthenes 筛法失效.

该例子表明, 只替换 $|A_d|$ 是不够的, 余项经常会大于主项使得筛法失效, 出现这种情况的原因是余项中的项数太多, 总共 $2^{\pi(z)}$ 项. 因此接下来的想法就是, 对 Möbius 函数 μ 进行一定的截断来得到更好的上下界估计.

定义 3 (上下界筛)**.** *设 $\mathcal{P}$ 是一些素数组成的集合, z 是正实数, λ^- 和 λ^+ 是算术函数, 满足 $\lambda^-(1)=\lambda^+(1)=1$, 若当 d 有 $\mathcal{P}$ 外的素因子时就有 $\lambda^-(d)=0$ 和 $\lambda^+(d)=0$, 并且对正整数 $n\mid P(z)$, 都有*

$$\sum_{d|n}\lambda^-(d)\leq\sum_{d|n}\mu(d)=\left[\frac{1}{n}\right]\leq\sum_{d|n}\lambda^+(d),$$

则称 λ^- 为下界筛, λ^+ 为上界筛, $\mathcal{P}$ 为 λ^- 和 λ^+ 的筛域.

若存在正数 D, 当 $d\geq D$ 时有 $\lambda^-(d)=0$ 和 $\lambda^+(d)=0$, 则称 D 为 λ^- 和 λ^+ 的支撑级.

引理 20. 设 λ^- 和 λ^+ 是以 D 为支撑级, $\mathcal{P}$ 为筛域的上下界筛, 则

$$\sum_{n=1}^{\infty} a(n)G_n(z,\lambda^-) + R^- \le S(A,\mathcal{P},z) \le \sum_{n=1}^{\infty} a(n)G_n(z,\lambda^+) + R^+,$$

其中

$$G_n(z,\lambda^-) = \sum_{d|P(z)} \lambda^-(d)g_n(d), \quad G_n(z,\lambda^+) = \sum_{d|P(z)} \lambda^+(d)g_n(d),$$

$$R^- = \sum_{\substack{d|P(z)\\ d<D}} \lambda^-(d)r(d), \quad R^+ = \sum_{\substack{d|P(z)\\ d<D}} \lambda^+(d)r(d).$$

证明. 由于 λ^- 和 λ^+ 只在有限个数处非零, 故级数

$$\sum_{n=1}^{\infty} a(n) \sum_{d|(n,P(z))} \lambda^-(d), \quad \sum_{n=1}^{\infty} a(n) \sum_{d|(n,P(z))} \lambda^+(d)$$

收敛, 故

$$\sum_{n=1}^{\infty} a(n) \sum_{d|(n,P(z))} \lambda^-(d) \le S(A,\mathcal{P},z) \le \sum_{n=1}^{\infty} a(n) \sum_{d|(n,P(z))} \lambda^+(d),$$

与之前类似, 容易证明

$$\sum_{n=1}^{\infty} a(n) \sum_{d|(n,P(z))} \lambda^+(d) = \sum_{n=1}^{\infty} a(n)G_n(z,\lambda^+) + R^+,$$

$$\sum_{n=1}^{\infty} a(n) \sum_{d|(n,P(z))} \lambda^-(d) = \sum_{n=1}^{\infty} a(n)G_n(z,\lambda^-) + R^-,$$

引理得证. □

引理 21. 符号如上, 设 $p_{\min}(d)$ 表示 d 的最小素因子, λ 是满足 $\lambda(1)=1$ 的算术函数, 则

$$\sum_{n=1}^{\infty} a(n) \sum_{d|(n,P(z))} \lambda(d) = S(A,\mathcal{P},z) + \sum_{\substack{d|P(z)\\ d>1}} \left(\lambda\left(\frac{d}{p_{\min}(d)}\right) + \lambda(d)\right) S(A_d,\mathcal{P},p_{\min}(d)).$$

证明. 由 Buchstab 恒等式知

$$|A_d| = S(A_d,\mathcal{P},p_{\min}(d)) + \sum_{q|P(p_{\min}(d))} S((A_d)_q,\mathcal{P},q),$$

其中 q 是素数, 令 $f=dq$, 当 $q \mid P(p_{\min}(d))$ 时 $p_f = q$, 再由 Buchstab 恒等式得,

$$\begin{aligned}\sum_{d|P(z)} \lambda(d)|A_d| &= |A| + \sum_{\substack{d|P(z)\\ d>1}} \lambda(d) \left(S(A_d,\mathcal{P},p_{\min}(d)) + \sum_{q|P(p_{\min}(d))} S((A_d)_q,\mathcal{P},q)\right)\\ &= S(A,\mathcal{P},z) + \sum_{p|P(z)} S(A_p,\mathcal{P},p) + \sum_{\substack{d|P(z)\\ d>1}} \lambda(d)S(A_d,\mathcal{P},p_{\min}(d))\end{aligned}$$

$$+\sum_{\substack{f|P(z)\\ \omega(f)>1}}\lambda\left(\frac{f}{p_f}\right)S(A_f,\mathcal{P},p_f),$$

而

$$\sum_{\substack{f|P(z)\\ \omega(f)>1}}\lambda\left(\frac{f}{p_f}\right)S(A_f,\mathcal{P},p_f)=\sum_{\substack{f|P(z)\\ f>1}}\lambda\left(\frac{f}{p_f}\right)S(A_f,\mathcal{P},p_f)-\sum_{p|P(z)}\lambda(1)\,S(A_p,\mathcal{P},p),$$

所以

$$\sum_{d|P(z)}\lambda(d)|A_d|=S(A,\mathcal{P},z)+\sum_{\substack{d|P(z)\\ d>1}}\lambda(d)S(A_d,\mathcal{P},p_{\min}(d))+\sum_{\substack{f|P(z)\\ f>1}}\lambda\left(\frac{f}{p_f}\right)S(A_f,\mathcal{P},p_f),$$

即

$$\sum_{n=1}^{\infty}a(n)\sum_{d|(n,P(z))}\lambda(d)=\sum_{d|P(z)}\lambda(d)|A_d|=S(A,\mathcal{P},z)+\sum_{\substack{d|P(z)\\ d>1}}\left(\lambda\left(\frac{d}{p_{\min}(d)}\right)+\lambda(d)\right)S(A_d,\mathcal{P},p_{\min}(d)),$$

引理成立. □

该引理说明要构造上下界筛, 就是要找到一对函数 $\lambda^{\pm}$ 满足 $\lambda^{\pm}(1)=1$, $\lambda^{-}(d/p_{\min}(d))+\lambda^{-}(d)\le 0$, $\lambda^{+}(d/p_{\min}(d))+\lambda^{+}(d)\ge 0$.

以下引理将用于后文对 Jurkat-Richert 定理的证明.

引理 22. *设 $\lambda_1^{\pm}$ 是筛域为 $\mathcal{P}_1$, 支撑级为 D 的上下界筛, 并且对所有 $d\ge 1$ 均有 $|\lambda_1^{\pm}(d)|\le 1$, 设 $\mathcal{Q}$ 为与 $\mathcal{P}_1$ 不相交的有限素数集, $\mathcal{P}=\mathcal{P}_1\sqcup\mathcal{Q}$, Q 为 $\mathcal{Q}$ 中所有素数的积, 设*

$$G_n(z,\lambda_1^{\pm})=\sum_{d|P_1(z)}\lambda_1^{\pm}(d)g_n(d),$$

则

$$S(A,\mathcal{P},z)\le\sum_{n=1}^{\infty}a(n)G_n(z,\lambda_1^{+})\prod_{q|Q(z)}(1-g_n(q))+R(DQ,\mathcal{P},z),$$

$$S(A,\mathcal{P},z)\ge\sum_{n=1}^{\infty}a(n)G_n(z,\lambda_1^{-})\prod_{q|Q(z)}(1-g_n(q))-R(DQ,\mathcal{P},z),$$

其中

$$R(DQ,\mathcal{P},z)=\sum_{\substack{d|P(z)\\ d<DQ}}|r(d)|.$$

证明. 对任意一个正整数 d, 一定可以写成 $d=d_1d_2$ 的形式, 其中 d_1 与 $\mathcal{Q}$ 中任一素数均互素, 而 d_2 是 $\mathcal{Q}$ 中素数的积, 定义

$$\lambda^{\pm}(d)=\lambda_1^{\pm}(d_1)\mu(d_2),$$

显然 $\lambda^{\pm}(1)=1$. 现设 m 是大于 1 正整数, 将其表示为 $m=m_1m_2$ 的形式, 其中 m_1 与 $\mathcal{Q}$ 中任一素数均互素, 而 m_2 是 $\mathcal{Q}$ 中素数的积, 则有

$$\sum_{d|m}\lambda^{+}(d)=\sum_{d_1|m_1}\sum_{d_2|m_2}\lambda^{+}(d_1d_2)=\sum_{d_1|m_1}\lambda_1^{+}(d_1)\sum_{d_2|m_2}\mu(d_2)\geq 0,$$

又因 $m>1$, 则 $m_1>1$ 和 $m_2>1$ 至少成立一个, 前者成立时有

$$\sum_{d_1|m_1}\lambda_1^{-}(d_1)\leq 0,$$

后者成立时有

$$\sum_{d_2|m_2}\mu(d_2)=0,$$

因此总有

$$\sum_{d|m}\lambda^{-}(d)=\sum_{d_1|m_1}\sum_{d_2|m_2}\lambda^{-}(d_1d_2)=\sum_{d_1|m_1}\lambda_1^{-}(d_1)\sum_{d_2|m_2}\mu(d_2)\leq 0,$$

因此 $\lambda^{\pm}$ 是上下界筛. 此外, 由 $\lambda^{\pm}$ 的定义立刻得知它们的筛域为 $\mathcal{P}=\mathcal{P}_1\sqcup\mathcal{Q}$, 支撑级为 DQ. 又由于 $P(z)=P_1(z)Q(z)$, 则有

$$\begin{aligned}
G_n(z,\lambda^{\pm})&=\sum_{d|P(z)}\lambda^{\pm}(d)g_n(d)\\
&=\sum_{d_1|P_1(z)}\sum_{d_2|Q(z)}\lambda^{\pm}(d_1d_2)g_n(d_1d_2)\\
&=\sum_{d_1|P_1(z)}\sum_{d_2|Q(z)}\lambda_1^{\pm}(d_1)g_n(d_1)\mu(d_2)g_n(d_2)\\
&=\sum_{d_1|P_1(z)}\lambda_1^{\pm}(d_1)g_n(d_1)\sum_{d_2|Q(z)}\mu(d_2)g_n(d_2)\\
&=G_n(z,\lambda_1^{\pm})\prod_{q|Q(z)}(1-g_n(q)).
\end{aligned}$$

故

$$S(A,\mathcal{P},z)\leq\sum_{n=1}^{\infty}a(n)G_n(z,\lambda_1^{+})\prod_{q|Q(z)}(1-g_n(q))+R(DQ,\mathcal{P},z),$$

$$S(A,\mathcal{P},z)\geq\sum_{n=1}^{\infty}a(n)G_n(z,\lambda_1^{-})\prod_{q|Q(z)}(1-g_n(q))-R(DQ,\mathcal{P},z)$$

成立. □

最后叙述筛法的维数.

定义 4. 若前述的函数 $g_n(d)$ 满足

$$\prod_{\substack{p\in\mathcal{P}\\ u\leq p<z}}(1-g_n(p))^{-1}\leq K\left(\frac{\log z}{\log u}\right)^{\kappa},$$

对任意正整数 n 和任意实数 $u \in (1, z)$ 都成立, 其中 $K > 1$ 和 $\kappa > 0$ 是与 n 无关的常数, 则称该筛法的维数为 κ, 当 $\kappa = 1$ 该不等式成立时则称为线性筛法.

一般来说, 维数未必是唯一的, 假设一个筛法有维数 κ, 则它也有任何大于 κ 的维数. 光从定义来看, 很难看出为什么 κ 叫维数这个名字, 接下来说明原因.

设 $\rho(p)$ 表示 $\mathcal{P}$ 中素数 p 筛掉的同余类个数, 例如在筛 $A = \{n : 1 \leq n \leq x\}$ 时每个素数只筛掉一个同余类 $0 \pmod p$, 故 $\rho(p) = 1$. 在筛 $A = \{n(n+2) : 1 \leq n \leq x\}$ 时每次筛掉两个同余类 $0 \pmod p$ 和 $p - 2 \pmod p$, 故当 p 为奇素数时 $\rho(p) = 2$, $\rho(2) = 1$. 现取 $g_n(p) = \rho(p)/p$, 并按乘性延拓到全体正整数上, 显然 $|A_p|$ 占 $|A|$ 的比例大约就是 $\rho(p)/p$. 由 Mertens 定理知

$$\sum_{p \leq z} \frac{1}{p} \approx \log\log z,$$

故 $\rho(p)$ 在加 $1/p$ 权后的加权均值就是

$$\sum_{p \leq z} \frac{\rho(p)}{p \log\log z},$$

而

$$\log \prod_{\substack{p \in \mathcal{P} \\ p < z}} \left(1 - \frac{\rho(p)}{p}\right)^{-1} \approx \sum_{p < z} \frac{\rho(p)}{p} \approx \kappa \log\log z,$$

因此该加权均值大约就是 κ, 即 κ 表示的就是被每一个素数筛掉的数的数量的加权均值. Legendre–Eratosthenes 筛法的维数为 1, 先前叙述的孪生素数猜想和强 Goldbach 猜想中的筛法的维数为 2, 之后我们将使用另一种 1 维筛法来研究强 Goldbach 猜想.

2.2 Brun 筛法

2.2.1 Brun 筛法的构造

本节我们叙述的是最简单版本的 Brun 筛法, 也称为 Brun 纯筛法, 因为 Brun 纯筛法本身实际上是纯组合的, 我们先使用组合语言叙述, 再使用筛法框架来严格化它.

约定当 $k > n$ 时 $\binom{n}{k} = 0$.

引理 23. 设 ℓ 和 m 是整数, 且满足 $\ell \geq 1$, $0 \leq m \leq \ell$, 则有组合恒等式

$$\sum_{k=0}^{m} (-1)^k \binom{\ell}{k} = (-1)^m \binom{\ell - 1}{m}.$$

证明. 当 $m = 0$ 时显然成立, 现设 $1 \leq m \leq \ell$, 且该恒等式对 $m - 1$ 成立, 则

$$\begin{aligned}
\sum_{k=0}^{m} (-1)^k \binom{\ell}{k} &= \sum_{k=0}^{m-1} (-1)^k \binom{\ell}{k} + (-1)^m \binom{\ell}{m} \\
&= (-1)^{m-1} \binom{\ell - 1}{m - 1} + (-1)^m \binom{\ell}{m} \\
&= (-1)^m \binom{\ell - 1}{m},
\end{aligned}$$

由归纳法知引理成立. □

定理 12. 设 X 是一个非空有限集, 记 $|X|=N$, 再设 $P_1,\dots,P_r$ 是关于 X 中元素的 r 个性质, 用 N_0 表示 X 中不满足任何一条性质的元素个数, 设 $I=\{i_1,\dots,i_k\}\subseteq\{1,\dots,r\}$, 用 $N(I)$ 表示 X 中同时满足性质 $P_{i_1},\dots,P_{i_k}$ 的元素个数, 并约定 $N(\emptyset)=|X|=N$, 则当 m 是非负偶数时, 有

$$N_0\le\sum_{k=0}^{m}(-1)^k\sum_{|I|=k}N(I),$$

当 m 是非负奇数时, 有

$$N_0\ge\sum_{k=0}^{m}(-1)^k\sum_{|I|=k}N(I).$$

证明. 我们考察 X 中每个元素对不等式两边的贡献, 设 $x\in X$ 满足恰好 ℓ 个性质, 当 $\ell=0$ 时, x 对左边的 N_0 贡献 1, 对右边的 $N(\emptyset)$ 贡献 1. 当 $\ell\ge1$ 时, x 对左边无贡献, 对于右边, 设 $|I|=k$, 显然只有 $k\le\ell$ 时才有贡献, 对于 $k=0,1,\dots,\ell$, 这样的 I 只有 $\binom{\ell}{k}$ 个, 因此, 若 $\ell\le m$, x 对右边的贡献为

$$\sum_{k=0}^{\ell}(-1)^k\binom{\ell}{k}=0,$$

若 $\ell>m$, 则 x 对右边贡献为

$$\sum_{k=0}^{m}(-1)^k\binom{\ell}{k}=(-1)^m\binom{\ell-1}{m},$$

若 m 为偶数, 则贡献 ≥0, 若 m 为奇数, 则贡献为 ≤0. 因此, 将所有 $x\in X$ 的贡献加起来, 当 m 是非负偶数时, 右边总贡献为 N_0 加一个 ≥0 的数, 因此

$$N_0\le\sum_{k=0}^{m}(-1)^k\sum_{|I|=k}N(I),$$

当 m 是非负奇数时, 右边总贡献为 N_0 加一个 ≤0 的数, 因此

$$N_0\ge\sum_{k=0}^{m}(-1)^k\sum_{|I|=k}N(I),$$

定理得证. □

现取集合 X 为正整数集的子集 A, 设 $\mathcal{P}$ 是一个素数集, $z\ge1$ 是正实数, 设 $\mathcal{P}$ 中小于 z 的素数分别为 $p_{i_1},\dots,p_{i_r}$, 取性质 P_k 为模素数 p_{i_k} 同余于 0, 则

$$N_0=S(A,\mathcal{P},z).$$

设 $d|P(z)$, 选定非负奇数 m_-, 定义

$$\lambda^-(d)=\begin{cases}\mu(d), & \omega(d)\le m_-,\\ 0, & \omega(d)>m_-,\end{cases}$$

选定非负偶数 m_+, 定义

$$\lambda^+(d) = \begin{cases} \mu(d), & \omega(d) \le m_+, \\ 0, & \omega(d) > m_+, \end{cases}$$

其中 $\omega(d)$ 表示 d 的素因子个数, 则,

$$\sum_{a\in A}\sum_{d|(a,P(z))}\lambda^-(d) = \sum_{k=0}^{m_-}(-1)^k\sum_{|I|=k}N(I) \le N_0 = S(A,\mathcal{P},z),$$

$$S(A,\mathcal{P},z) = N_0 \le \sum_{k=0}^{m_+}(-1)^k\sum_{|I|=k}N(I) = \sum_{a\in A}\sum_{d|(a,P(z))}\lambda^+(d),$$

因此这样我们就得到了上下界筛.

2.2.2 孪生素数倒数和

接下来我们使用 Brun 纯筛法来得到孪生素数计数函数 π_2 的上界估计, 从而证明孪生素数倒数和收敛.

设 x 和 y 是两个满足 $5 \le y < x$ 的实数, $A = \{n(n+2) : 1 \le n \le x\}$, $\mathcal{P}$ 为所有奇素数组成的集合, 对 $p \in \mathcal{P}$, 定义 $g(p) = 2/p$, 则对任意 $d \mid P(y)$, 有

$$|A_d| = \frac{2^{\omega(d)}x}{d} + r(d),$$

其中 $A_d = \{a \in A : d \mid a\}$, 所以有

$$S(A,\mathcal{P},y) \le |A|G(y,\lambda^+) + \sum_{\substack{d|P(y)\\ \omega(d)\le m_+}}\lambda^+(d)r(d),$$

其中

$$G(y,\lambda^+) = \sum_{d|P(y)}\frac{\lambda^+(d)2^{\omega(d)}}{d},$$

显然

$$\pi_2(x) \le y + S(A,\mathcal{P},y).$$

注意这里我们所取的 $\mathcal{P}$ 只有奇素数, 而且不要求 $y > \sqrt{x+2}$, 所以 $S(A,\mathcal{P},y)$ 中可能包含一些不对应孪生素数的 $n(n+2)$, 这样做的坏处是得到的上界更松, 但好处是分析起来更方便, 不需要单独处理 $p = 2$ 的情形, 并且得到的结果也足够我们使用.

引理 24. *符号如上, 对任意 $d \mid P(y)$, 有*

$$|r(d)| < 2^{\omega(d)}.$$

证明. 首先注意到, 对任何实数 $x \ge 1$, 任何正整数 k 和非负整数 $j < k$, 不超过 x 的所有整数中满足模 k 同余于 j 的数量有

$$\frac{x}{k} + \theta$$

个, 其中 $|\theta|<1$. 不妨设 d 的 $\omega(d)$ 个素因子为 $p_{i_1},\dots,p_{i_{\omega(d)}}$, 若 $a=n(n+2)\in A_d$, 则 n 必满足一个同余方程组

$$\begin{cases} n\equiv u_1 & (\mathrm{mod}\ p_{i_1}),\\ n\equiv u_2 & (\mathrm{mod}\ p_{i_2}),\\ \quad\vdots & \\ n\equiv u_{\omega(d)} & (\mathrm{mod}\ p_{i_{\omega(d)}}), \end{cases}$$

其中 $u_1,\dots,u_{\omega(d)}\in\{0,-2\}$, 总共 $\omega(d)$ 个式子, 由中国剩余定理知必存在非负整数 $j<d$ 使得

$$n\equiv j\pmod d,$$

该同余类中有 $x/d+\theta(j)$ 个数, 其中 $|\theta(j)|<1$, 而由于每个 u_i 有两种选择, 则这样的同余方程组共有 $2^{\omega(d)}$ 种, 因此

$$|A_d|=\sum\frac{x}{d}+\sum\theta(j)=\frac{x2^{\omega(d)}}{d}+\sum\theta(j),$$

其中求和符号对所有可能的同余方程组求和, 即有

$$|r(d)|=\left|\sum\theta(j)\right|\le\sum|\theta(j)|<2^{\omega(d)},$$

引理得证. □

定理 13. 设 $x\ge3$, 则

$$\pi_2(x)\ll\frac{x(\log\log x)^2}{(\log x)^2}.$$

证明. 不妨设 x 和 y 是两个满足 $5\le y<x$ 的实数, 设 $\mathcal{P}$ 中小于 y 的素数有 r 个, 分别为 $p_{i_1},\dots,p_{i_r}$, 设 m_+ 是小于等于 r 的正偶数, 则

$$\pi_2(x)\le y+|A|G(y,\lambda^+)+\sum_{\substack{d|P(y)\\ \omega(d)\le m_+}}\lambda^+(d)r(d).$$

首先估计 $|A|G(y,\lambda^+)$,

$$\begin{aligned}|A|G(y,\lambda^+)&\le x\sum_{d|P(y)}\frac{\lambda^+(d)2^{\omega(d)}}{d}\\ &=x\sum_{k=0}^{m_+}\sum_{\omega(d)=k}\frac{(-1)^k2^k}{d}\\ &=x\sum_{k=0}^{r}\sum_{\omega(d)=k}\frac{(-2)^k}{d}-x\sum_{k=m_++1}^{r}\sum_{\omega(d)=k}\frac{(-2)^k}{d},\end{aligned}$$

由 Mertens 定理知

$$x\sum_{k=0}^{r}\sum_{\omega(d)=k}\frac{(-2)^k}{d}=x\prod_{2<p<y}\left(1-\frac{2}{p}\right)\le x\prod_{2<p<y}\left(1-\frac{1}{p}\right)^2\ll\frac{x}{(\log y)^2}.$$

设 $\sigma_k(x_1,\dots,x_r)$ 表示 r 个变量的 k 次基本对称多项式, 则

$$\begin{aligned}\sigma_1(x_1,\dots,x_r)^k &= (x_1+\cdots+x_r)^k\\ &= \sum_{k_1+\cdots+k_r=k}\frac{k!}{k_1!k_2!\cdots k_r!}x_1^{k_1}x_2^{k_2}\cdots x_r^{k_r}\\ &\geq k!\sum_{\{i_1,\dots,i_k\}\subseteq\{1,\dots,r\}}x_{i_1}\cdots x_{i_k}\\ &= k!\cdot\sigma_k(x_1,\dots,x_r),\end{aligned}$$

所以

$$\sigma_k(x_1,\dots,x_r)\leq\frac{(\sigma_1(x_1,\dots,x_r))^k}{k!}<\left(\frac{e}{k}\right)^k\sigma_1(x_1,\dots,x_r)^k,$$

其中最后一个不等号是因为 $e^k>k^k/k!$, 所以有

$$\begin{aligned}\left|x\sum_{k=m_++1}^{r}\sum_{\omega(d)=k}\frac{(-2)^k}{d}\right| &\leq x\sum_{k=m_++1}^{r}\sum_{\{j_1,\dots,j_k\}\subseteq\{1,\dots,r\}}\frac{2^k}{p_{i_{j_1}}\cdots p_{i_{j_k}}}\\ &= x\sum_{k=m_++1}^{r}\sum_{\{j_1,\dots,j_k\}\subseteq\{1,\dots,r\}}\left(\frac{2}{p_{i_{j_1}}}\right)\cdots\left(\frac{2}{p_{i_{j_k}}}\right)\\ &= x\sum_{k=m_++1}^{r}\sigma_k\left(\frac{2}{p_{i_1}},\dots,\frac{2}{p_{i_r}}\right)\\ &< x\sum_{k=m_++1}^{r}\left(\frac{e}{k}\right)^k\sigma_1\left(\frac{2}{p_{i_1}},\dots,\frac{2}{p_{i_r}}\right)^k\\ &= x\sum_{k=m_++1}^{r}\left(\frac{e}{k}\right)^k\left(\frac{2}{p_{i_1}}+\cdots+\frac{2}{p_{i_r}}\right)^k\\ &< x\sum_{k=m_++1}^{r}\left(\frac{2e}{m_+}\right)^k\left(\sum_{p<y}\frac{1}{p}\right)^k\\ &< x\sum_{k=m_++1}^{r}\left(\frac{C\log\log y}{m_+}\right)^k,\end{aligned}$$

其中 C 是一个与 y 无关的绝对常数, 我们取偶数 m_+ 满足 $2C\log\log y<m_+<r$, 当 y 足够大时这总是能做到的, 所以有

$$\left|x\sum_{k=m_++1}^{r}\sum_{\omega(d)=k}\frac{(-2)^k}{d}\right|<x\sum_{k=m_++1}^{r}\left(\frac{C\log\log y}{m_+}\right)^k<x\sum_{k=m_++1}^{r}\frac{1}{2^k}<\frac{x}{2^{m_+}}.$$

接下来估计余项, 由 $|r(d)|<2^{\omega(d)}$ 知

$$\left|\sum_{\substack{d|P(y)\\ \omega(d)\leq m_+}}\lambda^+(d)r(d)\right|<\sum_{\substack{d|P(y)\\ \omega(d)\leq m_+}}|\lambda^+(d)|2^{\omega(d)}$$

$$
\begin{aligned}
&= \sum_{k=0}^{m_+} \sum_{\omega(d)=k} 2^k, \\
&\le \sum_{k=0}^{m_+} \binom{r}{k} 2^k \\
&< \sum_{k=0}^{m_+} (2r)^k \\
&\ll (2r)^{m_+} \\
&\le y^{m_+},
\end{aligned}
$$

最后一个不等式是因为小于 y 的奇素数个数 r 显然满足 $2r \le y$. 综上, 有

$$\pi_2(x) \ll y + \frac{x}{(\log y)^2} + \frac{x}{2^{m_+}} + y^{m_+} \ll \frac{x}{(\log y)^2} + \frac{x}{2^{m_+}} + y^{m_+}.$$

设 $C' = \max\{2C, 1/\log 2\}$, 令

$$y = \exp\left(\frac{\log x}{3C' \log\log x}\right),$$

$$m_+ = 2[C' \log\log x],$$

容易验证这样取的 y 和 m_+ 在 x 足够大的时候满足 $5 \le y < x$ 和 $m_+ > 2C \log\log y$. 于是有

$$\frac{x}{(\log y)^2} \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

$$\frac{x}{2^{m_+}} < \frac{x}{2^{2C' \log\log x - 2}} = \frac{4x}{(\log x)^{2C' \log 2}} \ll \frac{x}{(\log x)^2},$$

$$y^{m_+} \le y^{2C' \log\log x} = \exp\left(\frac{2C' \log x \log\log x}{3C' \log\log x}\right) = x^{2/3},$$

所以

$$\pi_2(x) \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

定理得证. □

定理 14 (Brun)**.** 设 $p_1, p_2, \cdots$ 是使得 $p_i + 2$ 也是素数的素数列 (可能有限也可能无限), 则级数

$$B_2 = \sum_{n \ge 1} \left(\frac{1}{p_n} + \frac{1}{p_n + 2}\right) = \frac{1}{3} + \frac{1}{5} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \cdots$$

收敛, B_2 称为 *Brun* 常数.

证明. 由于当 $x \ge 3$ 时,

$$\pi_2(x) \ll \frac{x(\log\log x)^2}{(\log x)^2} \ll \frac{x}{(\log x)^{3/2}},$$

所以当 $n \ge 2$ 时,

$$n = \pi_2(p_n) \ll \frac{p_n}{(\log p_n)^{3/2}} \le \frac{p_n}{(\log n)^{3/2}},$$

$$\frac{1}{p_n} \ll \frac{1}{n(\log n)^{3/2}},$$

故

$$B_2 = \frac{1}{3} + \frac{1}{5} + \sum_{n\geq 2}\left(\frac{1}{p_n} + \frac{1}{p_n+2}\right) < \frac{8}{15} + 2\sum_{n\geq 2}\frac{1}{p_n} \ll \frac{8}{15} + 2\sum_{n=2}^{\infty}\frac{1}{n(\log n)^{3/2}}$$

收敛, 定理得证. □

2.2.3 命题 9+9

不同于孪生素数倒数和问题, 命题 $9+9$ 需要的是下界, 而一般来说下界是比上界更困难一些的, 而且要直面所谓的 "奇偶障碍". 因此 Brun 对他的筛法进行了改进, 提出了同时限制的大素因子个数来构造上下界筛的方法.

具体来说, 改进的想法是将 2 到 z 划分为一些区间, 若 d 的素因子大多处于较小的区间时就保留, d 的素因子大多处于较大的区间时就被去掉.

设 $\Lambda > 0$ 是一个固定的正实数, $z > 2$, 定义有限数列 $\{z_n\}_{n=0}^m$ 满足

$$\log z_n = e^{-n\Lambda}\log z, \quad n = 0, 1, \ldots, m,$$

并且

$$1 < z_m \leq 2 < z_{m-1} < \cdots < z_1 < z_0 = z,$$

即 m 要满足

$$\frac{1}{\Lambda}\log\frac{\log z}{\log 2} \leq m < \frac{1}{\Lambda}\log\frac{\log z}{\log 2} + 1.$$

定义

$$d_n = (d, P(z_n, z)),$$

再选定正整数 b, 定义集合

$$\mathscr{D}^- = \{d \in \mathbb{Z}_{\geq 1} : d \mid P(z),\, \omega(d_n) \leq 2b + 2n - 3\,, n = 1, 2, \ldots, m\},$$

$$\mathscr{D}^+ = \{d \in \mathbb{Z}_{\geq 1} : d \mid P(z),\, \omega(d_n) \leq 2b + 2n - 2\,, n = 1, 2, \ldots, m\},$$

定义

$$\theta^{\pm}(d) = \begin{cases} 1, & d \in \mathscr{D}^{\pm}, \\ 0, & d \notin \mathscr{D}^{\pm}, \end{cases}$$

$$\lambda^{\pm}(d) = \theta^{\pm}(d)\mu(d),$$

接下来我们说明 $\lambda^{\pm}$ 是上下界筛.

- 首先, 显然 $1 \in \mathscr{D}^{\pm}$, 若素数 $p \mid P(z)$, 则 $p \in \mathscr{D}^{\pm}$, 若 $d \in \mathscr{D}^{\pm}$, 且 $f \mid d$, 则一定也有 $f \in \mathscr{D}^{\pm}$.

- 设 $d \mid P(z)$, 并且 $d > 1$, 设 d 的最小素因子是 $p_{\min}(d)$. 当 $\omega(d)$ 是偶数时, 若 $d/p_{\min}(d) \in \mathscr{D}^+$, 则 $d \in \mathscr{D}^+$. 当 $\omega(d)$ 是奇数时, 若 $d/p_{\min}(d) \in \mathscr{D}^-$, 则 $d \in \mathscr{D}^-$.

  这是因为由数列 z_n 的定义可知, 一定存在正整数 $k \leq m$ 使得 $z_k \leq p_{\min}(d) < z_{k-1}$, 所以 $d = d_k = (d, P(z_k, z))$, 当正整数 $n \geq k$ 时, 有 $\omega(d) = \omega(d_n) = \omega((d/p_{\min}(d))_n) + 1$, 而当正整数 $n < k$ 时, 有 $\omega(d_n) = \omega((d/p_{\min}(d))_n)$.

  若 $\omega(d)$ 是偶数, $d/p_{\min}(d) \in \mathscr{D}^+$ 推出 $\omega((d/p_{\min}(d))_n) \leq 2b + 2n - 2$, 所以 $\omega(d_n) \leq 2b + 2n - 1$, 右边是奇数, 故一定 $\omega(d_n) \leq 2b + 2n - 2$, 所以 $d \in \mathscr{D}^+$.

  若 $\omega(d)$ 是奇数, $d/p_{\min}(d) \in \mathscr{D}^-$ 推出 $\omega((d/p_{\min}(d))_n) \leq 2b + 2n - 3$, 所以 $\omega(d_n) \leq 2b + 2n - 2$, 右边是偶数, 故一定 $\omega(d_n) \leq 2b + 2n - 3$, 所以 $d \in \mathscr{D}^-$.

- 在上一点的条件下, 若 $d/p_{\min}(d) \in \mathscr{D}^+$, 则 $d \notin \mathscr{D}^+$ 当且仅当 $\omega(d) = 2b + 2k - 1$, 若 $d/p_{\min}(d) \in \mathscr{D}^-$, 则 $d \notin \mathscr{D}^-$ 当且仅当 $\omega(d) = 2b + 2k - 2$.

  由 $d_k = d$ 立刻知道 $\omega(d_k) = \omega(d) = 2b + 2k - 1 > 2b + 2k - 2$, 即 $d \notin \mathscr{D}^+$. 反过来, $d \notin \mathscr{D}^+$ 推出 $\omega(d) = \omega(d_k) > 2b + 2k - 2$, 而由上一点知 $d/p_{\min}(d) \in \mathscr{D}^+$ 推出 $\omega(d) \leq 2b + 2k - 1$, 所以只能 $\omega(d) = 2b + 2k - 1$, $\mathscr{D}^-$ 的情况同理.

- 由以上几点可以得到 $\lambda^{\pm}$ 的一些性质, $\lambda^{\pm}(1) = 1$, 若 $\lambda^{\pm}(d) = \mu(d)$, $f \mid d$, 则 $\lambda^{\pm}(f) = \mu(f)$. 若 $d \mid P(z)$ 且 $d > 1$, $\lambda^{\pm}(d/p_{\min}(d)) = \mu(d/p_{\min}(d))$, $\mu(d) = 1$ 推出 $\lambda^+(d) = \mu(d)$, $\mu(d) = -1$ 推出 $\lambda^-(d) = \mu(d)$.

- 设 $d > 1$, 当 $d \in \mathscr{D}^{\pm}$ 时, 也有 $d/p_{\min}(d) \in \mathscr{D}^{\pm}$, 故 $\lambda^{\pm}(d/p_{\min}(d)) + \lambda^{\pm}(d) = 1 - 1 = 0$, 当 $d \notin \mathscr{D}^{\pm}$, $d/p_{\min}(d) \notin \mathscr{D}^{\pm}$ 时, 也有 $\lambda^{\pm}(d/p_{\min}(d)) + \lambda^{\pm}(d) = 0 + 0 = 0$, 现考虑 $d/p_{\min}(d) \in \mathscr{D}^+$, 若 $\mu(d) = 1$, 由之前的讨论知 $\lambda^+(d/p_{\min}(d)) + \lambda^+(d) = -1 + 1 = 0$, 若 $\mu(d) = -1$, 则 $\lambda^+(d/p_{\min}(d)) = 1$, 无论 $\lambda^+(d)$ 是 0 还是 -1, 总有 $\lambda^+(d/p_{\min}(d)) + \lambda^+(d) \geq 0$, 总之对所有 $d \mid P(z)$, 一定都有 $\lambda^+(d/p_{\min}(d)) + \lambda^+(d) \geq 0$, 同理, 也一定有 $\lambda^-(d/p_{\min}(d)) + \lambda^-(d) \leq 0$, 由引理 21 知 $\lambda^{\pm}$ 确实是上下界筛.

直观来看, n 越小, z_n 与 z 的距离越小, $P(z_n, z)$ 中的素数越大, 因此 d_n 就只保留了 d 的大素因子, 而在 $\mathscr{D}^{\pm}$ 的定义中的 $2b + 2n - 2$ 和 $2b + 2n - 3$ 随 n 变小, 因此 d 的较大的素因子个数不能太多, 所以 d 要在 $\mathscr{D}^{\pm}$ 中, 要么 d 本身就比较小, 要么 d 是一堆小素数的乘积.

取偶数 $N \geq 2$, $A = \{n(N-n) : 1 \leq n < N\}$, $\mathcal{P}$ 为所有素数组成的集合, Brun 通过细致的分析和常数选取, 证明了当 N 足够大时有正下界

$$S(A, \mathcal{P}, N^{1/10}) \gg \frac{N}{(\log N)^2},$$

更精细的方法可以得到

$$S(A, \mathcal{P}, N^{1/8}) \gg \frac{N}{(\log N)^2},$$

现假设数 $n(N-n)$ 被筛函数 $S(A, \mathcal{P}, N^{1/10})$ 计数, 假设 $\Omega(n) \geq 10$, 这里 Ω 函数表示该数的素因子个数 (计重数), 设 n 最小的素因子为 p, 则由筛法知必然有 $p \geq N^{1/10}$, 所以 $n \geq p^{10} \geq N$, 这是不可能的,

同理 $\Omega(N-n)\geq 10$ 也是不可能的, 这就说明了命题 $9+9$ 是正确的, 即每个足够大的偶数都可以表示为两个至多 9 个素数的乘积的和. 命题 $7+7$ 也类似, 见 [12].

使用类似的方法还可以得到存在无穷多个数 n, 使得 n 和 $n+2$ 为至多 7 个素数的乘积 (可重复).

2.3 Rosser-Iwaniec 筛法

本节我们介绍 Iwaniec 改进的 Rosser 筛法, Rosser-Iwaniec 筛法同样通过限制 d 的大素因子来得到更精细的估计. Iwaniec 由此证明了 Jurkat-Richert 定理, 而该定理最初的证明使用的是 Selberg 筛法. Rosser-Iwaniec 筛法也叫 β-筛法.

2.3.1 Rosser-Iwaniec 筛法的构造

设 $\beta>1$ 和 $D>0$ 是选定的正实数, 若 $d|P(D)$, 设它的素因子分解为

$$d=p_1\dots p_k,\quad p_i\in\mathcal{P}, i=1,\dots,k,$$

并且这些素因子按降序排列,

$$D>p_1>p_2>\cdots>p_k,$$

设

$$\mathscr{D}^-=\left\{d\in\mathbb{Z}_{\geq 1}: d|P(D), p_m<\left(\frac{D}{p_1\dots p_m}\right)^{1/\beta}, 1\leq m\leq k, 2\mid m\right\},$$

$$\mathscr{D}^+=\left\{d\in\mathbb{Z}_{\geq 1}: d|P(D), p_m<\left(\frac{D}{p_1\dots p_m}\right)^{1/\beta}, 1\leq m\leq k, 2\nmid m\right\},$$

$$\lambda^{\pm}(d)=\begin{cases}\mu(d), & d\in\mathscr{D}^{\pm},\\ 0, & d\notin\mathscr{D}^{\pm},\end{cases}$$

这样定义的 $\mathscr{D}^{\pm}$ 和函数 $\lambda^{\pm}$ 有以下性质.

- 条件
$$p_m<\left(\frac{D}{p_1\dots p_m}\right)^{1/\beta}$$
显然等价于 $p_1\dots p_{m-1}p_m^{1+\beta}<D$.
- $1\in\mathscr{D}^{\pm}$, 因为定义中的条件对于 1 来说只是虚真论断.
- 若 $d\in\mathscr{D}^{\pm}$, 则 $d<D$.

  设 $d=p_1\dots p_k\in\mathscr{D}^+$, 若 k 是奇数, 则
$$d=p_1\cdots p_{k-1}p_k<p_1\cdots p_{k-1}p_k^{1+\beta}<D,$$
  若 k 是偶数, 则 $k-1$ 是奇数, 由 $p_k<p_{k-1}$ 得
$$d=p_1\cdots p_{k-1}p_k<p_1\cdots p_{k-1}^2<p_1\cdots p_{k-1}^{1+\beta}<D.$$

设 $d=p_1\dots p_k\in\mathscr{D}^-$, 当 $k\geq 2$ 时, 同理都有 $d<D$, 当 $k=1$ 时, 由 $p_1<D$ 知 $d<D$, 综上可知无论如何总有 $d<D$.

- 若 $d\in\mathscr{D}^\pm$, $f\mid d$, 则 $f\in\mathscr{D}^\pm$.

  假设 $f=p_{i_1}\dots p_{i_r}$, $p_{i_1}>\dots>p_{i_r}$, 其中 $\{i_1,\dots,i_r\}\subseteq\{1,\dots,k\}$, 则必有 $p_{i_1}\leq p_1$, $p_{i_2}\leq p_2$, …, $p_{i_r}\leq p_r$, 所以

  $$p_{i_m}\leq p_m<\left(\frac{D}{p_1\dots p_m}\right)^{1/\beta}\leq\left(\frac{D}{p_{i_1}\dots p_{i_m}}\right)^{1/\beta},$$

  故 $f\in\mathscr{D}^\pm$.

- 设 $d\mid P(z)$, 并且 $d>1$, 设 d 的最小素因子是 $p_{\min}(d)$. 当 k 是偶数时, 若 $d/p_{\min}(d)\in\mathscr{D}^+$, 则 $d\in\mathscr{D}^+$. 当 k 是奇数时, 若 $d/p_{\min}(d)\in\mathscr{D}^-$, 则 $d\in\mathscr{D}^-$.

  由定义知 $p_{\min}(d)=p_k$, 若 $d/p_k=p_1\dots p_{k-1}\in\mathscr{D}^+$, 由 k 是偶数可推出 $d\in\mathscr{D}^+$ 所需不等式自动满足, 同理, 若 $d/p_k\in\mathscr{D}^-$, 由 k 是奇数可推出 $d\in\mathscr{D}^-$ 所需不等式自动满足.

- 与此前对 Brun 筛法的讨论相同, 由引理 21 知这样定义的 $\lambda^\pm$ 确实是上下界筛, 筛域为 $\mathcal{P}$, 支撑级为 D.

引理 25. 设 $g(d)$ 是满足

$$0\leq g(p)<1,\quad p\in\mathcal{P}$$

的乘性函数, 设

$$V(z)=\prod_{p\mid P(z)}(1-g(p))=\sum_{d\mid P(z)}\mu(d)g(d),$$

则 $V(z)$ 是关于 z 的递减函数, 并且 $0<V(z)\leq 1$ 对任意 z 成立, 对任意 $1\leq w<z$, 有

$$\sum_{\substack{p\in\mathcal{P}\\ w\leq p<z}}g(p)V(p)=V(w)-V(z).$$

证明. 只有最后一个式子不是显然的, 设区间 $[w,z)$ 中包含在 $\mathcal{P}$ 中的素数个数为 k, 我们对 k 归纳. 当 $k=0$ 时等式左右均为 0, 假设素数个数为 $k-1$ 时等式成立, 设区间 $[w,z)$ 中在 $\mathcal{P}$ 中的最大素数为 p_1, 则

$$\begin{aligned}\sum_{\substack{p\in\mathcal{P}\\ w\leq p<z}}g(p)V(p)&=\sum_{\substack{p\in\mathcal{P}\\ w\leq p<p_1}}g(p)V(p)+g(p_1)V(p_1)\\&=V(w)-V(p_1)+g(p_1)V(p_1)\\&=V(w)-(1-g(p_1))V(p_1)\\&=V(w)-V(z),\end{aligned}$$

引理得证. □

引理 26. 设 $2 \le z \le D$, 记

$$y_m = \left(\frac{D}{p_1 \dots p_m}\right)^{1/\beta}, \qquad G(z, \lambda^{\pm}) = \sum_{d \mid P(z)} \lambda^{\pm}(d) g(d),$$

$$T_n(D, z) = \sum_{\substack{p_1, \dots, p_n \in \mathcal{P} \\ y_n \le p_n < \dots < p_1 < z \\ p_m < y_m, \forall m < n,\, m \equiv n \pmod 2}} g(p_1 \cdots p_n) V(p_n),$$

则有

$$G(z, \lambda^+) = V(z) + \sum_{\substack{n=1 \\ n \equiv 1 \pmod 2}}^{\infty} T_n(D, z), \qquad G(z, \lambda^-) = V(z) - \sum_{\substack{n=1 \\ n \equiv 0 \pmod 2}}^{\infty} T_n(D, z),$$

并且对所有 $n \ge 1$ 有 $T_n(D, z) \ge 0$, 即有 $G(z, \lambda^-) \le V(z) \le G(z, \lambda^+)$. 假如

$$\beta \le \frac{\log D}{\log z},$$

则对于所有 $n \le \log D / \log z - \beta$ 有 $T_n(D, z) = 0$.

证明. 由 $\lambda^{\pm}$ 的构造得

$$G(z, \lambda^+) = \sum_{\substack{d \in \mathscr{D}^+ \\ d \mid P(z)}} \mu(d) g(d) = \sum_{\substack{p_k < \dots < p_1 < z,\, p_i \in \mathcal{P} \\ p_m < y_m, \forall m \equiv 1 \pmod 2}} (-1)^k g(p_1 \cdots p_k),$$

$$G(z, \lambda^-) = \sum_{\substack{d \in \mathscr{D}^- \\ d \mid P(z)}} \mu(d) g(d) = \sum_{\substack{p_k < \dots < p_1 < z,\, p_i \in \mathcal{P} \\ p_m < y_m, \forall m \equiv 0 \pmod 2}} (-1)^k g(p_1 \cdots p_k),$$

展开 $V(z)$ 得

$$\begin{aligned}
V(z) &= \sum_{d \mid P(z)} \mu(d) g(d) = \sum_{p_k < \dots < p_1 < z,\, p_i \in \mathcal{P}} (-1)^k g(p_1 \cdots p_k) \\
&= \sum_{\substack{p_k < \dots < p_1 < z,\, p_i \in \mathcal{P} \\ p_m < y_m, \forall m \equiv 1 \pmod 2}} (-1)^k g(p_1 \cdots p_k) + \sum_{\substack{p_k < \dots < p_1 < z,\, p_i \in \mathcal{P} \\ \exists m \equiv 1 \pmod 2,\, p_m \ge y_m}} (-1)^k g(p_1 \cdots p_k) \\
&= G(z, \lambda^+) + \sum_{\substack{n=1 \\ n \equiv 1 \pmod 2}}^{\infty} \sum_{\substack{p_k < \dots < p_1 < z,\, p_i \in \mathcal{P} \\ p_m < y_m, \forall m < n,\, m \equiv 1 \pmod 2 \\ p_n \ge y_n}} (-1)^k g(p_1 \cdots p_k) \\
&= G(z, \lambda^+) + \sum_{\substack{n=1 \\ n \equiv 1 \pmod 2}}^{\infty} \left(\sum_{\substack{y_n \le p_n < \dots < p_1 < z \\ p_i \in \mathcal{P} \\ p_m < y_m, \forall m < n, \\ m \equiv 1 \pmod 2}} (-1)^n g(p_1 \cdots p_n) \sum_{\substack{p_k < \dots < p_{n+1} < p_n \\ p_i \in \mathcal{P}}} (-1)^{k-n} g(p_k \cdots p_{n+1}) \right) \\
&= G(z, \lambda^+) - \sum_{\substack{n=1 \\ n \equiv 1 \pmod 2}}^{\infty} \sum_{\substack{y_n \le p_n < \dots < p_1 < z,\, p_i \in \mathcal{P} \\ p_m < y_m, \forall m < n, \\ m \equiv n \pmod 2}} g(p_1 \cdots p_n) V(p_n)
\end{aligned}$$

$$= G(z,\lambda^+) - \sum_{\substack{n=1\\ n\equiv 1 \pmod 2}}^{\infty} T_n(D,z),$$

由 $0 < V(z) \le 1$ 和 $0 \le g(d) < 1$ 知 $T_n(D,z) \ge 0$, 所以

$$G(z,\lambda^+) = V(z) + \sum_{\substack{n=1\\ n\equiv 1 \pmod 2}}^{\infty} T_n(D,z) \ge V(z),$$

同理有

$$G(z,\lambda^-) = V(z) - \sum_{\substack{n=1\\ n\equiv 0 \pmod 2}}^{\infty} T_n(D,z) \le V(z).$$

最后, 若 $y_n \le p_n < \cdots < p_1 < z$, 则 $D \le p_1 \cdots p_n p_n^\beta < z^{n+\beta}$, 设 $D = z^s$, 则只有 $s < n + \beta$ 时满足 $T_n(D,z)$ 的求和下标的 p_i 才存在, 故当 $n \le s - \beta = \log D/\log z - \beta$ 时 $T_n(D,z) = 0$, 引理得证. □

以下均假设 $\beta = 2$, 则

$$y_m = \left(\frac{D}{p_1 \dots p_m}\right)^{1/2}.$$

记 $s = \log D/\log z$.

引理 27. *设 $z \ge 2$, $D > 0$, 当 $s \ge 3$ 时, $T_1(D,z) = 0$, 若 n 是奇数且 $3 > s \ge 1$, 或者 n 是偶数且 $3 > s \ge 2$, 则*

$$T_1(D,z) = V(D^{1/3}) - V(z),$$

当 $n \ge 2$ 时, 若 n 是偶数或 n 是奇数且 $s \ge 3$, 则

$$T_n(D,z) = \sum_{\substack{p\in\mathcal{P}\\ p<z}} g(p) T_{n-1}\left(\frac{D}{p}, p\right),$$

若 n 是奇数且 $1 \le s \le 3$, 则

$$T_n(D,z) = \sum_{\substack{p\in\mathcal{P}\\ p<D^{1/3}}} g(p) T_{n-1}\left(\frac{D}{p}, p\right).$$

证明. 由于 $y_1 = (D/p_1)^{1/2}$, 则

$$\begin{aligned} T_1(D,z) &= \sum_{\substack{p_1\in\mathcal{P}\\ y_1\le p_1<z}} g(p_1)V(p_1) \\ &= \sum_{\substack{p_1\in\mathcal{P}\\ D^{1/3}\le p_1<z}} g(p_1)V(p_1) \\ &= V(D^{1/3}) - V(z). \end{aligned}$$

若 n 是偶数, 则

$$\begin{aligned} T_n(D,z) &= \sum_{\substack{p_n<\cdots<p_1<z,\, p_i\in\mathcal{P}\\ p_1\cdots p_n p_n^2\geq D\\ p_1\cdots p_m p_m^2<D\\ \forall m<n,\, m\equiv n \pmod 2}} g(p_1\cdots p_n)V(p_n) \\ &= \sum_{\substack{p_1\in\mathcal{P}\\ p_1<z}} g(p_1) \sum_{\substack{p_n<\cdots<p_1,\, p_i\in\mathcal{P}\\ p_2\cdots p_n p_n^2\geq D/p_1\\ p_2\cdots p_m p_m^2<D/p_1\,\forall 2\leq m<n,\\ m-1\equiv n-1 \pmod 2}} g(p_2\cdots p_n)V(p_n) \\ &= \sum_{\substack{p_1\in\mathcal{P}\\ p_1<z}} g(p_1) T_{n-1}\left(\frac{D}{p_1}, p_1\right). \end{aligned}$$

若 n 是奇数, 则 p_1 必须同时满足 $p_1<y_1 \Leftrightarrow p_1<D^{1/3}$ 和 $p_1<z=D^{1/s}$, 即 $p_1<\min\{D^{1/3}, D^{1/s}\}$, 同理当 $s\geq 3$ 时

$$T_n(D,z) = \sum_{\substack{p\in\mathcal{P}\\ p<z}} g(p) T_{n-1}\left(\frac{D}{p}, p\right),$$

当 $1\leq s\leq 3$ 时

$$T_n(D,z) = \sum_{\substack{p\in\mathcal{P}\\ p<D^{1/3}}} g(p) T_{n-1}\left(\frac{D}{p}, p\right),$$

引理得证. □

2.3.2 微分-差分方程

为了估计 $T_n(D,z)$, 需要构造一个满足特定微分-差分方程的函数.

首先定义集合

$$\mathcal{R}_n(s) = \left\{ (t_1,\ldots,t_n)\in\mathbb{R}^n \,\middle|\, \begin{array}{l} 0<t_n<t_{n-1}<\cdots<t_1<\dfrac{1}{s},\\ t_1+\cdots+t_{n-1}+t_n+2t_n>1,\\ \forall m<n,\, m\equiv n \pmod 2,\ \left(\sum_{i=1}^{m} t_i\right)+2t_m<1 \end{array} \right\},\quad n\geq 1, s\geq 1,$$

它是有界开凸集, 再定义

$$f_n(s) = \frac{1}{s}\int_{\mathcal{R}_n(s)} \frac{\mathrm{d}t_1\ldots\mathrm{d}t_n}{t_1\ldots t_{n-1}t_n^2},$$

$\mathcal{R}_n(s)$ 的定义确保诸 t_i 均远离 0, 因此不涉及收敛问题. 定义

$$F(s) = 1 + \sum_{\substack{n=1\\ n\equiv 1 \pmod 2}}^{\infty} f_n(s), \qquad s\geq 1,$$

$$f(s) = 1 - \sum_{\substack{n=2\\ n\equiv 0 \pmod 2}}^{\infty} f_n(s), \qquad s\geq 2,$$

后面将会说明这两个级数均收敛.

试计算 $f_1(s)$, 容易看出

$$\mathcal{R}_1(s)=\begin{cases}\left(\dfrac{1}{3},\dfrac{1}{s}\right), & 1\le s<3,\\ \emptyset, & s\ge 3,\end{cases}$$

则

$$sf_1(s)=\begin{cases}\int_{1/3}^{1/s}\frac{\mathrm{d}t}{t^2}=3-s, & 1\le s<3,\\ 0, & s\ge 3.\end{cases}$$

引理 28. 设 $n\ge 2$, 则当 n 是偶数且 $s\ge 2$, 或 n 是奇数且 $s\ge 3$ 时

$$sf_n(s)=\int_s^\infty f_{n-1}(t-1)\,\mathrm{d}t,$$

当 n 是奇数且 $1\le s\le 3$ 时

$$sf_n(s)=3f_n(3)=\int_3^\infty f_{n-1}(t-1)\,\mathrm{d}t.$$

证明. 若 $\mathcal{R}_n(s)$ 是空集, 引理显然成立, 以下均设 $\mathcal{R}_n(s)$ 非空.

先设 n 是偶数且 $s\ge 2$, 或 n 是奇数且 $s\ge 3$, 由 $\mathcal{R}_n(s)$ 非空知

$$1<t_1+\cdots+t_{n-1}+3t_n<(n+2)t_1<\frac{n+2}{s},$$

$$\frac{1}{n+2}<t_1<\frac{1}{s},$$

故

$$sf_n(s)=\int_{\mathcal{R}_n(s)}\frac{\mathrm{d}t_1\cdots\mathrm{d}t_n}{t_1\cdots t_{n-1}t_n^2}=\int_{1/(n+2)}^{1/s}\left(\int_{\substack{0<t_n<\cdots<t_2<t_1\\ t_2+\cdots+t_n+2t_n>1-t_1\\ t_2+\cdots+t_m+2t_m<1-t_1\\ \forall 1<m<n,\,m\equiv n\pmod 2}}\frac{\mathrm{d}t_2\cdots\mathrm{d}t_n}{t_2\cdots t_{n-1}t_n^2}\right)\frac{\mathrm{d}t_1}{t_1},$$

换元 $t_i=(1-t_1)u_{i-1}$, $i>1$,

$$\begin{aligned}\int_{\substack{0<t_n<\cdots<t_2<t_1\\ t_2+\cdots+t_n+2t_n>1-t_1\\ t_2+\cdots+t_m+2t_m<1-t_1\\ \forall 1<m<n,\,m\equiv n\pmod 2}}\frac{\mathrm{d}t_2\cdots\mathrm{d}t_n}{t_2\ldots t_{n-1}t_n^2}&=\int_{\substack{0<u_{n-1}<\cdots<u_1<t_1/(1-t_1)\\ u_1+\cdots+u_{n-1}+2u_{n-1}>1\\ u_1+\cdots+u_{m-1}+2u_{m-1}<1\\ \forall 1<m<n,\,m-1\equiv n-1\pmod 2}}\frac{\mathrm{d}u_1\cdots\mathrm{d}u_{n-1}}{(1-t_1)u_1\ldots u_{n-2}u_{n-1}^2}\\ &=\frac{1}{1-t_1}\int_{\substack{0<u_{n-1}<\cdots<u_1<t_1/(1-t_1)\\ u_1+\cdots+u_{n-1}+2u_{n-1}>1\\ u_1+\cdots+u_{m-1}+2u_{m-1}<1\\ \forall 1<m<n,\,m-1\equiv n-1\pmod 2}}\frac{\mathrm{d}u_1\cdots\mathrm{d}u_{n-1}}{u_1\ldots u_{n-2}u_{n-1}^2}\\ &=\frac{1}{1-t_1}\int_{\mathcal{R}_{n-1}((1-t_1)/t_1)}\frac{\mathrm{d}u_1\cdots\mathrm{d}u_{n-1}}{u_1\ldots u_{n-2}u_{n-1}^2}\\ &=\frac{(1-t_1)/t_1}{1-t_1}f_{n-1}((1-t_1)/t_1)\\ &=\frac{1}{t_1}f_{n-1}\left(\frac{1}{t_1}-1\right),\end{aligned}$$

再换元 $t=1/t_1$ 得

$$\begin{aligned} sf_n(s) &= \int_{1/(n+2)}^{1/s} \frac{1}{t_1} f_{n-1}\left(\frac{1}{t_1}-1\right)\frac{\mathrm{d}t_1}{t_1} \\ &= -\int_{n+2}^{s} f_{n-1}(t-1)\,\mathrm{d}t \\ &= \int_{s}^{n+2} f_{n-1}(t-1)\,\mathrm{d}t \\ &= \int_{s}^{\infty} f_{n-1}(t-1)\,\mathrm{d}t, \end{aligned}$$

最后一步是因为 $t-1>n+2$ 时 $1/(n-1+2)>1/(t-1)$, $\mathcal{R}_{n-1}(t-1)$ 为空集, $f_{n-1}(t-1)=0$.

再设 n 是奇数且 $1\le s\le 3$, 由于 $n\ge 2$, 则必须 $n\ge 3$, 设 $(t_1,\dots,t_n)\in\mathcal{R}_n(s)$, 则 $t_1<1/s$, 取 $m=1\equiv n \pmod 2$ 得 $3t_1<1$, 故 $t_1<1/\max\{3,s\}$, 而 $s\le 3$ 推出 $t_1<1/3$, 因此 $(t_1,\dots,t_n)\in\mathcal{R}_n(3)$, $\mathcal{R}_n(s)\subseteq\mathcal{R}_n(3)$, 另外显然 $\mathcal{R}_n(3)\subseteq\mathcal{R}_n(s)$, 所以 $\mathcal{R}_n(s)=\mathcal{R}_n(3)$, 故

$$sf_n(s)=\int_{\mathcal{R}_n(s)}\frac{\mathrm{d}t_1\dots\mathrm{d}t_n}{t_1\dots t_{n-1}t_n^2}=\int_{\mathcal{R}_n(3)}\frac{\mathrm{d}t_1\dots\mathrm{d}t_n}{t_1\dots t_{n-1}t_n^2}=3f_n(3),$$

引理得证. □

定义辅助函数 $h(s)$ 和 $H(s)$ 为

$$h(s)=\begin{cases} e^{-2}, & 1\le s<2,\\ e^{-s}, & 2\le s<3,\\ 3s^{-1}e^{-s}, & 3\le s, \end{cases}\qquad s\in[1,+\infty),$$

$$H(s)=\int_s^{\infty} h(t-1)\,\mathrm{d}t,\qquad s\in[2,+\infty).$$

显然 $h(s)$ 和 $H(s)$ 均是单调递减的连续正函数. 此外, 做比并分段讨论即可推出 $h(s-1)<4h(s)$ 在 $s\ge 2$ 时成立.

设

$$\alpha=\frac{H(2)}{2h(2)},$$

计算可得该数大约为 $\alpha\approx 0.9606$.

引理 29. 当 $s\ge 2$ 时,

$$\alpha sh(s)\ge H(s),$$

当 $1\le s\le 3$ 时

$$\alpha sh(s)\ge H(3).$$

证明. 当 $s\ge 3$ 时, $h(s-1)\le e^{1-s}$, 则

$$H(s)\le\int_s^{\infty}e^{1-t}\,\mathrm{d}t=e^{1-s}=\frac{esh(s)}{3}<\alpha sh(s).$$

当 $2 \le s \le 3$ 时, 易证 $\alpha sh(s) - H(s)$ 在 $[2,3]$ 上递增且在 2 处取值为 $\alpha 2h(2) - H(2) = 0$, 所以 $\alpha sh(s) \ge H(s) \ge H(3)$.

当 $s \le 2$ 时, 由 $\alpha < 1$ 得 $h(2) > H(2)/2$, 于是

$$H(3) = H(2) - e^{-2} = H(2) - h(2) < \frac{H(2)}{2} = \alpha h(2) \le \alpha sh(2) = \alpha sh(s),$$

引理得证. □

引理 30. *当 n 是奇数且 $s \ge 1$, 或 n 是偶数且 $s \ge 2$ 时, 有*

$$f_n(s) \le 2e^2 \alpha^{n-1} h(s).$$

证明. 当 $n = 1$ 时, 分段讨论易证 $f_1(s) \le 2e^2 h(s)$. 现假设 $n \ge 2$ 且引理对 $n-1$ 成立, 当 n 是偶数且 $s \ge 2$, 或 n 是奇数且 $s \ge 3$ 时, 有

$$sf_n(s) = \int_s^\infty f_{n-1}(t-1)\,\mathrm{d}t \le 2e^2\alpha^{n-2} \int_s^\infty h(t-1)\,\mathrm{d}t = 2e^2\alpha^{n-2}H(s) \le 2e^2\alpha^{n-1}sh(s),$$

当 n 是奇数且 $1 \le s \le 3$ 时

$$sf_n(s) = \int_3^\infty f_{n-1}(t-1)\,\mathrm{d}t \le 2e^2\alpha^{n-2} \int_3^\infty h(t-1)\,\mathrm{d}t \le 2e^2\alpha^{n-2}H(3) \le 2e^2\alpha^{n-1}sh(s),$$

由归纳法知引理对所有正整数 n 成立. □

定理 15. *当 $s \ge 1$ 时, $F(s) = 1 + O(e^{-s})$, 当 $s \ge 2$ 时, $f(s) = 1 + O(e^{-s})$.*

证明. 在相应条件下, 由

$$0 \le f_n(s) \le 2e^2\alpha^{n-1}h(s) \le 2e^2\alpha^{n-1}e^{-s}$$

知

$$\sum_{\substack{n=1 \\ n\equiv 1 \pmod 2}}^{\infty} f_n(s) \ll e^{-s}, \qquad s \ge 1,$$

$$\sum_{\substack{n=2 \\ n\equiv 0 \pmod 2}}^{\infty} f_n(s) \ll e^{-s}, \qquad s \ge 2,$$

由 $F(s)$ 和 $f(s)$ 的定义即可推出定理. □

为方便起见, 以下设 $1 \le s \le 2$ 时 $f(s) = 0$.

定理 16. *上述定义的函数 F 和 f 在 $s > 2$ 时满足以下微分-差分方程组,*

$$\begin{cases} (sF(s))' = f(s-1), \\ (sf(s))' = F(s-1). \end{cases}$$

证明. 令 $n \geq 2$, 当 n 是偶数且 $s > 2$, 或 n 是奇数且 $s > 3$ 时, 有

$$(sf_n(s))' = \frac{\mathrm{d}}{\mathrm{d}s}\int_s^\infty f_{n-1}(t-1)\,\mathrm{d}t = -f_{n-1}(s-1).$$

当 $s > 2$ 时有

$$\begin{aligned}
(sf(s))' &= \left(s - \sum_{\substack{n=2\\ n\equiv 0 \pmod 2}}^{\infty} sf_n(s)\right)' \\
&= 1 + \sum_{\substack{n=2\\ n\equiv 0 \pmod 2}}^{\infty} f_{n-1}(s-1) \\
&= 1 + \sum_{\substack{n=1\\ n\equiv 1 \pmod 2}}^{\infty} f_n(s-1) \\
&= F(s-1).
\end{aligned}$$

当 $s > 3$ 时, $sf_1(s) = 0$, 所以有

$$\begin{aligned}
(sF(s))' &= \left(s + \sum_{\substack{n=1\\ n\equiv 1 \pmod 2}}^{\infty} sf_n(s)\right)' \\
&= \left(s + \sum_{\substack{n=3\\ n\equiv 1 \pmod 2}}^{\infty} sf_n(s)\right)' \\
&= 1 - \sum_{\substack{n=3\\ n\equiv 1 \pmod 2}}^{\infty} f_{n-1}(s-1) \\
&= 1 - \sum_{\substack{n=2\\ n\equiv 0 \pmod 2}}^{\infty} f_n(s-1) \\
&= f(s-1).
\end{aligned}$$

此外, 当 $2 < s \leq 3$ 时, $sf_1(s) = 3 - s$, 而 n 是大于 1 的奇数时 $sf_n(s) = 3f_n(3)$, 所以

$$sF(s) = s + sf_1(s) + \sum_{\substack{n=3\\ n\equiv 1 \pmod 2}}^{\infty} sf_n(s) = 3 + \sum_{\substack{n=3\\ n\equiv 1 \pmod 2}}^{\infty} 3f_n(3) = 3F(3),$$

注意到当 $2 < s \leq 3$ 时 $1 < s - 1 \leq 2$, 由约定 $f(s-1) = 0$, 从而 $(sF(s))' = f(s-1)$ 在 $s > 2$ 时都成立. □

该微分-差分方程可以分段的解出, 条件

$$\begin{cases}(sF(s))'=f(s-1), s>2,\\ (sf(s))'=F(s-1), s>2,\\ sF(s)=3F(3), 1\le s\le 3,\\ f(s)=1+O(e^{-s}),\\ F(s)=1+O(e^{-s}),\end{cases}$$

足以解出

$$\begin{cases}F(s)=\dfrac{2e^{\gamma}}{s}, & 1\le s\le 3,\\ f(s)=\dfrac{2e^{\gamma}\log(s-1)}{s}, & 2\le s\le 4,\end{cases}$$

其中 γ 是欧拉常数, 其余区间上的解可以由微分-差分方程递推得到, 见 [7] 9.5 节.

2.4 线性筛法与 Jurkat-Richert 定理

本节证明线性筛法中的 Jurkat-Richert 定理. 本节依旧假设 $\beta=2$.

引理 31. *设 $z\ge 2$ 且 $1<w<z$, $g(d)$ 为一个乘性函数, 满足对所有 $p\in\mathcal{P}$ 均有 $0\le g(p)<1$, 且存在某个常数 $K>1$ 使得*

$$\prod_{\substack{p\in\mathcal{P}\\ u\le p<z}}(1-g(p))^{-1}\le K\frac{\log z}{\log u}$$

对所有 $1<u<z$ 成立, 设 Φ 为区间 $[w,z]$ 上的连续单调递增函数, 则有

$$\sum_{\substack{p\in\mathcal{P}\\ w\le p<z}}g(p)V(p)\Phi(p)\le (K-1)V(z)\Phi(z)-KV(z)\int_w^z\Phi(u)\,\mathrm{d}\left(\frac{\log z}{\log u}\right).$$

证明. 记函数

$$S(u)=\sum_{\substack{p\in\mathcal{P}\\ u\le p<z}}g(p)V(p),$$

它是递减的非负函数, 并且

$$\begin{aligned}S(u)&=V(u)-V(z)\\ &=\left(\frac{V(u)}{V(z)}-1\right)V(z)\\ &=\left(\prod_{\substack{p\in\mathcal{P}\\ u\le p<z}}(1-g(p))^{-1}-1\right)V(z)\\ &\le\left(K\frac{\log z}{\log u}-1\right)V(z),\end{aligned}$$

设区间 $[w,z)$ 中在 $\mathcal{P}$ 里的所有素数为 $p_1,\dots,p_k$, 并且 $w\le p_k<\cdots<p_1<z$, 则显然 $S(p_k)=S(w)$, $S(p_1)=g(p_1)V(p_1)$, 当 $p_1<u<z$ 时 $S(u)=0$, 所以由 Riemann-Stieltjes 积分的分部积分得

$$\begin{aligned}
\sum_{\substack{p\in\mathcal{P}\\ w\le p<z}} g(p)V(p)\Phi(p) &= \sum_{i=1}^{k} g(p_i)V(p_i)\Phi(p_i)\\
&= \sum_{i=2}^{k}(S(p_i)-S(p_{i-1}))\Phi(p_i)+S(p_1)\Phi(p_1)\\
&= \sum_{i=1}^{k} S(p_i)\Phi(p_i)-\sum_{i=1}^{k-1} S(p_i)\Phi(p_{i+1})\\
&= S(p_k)\Phi(p_k)+\sum_{i=1}^{k-1} S(p_i)(\Phi(p_i)-\Phi(p_{i+1}))\\
&= S(w)\Phi(w)+S(p_k)(\Phi(p_k)-\Phi(w))+\sum_{i=1}^{k-1} S(p_i)(\Phi(p_i)-\Phi(p_{i+1}))\\
&= S(w)\Phi(w)+\int_w^{p_1} S(u)\,\mathrm{d}\Phi(u)\\
&= S(w)\Phi(w)+\int_w^{z} S(u)\,\mathrm{d}\Phi(u)\\
&= S(z)\Phi(z)-\int_w^{z} \Phi(u)\,\mathrm{d}S(u)\\
&\le (K-1)V(z)\Phi(z)-KV(z)\int_w^{z}\Phi(u)\,\mathrm{d}\left(\frac{\log z}{\log u}\right),
\end{aligned}$$

引理得证. □

引理 32. *在以上条件下, 若 $s=\log D/\log z$, 当 n 是奇数时 $s\ge 1$, n 是偶数时 $s\ge 2$, 再假设常数 K 满足 $1<K<201/200$, 则*

$$T_n(D,z)<V(z)\left(f_n(s)+(K-1)\left(\frac{99}{100}\right)^n e^{10-s}\right).$$

证明. 设 $\tau=\alpha+5(K-1)+11e^{-8}$, 定义辅助函数 $h_n(s)=(K-1)\tau^n e^{10}h(s)$, $n\ge 1$, 直接计算可得 $\alpha<\tau<99/100$, 结合 $h(s)\le e^{-s}$ 知只需证明

$$T_n(D,z)<V(z)\left(f_n(s)+h_n(s)\right).$$

当 $n=1$ 时, 由于 $n\le s-\beta$ 时 $T_n(D,z)=0$, 所以 $3\le s$ 时 $T_1(D,z)=0$, 引理显然成立, 现设 $1\le s\le 3$, 此时又有 $T_1(D,z)=V(D^{1/3})-V(z)$, 则

$$\begin{aligned}
T_1(D,z) &= \left(\frac{V(D^{1/3})}{V(z)}-1\right)V(z)\\
&= \left(\prod_{D^{1/3}\le p<z}(1-g(p))^{-1}-1\right)V(z)
\end{aligned}$$

$$
\begin{aligned}
&\leq \left(3K\frac{\log z}{\log D}-1\right)V(z)\\
&=\left(\frac{3K}{s}-1\right)V(z)\\
&=\left(\left(\frac{3}{s}-1\right)+\frac{3}{s}(K-1)\right)V(z)\\
&\leq \big(f_1(s)+3(K-1)\big)V(z)\\
&<\big(f_1(s)+h_1(s)\big)V(z),
\end{aligned}
$$

最后一步是因为此时 $h(s)\geq e^{-3}$, 计算可得 $h_1(s)>3(K-1)$.

现设 $n\geq 2$, 并且 $T_{n-1}(D,z)<V(z)\left(f_{n-1}(s)+h_{n-1}(s)\right)$. 当 n 为偶数且 $s\geq 2$, 或 n 为奇数且 $s\geq 3$ 时, 构造函数

$$
\Phi(u)=f_{n-1}\left(\frac{\log D}{\log u}-1\right)+h_{n-1}\left(\frac{\log D}{\log u}-1\right),\qquad 1<u\leq z,
$$

显然 $\Phi(u)$ 是连续递增的正函数, 此外 $\Phi(z)=f_{n-1}(s-1)+h_{n-1}(s-1)$, $\log(D/p)/\log p=\log D/\log p-1$, 所以取 $1<w<2$, 由此前的引理可得

$$
\begin{aligned}
T_n(D,z)&=\sum_{\substack{p\in\mathcal{P}\\ p<z}}g(p)T_{n-1}\left(\frac{D}{p},p\right)\\
&<\sum_{\substack{p\in\mathcal{P}\\ p<z}}g(p)V(p)\Phi(p)\\
&\leq (K-1)V(z)\Phi(z)-KV(z)\lim_{w\to 1^+}\int_w^z\Phi(u)\,\mathrm{d}\left(\frac{\log z}{\log u}\right)\\
&=(K-1)V(z)(f_{n-1}(s-1)+h_{n-1}(s-1))-\frac{KV(z)}{s}\lim_{w\to 1^+}\int_w^z\Phi(u)\,\mathrm{d}\left(\frac{\log D}{\log u}\right)\\
&=(K-1)V(z)(f_{n-1}(s-1)+h_{n-1}(s-1))+\frac{KV(z)}{s}\int_s^\infty f_{n-1}(t-1)+h_{n-1}(t-1)\,\mathrm{d}t\\
&=(K-1)V(z)(f_{n-1}(s-1)+h_{n-1}(s-1))+KV(z)\left(f_n(s)+\frac{1}{s}(K-1)\tau^{n-1}e^{10}H(s)\right)\\
&\leq (K-1)V(z)(2e^2\alpha^{n-2}h(s-1)+h_{n-1}(s-1))+KV(z)\left(f_n(s)+\alpha(K-1)\tau^{n-1}e^{10}h(s)\right)\\
&<(K-1)V(z)(8e^2\alpha^{n-2}h(s)+4h_{n-1}(s))+KV(z)\left(f_n(s)+\alpha h_{n-1}(s)\right)\\
&=8e^{-8}V(z)\left(\frac{\alpha}{\tau}\right)^{n-1}\alpha^{-1}h_{n-1}(s)+4(K-1)V(z)h_{n-1}(s)+KV(z)\left(f_n(s)+\alpha h_{n-1}(s)\right)\\
&<9e^{-8}V(z)h_{n-1}(s)+4(K-1)V(z)h_{n-1}(s)+KV(z)\left(f_n(s)+\alpha h_{n-1}(s)\right)\\
&=V(z)f_n(s)+(K-1)V(z)f_n(s)+V(z)\left(9e^{-8}+4(K-1)+\alpha K\right)h_{n-1}(s)\\
&\leq V(z)f_n(s)+V(z)\left(11e^{-8}+4(K-1)+\alpha+K-1\right)h_{n-1}(s)\\
&=V(z)f_n(s)+V(z)\left(11e^{-8}+5(K-1)+\alpha\right)h_{n-1}(s)\\
&=V(z)f_n(s)+V(z)\tau h_{n-1}(s)\\
&=V(z)f_n(s)+V(z)h_n(s),
\end{aligned}
$$

当 n 是大于 1 的奇数且 $1 \le s \le 3$ 时, 同理可得

$$\begin{aligned} T_n(D,z) &= \sum_{\substack{p\in\mathcal{P}\\ p<D^{1/3}}} g(p)T_{n-1}\left(\frac{D}{p},p\right) \\ &< \sum_{\substack{p\in\mathcal{P}\\ p<D^{1/3}}} g(p)V(p)\Phi(p) \\ &< (f_n(3)+h_n(3))V(z) \\ &\le (f_n(s)+h_n(s))V(z), \end{aligned}$$

由归纳法知对所有正整数 n 都有

$$T_n(D,z) < V(z)\left(f_n(s)+h_n(s)\right) < V(z)\left(f_n(s)+(K-1)\left(\frac{99}{100}\right)^n e^{10-s}\right),$$

引理得证. □

引理 33. *在以上条件下, 设 $K = 1+\varepsilon$, 其中 $0<\varepsilon<1/200$, 则有*

$$G(z,\lambda^+) < V(z)\left(F(s)+\varepsilon e^{14-s}\right),$$

$$G(z,\lambda^-) > V(z)\left(f(s)-\varepsilon e^{14-s}\right).$$

证明. 直接计算可以得到几何级数

$$\sum_{\substack{n=0\\ n\equiv 0 \pmod 2}}^{\infty}\left(\frac{99}{100}\right)^n < e^4,$$

所以

$$\begin{aligned} G(z,\lambda^+) &= V(z) + \sum_{\substack{n=1\\ n\equiv 1 \pmod 2}}^{\infty} T_n(D,z) \\ &< V(z)\left(1+\sum_{\substack{n=1\\ n\equiv 1 \pmod 2}}^{\infty} f_n(s)+\varepsilon e^{10-s}\sum_{\substack{n=1\\ n\equiv 1 \pmod 2}}^{\infty}\left(\frac{99}{100}\right)^n\right) \\ &< V(z)\left(F(s)+\varepsilon e^{14-s}\right), \end{aligned}$$

同理

$$\begin{aligned} G(z,\lambda^-) &= V(z) - \sum_{\substack{n=1\\ n\equiv 0 \pmod 2}}^{\infty} T_n(D,z) \\ &> V(z)\left(1-\sum_{\substack{n=1\\ n\equiv 0 \pmod 2}}^{\infty} f_n(s)-\varepsilon e^{10-s}\sum_{\substack{n=1\\ n\equiv 0 \pmod 2}}^{\infty}\left(\frac{99}{100}\right)^n\right) \end{aligned}$$

$$> V(z)\left(f(s)-\varepsilon e^{14-s}\right),$$

引理得证. □

定理 17 (Jurkat-Richert 定理)**.** 设 $A=\{a(n)\}_{n=1}^{\infty}$ 是一列非负实数列, 并且 $|A|=\sum_{n=1}^{\infty}a(n)$ 收敛, 设 $\mathcal{P}$ 是一些素数组成的集合, 对 $z\geq 2$, 定义

$$P(z)=\prod_{\substack{p\in\mathcal{P}\\ p<z}}p,\qquad S(A,\mathcal{P},z)=\sum_{(n,P(z))=1}a(n).$$

对每个正整数 n, 设 $g_n(d)$ 是乘性函数, 它在每个 $\mathcal{P}$ 中素数 p 上的值满足 $0\leq g_n(p)<1$, 定义 $|A_d|=\sum_{d|n}a(n)$, $r(d)=|A_d|-\sum_{n=1}^{\infty}a(n)g_n(d)$. 设 $\mathcal{Q}$ 是 $\mathcal{P}$ 的有限子集, $Q=\prod_{p\in\mathcal{Q}}p$, 再假设存在实数 ε 满足 $0<\varepsilon<1/200$, 使得不等式

$$\prod_{\substack{p\in\mathcal{P}-\mathcal{Q}\\ u\leq p<z}}(1-g_n(p))^{-1}<(1+\varepsilon)\frac{\log z}{\log u}$$

对所有正整数 n 和满足 $1<u<z$ 的实数 u 成立. 设 D 是一个正实数, 要求 $s=\log D/\log z\geq 1$, 对所有正整数 n 定义

$$\mathcal{R}_n(s)=\left\{(t_1,\dots,t_n)\in\mathbb{R}^n\;\middle|\;\begin{array}{l}0<t_n<t_{n-1}<\cdots<t_1<\dfrac{1}{s},\\ t_1+\cdots+t_{n-1}+t_n+2t_n>1,\\ \forall m<n,\ m\equiv n\pmod 2,\ \left(\displaystyle\sum_{i=1}^{m}t_i\right)+2t_m<1\end{array}\right\},$$

$$f_n(s)=\frac{1}{s}\int_{\mathcal{R}_n(s)}\frac{\mathrm{d}t_1\dots\mathrm{d}t_n}{t_1\dots t_{n-1}t_n^2},$$

再定义

$$F(s)=1+\sum_{\substack{n=1\\ n\equiv 1\pmod 2}}^{\infty}f_n(s),\qquad s\geq 1,$$

$$f(s)=1-\sum_{\substack{n=2\\ n\equiv 0\pmod 2}}^{\infty}f_n(s),\qquad s\geq 2,$$

则有不等式

$$S(A,\mathcal{P},z)<\left(F(s)+\varepsilon e^{14-s}\right)X+R$$

成立, 若再要求 $s\geq 2$, 则有不等式

$$S(A,\mathcal{P},z)>\left(f(s)-\varepsilon e^{14-s}\right)X-R$$

成立, 其中

$$X=\sum_{n=1}^{\infty}a(n)\prod_{p|P(z)}(1-g_n(p)),\qquad R=\sum_{\substack{d|P(z)\\ d<DQ}}|r(d)|.$$

证明. 设 $\mathcal{P}_1 = \mathcal{P} - \mathcal{Q}$, 由 Rosser-Iwaniec 筛法的构造知存在以 $\mathcal{P}_1$ 为筛域, D 为支撑级的上下界筛 $\lambda_1^{\pm}$, 由引理 22 知它可以生成以 $\mathcal{P}$ 为筛域, DQ 为支撑级的上下界筛 $\lambda^{\pm}$, 与 $P(z)$ 类似的定义 $P_1(z)$ 和 $Q(z)$, 再设

$$G_n(z,\lambda_1^{\pm}) = \sum_{d|P_1(z)} \lambda_1^{\pm}(d) g_n(d), \qquad V_n(z) = \prod_{p|P_1(z)} (1 - g_n(p)),$$

因为 g_n 是乘性函数, 由引理知在相应条件下有

$$G_n(z,\lambda_1^{+}) < V_n(z)\left(F(s) + \varepsilon e^{14-s}\right), \qquad G_n(z,\lambda_1^{-}) > V_n(z)\left(f(s) - \varepsilon e^{14-s}\right),$$

对所有 n 成立, 所以由引理 22 得

$$\begin{aligned} S(A,\mathcal{P},z) &\le \sum_{n=1}^{\infty} a(n) G_n(z,\lambda_1^{+}) \prod_{q|Q(z)} (1 - g_n(q)) + R \\ &< (F(s) + \varepsilon e^{14-s}) \sum_{n=1}^{\infty} a(n) V_n(z) \prod_{q|Q(z)} (1 - g_n(q)) + R \\ &= (F(s) + \varepsilon e^{14-s}) \sum_{n=1}^{\infty} a(n) \prod_{p|P(z)} (1 - g_n(p)) + R \\ &= (F(s) + \varepsilon e^{14-s}) X + R, \end{aligned}$$

下界同理可得. □

在一些更常见的情形中, 函数族 $g_n(d)$ 与 n 无关, 设它们都等于 $g(d)$, 则定理中的 X 变为

$$X = |A| V(z), \qquad V(z) = \prod_{p|P(z)} (1 - g(p)).$$

2.5 Selberg 筛法

Selberg 筛法不截断 Möbius 函数, 而是使用二次型极值方法来得到上界, 因此也称为 Selberg 上界筛法或 Λ^2-筛法 [8].

引理 34. 令 $a_1, \dots, a_n$ 为任意的 n 个正实数, $b_1, \dots, b_n$ 为任意的 n 个实数, 则二次型

$$Q(y_1, \dots, y_n) = a_1 y_1^2 + \cdots + a_n y_n^2$$

在条件 $b_1 y_1 + \cdots + b_n y_n = 1$ 下的极小值为

$$m = \left(\sum_{i=1}^{n} \frac{b_i^2}{a_i} \right)^{-1},$$

二次型 Q 取极小值当且仅当

$$y_i = \frac{m b_i}{a_i}, \qquad i = 1, \dots, n.$$

证明. 由 Cauchy-Schwarz 不等式知

$$\begin{aligned}1&=\left(\sum_{i=1}^{n}b_iy_i\right)^2\\&=\left(\sum_{i=1}^{n}\left(\frac{b_i}{\sqrt{a_i}}\right)(\sqrt{a_i}y_i)\right)^2\\&\le\left(\sum_{i=1}^{n}\frac{b_i^2}{a_i}\right)\left(\sum_{i=1}^{n}a_iy_i^2\right),\end{aligned}$$

所以

$$Q(y_1,\dots,y_n)=\sum_{i=1}^{n}a_iy_i^2\ge\left(\sum_{i=1}^{n}\frac{b_i^2}{a_i}\right)^{-1}=m.$$

由 Cauchy-Schwarz 不等式的取等条件知, $Q(y_1,\dots,y_n)=m$ 当且仅当存在实数 t 使得

$$\sqrt{a_i}y_i=t\frac{b_i}{\sqrt{a_i}},\qquad i=1,\dots,n,$$

即 $y_i=b_it/a_i$, 由条件 $b_1y_1+\cdots+b_ny_n=1$ 知

$$1=\sum_{i=1}^{n}b_iy_i=t\sum_{i=1}^{n}\frac{b_i^2}{a_i}=\frac{t}{m},$$

则有 $t=m$, 所以二次型 Q 取极小值 m 当且仅当

$$y_i=\frac{mb_i}{a_i},\qquad i=1,\dots,n.$$

□

定理 18. 设 $A=\{a(n)\}_{n=1}^{\infty}$ 是一列非负实数列, 并且 $|A|=\sum_{n=1}^{\infty}a(n)$ 收敛, 设 $\mathcal{P}$ 是一些素数组成的集合, 对 $z\ge2$, 定义

$$P(z)=\prod_{\substack{p\in\mathcal{P}\\p<z}}p,\qquad S(A,\mathcal{P},z)=\sum_{(n,P(z))=1}a(n).$$

设 $g(d)$ 是完全乘性函数, 它在每个 $\mathcal{P}$ 中素数 p 上的值满足 $0<g(p)<1$, 定义 $|A_d|=\sum_{d|n}a(n)$, $r(d)=|A_d|-\sum_{n=1}^{\infty}a(n)g(d)$,

$$G(z)=\sum_{\substack{m<z\\p|m\Rightarrow p\in\mathcal{P}}}g(m),$$

则

$$S(A,\mathcal{P},z)\le\frac{|A|}{G(z)}+\sum_{\substack{d<z^2\\d|P(z)}}3^{\omega(d)}|r(d)|.$$

证明. 令 $z\ge2$, 对 $P(z)$ 的每个因子 d, 设 λ_d 为实数, 满足 $\lambda_1=1$, $d\ge z$ 时 $\lambda_d=0$, 显然

$$\left(\sum_{d|(n,P(z))}\lambda_d\right)^2\ge0,$$

并且当 $(n,P(z))=1$ 时

$$\left(\sum_{d|(n,P(z))}\lambda_d\right)^2=1,$$

所以

$$\begin{aligned}
S(A,\mathcal{P},z)&=\sum_{(n,P(z))=1}a(n)\\
&\le\sum_{n\ge1}a(n)\left(\sum_{\substack{d|n\\ d|P(z)}}\lambda_d\right)^2\\
&=\sum_{n\ge1}a(n)\sum_{\substack{d_1|n,\ d_1|P(z)\\ d_2|n,\ d_2|P(z)}}\lambda_{d_1}\lambda_{d_2}\\
&=\sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\sum_{\substack{n\ge1\\ [d_1,d_2]|n}}a(n)\\
&=\sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}|A_{[d_1,d_2]}|\\
&=\sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\left(g([d_1,d_2])|A|+r([d_1,d_2])\right)\\
&=|A|\sum_{d_1,d_2|P(z)}g([d_1,d_2])\lambda_{d_1}\lambda_{d_2}+\sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}r([d_1,d_2])\\
&=|A|\sum_{\substack{d_1,d_2<z\\ d_1,d_2|P(z)}}\frac{g(d_1)\lambda_{d_1}g(d_2)\lambda_{d_2}}{g((d_1,d_2))}+\sum_{\substack{d_1,d_2<z\\ d_1,d_2|P(z)}}\lambda_{d_1}\lambda_{d_2}r([d_1,d_2]),
\end{aligned}$$

最后一步是因为 $d_1d_2=(d_1,d_2)[d_1,d_2]$ 以及当 $d\ge z$ 时 $\lambda_d=0$. 以下设

$$Q=\sum_{\substack{d_1,d_2<z\\ d_1,d_2|P(z)}}\frac{g(d_1)\lambda_{d_1}g(d_2)\lambda_{d_2}}{g((d_1,d_2))},\qquad R=\sum_{\substack{d_1,d_2<z\\ d_1,d_2|P(z)}}\lambda_{d_1}\lambda_{d_2}r([d_1,d_2]).$$

设

$$\mathcal{D}_z=\{k:k\mid P(z)\,,1\le k<z\},$$

定义算术函数 f 为

$$f(1)=1,\qquad f(p)=\frac{1-g(p)}{g(p)},$$

并按完全乘性延拓到正整数集上, 由 $g(p)<1$ 知 $f(k)>0$, 对每个 $k\in\mathcal{D}_z$, 有

$$f(k)=\frac{1}{g(k)}\prod_{p|k}(1-g(p))=\frac{1}{g(k)}\sum_{d|k}\mu(d)g(d)=\sum_{d|k}\frac{\mu(d)}{g(k/d)},$$

所以由 Möbius 反演知

$$\frac{1}{g(k)}=\sum_{d|k}f(d),\qquad k\in\mathcal{D}_z,$$

则

$$\begin{aligned} Q &= \sum_{d_1,d_2\in\mathcal{D}_z} g(d_1)\lambda_{d_1} g(d_2)\lambda_{d_2} \sum_{\substack{k\mid d_1\\ k\mid d_2}} f(k) \\ &= \sum_{k\in\mathcal{D}_z} f(k) \left(\sum_{\substack{d\in\mathcal{D}_z\\ k\mid d}} g(d)\lambda_d \right)^2 \\ &= \sum_{k\in\mathcal{D}_z} f(k) y_k^2, \end{aligned}$$

其中

$$y_k = \sum_{\substack{d\in\mathcal{D}_z\\ k\mid d}} g(d)\lambda_d,$$

则 Q 就是一个关于 y_k 的二次型, 由 Möbius 反演得

$$g(d)\lambda_d = \sum_{\substack{k\in\mathcal{D}_z\\ d\mid k}} \mu\left(\frac{k}{d}\right) y_k,$$

取 $d=1$ 即得

$$\sum_{k\in\mathcal{D}_z} \mu(k) y_k = 1,$$

所以二次型 Q 有极小值

$$\left(\sum_{k\in\mathcal{D}_z} \frac{\mu(k)^2}{f(k)} \right)^{-1} = \left(\sum_{k\in\mathcal{D}_z} \frac{1}{f(k)} \right)^{-1},$$

下设

$$\sum_{k\in\mathcal{D}_z} \frac{1}{f(k)} = F(z),$$

而

$$\begin{aligned} F(z) = \sum_{k\in\mathcal{D}_z} \frac{1}{f(k)} &= \sum_{k\in\mathcal{D}_z} g(k) \prod_{p\mid k} (1-g(p))^{-1} \\ &= \sum_{k\in\mathcal{D}_z} g(k) \prod_{p\mid k} \sum_{r=0}^{\infty} g(p^r) \\ &= \sum_{k\in\mathcal{D}_z} g(k) \sum_{\substack{\ell=1\\ p\mid\ell\Rightarrow p\mid k}}^{\infty} g(\ell) \\ &= \sum_{k\in\mathcal{D}_z} \sum_{\substack{\ell=1\\ p\mid\ell\Rightarrow p\mid k}}^{\infty} g(k\ell) \\ &= \sum_{k\in\mathcal{D}_z} \sum_{\substack{m=1\\ k\mid m\\ p\mid(m/k)\Rightarrow p\mid k}}^{\infty} g(m) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{m=1}^{\infty} g(m) \left(\sum_{\substack{k\in\mathcal{D}_z \\ k\mid m \\ p\mid(m/k)\Rightarrow p\mid k}} 1 \right) \\
&\geq \sum_{\substack{m<z \\ p\mid m\Rightarrow p\in\mathcal{P}}} g(m) \left(\sum_{\substack{k\in\mathcal{D}_z \\ k\mid m \\ p\mid(m/k)\Rightarrow p\mid k}} 1 \right) \\
&\geq \sum_{\substack{m<z \\ p\mid m\Rightarrow p\in\mathcal{P}}} g(m) \\
&= G(z),
\end{aligned}
$$

因此可选取诸 λ_d 使得

$$
Q = \frac{1}{F(z)} \leq \frac{1}{G(z)}.
$$

接下来估计 R, 我们考虑 Q 取到极小值 $1/F(z)$ 的条件为

$$
y_k = \frac{\mu(k)}{F(z)f(k)},
$$

由此及

$$
g(d)\lambda_d = \sum_{\substack{k\in\mathcal{D}_z \\ d\mid k}} \mu\left(\frac{k}{d}\right) y_k,
$$

可反解出

$$
\begin{aligned}
\lambda_d = \frac{\mu(d)}{g(d)} \sum_{\substack{k\in\mathcal{D}_z \\ d\mid k}} \mu(k)y_k &= \frac{\mu(d)}{g(d)} \sum_{\substack{d\ell<z \\ d\ell\mid P(z)}} \mu(d\ell)y_{d\ell} \\
&= \frac{\mu(d)}{g(d)} \sum_{\substack{\ell<z/d \\ d\ell\mid P(z)}} \mu(d\ell) \left(\frac{\mu(d\ell)}{F(z)f(d\ell)} \right) \\
&= \frac{\mu(d)}{f(d)g(d)F(z)} \sum_{\substack{\ell<z/d \\ d\ell\mid P(z)}} \frac{1}{f(\ell)} \\
&= \frac{\mu(d)F_d(z)}{f(d)g(d)F(z)},
\end{aligned}
$$

其中

$$
F_d(z) = \sum_{\substack{\ell<z/d \\ d\ell\mid P(z)}} \frac{1}{f(\ell)}.
$$

固定 $d \mid P(z)$, 因为

$$
F(z) = \sum_{k\in\mathcal{D}_z} \frac{1}{f(k)} = \sum_{\ell\mid d} \sum_{\substack{k\in\mathcal{D}_z \\ (k,d)=\ell}} \frac{1}{f(k)}
$$

$$
\begin{aligned}
&= \sum_{\ell|d} \sum_{\substack{\ell m<z \\ \ell m|P(z) \\ (\ell m,d)=\ell}} \frac{1}{f(\ell m)} \\
&= \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/\ell \\ \ell m|P(z) \\ (m,d/\ell)=1}} \frac{1}{f(m)} \\
&= \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/\ell \\ m|P(z) \\ (m,d)=1}} \frac{1}{f(m)} \\
&= \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/\ell \\ dm|P(z)}} \frac{1}{f(m)} \\
&\geq \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/d \\ dm|P(z)}} \frac{1}{f(m)} \\
&= F_d(z) \sum_{\ell|d} \frac{1}{f(\ell)} \\
&= \frac{F_d(z)}{f(d)} \sum_{\ell|d} f(d/\ell) \\
&= \frac{F_d(z)}{f(d)g(d)},
\end{aligned}
$$

所以

$$
|\lambda_d| = \frac{F_d(z)}{f(d)g(d)F(z)} \leq 1,
$$

由此即得 R 的估计

$$
|R| = \left| \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} \lambda_{d_1}\lambda_{d_2} r([d_1,d_2]) \right| \leq \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} |r([d_1,d_2])|,
$$

而当 d 是无平方因子数时, 使得 $[d_1,d_2]=d$ 的有序对 d_1,d_2 的解数为

$$
\binom{\omega(d)}{0}2^0 + \binom{\omega(d)}{1}2^1 + \cdots + \binom{\omega(d)}{\omega(d)}2^{\omega(d)} = 3^{\omega(d)},
$$

所以

$$
|R| \leq \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} |r([d_1,d_2])| \leq \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)|,
$$

综上可得

$$
S(A,\mathcal{P},z) \leq |A|Q + R \leq \frac{|A|}{G(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)|,
$$

定理得证. □

使用 Selberg 筛法可以得到比 Brun 筛法更强的结果.

定理 19. 设 N 是一个正偶数, 定义 $r_2(N)$ 为将 N 表示为两个素数的和的方法数, 则

$$r_2(N) \ll \frac{N}{(\log N)^2} \prod_{p|N} \left(1+\frac{1}{p}\right),$$

设 x 是正实数, 定义 $\pi_N(x)$ 为不超过 x 的使得 $p+N$ 也为素数的素数 p 的个数, 则

$$\pi_N(x) \ll \frac{x}{(\log x)^2} \prod_{p|N} \left(1+\frac{1}{p}\right).$$

证明. 先证关于 $r_2(N)$ 的断言, 设 $A=\{n(N-n): 1\le n<N\}$, $\mathcal{P}$ 为全体素数组成的集合, $z=N^{1/8}$, 则 $|A|=N/2$,

$$r_2(N) \le 2N^{1/8} + 2S(A,\mathcal{P},z),$$

取

$$g(p)=\begin{cases} \dfrac{1}{p}, & p \mid N, \\ \dfrac{2}{p}, & p \nmid N \end{cases}$$

并按完全乘性延拓, 则由 Selberg 筛法知

$$S(A,\mathcal{P},z) \le \frac{|A|}{G(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)|, \qquad G(z)=\sum_{m<z} g(m).$$

对于余项, 设 $\rho(d)$ 为满足同余方程 $n(N-n)\equiv 0 \pmod d$ 的同余类个数, 若 $d \mid P(z)$, 则显然

$$\rho(d)=\prod_{p|d}\rho(p),$$

而

$$\rho(p)=\begin{cases} 1, & p \mid N, \\ 2, & p \nmid N, \end{cases}$$

所以 $\rho(d)\le 2^{\omega(d)}$, 由于在 $1\le n\le N/2$ 这 $N/2$ 个数中属于某模 d 的同余类的个数与 $N/(2d)$ 的差小于 1, 所以将满足同余方程 $n(N-n)\equiv 0 \pmod d$ 的 $\rho(d)$ 个同余类加起来就得到

$$|A_d| = \frac{N\rho(d)}{2d} + r(d) = |A|g(d) + r(d),$$

其中 $|r(d)|\le \rho(d)\le 2^{\omega(d)}$, 于是由 $2^{\omega(d)}\le d$ 知

$$3^{\omega(d)}|r(d)| \le 6^{\omega(d)} \le d^{\log 6/\log 2},$$

所以

$$\sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)| \le \sum_{\substack{d<z^2 \\ d|P(z)}} d^{\log 6/\log 2} \le z^{2+2\log 6/\log 2} < z^{7.2} = N^{9/10}.$$

对于主项, 我们来估计 $G(z)$, 对每个正整数 $m<z$, 都可以分解为 $m=u_mv_m$, 其中 u_m 的素因子均为 N 的素因子, 而 v_m 与 N 互素, 那么显然 $g(m)=2^{\Omega(v_m)}/m$, 又易证 $2^{\Omega(v_m)}\geq d(v_m)$, 所以

$$G(z)=\sum_{m<z}g(m)\geq\sum_{m<z}\frac{d(v_m)}{m},$$

因为

$$\prod_{p|N}\left(1-\frac{1}{p}\right)^{-1}=\sum_{\substack{t=1\\p|t\Rightarrow p|N}}\frac{1}{t},$$

则有

$$\prod_{p|N}\left(1-\frac{1}{p}\right)^{-1}G(z)\geq\sum_{m<z}\frac{d(v_m)}{m}\sum_{\substack{t=1\\p|t\Rightarrow p|N}}^{\infty}\frac{1}{t}=\sum_{\substack{m<z\\t\geq1\\p|t\Rightarrow p|N}}\frac{d(v_m)}{mt}\geq\sum_{\substack{mt<z\\p|t\Rightarrow p|N}}\frac{d(v_m)}{mt},$$

设 $k=mt$, 将上式右边和式按 k 重新求和, 因为 $p|t\Rightarrow p|N$, 所以 $u_k=tu_m$, $v_k=v_m$, 故 $d(v_m)/mt$ 变为 $d(v_k)/k$, 而和式中等于 $d(v_k)/k$ 的共有 $d(u_k)$ 项, 所以

$$\sum_{\substack{mt<z\\p|t\Rightarrow p|N}}\frac{d(v_m)}{mt}=\sum_{k<z}\frac{d(u_k)d(v_k)}{k}=\sum_{k<z}\frac{d(k)}{k},$$

由 Dirichlet 除数定理

$$\sum_{k<z}d(k)=z\log z+(2\gamma-1)z+O(z^{1/2})$$

配合 Abel 求和法即得

$$\sum_{k<z}\frac{d(k)}{k}=\frac{(\log z)^2}{2}+O(\log z),$$

所以

$$\prod_{p|N}\left(1-\frac{1}{p}\right)^{-1}G(z)\gg(\log z)^2\gg(\log N)^2,$$

于是主项有上界

$$\begin{aligned}\frac{|A|}{G(z)}&\ll\frac{N}{2(\log N)^2}\prod_{p|N}\left(1-\frac{1}{p}\right)^{-1}\\&=\frac{N}{2(\log N)^2}\prod_{p|N}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p|N}\left(1+\frac{1}{p}\right)\\&\leq\zeta(2)\frac{N}{2(\log N)^2}\prod_{p|N}\left(1+\frac{1}{p}\right)\\&\ll\frac{N}{2(\log N)^2}\prod_{p|N}\left(1+\frac{1}{p}\right),\end{aligned}$$

综上有

$$r_2(N)\ll2N^{1/8}+\frac{N}{(\log N)^2}\prod_{p|N}\left(1+\frac{1}{p}\right)+N^{9/10}\ll\frac{N}{(\log N)^2}\prod_{p|N}\left(1+\frac{1}{p}\right).$$

再证关于 $\pi_N(x)$ 的断言, 设 $B=\{n(n+N):1\leq n\leq x\}$, $\mathcal{P}$ 为全体素数组成的集合, $z=x^{1/8}$, 则 $|B|=[x]$,

$$\pi_N(x)\leq x^{1/8}+S(B,\mathcal{P},z),$$

取

$$g(p)=\begin{cases}\dfrac{1}{p}, & p\mid N,\\[2ex] \dfrac{2}{p}, & p\nmid N\end{cases}$$

并按完全乘性延拓, 则由 Selberg 筛法知

$$S(B,\mathcal{P},z)\leq\frac{x}{G(z)}+\sum_{\substack{d<z^2\\ d\mid P(z)}}3^{\omega(d)}|r(d)|,\qquad G(z)=\sum_{m<z}g(m),$$

由此前关于 $r_2(N)$ 的讨论立刻得到

$$\pi_N(x)\ll x^{1/8}+\frac{x}{(\log x)^2}\prod_{p\mid N}\left(1+\frac{1}{p}\right)+x^{9/10}\ll\frac{x}{(\log x)^2}\prod_{p\mid N}\left(1+\frac{1}{p}\right),$$

定理得证. □

作为推论, 取 $N=2$ 即得不超过 x 的孪生素数对的数量的上界

$$\pi_2(x)\ll\frac{x}{(\log x)^2},$$

这比 Brun 的结果少了分子上的 $(\log\log x)^2$.

2.6 大筛法

筛法可分为小筛法与大筛法, 通常所说的筛法总是指小筛法, 因为大筛法与此前介绍的所有筛法都有本质区别, 但大筛法本身仍然是十分重要的, 在陈景润定理的证明中也用到了它.

设 M 和 N 是任意的两个正整数, $M+1$ 到 $M+N$ 是 N 个正整数, $\mathscr{P}$ 是一个素数集, 这里我们要求它是一个有限集, 并且其中的素数都不超过正整数 Q. 与小筛法相同, 我们想要将 $M+1$ 到 $M+N$ 这 N 个数中满足一些同余条件的数筛掉, 例如, 设 $p\in\mathscr{P}$, $1\leq\rho(p)\leq p-1$, $k_1,\ldots,k_{\rho(p)}$ 是模 p 的 $\rho(p)$ 个同余类, 当 n 满足 $n\equiv k_i\pmod p$ 对某个 i 成立时, 就将 n 去掉, 将剩余的集合记为 E, 则 $E\subseteq(M,M+N]$, 大筛法就是要得到 $Z=|E|$ 的上界估计.

不同于小筛法将 $Z=|E|$ 逐素数分拆为主项和误差项, 大筛法通过不同的方法得到一个精确的上界. 实践表明, 在小筛法中, 一般需要 $\rho(p)$ 是比较小的数时才能得到比较好的估计, 例如此前我们只使用过 $\rho(p)=1$ 或 2, 而在大筛法中得到的上界无论 $\rho(p)$ 取多少都是成立的, 这就是大筛法中大字的来源.

设 a_n 为集合 E 的指示函数

$$a_n=\begin{cases}1, & n\in E,\\ 0, & n\notin E,\end{cases}$$

则

$$Z=\sum_{n=1}^{\infty}a_n,$$

设

$$Z(q,j)=\sum_{n\equiv j\pmod q}a_n,$$

它表示 E 中模 q 同余于 j 的数的个数, 假设 E 中的数在模 q 的诸同余类中分布是均匀的, 那么 $Z(q,j)$ 就应该大约是 Z/q, 再定义某种 "方差" 为

$$D(q)=\sum_{j=0}^{q-1}\left(Z(q,j)-\frac{Z}{q}\right)^2,$$

再设

$$S(x)=\sum_{n=M+1}^{M+N}a_n e(nx),$$

显然 $S(0)=Z$, Bombieri 注意到关系式

$$pD(p)=\sum_{a=1}^{p-1}\left|S\left(\frac{a}{p}\right)\right|^2,$$

我们证明一个更一般的关系式.

引理 35. *符号如上, 有关系式*

$$\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2=\frac{1}{q}\sum_{j=1}^{q}\left|\sum_{d|q}\frac{\mu(d)q}{d}Z\left(\frac{q}{d},j\right)\right|^2$$

对所有正整数 q 成立, 当 q 取素数 p 时即得

$$pD(p)=\sum_{a=1}^{p-1}\left|S\left(\frac{a}{p}\right)\right|^2.$$

证明. 设

$$f_j(x)=S(x)e(-jx),\qquad F_j(q)=\sum_{a=1}^{q}f_j\left(\frac{a}{q}\right),\qquad F_j^*(q)=\sum_{\substack{a=1\\(a,q)=1}}^{q}f_j\left(\frac{a}{q}\right),$$

将 $F_j(q)$ 中的 a/q 约分, 并按分母分类即得

$$F_j(q)=\sum_{d|q}\sum_{\substack{a=1\\(a,d)=1}}^{d}f_j\left(\frac{a}{d}\right)=\sum_{d|q}F_j^*(d),$$

再由 Möbius 反演得

$$F_j^*(q)=\sum_{d|q}\mu(d)F_j\left(\frac{q}{d}\right),$$

而

$$F_j(q)=\sum_{a=1}^{q}S\left(\frac{a}{q}\right)e\left(-\frac{ja}{q}\right)=\sum_{a=1}^{q}\sum_{n=M+1}^{M+N}a_ne\left(\frac{a(n-j)}{q}\right)=q\sum_{n\equiv j\pmod q}a_n=qZ(q,j),$$

$$\sum_{j=1}^{q}|F_j^*(q)|^2=\sum_{j=1}^{q}\left|\sum_{\substack{a=1\\(a,q)=1}}^{q}S\left(\frac{a}{q}\right)e\left(-\frac{ja}{q}\right)\right|^2=q\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2,$$

所以

$$\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2=\frac{1}{q}\sum_{j=1}^{q}|F_j^*(q)|^2=\frac{1}{q}\sum_{j=1}^{q}\left|\sum_{d|q}\frac{\mu(d)q}{d}Z\left(\frac{q}{d},j\right)\right|^2,$$

当 q 取素数 p 时, 等式左边就是

$$\sum_{a=1}^{p-1}\left|S\left(\frac{a}{p}\right)\right|^2,$$

等式右边就是

$$\frac{1}{p}\sum_{j=1}^{p}|pZ(p,j)-Z(1,j)|^2=p\sum_{j=1}^{p}\left|Z(p,j)-\frac{Z}{p}\right|^2=pD(p),$$

引理得证. □

由此可见研究形如

$$\sum_i S(x_i)$$

的和式对于 Z 的估计是有帮助的, 这就导致所谓大筛法的分析形式.

2.6.1 大筛法的分析形式

设 $x_1,x_2,\dots,x_R$ 是一组实数, 满足

$$\min_{i\neq j}\|x_i-x_j\|=\delta>0,$$

大筛法的分析形式就是要得到形如

$$\sum_{r=1}^{R}|S(x_r)|^2\leq\Delta(N,\delta)\sum_{n=M+1}^{M+N}|a_n|^2$$

的不等式, 其中 $\Delta(N,\delta)$ 是只关于 N 和 δ 的正常数, 数列 a_n 未必是集合 E 的指示函数, 而可以是任意复数列. $\Delta(N,\delta)=N+\delta^{-1}-1$ 是最优系数, 后面将会构造出恰好取等号的例子. 本节我们介绍 Selberg 使用 Bessel 不等式得到的证明, 为方便, 我们假设

$$\begin{cases}0\leq x_1<x_2<\cdots<x_R<1,\\ x_{r+1}-x_r\geq\delta,\qquad 1\leq r\leq R-1,\\ x_1+1-x_R\geq\delta,\end{cases}$$

显然必须有 $R\leq[\delta^{-1}]$. 在实践中, 经常取诸 x_r 为 Farey 分数列.

引理 36. 设 $\Phi_1,\dots,\Phi_R$ 和 ξ 是内积空间中的任意 $R+1$ 个向量, 设

$$A=\max_{1\le r\le R}\sum_{s=1}^{R}|(\Phi_r,\Phi_s)|,$$

则

$$\sum_{r=1}^{R}|(\Phi_r,\xi)|^2\le A\|\xi\|^2.$$

证明. 设 $u_1,\dots,u_R$ 是任意的 R 个复数, 由 $2|u_r\overline{u_s}|\le|u_r|^2+|u_s|^2$ 及 $|(\Phi_r,\Phi_s)|=|(\Phi_s,\Phi_r)|$ 得

$$\begin{aligned}\left|\sum_{1\le r,s\le R}u_r\overline{u_s}(\Phi_r,\Phi_s)\right|&\le\sum_{1\le r,s\le R}|u_r\overline{u_s}|\,|(\Phi_r,\Phi_s)|\\&\le\frac{1}{2}\sum_{1\le r,s\le R}\big(|u_r|^2+|u_s|^2\big)|(\Phi_r,\Phi_s)|\\&=\sum_{1\le r,s\le R}|u_r|^2|(\Phi_r,\Phi_s)|\\&=\sum_{r=1}^{R}|u_r|^2\sum_{s=1}^{R}|(\Phi_r,\Phi_s)|\\&\le A\sum_{r=1}^{R}|u_r|^2,\end{aligned}$$

注意到

$$\begin{aligned}0\le\left\|\xi-\sum_{r=1}^{R}u_r\Phi_r\right\|^2&=\|\xi\|^2-2\,\mathrm{Re}\sum_{r=1}^{R}\overline{u_r}(\Phi_r,\xi)+\sum_{1\le r,s\le R}u_r\overline{u_s}(\Phi_r,\Phi_s)\\&\le\|\xi\|^2-2\,\mathrm{Re}\sum_{r=1}^{R}\overline{u_r}(\Phi_r,\xi)+A\sum_{r=1}^{R}|u_r|^2,\end{aligned}$$

取 $u_r=\dfrac{(\Phi_r,\xi)}{A}$, 则

$$\mathrm{Re}\sum_{r=1}^{R}\overline{u_r}(\Phi_r,\xi)=\frac{1}{A}\sum_{r=1}^{R}\big|(\Phi_r,\xi)\big|^2,\qquad A\sum_{r=1}^{R}|u_r|^2=\frac{1}{A}\sum_{r=1}^{R}\big|(\Phi_r,\xi)\big|^2,$$

代入得

$$0\le\|\xi\|^2-\frac{1}{A}\sum_{r=1}^{R}\big|(\Phi_r,\xi)\big|^2,$$

即

$$\sum_{r=1}^{R}\big|(\Phi_r,\xi)\big|^2\le A\|\xi\|^2,$$

引理得证. □

当诸 Φ_r 正交时, 该不等式就是 Bessel 不等式.

我们取内积空间为 $\ell^2(\mathbb{Z})$

$$\ell^2(\mathbb{Z}) = \left\{ (b_n)_{n\in\mathbb{Z}} : \sum_{n=-\infty}^{\infty} |b_n|^2 < \infty \right\},$$

任取 $(b_n) \in \ell^2(\mathbb{Z})$, 满足 $b_n \geq 0$, 并且当 $M+1 \leq n \leq M+N$ 时, $b_n > 0$, 再取

$$\xi_n = \begin{cases} a_n b_n^{-1/2}, & M+1 \leq n \leq M+N, \\ 0, & \text{其他}, \end{cases}$$

$$\Phi_r = (\Phi_{r,n}), \qquad \Phi_{r,n} = b_n^{1/2} e(-nx_r),$$

则由引理得

$$\sum_{r=1}^{R} |S(x_r)|^2 \leq B \sum_{n=M+1}^{M+N} |a_n|^2 b_n^{-1},$$

其中

$$B = \max_{1\leq r\leq R} \sum_{1\leq s\leq R} \left| \sum_{n=-\infty}^{\infty} b_n e(n(x_s - x_r)) \right|.$$

接下来就是构造 b_n.

引理 37. 设

$$F(z) = \left(\frac{\sin \pi z}{\pi}\right)^2 \left(\sum_{n\geqslant 0} \frac{1}{(z-n)^2} - \sum_{n\geqslant 1} \frac{1}{(z+n)^2} + \frac{2}{z} \right),$$

则 $F(z)$ 是一个整函数, 且 $F(0) = 1$, $F(x+iy) \ll e^{2\pi|y|}$, 限制在实数域上时有 $F(x) \geq \operatorname{sgn}(x)$,

$$\int_{-\infty}^{\infty} F(x) - \operatorname{sgn}(x)\, \mathrm{d}x = 1,$$

其中 $\operatorname{sgn}(x)$ 为符号函数.

证明. F 的可能奇点只在整数点 $\mathbb{Z}$ 处, 无论哪一点, 前一个括号内有一个二阶零点, 后一个括号内有一个二阶极点, 因此 F 在全平面全纯. 在 $z = 0$ 附近,

$$F(0) = \lim_{z\to 0} \left(z^2 + O(z^4)\right) \left(\frac{1}{z^2} + \frac{2}{z} + O(1) \right) = 1.$$

由于

$$|\sin \pi(x+iy)|^2 = \sin^2(\pi x) + \sinh^2(\pi y) \leq \cosh^2(\pi y) \ll e^{2\pi|y|},$$

而当 $|y| \geq 1$ 时, 对任意 $n \in \mathbb{Z}$ 有 $|z \pm n|^2 = (x \pm n)^2 + y^2 \geq y^2 \geq 1$, 所以

$$\left| \sum_{n\geq 0} \frac{1}{(z-n)^2} \right| \leq \sum_{n=0}^{\infty} \frac{1}{(x-n)^2 + y^2} \ll \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{t^2 + y^2} = \frac{\pi}{|y|} \leqslant \pi,$$

$$\left|\sum_{n\geq 1}\frac{1}{(z+n)^2}\right| \leq \sum_{n=1}^{\infty}\frac{1}{(x+n)^2+y^2} \ll \int_{-\infty}^{\infty}\frac{\mathrm{d}t}{t^2+y^2} = \frac{\pi}{|y|} \leqslant \pi,$$

$$\left|\frac{2}{z}\right| \leq 2,$$

因此,

$$F(x+iy) \ll e^{2\pi|y|}\cdot O(1) \ll e^{2\pi|y|}.$$

注意到当 $x>0$ 时,

$$\sum_{n\geqslant 1}\frac{1}{(x+n)^2} \leqslant \int_x^{\infty}\frac{\mathrm{d}u}{u^2} = \frac{1}{x} \leqslant \sum_{n\geqslant 0}\frac{1}{(x+n)^2},$$

所以

$$\frac{1}{x}-\sum_{n\geqslant 1}\frac{1}{(x+n)^2} \geqslant 0, \qquad \sum_{n\geqslant 0}\frac{1}{(x+n)^2}-\frac{1}{x} \geqslant 0,$$

熟知

$$\left(\frac{\sin\pi z}{\pi}\right)^2\sum_{n\in\mathbb{Z}}\frac{1}{(z-n)^2} = 1,$$

所以当 $x>0$ 时有

$$F(x) = \left(\frac{\sin\pi x}{\pi}\right)^2\left\{\sum_{n\in\mathbb{Z}}\frac{1}{(x-n)^2}-2\sum_{n\geqslant 1}\frac{1}{(x+n)^2}+\frac{2}{x}\right\} \geq 1,$$

而当 $x<0$ 时, 设 $y=-x$, 则

$$F(x) = \left(\frac{\sin\pi x}{\pi}\right)^2\left\{-\sum_{n\in\mathbb{Z}}\frac{1}{(x-n)^2}+2\sum_{n\geqslant 0}\frac{1}{(y+n)^2}-\frac{2}{y}\right\} \geq -1,$$

而 $F(0)=1>0=\operatorname{sgn}(0)$, 故 $F(x)\geq\operatorname{sgn}(x)$.

最后,

$$\begin{aligned}
\int_{-\infty}^{+\infty}F(x)-\operatorname{sgn}(x)\mathrm{d}x &= \int_0^{\infty}F(x)-1\,\mathrm{d}x+\int_0^{\infty}F(-y)+1\,\mathrm{d}y\\
&= \int_0^{\infty}F(x)+F(-x)\,\mathrm{d}x\\
&= \int_0^{\infty}\left(\frac{\sin\pi x}{\pi}\right)^2\cdot\frac{2}{x^2}\,\mathrm{d}x\\
&= 2\int_0^{\infty}\left(\frac{\sin\pi x}{\pi x}\right)^2\,\mathrm{d}x\\
&= 1
\end{aligned}$$

引理得证. □

定理 20 (大筛法不等式)**.** 设 M 和 N 是任意整数, $N \geq 1$, a_n 是任意复数列,

$$S(x) = \sum_{n=M+1}^{M+N} a_n e(nx),$$

再设 $x_1, x_2, \ldots, x_R$ 是一组实数, 满足

$$\min_{i \neq j} \|x_i - x_j\| = \delta > 0,$$

则

$$\sum_{r=1}^{R} |S(x_r)|^2 \leq (N + \delta^{-1} - 1) \sum_{n=M+1}^{M+N} |a_n|^2.$$

证明. 设

$$b(t) = \frac{1}{2}\Big(F(\delta(t - M - 1)) + F(\delta(M + N - t))\Big), \quad t \in \mathbb{R},$$

并取 $b_n = b(n)$, $n \in \mathbb{Z}$.

首先, 对任意 n, $M+1 \leq n \leq M+N$, 有 $\delta(n-M-1) \geq 0$ 且 $\delta(M+N-n) \geq 0$, 由 $F(x) \geq \operatorname{sgn}(x)$ 和 $F(0) = 1$ 知对所有 $M + 1 \leq n \leq M + N$, 均有 $b_n \geq 1$. 其次, 对任意 $t \in \mathbb{R}$, $\delta(n - M - 1)$ 和 $\delta(M + N - n)$ 不可能同时为负, 所以必然有 $b(t) \geq 0$ 对任意 $t \in \mathbb{R}$ 恒成立.

接下来计算

$$B = \max_{1 \leq r \leq R} \sum_{1 \leq s \leq R} \left| \sum_{n=-\infty}^{\infty} b_n e(n(x_s - x_r)) \right|,$$

由 Poisson 求和公式知

$$\sum_{n=-\infty}^{\infty} b(n) e(n\theta) = \sum_{k=-\infty}^{\infty} \widehat{b}(\theta + k),$$

其中 $\widehat{b}(y)$ 为 $b(t)$ 的傅里叶变换, θ 为任意实数. 因为 $F(x + iy) \ll e^{2\pi|y|}$, 由 Paley-Wiener 定理知, F 的傅里叶变换 $\widehat{F}(y)$ 的支集满足 $\operatorname{supp}(\widehat{F}) \subseteq [-1, 1]$, 由此可知 $b(t)$ 的傅里叶变换满足

$$\operatorname{supp}(\widehat{b}) \subseteq [-\delta, \delta],$$

由 $b(t)$ 的定义知

$$\begin{aligned} b(t) = \mathbf{1}_{[M+1, M+N]}(t) &+ \frac{1}{2}(F(\delta(t - M - 1)) - \operatorname{sgn}(\delta(t - M - 1))) \\ &+ \frac{1}{2}(F(\delta(M + N - t)) - \operatorname{sgn}(\delta(M + N - t))) \end{aligned}$$

在 $t \neq M + 1, M + N$ 时成立, 所以在勒贝格积分意义下有

$$\widehat{b}(0) = \int_{-\infty}^{\infty} b(t)\,\mathrm{d}t = N - 1 + \frac{1}{\delta}\int_{-\infty}^{\infty} F(u) - \operatorname{sgn}(u)\,\mathrm{d}u = N + \delta^{-1} - 1.$$

现考虑

$$\sum_{n=-\infty}^{\infty} b(n) e(n(x_s - x_r)),$$

当 $r=s$ 时, $\theta=0$, 因 $\delta=\min_{i\neq j}\|x_i-x_j\|\leq 1/2$, 在 $\sum\widehat{b}(k)$ 中, 仅 $k=0$ 落在支集 $[-\delta,\delta]$ 中, 其余项均等于 0, 故

$$\sum_{n=-\infty}^{\infty} b_n=\widehat{b}(0)=N+\delta^{-1}-1.$$

当 $r\neq s$ 时, 设 $\theta=x_s-x_r$, 由条件 $\|\theta\|=\|x_s-x_r\|\geq\delta$ 知, 对任意 $k\in\mathbb{Z}$ 均有 $|\theta+k|\geq\min_{k\in\mathbb{Z}}|\theta+k|=\|\theta\|\geq\delta$, 因此

$$\sum_{n=-\infty}^{\infty} b_n e(n(x_s-x_r))=0.$$

所以对任意 $1\leq r\leq R$, 都有

$$\sum_{s=1}^{R}\left|\sum_{n=-\infty}^{\infty} b_n e(n(x_s-x_r))\right|=\widehat{b}(0)=N+\delta^{-1}-1,$$

即 $B=N+\delta^{-1}-1$.

代入此前得到的不等式即得

$$\sum_{r=1}^{R}|S(x_r)|^2\leq(N+\delta^{-1}-1)\sum_{n=M+1}^{M+N}|a_n|^2b_n^{-1}\leq(N+\delta^{-1}-1)\sum_{n=M+1}^{M+N}|a_n|^2.$$

定理得证. □

例 7. 该例子说明大筛法不等式已是最优的. 令 $R\geq 2$, $x_r=r/R$, $r=0,1,\ldots,R-1$, 则 $\delta=1/R$, 设 $M=0$, $N=R+1$, $a_1=a_{R+1}=1$, 其余 a_n 均为 0, 则 $S(x)=e(x)+e((R+1)x)$,

$$S\left(\frac{r}{R}\right)=e\left(\frac{r}{R}\right)+e\left(\frac{r}{R}\right)e(r)=2e\left(\frac{r}{R}\right),$$

所以

$$\sum_{r=1}^{R}|S(x_r)|^2=4R,$$

而

$$\sum_{n=1}^{R+1}|a_n|^2=2,$$

且 $N+\delta^{-1}-1=R+1+R-1=2R$, 所以

$$\sum_{r=1}^{R}|S(x_r)|^2=4R=(N+\delta^{-1}-1)\sum_{n=1}^{R+1}|a_n|^2,$$

等号成立.

2.6.2 大筛法的算术形式

引理 38. 设 M 和 N 是整数, $N>0$, 对素数 p, 给定 $\rho(p)$ 个不同的同余类, $0\leq\rho(p)\leq p-1$, 再设 $\{a_n\}_{n=M+1}^{M+N}$ 是一复数列, 满足若存在素数 p, n 在上述的 $\rho(p)$ 个同余类中的某个中, 就有 $a_n=0$. 则对任意正整数 q, 有

$$\mu(q)^2\left(\prod_{p\mid q}\frac{\rho(p)}{p-\rho(p)}\right)\left|\sum_{n=M+1}^{M+N}a_n\right|^2\leq\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2.$$

证明. 当 $q=1$ 或 $\mu(q)=0$ 或存在某个 $p\mid q$ 使得 $\rho(p)=0$ 时, 引理显然成立, 所以以下假设 $q>1$, $\mu(q)\neq 0$, 从而 $\mu(q)^2=1$, 并且当 $p\mid q$ 时, $\rho(p)\geq 1$. 设模 p 的 $\rho(p)$ 个同余类组成的集合为 Ω_p.

我们证明对任意使得 $\mu(q)\neq 0$ 的 q 与实数 θ,

$$\left(\prod_{p\mid q}\frac{\rho(p)}{p-\rho(p)}\right)|S(\theta)|^2\leq \sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}+\theta\right)\right|^2$$

成立. 我们对 q 的素因子个数 $\omega(q)$ 归纳, 首先, 当 $\omega(q)=1$ 时, 设 $q=p$, 设

$$S(p,j)=\sum_{\substack{M+1\leq n\leq M+N\\ n\equiv j\pmod p}}a_n e(n\theta),$$

则

$$\sum_{j=0}^{p-1}S(p,j)=S(\theta),$$

计算 $S(p,j)$ 的有限傅里叶变换为

$$\begin{aligned}\widehat{S}(p,k)&=\sum_{j=0}^{p-1}S(p,j)e\left(-\frac{jk}{p}\right)\\&=\sum_{j=0}^{p-1}\sum_{\substack{M+1\leq n\leq M+N\\ n\equiv j\pmod p}}a_n e(n\theta)e\left(-\frac{jk}{p}\right)\\&=\sum_{M+1\leq n\leq M+N}a_n e(n\theta)e\left(-\frac{nk}{p}\right)\\&=S\left(\theta-\frac{k}{p}\right),\end{aligned}$$

故由 $\mathbb{Z}/p\mathbb{Z}$ 上的 Parseval 恒等式得

$$\sum_{k=0}^{p-1}\left|S\left(\theta-\frac{k}{p}\right)\right|^2=p\sum_{j=0}^{p-1}|S(p,j)|^2,$$

从左端求和中分离出 $k=0$ 的情况即得

$$\sum_{k=1}^{p-1}\left|S\left(\theta-\frac{k}{p}\right)\right|^2=p\sum_{j=0}^{p-1}|S(p,j)|^2-|S(\theta)|^2.$$

又由 Cauchy-Schwarz 不等式得

$$\begin{aligned}|S(\theta)|^2=\left|\sum_{j\notin\Omega_p}1\cdot S(p,j)\right|^2&\leq\left(\sum_{j\notin\Omega_p}1^2\right)\left(\sum_{j\notin\Omega_p}|S(p,j)|^2\right)\\&=(p-\rho(p))\sum_{j\notin\Omega_p}|S(p,j)|^2\end{aligned}$$

$$\leq (p-\rho(p))\sum_{j=0}^{p-1}|S(p,j)|^2,$$

所以

$$\sum_{k=1}^{p-1}\left|S\left(\theta-\frac{k}{p}\right)\right|^2 \geq \frac{p}{p-\rho(p)}|S(\theta)|^2-|S(\theta)|^2=\frac{\rho(p)}{p-\rho(p)}|S(\theta)|^2,$$

换元 $a=-k$, 由 $S(x)$ 的定义知

$$\frac{\rho(p)}{p-\rho(p)}\,|S(\theta)|^2 \leq \sum_{k=1}^{p-1}\left|S\left(\theta-\frac{k}{p}\right)\right|^2=\sum_{a=1}^{p-1}\left|S\left(\frac{a}{p}+\theta\right)\right|^2,$$

$\omega(q)=1$ 的情形得证.

接下来设 $q=q_1q_2$, 其中 $(q_1,q_2)=1$, $q_1,q_2>1$, 且

$$\left(\prod_{p|q_1}\frac{\rho(p)}{p-\rho(p)}\right)|S(\theta)|^2 \leq \sum_{\substack{a=1\\(a,q_1)=1}}^{q_1}\left|S\left(\frac{a}{q_1}+\theta\right)\right|^2,$$

$$\left(\prod_{p|q_2}\frac{\rho(p)}{p-\rho(p)}\right)|S(\theta)|^2 \leq \sum_{\substack{a=1\\(a,q_2)=1}}^{q_2}\left|S\left(\frac{a}{q_2}+\theta\right)\right|^2$$

成立, 由中国剩余定理, 映射

$$(b,c)\mapsto bq_2+cq_1 \pmod{q_1q_2}$$

给出 $(\mathbb{Z}/q_1\mathbb{Z})^\times\times(\mathbb{Z}/q_2\mathbb{Z})^\times\to(\mathbb{Z}/(q_1q_2)\mathbb{Z})^\times$ 的双射, 且

$$\frac{bq_2+cq_1}{q_1q_2}\equiv\frac{b}{q_1}+\frac{c}{q_2} \pmod 1,$$

所以

$$\begin{aligned}
\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}+\theta\right)\right|^2 &= \sum_{\substack{b=1\\(b,q_1)=1}}^{q_1}\sum_{\substack{c=1\\(c,q_2)=1}}^{q_2}\left|S\left(\frac{b}{q_1}+\frac{c}{q_2}+\theta\right)\right|^2\\
&\geq \sum_{\substack{b=1\\(b,q_1)=1}}^{q_1}\left(\prod_{p|q_2}\frac{\rho(p)}{p-\rho(p)}\right)\left|S\left(\frac{b}{q_1}+\theta\right)\right|^2\\
&\geq \left(\prod_{p|q_2}\frac{\rho(p)}{p-\rho(p)}\right)\left(\prod_{p|q_1}\frac{\rho(p)}{p-\rho(p)}\right)|S(\theta)|^2\\
&= \left(\prod_{p|q}\frac{\rho(p)}{p-\rho(p)}\right)|S(\theta)|^2.
\end{aligned}$$

综上, 对任意使得 $\mu(q)\neq 0$ 的 q 与实数 θ,

$$\left(\prod_{p|q}\frac{\rho(p)}{p-\rho(p)}\right)|S(\theta)|^2 \leq \sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}+\theta\right)\right|^2$$

成立, 取 $\theta=0$ 即得

$$\left(\prod_{p\mid q}\frac{\rho(p)}{p-\rho(p)}\right)\left|\sum_{n=M+1}^{M+N}a_n\right|^2\le\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2,$$

引理得证. □

定理 21 (大筛法的算术形式)**.** 设 M 和 N 是两个整数, $N>0$, $\mathscr{P}$ 是一个素数集, 其中的素数都不超过正整数 Q. 设 $p\in\mathscr{P}$, $0\le\rho(p)\le p-1$, $k_1,\dots,k_{\rho(p)}$ 是模 p 的 $\rho(p)$ 个同余类, 当 n 满足 $n\equiv k_i\pmod p$ 对某个 i 成立时, 就将 n 去掉, 将剩余的集合记为 E, $Z=|E|$, 则

$$Z<\frac{N+Q^2}{L},$$

其中

$$L=\sum_{q\le Q}\mu(q)^2\prod_{p\mid q}\frac{\rho(p)}{p-\rho(p)}.$$

证明. 设 a_n 为集合 E 的指示函数

$$a_n=\begin{cases}1, & n\in E,\\ 0, & n\notin E,\end{cases}$$

则

$$Z=\sum_{n=M+1}^{M+N}a_n,$$

由上一个引理得

$$\sum_{q\le Q}\mu(q)^2\left(\prod_{p\mid q}\frac{\rho(p)}{p-\rho(p)}\right)\left|\sum_{n=M+1}^{M+N}a_n\right|^2\le\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2,$$

在大筛法不等式中取 $\{x_r\}_{r=1}^{R}$ 为 Q 阶 Farey 数列, 则由 Farey 数列的性质知 $\delta=1/(Q(Q-1))$, 所以

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2\le(N+Q(Q-1)-1)\sum_{n=M+1}^{M+N}|a_n|^2,$$

由于 a_n 只取 0 或 1, 所以 $|a_n|^2=a_n$, 所以

$$Z^2\sum_{q\le Q}\mu(q)^2\left(\prod_{p\mid q}\frac{\rho(p)}{p-\rho(p)}\right)\le Z(N+Q(Q-1)-1),$$

故

$$Z\le\frac{N+Q(Q-1)-1}{L}<\frac{N+Q^2}{L},$$

定理得证. □

最后一步放缩仅是为了使用方便. 接下来展示一些大筛法的应用.

例 8. 我们证明对任意正整数 M 和 N, 若 $M \geq N^{1/2}$, 则

$$\pi(M+N)-\pi(M)<\frac{4N}{\log N}.$$

取 $\mathscr{P}$ 为小于 $N^{1/2}$ 的所有素数, 即 $Q=N^{1/2}$, 对所有 $p\in\mathscr{P}$ 取 $\rho(p)=1$, 则

$$L=\sum_{\substack{q\leq Q\\ \mu(q)\neq 0}}\prod_{p\mid q}\frac{1}{p-1}=\sum_{\substack{q\leq Q\\ \mu(q)\neq 0}}\prod_{p\mid q}\sum_{k=1}^{\infty}\frac{1}{p^k}>\sum_{n\leq Q}\frac{1}{n}>\log Q=\frac{1}{2}\log N,$$

所以

$$\pi(M+N)-\pi(M)<\frac{N+Q^2}{\log Q}=\frac{4N}{\log N}.$$

接下来使用大筛法证明一种特征和的估计.

定理 22. 对任意实数 $Q\geq 1$, 有

$$\sum_{q\leq Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\left|\sum_{n=M+1}^{M+N}a_n\chi(n)\right|^2\leq (N+Q^2)\sum_{n=M+1}^{M+N}|a_n|^2,$$

其中 $\sum^*_{\chi \bmod q}$ 表示对模 q 的所有原特征求和

证明. 由原特征的性质知, 原特征 χ 满足

$$\chi(n)=\frac{G(n,\overline{\chi})}{\tau(\overline{\chi})},$$

其中 G 是 Gauss 和, $\tau(\overline{\chi})=G(1,\overline{\chi})$, 两边同时乘 a_n 并求和即得

$$\sum_{n=M+1}^{M+N}a_n\chi(n)=\frac{1}{\tau(\overline{\chi})}\sum_{n=M+1}^{M+N}a_n\sum_{j=1}^{q}\overline{\chi}(j)e\left(\frac{jn}{q}\right)=\frac{1}{\tau(\overline{\chi})}\sum_{j=1}^{q}\overline{\chi}(j)S\left(\frac{j}{q}\right),$$

由于 $|\tau(\overline{\chi})|=\sqrt{q}$, 对所有模 q 的原特征求和得

$$\sideset{}{^*}\sum_{\chi \bmod q}\left|\sum_{n=M+1}^{M+N}a_n\chi(n)\right|^2=\frac{1}{q}\sideset{}{^*}\sum_{\chi \bmod q}\left|\sum_{j=1}^{q}\overline{\chi}(j)S\left(\frac{j}{q}\right)\right|^2,$$

而由特征的正交性知

$$\sum_{\chi \bmod q}\left|\sum_{j=1}^{q}\overline{\chi}(j)S\left(\frac{j}{q}\right)\right|^2=\sum_{j=1}^{q}\sum_{k=1}^{q}S\left(\frac{j}{q}\right)\overline{S\left(\frac{k}{q}\right)}\sum_{\chi \bmod q}\overline{\chi}(j)\chi(k)=\varphi(q)\sum_{\substack{j=1\\(j,q)=1}}^{q}\left|S\left(\frac{j}{q}\right)\right|^2.$$

所以

$$\sum_{q\leq Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\left|\sum_{n=M+1}^{M+N}a_n\chi(n)\right|^2=\sum_{q\leq Q}\frac{1}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\left|\sum_{j=1}^{q}\overline{\chi}(j)S\left(\frac{j}{q}\right)\right|^2$$

$$
\begin{aligned}
&\leq \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\left|\sum_{j=1}^{q}\overline{\chi}(j)S\left(\frac{j}{q}\right)\right|^2\\
&=\sum_{q\leq Q}\sum_{\substack{j=1\\(j,q)=1}}^{q}\left|S\left(\frac{j}{q}\right)\right|^2\\
&\leq (N+Q^2)\sum_{n=M+1}^{M+N}|a_n|^2,
\end{aligned}
$$

定理得证. □

接下来这个引理会在陈景润定理的证明中用到.

引理 39. 设 $\{a_n\}_{n=1}^{\infty}$ 是一个复数列, 满足 $|a_n|\leq 1$ 对所有正整数 n 成立, 设 A, X 和 Y 正数, 满足 $X>(\log Y)^{2A}$, 再记

$$
D^*=\frac{(XY)^{1/2}}{(\log Y)^A},
$$

则对任意小于 Y 的正数 Z 有

$$
\sum_{d<D^*}\max_{(a,d)=1}\left|\sum_{n<X}\sum_{\substack{Z\leq p<Y\\ np\equiv a \pmod d}}a_n-\frac{1}{\varphi(d)}\sum_{n<X}\sum_{\substack{Z\leq p<Y\\(np,d)=1}}a_n\right|\ll\frac{XY(\log XY)^2}{(\log Y)^A},
$$

其中 $\ll$ 常数只与 A 有关.

证明. 固定正整数 a 和 d 满足 $d<D^*$, $(a,d)=1$, 由 Dirichlet 特征的正交性可得

$$
\sum_{\chi \bmod d}\overline{\chi}(a)\chi(np)=\begin{cases}\varphi(d), & np\equiv a \pmod d,\\ 0, & np\not\equiv a \pmod d,\end{cases}
$$

因此

$$
\begin{aligned}
\sum_{n<X}\sum_{\substack{Z\leq p<Y\\ np\equiv a \pmod d}}a_n&=\sum_{n<X}\sum_{Z\leq p<Y}\frac{a_n}{\varphi(d)}\sum_{\chi \bmod d}\overline{\chi}(a)\chi(np)\\
&=\frac{1}{\varphi(d)}\sum_{\chi \bmod d}\overline{\chi}(a)\left(\sum_{n<X}a_n\chi(n)\right)\left(\sum_{Z\leq p<Y}\chi(p)\right),
\end{aligned}
$$

主特征 χ_0 对等式右边的贡献为

$$
\frac{1}{\varphi(d)}\sum_{n<X}\sum_{\substack{Z\leq p<Y\\(np,d)=1}}a_n,
$$

因此有

$$
\left|\sum_{n<X}\sum_{\substack{Z\leq p<Y\\ np\equiv a \pmod d}}a_n-\frac{1}{\varphi(d)}\sum_{n<X}\sum_{\substack{Z\leq p<Y\\(np,d)=1}}a_n\right|\leq\frac{1}{\varphi(d)}\sum_{\substack{\chi \bmod d\\ \chi\neq\chi_0}}\left|\sum_{n<X}a_n\chi(n)\right|\left|\sum_{Z\leq p<Y}\chi(p)\right|,
$$

而该不等式右边是与 a 无关的, 所以

$$\sum_{d<D^*}\max_{(a,d)=1}\left|\sum_{n<X}\sum_{\substack{Z\le p<Y\\ np\equiv a \pmod d}}a_n-\frac{1}{\varphi(d)}\sum_{n<X}\sum_{\substack{Z\le p<Y\\ (np,d)=1}}a_n\right|$$
$$\le\sum_{d<D^*}\frac{1}{\varphi(d)}\sum_{\substack{\chi \bmod d\\ \chi\ne\chi_0}}\left|\sum_{n<X}a_n\chi(n)\right|\left|\sum_{Z\le p<Y}\chi(p)\right|.$$

因为每一个模 d 的非主特征 χ 都可以唯一地表示为一个模 r 的原特征与一个模 s 的主特征的乘积, 其中 $rs=d$, $r>1$, 因此上式右边可以写成

$$\sum_{\substack{rs<D^*\\ r>1}}\frac{1}{\varphi(rs)}\sideset{}{^*}\sum_{\chi \bmod r}\left|\sum_{\substack{n<X\\ (n,s)=1}}a_n\chi(n)\right|\left|\sum_{\substack{Z\le p<Y\\ (p,s)=1}}\chi(p)\right|,$$

其中 $\sum^*_{\chi \bmod r}$ 表示对模 r 的所有原特征求和. 由 $\varphi(rs)\ge\varphi(r)\varphi(s)$ 可得

$$\sum_{\substack{rs<D^*\\ r>1}}\frac{1}{\varphi(rs)}\sideset{}{^*}\sum_{\chi \bmod r}\left|\sum_{\substack{n<X\\ (n,s)=1}}a_n\chi(n)\right|\left|\sum_{\substack{Z\le p<Y\\ (p,s)=1}}\chi(p)\right|$$
$$\le\sum_{s<D^*}\frac{1}{\varphi(s)}\sum_{\substack{r<D^*\\ r>1}}\frac{1}{\varphi(r)}\sideset{}{^*}\sum_{\chi \bmod r}\left|\sum_{\substack{n<X\\ (n,s)=1}}a_n\chi(n)\right|\left|\sum_{\substack{Z\le p<Y\\ (p,s)=1}}\chi(p)\right|.$$

我们先来估计内部和

$$\left|\sum_{\substack{Z\le p<Y\\ (p,s)=1}}\chi(p)\right|,$$

其中 χ 是模 r 的原特征. 设 $B=4A$, 当 $r\le(\log Y)^{B-1}$ 时, 由 Siegel-Walfisz 定理, 对任意正整数 $k\le r$, $(k,r)=1$, 都有

$$\pi(Y;r,k)=\frac{\mathrm{Li}(Y)}{\varphi(r)}+O\left(\frac{Y}{(\log Y)^B}\right),$$

其中 O 常数依赖于 A. 对小于 Y 的素数模 r 分类得

$$\sum_{p<Y}\chi(p)=\sum_{k=1}^{r}\sum_{\substack{p<Y\\ p\equiv k \pmod r}}\chi(p)=\sum_{k=1}^{r}\chi(k)\pi(Y;r,k),$$

因此

$$\sum_{p<Y}\chi(p)=\frac{\mathrm{Li}(Y)}{\varphi(r)}\sum_{k=1}^{r}\chi(k)+O\left(\frac{rY}{(\log Y)^B}\right),$$

由于 χ 是模 r 的原特征且 $r>1$, 所以 χ 是非主特征, 所以由正交性

$$\sum_{k=1}^{r}\chi(k)=0$$

得

$$\left|\sum_{p<Y}\chi(p)\right|\ll\frac{rY}{(\log Y)^B}.$$

另一方面, 当 $r>(\log Y)^{B-1}$ 时, 有

$$\left|\sum_{p<Y}\chi(p)\right|\le\pi(Y)\ll\frac{Y}{\log Y}\le\frac{rY}{(\log Y)^B},$$

所以对所有 r, $1<r<D^*$, 都有

$$\left|\sum_{p<Y}\chi(p)\right|\ll\frac{rY}{(\log Y)^B},$$

同理,

$$\left|\sum_{p<Z}\chi(p)\right|\ll\frac{rZ}{(\log Z)^B}\ll\frac{rY}{(\log Y)^B},$$

从而有

$$\left|\sum_{Z\le p<Y}\chi(p)\right|\le\left|\sum_{p<Y}\chi(p)\right|+\left|\sum_{p<Z}\chi(p)\right|\ll\frac{rY}{(\log Y)^B},$$

此外, 因为我们在求和中去掉了条件 $(p,s)=1$, 这最多去掉了 $\omega(s)$ 项, 再结合 $\omega(s)\ll\log s\ll\log D^*$ 可得

$$\left|\sum_{\substack{Z\le p<Y\\(p,s)=1}}\chi(p)\right|\le\frac{rY}{(\log Y)^B}+\log D^*.$$

而对于和

$$\left|\sum_{\substack{n<X\\(n,s)=1}}a_n\chi(n)\right|,$$

由 $|a_n|\le1$ 即得估计

$$\left|\sum_{\substack{n<X\\(n,s)=1}}a_n\chi(n)\right|\le\sum_{\substack{n<X\\(n,s)=1}}1\le X.$$

现取 $D_0^*=(\log Y)^A\ll D^*$, 将 $1<r<D^*$ 分割为 $1<r<D_0^*$ 和 $D_0^*\le r<D^*$, 则对第一部分有

$$\sum_{1<r<D_0^*}\frac{1}{\varphi(r)}\sideset{}{^*}\sum_{\chi\bmod r}\left|\sum_{\substack{n<X\\(n,s)=1}}a_n\chi(n)\right|\left|\sum_{\substack{Z\le p<Y\\(p,s)=1}}\chi(p)\right|$$

$$\ll \sum_{r<D_0^*} \frac{rX}{\varphi(r)} \left(\frac{rY}{(\log Y)^B} + \log D^* \right)$$
$$\ll \frac{D_0^{*3} XY \log D^*}{(\log Y)^B}.$$

对于 $D_0^* \le r < D^*$ 的部分, 我们做划分 $D_k^* = 2^k D_0^*$, $k = 0, 1, \dots, [\log(D^*/D_0^*)/\log 2] + 1 \ll \log D^*$, 对每个小区间使用 Cauchy-Schwarz 不等式, 有

$$\sum_{\substack{D_k^* \le r < D_{k+1}^* \\ D_0^* \le r < D^*}} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right|$$
$$\le \frac{1}{D_k^*} \sum_{\substack{D_k^* \le r < D_{k+1}^* \\ D_0^* \le r < D^*}} \sideset{}{^*}\sum_{\chi \bmod r} \left(\left(\frac{r}{\varphi(r)} \right)^{1/2} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \right) \left(\left(\frac{r}{\varphi(r)} \right)^{1/2} \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right| \right)$$
$$\le \frac{1}{D_k^*} \left(\sum_{D_k^* \le r < D_{k+1}^*} \frac{r}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right|^2 \right)^{1/2} \left(\sum_{D_k^* \le r < D_{k+1}^*} \frac{r}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right|^2 \right)^{1/2},$$

将上一个定理应用到该式的两个因子即得

$$\sum_{\substack{D_k^* \le r < D_{k+1}^* \\ D_0^* \le r < D^*}} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right| \ll \frac{1}{D_k^*} \left((D_k^{*2} + X)X \right)^{1/2} \left((D_k^{*2} + Y)Y \right)^{1/2}$$
$$= \left(\left(D_k^{*2} + X + Y + \frac{XY}{D_k^{*2}} \right) XY \right)^{1/2}$$
$$\ll \left(D_k^* + X^{1/2} + Y^{1/2} + \frac{(XY)^{1/2}}{D_k^*} \right) (XY)^{1/2}$$
$$\ll \left(D^* + X^{1/2} + Y^{1/2} + \frac{(XY)^{1/2}}{D_0^*} \right) (XY)^{1/2},$$

将各部分加起来, 因为 $k \ll \log D^*$, 所以

$$\sum_{d<D^*} \frac{1}{\varphi(d)} \sideset{}{^*}\sum_{\substack{\chi \pmod d \\ \chi \ne \chi_0}} \left| \sum_{n<X} a_n \chi(n) \right| \left| \sum_{Z \le p < Y} \chi(p) \right|$$
$$\le \sum_{s<D^*} \frac{1}{\varphi(s)} \sum_{1<r<D^*} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right|$$
$$\ll \sum_{s<D^*} \frac{1}{\varphi(s)} \frac{D_0^{*3} XY \log D^*}{(\log Y)^B} + \sum_{s<D^*} \frac{1}{\varphi(s)} \left(D^* + X^{1/2} + Y^{1/2} + \frac{(XY)^{1/2}}{D_0^*} \right) (XY)^{1/2} \log D^*$$

$$\ll \frac{D_0^{*3}XY(\log D^*)^2}{(\log Y)^B} + \left(D^* + X^{1/2} + Y^{1/2} + \frac{(XY)^{1/2}}{D_0^*}\right)(XY)^{1/2}(\log D^*)^2,$$

其中最后一步使用了

$$\sum_{s<D^*} \frac{1}{\varphi(s)} \ll \log D^*,$$

代回 $B = 4A$, $D_0^* = (\log Y)^A$ 和 $D^* = (XY)^{1/2}/(\log Y)^A$ 即得

$$\begin{aligned}
&\sum_{d<D^*} \max_{(a,d)=1} \left| \sum_{n<X} \sum_{\substack{Z\le p<Y \\ np\equiv a \pmod d}} a_n - \frac{1}{\varphi(d)} \sum_{n<X} \sum_{\substack{Z\le p<Y \\ (np,d)=1}} a_n \right| \\
&\ll \frac{XY(\log D^*)^2}{(\log Y)^A} + \left(\frac{D^*}{(XY)^{1/2}} + \frac{1}{X^{1/2}} + \frac{1}{Y^{1/2}} + \frac{1}{(\log Y)^A}\right) XY(\log D^*)^2 \\
&\ll \left(\frac{1}{X^{1/2}} + \frac{1}{Y^{1/2}} + \frac{1}{(\log Y)^A}\right) XY(\log XY)^2 \\
&\ll \frac{XY(\log XY)^2}{(\log Y)^A},
\end{aligned}$$

引理得证. □

2.7 陈景润定理

本节中对陈景润定理的证明由 Iwaniec 简化, 参考自 [7].

2.7.1 加权筛的构造

固定偶数 $N > 4^8$, 设 $z = N^{1/8}$, $y = N^{1/3}$, 则 $z > 4$, 设权函数

$$w(n) = 1 - \frac{1}{2} \sum_{\substack{z\le p<y \\ p^k \| n}} k - \frac{1}{2} \sum_{\substack{p_1p_2p_3=n \\ z\le p_1<y\le p_2\le p_3}} 1, \qquad n \ge 1,$$

显然 $w(n) \le 1$, $w(1) = 1$. 再设 $\mathcal{P}$ 为不整除 N 的所有素数组成的集合, 即

$$\mathcal{P} = \{p : p \nmid N\},$$

由 N 是偶数知 $2 \notin \mathcal{P}$.

定义 $r(N)$ 为将偶数 N 表示为 $N = p + n$ 的形式的方法数, 其中 p 是一个奇素数, n 是至多两个素数的积. 设

$$A = \{N - p : p \le N, p \in \mathcal{P}\},$$

$$B = \{N - p_1p_2p_3 : p_1p_2p_3 < N, (p_1p_2p_3, N) = 1, z \le p_1 < y \le p_2 \le p_3\}.$$

接下来我们将说明, 将权重 $w(n)$ 添加到集合 A 上的加权筛

$$\sum_{\substack{n\in A \\ (n,P(z))=1}} w(n)$$

可以给出 $r(N)$ 的下界.

引理 40. 符号如上, 则有

$$r(N) > S(A,\mathcal{P},z) - \frac{1}{2}\sum_{z\le p<y} S(A_p,\mathcal{P},z) - \frac{1}{2}S(B,\mathcal{P},y) - N^{7/8} - \frac{1}{2}N^{1/3}.$$

证明. 设 $\Omega(n)$ 表示 n 的素因子个数 (按重数算), 则由 $r(N)$ 的定义知

$$\begin{aligned} r(N) &\ge \sum_{\substack{n\in A\\(n,P(z))=1\\ \Omega(n)\le 2}} 1 \\ &\ge \sum_{\substack{n\in A\\(n,P(z))=1\\ \Omega(n)\le 2}} w(n) \\ &= \sum_{\substack{n\in A\\(n,P(z))=1}} w(n) - \sum_{\substack{n\in A\\(n,P(z))=1\\ \Omega(n)>2}} w(n) \end{aligned}$$

若 $n\in A$ 且 $(n,P(z))=1$, 设 $n=N-p$, 若 $(n,N)>1$, 设素数 $p'|(n,N)$, 则 $p'|N-n=p$, 故 $p=p'$, 所以 $p\notin\mathcal{P}$, 这与集合 A 的定义矛盾, 所以必须 $(n,N)=1$. 此时 n 的素因子只能是 $\mathcal{P}$ 中大于等于 z 的素数, 不妨设 $n=p_1\dots p_s p_{s+1}\dots p_{s+t}$, 其中 $z\le p_1\le\cdots\le p_s<y\le p_{s+1}\le\cdots\le p_{s+t}$, 由于 $N^{t/3}=y^t\le p_{s+1}\dots p_{s+t}\le n<N$, 所以 t 只能取 0 或 1 或 2. 现设 $w(n)>0$, 由

$$\frac{1}{2}\sum_{\substack{z\le p<y\\ p^k\| n}} k = \frac{s}{2},$$

知 s 只能取 0 或 1, 当 s 取 1 且 t 取 2 时, 即 $n=p_1p_2p_3$, $z\le p_1<y\le p_2\le p_3$, 则 $w(n)=1-1/2-1/2=0$, 与 $w(n)>0$ 矛盾, 所以要 $w(n)>0$ 必须有 $\Omega(n)=s+t\le 2$, 即 $\Omega(n)>2$ 时必有 $w(n)\le 0$, 所以

$$r(N)\ge \sum_{\substack{n\in A\\(n,P(z))=1}} w(n) = \left(\sum_{\substack{n\in A\\(n,P(z))=1}} 1\right) - \left(\frac{1}{2}\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le p<y\\ p^k\| n}} k\right) - \left(\frac{1}{2}\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{p_1p_2p_3=n\\ z\le p_1<y\le p_2\le p_3}} 1\right).$$

显然右边第一项就是 $S(A,\mathcal{P},z)$. 对于第二项,

$$\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le p<y\\ p^k\| n}} k = \sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le p<y\\ p\mid n}} 1 + \sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le p<y\\ p^k\| n,\, k\ge 2}} (k-1),$$

而

$$\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le p<y\\ p\mid n}} 1 = \sum_{z\le p<y}\sum_{\substack{n\in A,\, p\mid n\\(n,P(z))=1}} 1 = \sum_{z\le p<y} S(A_p,\mathcal{P},z),$$

$$\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le p<y\\ p^k\| n\\ k\ge 2}} (k-1) = \sum_{z\le p<y}\sum_{k=2}^{\infty}\sum_{\substack{n\in A\\(n,P(z))=1\\ p^k\| n}} (k-1) \le \sum_{z\le p<y}\sum_{k=2}^{\infty}\sum_{\substack{n<N\\ p^k\| n}} (k-1)$$

$$
\begin{aligned}
&< \sum_{z\le p<y}\sum_{k=2}^{\infty}\frac{N}{p^k}(k-1) = N\sum_{z\le p<y}\sum_{k=2}^{\infty}\frac{k-1}{p^k}\\
&= N\sum_{z\le p<y}\frac{1}{(p-1)^2} < N\sum_{k=\lceil z\rceil}^{\infty}\frac{1}{(k-1)(k-2)}\\
&= N\sum_{k=\lceil z\rceil}^{\infty}\left(\frac{1}{k-2}-\frac{1}{k-1}\right) < \frac{N}{z-2}\le\frac{2N}{z}\\
&= 2N^{7/8},
\end{aligned}
$$

所以

$$
\frac{1}{2}\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le p<y\\p^k\| n}}k < \frac{1}{2}\sum_{z\le p<y}S(A_p,\mathcal{P},z)+N^{7/8}.
$$

对于第三项, 由于 $p_1,p_2,p_3\ge z$, 当然有 $(n,P(z))=1$, 设 $n=N-p$, 则由 B 的定义知 $p\in B$, 所以

$$
\begin{aligned}
\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{p_1p_2p_3=n\\z\le p_1<y\le p_2\le p_3}}1 &= \sum_{\substack{p_1p_2p_3\in A\\p_1<y\le p_2\le p_3}}1 = \sum_{p\in B}1 = \sum_{\substack{p\in B\\p<y}}1+\sum_{\substack{p\in B\\p\ge y}}1\\
&< y+\sum_{\substack{n\in B\\(n,P(y))=1}}1\\
&= N^{1/3}+S(B,\mathcal{P},y),
\end{aligned}
$$

综上即得

$$
r(N) > S(A,\mathcal{P},z)-\frac{1}{2}\sum_{z\le p<y}S(A_p,\mathcal{P},z)-\frac{1}{2}S(B,\mathcal{P},y)-N^{7/8}-\frac{1}{2}N^{1/3},
$$

引理得证. □

因此接下来只需得到 $S(A,\mathcal{P},z)$ 的下界和 $S(B,\mathcal{P},y)+\sum S(A_p,\mathcal{P},z)$ 的上界即可.

2.7.2 线性筛的应用

先考虑 A_d 在 A 中的密度, 其中 d 不整除 N, 显然 $|A|=\pi(N)-\omega(N)$, 而 $N-p$ 是 d 的倍数就是说 $p\equiv N\pmod d$, 由算术数列中的素数定理知 $|A_d|\sim\pi(N)/\varphi(d)$, 所以 A_d 在 A 中的密度就是 $1/\varphi(d)$, 取 $g(d)=1/\varphi(d)$, 它显然是乘性函数, 并且由 $2\notin\mathcal{P}$ 知当 $p\in\mathcal{P}$ 时 $0<g(p)<1$.

引理 41. *对任意正数 $\varepsilon>0$, 都存在一个只与 ε 有关的正数 $u_1>0$, 使得*

$$
\prod_{u\le p<z}\left(1-\frac{1}{p}\right)^{-1} < (1+\varepsilon)\frac{\log z}{\log u}
$$

对任意 $u\in[u_1,z)$ 成立.

证明. 设 γ 是欧拉常数, 选取 $\delta>0$ 使得

$$
\frac{e^{\gamma}+\delta}{e^{\gamma}-\delta} < 1+\varepsilon,
$$

成立, 由 Mertens 定理知

$$\prod_{p<z}\left(1-\frac{1}{p}\right)^{-1}\sim e^{\gamma}\log z,$$

所以存在正数 $u_1>0$, 使得

$$(e^{\gamma}-\delta)\log z<\prod_{p<z}\left(1-\frac{1}{p}\right)^{-1}<(e^{\gamma}+\delta)\log z$$

对所有 $z>u_1$ 都成立, 因此, 只要 $u\in[u_1,z)$, 就有

$$\prod_{u\le p<z}\left(1-\frac{1}{p}\right)^{-1}=\frac{\prod_{p<z}\left(1-\frac{1}{p}\right)^{-1}}{\prod_{p<u}\left(1-\frac{1}{p}\right)^{-1}}<\frac{(e^{\gamma}+\delta)\log z}{(e^{\gamma}-\delta)\log u}<(1+\varepsilon)\frac{\log z}{\log u},$$

引理得证. □

引理 42. *对任意正数 $\varepsilon\in(0,1/200)$, 都存在一个只关于 ε 的正数 u_0, 使得*

$$\prod_{\substack{p\in\mathcal{P}-\mathcal{Q}\\ u\le p<z}}(1-g(p))^{-1}<(1+\varepsilon)\frac{\log z}{\log u}$$

对所有 $u\in(1,z)$ 都成立, 其中 $\mathcal{Q}$ 表示 $\mathcal{P}$ 中所有小于 u_0 的素数组成的集合.

证明. 由上一引理知存在正数 u_1, 使得

$$\prod_{u\le p<z}\left(1-\frac{1}{p}\right)^{-1}<\left(1+\frac{\varepsilon}{3}\right)\frac{\log z}{\log u}$$

对任意 $u\in[u_1,z)$ 成立. 因为无穷乘积

$$\prod_{p>2}\frac{(p-1)^2}{p(p-2)}=\prod_{p>2}\left(1+\frac{1}{p(p-2)}\right)$$

收敛, 所以存在正数 u_2 使得

$$\prod_{p\ge u_2}\frac{(p-1)^2}{p(p-2)}<1+\frac{\varepsilon}{3}$$

成立, 取 $u_0=\max\{u_1,u_2\}$, 不妨设 N 足够大以满足 $u_0<z$, 则对任意 $u\in[u_0,z)$, 有

$$\begin{aligned}\prod_{\substack{p\in\mathcal{P}-\mathcal{Q}\\ u\le p<z}}(1-g(p))^{-1}&\le\prod_{u\le p<z}(1-g(p))^{-1}\\&=\prod_{u\le p<z}\left(1-\frac{1}{p-1}\right)^{-1}\\&=\prod_{u\le p<z}\frac{(p-1)^2}{p(p-2)}\prod_{u\le p<z}\left(1-\frac{1}{p}\right)^{-1}\end{aligned}$$

$$< \left(1+\frac{\varepsilon}{3}\right)^2 \frac{\log z}{\log u}$$
$$< (1+\varepsilon)\frac{\log z}{\log u},$$

而当 $u \in (1, u_0)$ 时,

$$\prod_{\substack{p\in\mathcal{P}-\mathcal{Q}\\ u\le p<z}} (1-g(p))^{-1} \le \prod_{u_0\le p<z} (1-g(p))^{-1} < (1+\varepsilon)\frac{\log z}{\log u_0} < (1+\varepsilon)\frac{\log z}{\log u},$$

综上, 引理得证. □

该引理说明我们这样构造的 $g(d)$ 确实是线性筛法, 满足了 Jurkat-Richert 定理的条件.

该引理中的 $\mathcal{Q}$ 只与 ε 有关, 与 N 无关, 所以当 N 足够大时, 总是可以保证 $Q < \log N$, 这里 Q 是 $\mathcal{Q}$ 中所有素数的乘积.

引理 43. 设

$$V(z) = \prod_{p|P(z)} (1-g(p)) = \prod_{\substack{p<z\\ (p,N)=1}} \left(1-\frac{1}{p-1}\right),$$

则

$$V(z) = \mathfrak{S}_2(N)\frac{e^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right),$$

其中 $\mathfrak{S}_2$ 是强 *Goldbach* 猜想中的奇异级数

$$\mathfrak{S}_2(N) = \prod_{p|N}\left(1+\frac{1}{p-1}\right)\prod_{p\nmid N}\left(1-\frac{1}{(p-1)^2}\right).$$

证明. 设

$$W(z) = \prod_{2<p<z}\left(1-\frac{1}{p-1}\right),$$

则

$$\frac{V(z)}{W(z)} = \prod_{\substack{2<p<z\\ p|N}}\left(1-\frac{1}{p-1}\right)^{-1} = \prod_{\substack{p>2\\ p|N}}\left(1-\frac{1}{p-1}\right)^{-1}\prod_{\substack{p\ge z\\ p|N}}\left(1-\frac{1}{p-1}\right)$$

而由于当 $0 < x < (\log 2)/2$ 时 $1 - x > e^{-2x}$, 以及对所有实数 x 都有 $1 - x < e^{-x}$, 所以

$$1 \ge \prod_{\substack{p\ge z\\ p|N}}\left(1-\frac{1}{p-1}\right) > \prod_{\substack{p\ge z\\ p|N}}\exp\left(-\frac{2}{p-1}\right)$$
$$= \exp\left(-2\sum_{\substack{p\ge z\\ p|N}}\frac{1}{p-1}\right)$$
$$\ge \exp\left(\frac{-2\omega(N)}{z-1}\right)$$

$$\begin{aligned}
&\geq \exp\left(\frac{-2\log N/\log 2}{z/2}\right)\\
&> \exp\left(\frac{-8\log N}{z}\right)\\
&= \exp\left(\frac{-8\log N}{N^{1/8}}\right)\\
&> 1-\frac{8\log N}{N^{1/8}},
\end{aligned}$$

所以有

$$\frac{V(z)}{W(z)}=\prod_{\substack{p>2\\ p\mid N}}\left(1-\frac{1}{p-1}\right)^{-1}\left(1+O\left(\frac{\log N}{N^{1/8}}\right)\right).$$

现考虑

$$\begin{aligned}
W(z)\prod_{p<z}\left(1-\frac{1}{p}\right)^{-1} &= \prod_{2<p<z}\left(1-\frac{1}{p-1}\right)\prod_{p<z}\left(1-\frac{1}{p}\right)^{-1}\\
&= 2\prod_{2<p<z}\frac{p(p-2)}{(p-1)^2}\\
&= 2\prod_{2<p<z}\left(1-\frac{1}{(p-1)^2}\right)\\
&= 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\geq z}\left(1-\frac{1}{(p-1)^2}\right)^{-1}\\
&= 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\geq z}\left(1+\frac{1}{p(p-2)}\right),
\end{aligned}$$

由于 $0<x<\log 2$ 时有 $1+x<e^x<1+2x$, 所以

$$\begin{aligned}
1<\prod_{p\geq z}\left(1+\frac{1}{p(p-2)}\right) &< \exp\left(\sum_{p\geq z}\frac{1}{p(p-2)}\right)\\
&< \exp\left(\sum_{n\geq z}\frac{1}{n(n-2)}\right)\\
&\leq \exp\left(\frac{1}{z-2}\right)\\
&\leq \exp\left(\frac{2}{z}\right)\\
&< 1+\frac{4}{z},
\end{aligned}$$

再由 Mertens 定理知

$$W(z)=2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\left(1+O\left(\frac{1}{z}\right)\right)\prod_{p<z}\left(1-\frac{1}{p}\right)$$

$$= 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\left(1+O\left(\frac{1}{z}\right)\right)\frac{e^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right)$$
$$= 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\frac{e^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log N}\right)\right).$$

综上可得

$$\begin{aligned}V(z) &= \frac{V(z)}{W(z)}W(z)\\ &= 2\prod_{\substack{p>2\\ p\mid N}}\left(1-\frac{1}{p-1}\right)^{-1}\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\frac{e^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log N}\right)\right)\\ &= 2\prod_{\substack{p>2\\ p\mid N}}\left(1+\frac{1}{p-1}\right)\prod_{\substack{p>2\\ p\nmid N}}\left(1-\frac{1}{(p-1)^2}\right)\frac{e^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log N}\right)\right)\\ &= \mathfrak{S}_2(N)\frac{e^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log N}\right)\right),\end{aligned}$$

引理得证. □

2.7.3 三个筛函数的估计

我们需要以下形式的 Bombieri-Vinogradov 定理, 它的证明见附录.

定理 23 (Bombieri-Vinogradov 定理)**.** *对任意实数 $A>0$, 总存在一个依赖 A 的正数 $B(A)$, 使得*

$$\sum_{q\le M}\max_{y\le x}\max_{(a,q)=1}\left|\pi(y;q,a)-\frac{\pi(y)}{\varphi(q)}\right| \ll \frac{x}{(\log x)^A}$$

对任意实数 $x>1$ 成立, 其中

$$M=\frac{x^{1/2}}{(\log x)^{B(A)}},$$

$\ll$ 常数只依赖于 A.

先估计 $S(A,\mathcal{P},z)$ 的下界.

引理 44. *设 $0<\varepsilon<1/200$, 则当 N 足够大时有*

$$S(A,\mathcal{P},z) > \left(\frac{e^\gamma\log 3}{2}+O(\varepsilon)\right)\frac{NV(z)}{\log N}.$$

证明. 由 Jurkat-Richert 定理得

$$S(A,\mathcal{P},z) > (f(s)-\varepsilon e^{14-s})|A|V(z) - \sum_{\substack{d\mid P(z)\\ d<DQ}}|r(d)|,$$

其中 D 待定, $s=\log D/\log z$. 由带余项的素数定理得

$$|A| = \sum_{\substack{p<N\\ (p,N)=1}}1$$

$$
\begin{aligned}
&= \pi(N) - \omega(N) \\
&= \pi(N) + O(\log N) \\
&= \frac{N}{\log N}\left(1 + O\left(\frac{1}{\log N}\right)\right).
\end{aligned}
$$

而

$$
\begin{aligned}
|A_d| &= \sum_{\substack{N-p\in A \\ N-p\equiv 0 \pmod d}} 1 \\
&= \sum_{\substack{p\in\mathcal{P},\, p\le N \\ p\equiv N \pmod d}} 1 \\
&= \sum_{\substack{p\le N \\ p\equiv N \pmod d}} 1 + O(\omega(N)) \\
&= \pi(N; d, N) + O(\log N),
\end{aligned}
$$

所以

$$
r(d) = |A_d| - \frac{|A|}{\varphi(d)} = \pi(N; d, N) - \frac{\pi(N)}{\varphi(d)} + O(\log N),
$$

在 Bombieri-Vinogradov 定理中取 $A = 3$, 再取

$$
D = \frac{N^{1/2}}{(\log N)^{B(3)+1}},
$$

则由 $Q < \log N$ 可得

$$
\begin{aligned}
\sum_{\substack{d\mid P(z) \\ d<DQ}} |r(d)| &\le \sum_{\substack{(d,N)=1 \\ d<DQ}} |r(d)| \\
&\le \sum_{\substack{(d,N)=1 \\ d<DQ}} \left|\pi(N; d, N) - \frac{\pi(N)}{\varphi(d)}\right| + O(DQ\log N) \\
&\le \sum_{d<DQ} \max_{y\le N} \max_{(a,d)=1} \left|\pi(y; d, a) - \frac{\pi(y)}{\varphi(d)}\right| + O(DQ\log N) \\
&\ll \frac{N}{(\log N)^3} + \frac{N^{1/2}}{(\log N)^{B(3)-1}} \\
&\ll \frac{N}{(\log N)^3}.
\end{aligned}
$$

对于主项, 由 $z = N^{1/8}$ 和 $D = N^{1/2}/(\log N)^{B(3)+1}$ 得

$$
s = \frac{4\log N - 8(B(3)+1)\log\log N}{\log N} = 4 - \frac{8(B(3)+1)\log\log N}{\log N},
$$

当 N 足够大时总能保证 $s \in (4-\varepsilon, 4]$, 所以有 $s = 4 - O(\varepsilon)$, 所以

$$
\log(s-1) = \log\left(3 - O(\varepsilon)\right) = \log\left(3\left(1 - O(\varepsilon)\right)\right) = \log 3 + \log\left(1 - O(\varepsilon)\right) = \log 3 + O(\varepsilon),
$$

$$f(s)=\frac{2e^{\gamma}\log(s-1)}{s}=\frac{2e^{\gamma}\log(3)+O(\varepsilon)}{4(1-O(\varepsilon))}=\frac{e^{\gamma}\log 3}{2}+O(\varepsilon),$$

由上一节知 $NV(z)/(\log N)\gg N/(\log N)^2\gg N/(\log N)^3$, 所以

$$\begin{aligned}S(A,\mathcal{P},z)&>(f(s)-\varepsilon e^{14-s})|A|V(z)-\sum_{\substack{d\mid P(z)\\ d<DQ}}|r(d)|\\&>(f(s)-\varepsilon e^{11})V(z)\frac{N}{\log N}\left(1+O\left(\frac{1}{\log N}\right)\right)-O\left(\frac{N}{(\log N)^3}\right)\\&>\left(\frac{e^{\gamma}\log 3}{2}+O(\varepsilon)\right)\frac{NV(z)}{\log N},\end{aligned}$$

引理得证. □

接下来估计 $\sum S(A_p,\mathcal{P},z)$.

引理 45. 设 $0<\varepsilon<1/200$, 则当 N 足够大时有

$$\sum_{z\le p<y}S(A_p,\mathcal{P},z)<\left(\frac{e^{\gamma}\log 6}{2}+O(\varepsilon)\right)\frac{NV(z)}{\log N}.$$

证明. 当 $p\mid N$ 时, 由 A_p 的定义知 A_p 中的元素形如 $N-p'$, 其中 $p\mid(N-p')$, $p'\nmid N$, 这是不可能的, 所以 A_p 是空集, 因此以下均设 $(p,N)=1$.

设 $r_p(d)=|(A_p)_d|-|A_p|/\varphi(d)$, 则

$$\begin{aligned}r_p(d)&=|A_{pd}|-\frac{|A_p|}{\varphi(d)}\\&=|A_{pd}|-\frac{|A|}{\varphi(pd)}+\frac{|A|}{\varphi(pd)}-\frac{|A_p|}{\varphi(d)}\\&=r(pd)-\frac{r(p)}{\varphi(d)},\end{aligned}$$

在 Bombieri-Vinogradov 定理中取 $A=4$, 再设

$$D=\frac{N^{1/2}}{(\log N)^{B(4)+1}},\qquad D_p=\frac{N^{1/2}}{p(\log N)^{B(4)+1}}=\frac{D}{p},\qquad s_p=\frac{\log D_p}{\log z},$$

则

$$\sum_{\substack{d<QD_p\\ d\mid P(z)}}|r_p(d)|\le\sum_{\substack{d<QD_p\\ d\mid P(z)}}|r(pd)|+|r(p)|\sum_{\substack{d<QD_p\\ d\mid P(z)}}\frac{1}{\varphi(d)},$$

由 Jurkat-Richert 定理得

$$\sum_{\substack{z\le p<y\\ (p,N)=1}}S(A_p,\mathcal{P},z)<\sum_{\substack{z\le p<y\\ (p,N)=1}}\left(F(s_p)+\varepsilon e^{14}\right)|A_p|V(z)+R',$$

其中

$$R'=\sum_{\substack{z\le p<y\\ (p,N)=1}}\sum_{\substack{d<QD_p\\ d\mid P(z)}}|r_p(d)|$$

$$\leq \sum_{\substack{z\leq p<y\\(p,N)=1}}\sum_{\substack{d<QD/p\\d|P(z)}}|r(pd)|+\sum_{\substack{z\leq p<y\\(p,N)=1}}|r(p)|\sum_{\substack{d<QD/p\\d|P(z)}}\frac{1}{\varphi(d)}$$
$$\leq \sum_{\substack{d'<QD\\(d',N)=1}}|r(d')|+\sum_{\substack{z\leq p<y\\(p,N)=1}}|r(p)|\sum_{d<N^{1/2}}\frac{1}{\varphi(d)}$$

与上一个引理的证明类似可得

$$\sum_{\substack{d'<QD\\(d',N)=1}}|r(d')|\leq\sum_{\substack{d'<QD\\(d',N)=1}}\left|\pi(N;d',N)-\frac{\pi(N)}{\varphi(d')}\right|+O(DQ\log N)\ll\frac{N}{(\log N)^4},$$

而又由于当 N 足够大时有 $y=N^{1/3}<D\leq QD$, 所以类似的也有

$$\sum_{\substack{z\leq p<y\\(p,N)=1}}|r(p)|\ll\frac{N}{(\log N)^4},$$

再结合

$$\sum_{d<N}\frac{1}{\varphi(d)}\ll\log N$$

可得

$$R'\ll\frac{N}{(\log N)^3}.$$

对于主项, 由于 $N^{1/8}\leq p<N^{1/3}$, 所以

$$\frac{4}{3}<\frac{8\log\big(N^{1/2}/p\big)}{\log N}\leq 3,$$

故当 N 足够大时

$$s_p=\frac{\log(D/p)}{\log z}=\frac{8\log\big(N^{1/2}/p\big)}{\log N}-\frac{8(B(4)+1)\log\log N}{\log N}\in[1,3],$$

进一步的也可以有 $s_p=8\log\big(N^{1/2}/p\big)/\log N-O(\varepsilon)$, 类似上一个引理的证明, 有

$$F(s_p)+\varepsilon e^{14}=\frac{2e^\gamma}{s_p}+\varepsilon e^{14}=\frac{e^\gamma\log N}{4\log(N^{1/2}/p)}+O(\varepsilon).$$

而

$$\begin{aligned}|A_p|&=\pi(N;p,N)+O(\log N)\\&=\frac{\pi(N)}{\varphi(p)}+\pi(N;p,N)-\frac{\pi(N)}{\varphi(p)}+O(\log N)\\&=\frac{N}{\varphi(p)\log N}\left(1+O\left(\frac{1}{\log N}\right)\right)+\pi(N;p,N)-\frac{\pi(N)}{\varphi(p)},\end{aligned}$$

因此

$$\sum_{\substack{z\leq p<y\\(p,N)=1}}(F(s_p)+\varepsilon e^{14})|A_p|=\sum_{\substack{z\leq p<y\\(p,N)=1}}\left(\frac{e^\gamma\log N}{4\log(N^{1/2}/p)}+O(\varepsilon)\right)\frac{N}{\varphi(p)\log N}\left(1+O\left(\frac{1}{\log N}\right)\right)$$

$$
\begin{aligned}
&+\sum_{\substack{z\le p<y\\(p,N)=1}}(F(s_p)+\varepsilon e^{14})\left(\pi(N;p,N)-\frac{\pi(N)}{\varphi(p)}\right)\\
&=\frac{e^{\gamma}N}{4}\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{\varphi(p)\log(N^{1/2}/p)}+O\left(\frac{N}{\log N}\right)\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{\varphi(p)\log(N^{1/2}/p)}\\
&\quad+O\left(\frac{\varepsilon N}{\log N}\right)\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{\varphi(p)}+O\left(\sum_{\substack{z\le p<y\\(p,N)=1}}\left(\pi(N;p,N)-\frac{\pi(N)}{\varphi(p)}\right)\right),
\end{aligned}
$$

对于第四项, 由 Bombieri-Vinogradov 定理知第四项即为 $O(N/(\log N)^3)$, 由 Mertens 定理得

$$
\begin{aligned}
\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{\varphi(p)}&=\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{p-1}\\
&\le 2\sum_{z\le p<y}\frac{1}{p}\\
&=2\log\log y-2\log\log z+O\left(\frac{1}{\log N}\right)\\
&=2\log(8/3)+O\left(\frac{1}{\log N}\right)\\
&=O(1),
\end{aligned}
$$

因此第三项就是 $O(\varepsilon N/\log N)$, 第二项就是

$$
\begin{aligned}
\frac{N}{\log N}\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{\varphi(p)\log(N^{1/2}/p)}&=\frac{N}{(\log N)^2}\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{\log N}{\varphi(p)\log(N^{1/2}/p)}\\
&\ll\frac{N}{(\log N)^2}\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{\varphi(p)}\\
&\ll\frac{N}{(\log N)^2},
\end{aligned}
$$

故

$$
\sum_{\substack{z\le p<y\\(p,N)=1}}(F(s_p)+\varepsilon e^{14})|A_p|=\frac{e^{\gamma}N}{4}\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{\varphi(p)\log(N^{1/2}/p)}+O\left(\frac{\varepsilon N}{\log N}\right).
$$

代入

$$
\frac{1}{\varphi(p)}=\frac{1}{p-1}=\frac{1}{p}+O\left(\frac{1}{p^2}\right)
$$

得

$$
\frac{e^{\gamma}N}{4}\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{\varphi(p)\log(N^{1/2}/p)}=\frac{e^{\gamma}N}{4}\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{p\log(N^{1/2}/p)}+O\left(N\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{p^2\log(N^{1/2}/p)}\right),
$$

上式中第二项就是

$$\begin{aligned} N\sum_{\substack{z\le p<y\\(p,N)=1}}\frac{1}{p^2\log(N^{1/2}/p)} &\le N\sum_{z\le p<y}\frac{1}{p^2\log(N^{1/2}/y)}\\ &=\frac{6N}{\log N}\sum_{z\le p<y}\frac{1}{p^2}\\ &=\frac{6N}{\log N}\sum_{n\ge z}\frac{1}{n^2}\\ &\ll\frac{N}{z\log N}\\ &=\frac{N^{7/8}}{\log N}. \end{aligned}$$

现设

$$S(t)=\sum_{p<t}\frac{1}{p}=\log\log t+M+O\left(\frac{1}{\log t}\right),\qquad u(t)=\frac{1}{\log(N^{1/2}/t)},$$

其中 M 是 Mertens 常数, 则由 Riemann-Stieltjes 积分的分部积分得

$$\begin{aligned} \sum_{z\le p<y}\frac{1}{p\log(N^{1/2}/p)} &=\int_z^y\frac{\mathrm{d}S(t)}{\log(N^{1/2}/t)}=\int_z^y u(t)\,\mathrm{d}S(t)\\ &=u(y)S(y)-u(z)S(z)-\int_z^y S(t)\,\mathrm{d}u(t)\\ &=u(y)(\log\log y+M)-u(z)(\log\log z+M)-\int_z^y(\log\log t+M)\,\mathrm{d}u(t)\\ &\quad+O\left(\frac{u(y)}{\log z}\right)+O\left(\int_z^y\frac{\mathrm{d}u(t)}{\log t}\right)\\ &=\int_z^y u(t)\,\mathrm{d}\log\log t+O\left(\frac{1}{(\log N)^2}\right)\\ &=\int_z^y\frac{\mathrm{d}t}{t\log t\log(N^{1/2}/t)}+O\left(\frac{1}{(\log N)^2}\right)\\ &=\frac{1}{\log N}\int_{1/8}^{1/3}\frac{\mathrm{d}\alpha}{\alpha((1/2)-\alpha)}+O\left(\frac{1}{(\log N)^2}\right)\\ &=\frac{2\log 6}{\log N}+O\left(\frac{1}{(\log N)^2}\right), \end{aligned}$$

其中使用了换元 $t=N^{\alpha}$. 综上, 有

$$\sum_{\substack{z\le p<y\\(p,N)=1}}(F(s_p)+\varepsilon e^{14})|A_p|=\frac{e^{\gamma}N\log 6}{2\log N}+O\left(\frac{\varepsilon N}{\log N}\right)=\left(\frac{e^{\gamma}\log 6}{2}+O(\varepsilon)\right)\frac{N}{\log N},$$

故

$$\sum_{z\le p<y}S(A_p,\mathcal{P},z)<\left(\frac{e^{\gamma}\log 6}{2}+O(\varepsilon)\right)\frac{NV(z)}{\log N},$$

引理得证. □

最后估计 $S(B,\mathcal{P},y)$.

依旧选定 $\varepsilon\in(0,1/200)$, 定义

$$\ell_k=z(1+\varepsilon)^k,$$

使得 $z\le\ell_k<y$, 则

$$0\le k\le\frac{\log(y/z)}{\log(1+\varepsilon)}\ll\frac{\log N}{\varepsilon},$$

再定义

$$B^{(k)}=\{N-p_1p_2p_3:z\le p_1<y\le p_2\le p_3,\,\ell_k\le p_1<\ell_{k+1},\,\ell_kp_2p_3<N,\,(p_2p_3,N)=1\},$$

$$\tilde{B}=\bigcup_k B^{(k)},$$

回忆 B 的定义

$$B=\{N-p_1p_2p_3:p_1p_2p_3<N,\,(p_1p_2p_3,N)=1,\,z\le p_1<y\le p_2\le p_3\}$$

可知

$$B\subseteq\tilde{B}\subseteq\{N-p_1p_2p_3:z\le p_1<y\le p_2\le p_3,\,p_1p_2p_3<(1+\varepsilon)N\},$$

显然诸 $B^{(k)}$ 是无交的, 所以

$$|\tilde{B}|=\sum_k|B^{(k)}|,\qquad S(B,\mathcal{P},y)\le S(\tilde{B},\mathcal{P},y)=\sum_k S(B^{(k)},\mathcal{P},y).$$

所以问题就转化为了估计 $S(B^{(k)},\mathcal{P},y)$, 由 Jurkat-Richert 定理得

$$S(B^{(k)},\mathcal{P},y)<(F(s)+\varepsilon e^{14})|B^{(k)}|V(y)+\sum_{\substack{d|P(y)\\d<D}}|r_d^{(k)}|,$$

其中

$$D=\frac{N^{1/2}}{(\log N)^A},\qquad r_d^k=|B_d^{(k)}|-\frac{|B^{(k)}|}{\varphi(d)},\qquad s=\frac{\log D}{\log y}$$

常数 A 待定.

引理 46.

$$\sum_{\substack{d|P(y)\\d<D}}|r_d^{(k)}|\ll\frac{N}{(\log N)^4}.$$

证明. 由定义可知

$$\begin{aligned}r_d^{(k)}&=|B_d^{(k)}|-\frac{|B^{(k)}|}{\varphi(d)}\\&=\sum_{\substack{z\le p_1<y\le p_2\le p_3\\\ell_k\le p_1\le\ell_{k+1}\\\ell_kp_2p_3<N\\p_1p_2p_3\equiv N\pmod d}}1-\frac{1}{\varphi(d)}\sum_{\substack{z\le p_1<y\le p_2\le p_3\\\ell_k\le p_1\le\ell_{k+1}\\\ell_kp_2p_3<N\\(p_2p_3,N)=1}}1\end{aligned}$$

$$= \sum_{\substack{z\le p_1<y\le p_2\le p_3\\ \ell_k\le p_1\le \ell_{k+1}\\ \ell_k p_2p_3<N\\ p_1p_2p_3\equiv N \pmod d}} 1 - \frac{1}{\varphi(d)} \sum_{\substack{z\le p_1<y\le p_2\le p_3\\ \ell_k\le p_1\le \ell_{k+1}\\ \ell_k p_2p_3<N\\ (p_2p_3,N)=1\\ (p_1p_2p_3,d)=1}} 1 - \frac{1}{\varphi(d)} \sum_{\substack{z\le p_1<y\le p_2\le p_3\\ \ell_k\le p_1\le \ell_{k+1}\\ \ell_k p_2p_3<N\\ (p_2p_3,N)=1\\ (p_1p_2p_3,d)\ne 1}} 1,$$

由 $d \mid P(y)$ 知 $(p_2p_3, d) = 1$, 所以 $(p_1p_2p_3, d) \ne 1$ 等价于 $p_1 \mid d$, 所以

$$\begin{aligned} 0 \le \frac{1}{\varphi(d)} \sum_{\substack{z\le p_1<y\le p_2\le p_3\\ \ell_k\le p_1\le \ell_{k+1}\\ \ell_k p_2p_3<N\\ (p_2p_3,N)=1\\ (p_1p_2p_3,d)\ne 1}} 1 &\le \frac{1}{\varphi(d)} \sum_{\substack{p_1p_2p_3<(1+\varepsilon)N\\ p_1\mid d,\, p_1\ge z}} 1 \\ &= \frac{1}{\varphi(d)} \sum_{p_1\mid d,\, p_1\ge z} \sum_{p_2p_3<(1+\varepsilon)N/p_1} 1 \\ &\le \frac{(1+\varepsilon)N}{\varphi(d)} \sum_{p_1\mid d,\, p_1\ge z} \frac{1}{p_1} \\ &\le \frac{(1+\varepsilon)N\omega(d)}{z\varphi(d)} \\ &\ll \frac{N\log d}{z\varphi(d)}. \end{aligned}$$

现定义集合

$$B' = \{n = p_2p_3 : y \le p_2 \le p_3,\, (p_2p_3, N) = 1\},$$

设

$$a_n = \begin{cases} 1, & n \in B', \\ 0, & n \notin B', \end{cases}$$

则可将 $r_d^{(k)}$ 写为

$$r_d^{(k)} = \sum_{n<X} \sum_{\substack{Z\le p<Y\\ np\equiv N \pmod d}} a_n - \frac{1}{\varphi(d)} \sum_{n<X} \sum_{\substack{Z\le p<Y\\ (np,d)=1}} a_n + O\left(\frac{N\log d}{z\varphi(d)}\right),$$

其中 $X = N/\ell_k$, $Y = \min\{y, \ell_{k+1}\}$, $Z = \max\{z, \ell_k\}$, 再设

$$D^* = \frac{(XY)^{1/2}}{(\log Y)^A},$$

由 $\ell_k < y$ 知 $y/\ell_k > 1$, 再结合 $1 + \varepsilon > 1$ 得

$$D^* = \frac{(XY)^{1/2}}{(\log Y)^A} \ge \frac{N^{1/2}\min\{y/\ell_k, 1+\varepsilon\}^{1/2}}{(\log y)^A} > \frac{N^{1/2}}{(\log N)^A} = D,$$

并且

$$D^* < (XY)^{1/2} \le (Ny)^{1/2} < N.$$

在引理 39 中取 $A=6$ 即得

$$\begin{aligned}\sum_{\substack{d<D\\ d\mid P(y)}}|r_d^{(k)}| &\le \sum_{d<D^*}|r_d^{(k)}|\\ &= \sum_{d<D^*}\left|\sum_{n<X}\sum_{\substack{Z\le p<Y\\ np\equiv N \pmod d}}a_n-\frac{1}{\varphi(d)}\sum_{n<X}\sum_{\substack{Z\le p<Y\\ (np,d)=1}}a_n\right|+\sum_{d<D^*}O\left(\frac{N\log d}{z\varphi(d)}\right)\\ &\ll \frac{XY(\log XY)^2}{(\log Y)^6}+\frac{N\log D^*}{z}\sum_{d<D^*}\frac{1}{\varphi(d)}\\ &\ll \frac{N}{(\log N)^{6-2}}+N^{7/8}(\log D^*)^2\\ &\ll \frac{N}{(\log N)^4}+N^{7/8}(\log N)^2\\ &\ll \frac{N}{(\log N)^4},\end{aligned}$$

引理得证. □

引理 47. 设 $0<\varepsilon<1/200$, 则当 N 足够大时有

$$S(B,\mathcal{P},y)<\left(\frac{ce^\gamma}{2}+O(\varepsilon)\right)\frac{NV(z)}{\log N}+O\left(\frac{N}{\varepsilon(\log N)^3}\right),$$

其中

$$c=\int_{1/8}^{1/3}\frac{\log(2-3\beta)}{\beta(1-\beta)}\mathrm{d}\beta=0.363\ldots$$

是一个常数.

证明. 与之前相同, 当 N 足够大时,

$$s=\frac{\log D}{\log y}=\frac{3}{2}+O\left(\frac{\log\log N}{\log N}\right)\in[1,3],$$

所以

$$F(s)=\frac{2e^\gamma}{s}=\frac{4e^\gamma}{3}+O\left(\frac{\log\log N}{\log N}\right)=\frac{4e^\gamma}{3}+O\left(\varepsilon\right).$$

由于

$$\frac{V(y)}{V(z)}=\frac{\mathfrak{S}_2(N)e^{-\gamma}/\log y\,(1+O\left(1/\log N\right))}{\mathfrak{S}_2(N)e^{-\gamma}/\log z\,(1+O\left(1/\log N\right))}=\frac{\log z}{\log y}\left(1+O\left(\frac{1}{\log N}\right)\right)=\frac{3}{8}+O\left(\frac{1}{\log N}\right),$$

所以

$$\begin{aligned}S(B^{(k)},\mathcal{P},y)&<\left(\frac{4e^\gamma}{3}+O(\varepsilon)\right)\left(\frac{3}{8}+O\left(\frac{1}{\log N}\right)\right)|B^{(k)}|V(z)+O\left(\frac{N}{(\log N)^4}\right)\\ &<\left(\frac{e^\gamma}{2}+O(\varepsilon)\right)|B^{(k)}|V(z)+O\left(\frac{N}{(\log N)^4}\right),\end{aligned}$$

求和得

$$S(B,\mathcal{P},y)\le\sum_k S(B^{(k)},\mathcal{P},y)<\left(\frac{e^\gamma}{2}+O(\varepsilon)\right)|\tilde{B}|V(z)+O\left(\frac{N}{\varepsilon(\log N)^3}\right),$$

其中对余项使用了 $k\ll\log N/\varepsilon$.

接下来估计 $|\tilde{B}|$, 由素数定理知对足够大的 N, 有

$$\pi\left(\frac{(1+\varepsilon)N}{p_1p_2}\right)<\frac{C(1+\varepsilon)N}{p_1p_2\log((1+\varepsilon)N/(p_1p_2))}<\frac{(1+2\varepsilon)N}{p_1p_2\log(N/(p_1p_2))},$$

其中 C 是一个正常数, 若 $p_1\le p_2\le p_3$ 且 $p_1p_2p_3<(1+\varepsilon)N$, 则 $p_1p_2^2<(1+\varepsilon)N$, $p_3<(1+\varepsilon)N/(p_1p_2)$, 所以

$$\begin{aligned}|\tilde{B}|&=\sum_{N-p_1p_2p_3\in\tilde{B}}1\le\sum_{\substack{z\le p_1<y\le p_2\le p_3\\ p_1p_2p_3<(1+\varepsilon)N}}1\\&\le\sum_{\substack{z\le p_1<y\le p_2\\ p_1p_2^2<(1+\varepsilon)N}}\pi\left(\frac{(1+\varepsilon)N}{p_1p_2}\right)\\&<(1+2\varepsilon)N\sum_{z\le p_1<y}\frac{1}{p_1}\sum_{y\le p_2<((1+\varepsilon)N/p_1)^{1/2}}\frac{1}{p_2\log(N/(p_1p_2))}.\end{aligned}$$

设

$$h(t)=\frac{1}{\log(N/p_1t)},\qquad H(u)=\int_y^{(N/u)^{1/2}}\frac{1}{\log(N/ut)}\,\mathrm{d}\log\log t,$$

显然 h 在 $(0,N/p_1)$ 上递增, 由 $y=N^{1/3}$ 知 $(N/y)^{1/2}=y$, 所以 $H(y)=0$. 而 $H(z)$ 则可由换元 $t=N^\alpha$ 得到

$$\begin{aligned}0<H(z)&=\int_{N^{1/3}}^{N^{7/16}}\frac{1}{\log(N^{7/8}/t)}\,\mathrm{d}\log\log t\\&=\frac{1}{\log N}\int_{1/3}^{7/16}\frac{\mathrm{d}\alpha}{7\alpha/8-\alpha^2}\\&=O\left(\frac{1}{\log N}\right),\end{aligned}$$

此外, 容易证明 H 在 $[N^{1/8},N^{1/3}]$ 上单调递减.

设

$$S(t)=\sum_{p<t}\frac{1}{p}=\log\log t+M+O\left(\frac{1}{\log t}\right),$$

其中 M 是 Mertens 常数, 由 Riemann-Stieltjes 积分知

$$\begin{aligned}\sum_{y\le p_2<((1+\varepsilon)N/p_1)^{1/2}}\frac{1}{p_2\log(N/(p_1p_2))}&=\sum_{y\le p_2<((1+\varepsilon)N/p_1)^{1/2}}\frac{h(p_2)}{p_2}\\&=\int_y^{((1+\varepsilon)N/p_1)^{1/2}}h(t)\,\mathrm{d}S(t)\end{aligned}$$

$$
\begin{aligned}
&= \int_y^{((1+\varepsilon)N/p_1)^{1/2}} h(t)\,\mathrm{d}\log\log t + O\left(\frac{h(((1+\varepsilon)N/p_1)^{1/2})}{\log y}\right)\\
&= \int_y^{(N/p_1)^{1/2}} \frac{1}{\log(N/p_1t)}\,\mathrm{d}\log\log t\\
&\quad + \int_{(N/p_1)^{1/2}}^{((1+\varepsilon)N/p_1)^{1/2}} \frac{1}{\log(N/p_1t)}\,\mathrm{d}\log\log t\\
&\quad + O\left(\frac{h(((1+\varepsilon)N/p_1)^{1/2})}{\log y}\right),
\end{aligned}
$$

再由

$$
\begin{aligned}
\frac{h(((1+\varepsilon)N/p_1)^{1/2})}{\log y} &= \frac{2}{\log\left(\frac{N}{(1+\varepsilon)p_1}\right)\log y}\\
&\le \frac{2}{\log\left(\frac{N}{(1+\varepsilon)y}\right)\log y}\\
&= \frac{2}{\log\left(\frac{N^{2/3}}{1+\varepsilon}\right)\log N^{1/3}}\\
&\ll \frac{1}{(\log N)^2}
\end{aligned}
$$

和

$$
\begin{aligned}
\int_{(N/p_1)^{1/2}}^{((1+\varepsilon)N/p_1)^{1/2}} \frac{1}{\log(N/p_1t)}\,\mathrm{d}\log\log t &= \int_{(N/p_1)^{1/2}}^{((1+\varepsilon)N/p_1)^{1/2}} \frac{1}{t\log t\log(N/p_1t)}\,\mathrm{d}t\\
&= \int_1^{(1+\varepsilon)^{1/2}} \frac{\mathrm{d}s}{s\log\left((N/p_1)^{1/2}s\right)\log\left((N/p_1)^{1/2}s^{-1}\right)}\\
&= \int_1^{(1+\varepsilon)^{1/2}} \frac{\mathrm{d}s}{s\left(\log\left((N/p_1)^{1/2}\right)+\log s\right)\left(\log\left((N/p_1)^{1/2}\right)-\log s\right)}\\
&= \int_1^{(1+\varepsilon)^{1/2}} \frac{\mathrm{d}s}{s\left(\left(\log\left((N/p_1)^{1/2}\right)\right)^2-(\log s)^2\right)}\\
&\ll \frac{1}{(\log N)^2}\int_1^{(1+\varepsilon)^{1/2}} \frac{\mathrm{d}s}{s}\\
&\ll \frac{1}{(\log N)^2}
\end{aligned}
$$

知

$$
\sum_{y\le p_2<((1+\varepsilon)N/p_1)^{1/2}} \frac{1}{p_2\log(N/(p_1p_2))} = H(p_1) + O\left(\frac{1}{(\log N)^2}\right),
$$

所以

$$
\sum_{z\le p_1<y}\frac{1}{p_1}\sum_{y\le p_2<((1+\varepsilon)N/p_1)^{1/2}} \frac{1}{p_2\log(N/(p_1p_2))} = \sum_{z\le p_1<y}\frac{H(p_1)}{p_1} + O\left(\frac{1}{(\log N)^2}\right)\sum_{z\le p_1<y}\frac{1}{p_1},
$$

对于上式第二项,

$$\begin{aligned}\sum_{z\le p_1<y}\frac{1}{p_1}&=\log\log y-\log\log z+O\left((\log z)^{-1}\right)\\&=\log(8/3)+O\left((\log N)^{-1}\right)\\&=O(1),\end{aligned}$$

对于第一项, 做换元 $t=N^{\alpha}$, $u=N^{\beta}$,

$$\begin{aligned}\sum_{z\le p_1<y}\frac{H(p_1)}{p_1}&=\int_z^y H(u)\,\mathrm{d}S(u)\\&=\int_z^y H(u)\,\mathrm{d}\log\log u+O\left(\frac{H(z)}{\log y}\right)\\&=\int_{N^{1/8}}^{N^{1/3}}\int_{N^{1/3}}^{(N/u)^{1/2}}\frac{1}{\log(N/ut)}\,\mathrm{d}\log\log t\,\mathrm{d}\log\log u+O\left(\frac{1}{(\log N)^2}\right)\\&=\frac{1}{\log N}\int_{1/8}^{1/3}\int_{1/3}^{(1-\beta)/2}\frac{\mathrm{d}\alpha\,\mathrm{d}\beta}{\alpha\beta(1-\alpha-\beta)}+O\left(\frac{1}{(\log N)^2}\right)\\&=\frac{1}{\log N}\int_{1/8}^{1/3}\frac{\log(2-3\beta)}{\beta(1-\beta)}\,\mathrm{d}\beta+O\left(\frac{1}{(\log N)^2}\right)\\&=\frac{c}{\log N}+O\left(\frac{1}{(\log N)^2}\right),\end{aligned}$$

其中

$$c=\int_{1/8}^{1/3}\frac{\log(2-3\beta)}{\beta(1-\beta)}\mathrm{d}\beta,$$

所以

$$|\tilde{B}|<(1+2\varepsilon)N\sum_{z\le p_1<y}\frac{1}{p_1}\sum_{y\le p_2<((1+\varepsilon)N/p_1)^{1/2}}\frac{1}{p_2\log(N/(p_1p_2))}=\frac{(1+O(\varepsilon))cN}{\log N}+O\left(\frac{N}{(\log N)^2}\right),$$

$$S(B,\mathcal{P},y)<\left(\frac{e^{\gamma}}{2}+O(\varepsilon)\right)|\tilde{B}|V(z)+O\left(\frac{N}{\varepsilon(\log N)^3}\right)<\left(\frac{ce^{\gamma}}{2}+O(\varepsilon)\right)\frac{NV(z)}{\log N}+O\left(\frac{N}{\varepsilon(\log N)^3}\right),$$

引理得证. □

2.7.4 陈景润定理的证明

定理 24 (陈景润)**.** 设 $r(N)$ 为将偶数 N 表示为 $N=p+n$ 的形式的方法数, 其中 p 是一个奇素数, n 是至多两个素数的积, 则对于足够大的 N, 有

$$r(N)>0.084\frac{\mathfrak{S}_2(N)N}{(\log N)^2}>0.$$

证明. 由

$$V(z)=\mathfrak{S}_2(N)\frac{e^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right)=\mathfrak{S}_2(N)\frac{8e^{-\gamma}}{\log N}\left(1+O\left(\frac{1}{\log N}\right)\right),$$

和上一节的三个估计可得

$$\begin{aligned} r(N) &> S(A,\mathcal{P},z) - \frac{1}{2}\sum_{z\le q<y} S(A_q,\mathcal{P},z) - \frac{1}{2}S(B,\mathcal{P},y) - 2N^{7/8} - N^{1/3} \\ &> (2\log 3 - \log 6 - c - O(\varepsilon))\frac{e^\gamma NV(z)}{4\log N} + O\left(\frac{N}{\varepsilon(\log N)^3}\right) - 2N^{7/8} - N^{1/3} \\ &> (2\log 3 - \log 6 - c - O(\varepsilon))\mathfrak{S}_2(N)\frac{2N}{(\log N)^2}\left(1 + O\left(\frac{1}{\log N}\right)\right) + O\left(\frac{N}{\varepsilon(\log N)^3}\right), \end{aligned}$$

数值计算得到

$$2\log 3 - \log 6 - c \approx 0.0423\ldots > 0,$$

因为式中 $O(\varepsilon)$ 的 O 常数与 ε 无关, 所以可取 ε 足够小使得

$$2\log 3 - \log 6 - c - O(\varepsilon) > 0.0421 > 0,$$

此时 $O(N/(\varepsilon(\log N)^3))$ 就变为 $O(N/(\log N)^3)$, 因此当 N 足够大时, 总有

$$r(N) > 0.0842\frac{\mathfrak{S}_2(N)N}{(\log N)^2} + O\left(\frac{N}{(\log N)^3}\right) > 0.084\frac{\mathfrak{S}_2(N)N}{(\log N)^2} > 0,$$

定理得证. □

2.8 奇偶障碍

通过类似的方法, 陈景润定理也可以类比到孪生素数问题上, 但实践表明, 只使用筛法很难将 “至多两个素因子” 降为 “素数”, 更准确的说, 筛法无法区分一个数的素因子个数的奇偶, 这一困难最早被 Selberg 发现, 现被称为奇偶障碍, 这就是只使用筛法无法证明 Goldbach 猜想和孪生素数猜想的原因 [8].

本节的所有讨论都是非正式的.

奇偶障碍. 设 S 是一个正整数集合, 对于其中的任一元素 n, 都满足 $\Omega(n)$ 为奇数 (或偶数), 则只使用筛法无法得到 $|S|$ 的非平凡下界估计.

在筛法的一般框架中, 假设 A 是一个整数集合, $\mathcal{P}$ 是一些素数组成的集合,

$$P(z) = \prod_{\substack{p\in\mathcal{P}\\ p<z}} p,$$

则筛法估计

$$S(A,\mathcal{P},z) = \sum_{\substack{n\in A\\ (n,P(z))=1}} 1,$$

而对于一般的 z, 被上式计数的数中, 虽然不能是小于 z 的 $\mathcal{P}$ 中素数的倍数, 但仍可能是大于等于 z 的素数的倍数, 特别的, 有可能是合数, 如果按照素因子个数 Ω 分类, 就有

$$S(A,\mathcal{P},z) = \sum_{\substack{n\in A\\ (n,P(z))=1\\ \Omega(n)=0}} 1 + \sum_{\substack{n\in A\\ (n,P(z))=1\\ \Omega(n)=1}} 1 + \sum_{\substack{n\in A\\ (n,P(z))=1\\ \Omega(n)=2}} 1 + \cdots$$

在解析数论中, 我们非常关心 $\Omega(n)$ 只为奇数或偶数的情形, 所以我们想要估计和式

$$\sum_{\substack{n\in A\\(n,P(z))=1\\ \Omega(n)\equiv 1 \pmod 2}} 1 = \sum_{\substack{n\in A\\ \Omega(n)\equiv 1 \pmod 2}} \sum_{d\mid (n,P(z))} \mu(d),$$

以下假设 $i=0$ 或 1,

$$A^{(i)} = \{n\in A : \Omega(n)\equiv i \pmod 2\}, \qquad S^{(i)} = \sum_{\substack{n\in A\\(n,P(z))=1\\ \Omega(n)\equiv i \pmod 2}} 1,$$

则

$$S^{(i)} = \sum_{n\in A^{(i)}} \sum_{d\mid (n,P(z))} \mu(d) = \sum_{d\mid P(z)} \mu(d)|A_d^{(i)}|,$$

在筛法中, 我们设

$$\sum_{d\mid n} \lambda^-(d) \le \sum_{d\mid n} \mu(d) \le \sum_{d\mid n} \lambda^+(d),$$

则

$$\sum_{d\mid P(z)} \lambda^-(d)|A_d^{(i)}| \le S^{(i)} \le \sum_{d\mid P(z)} \lambda^+(d)|A_d^{(i)}|,$$

设

$$a_n^{(i)} = \frac{1+(-1)^i\lambda(n)}{2} = \begin{cases} 1, & \Omega(n)\equiv i \pmod 2,\\ 0, & \Omega(n)\not\equiv i \pmod 2, \end{cases}$$

其中 λ 是 Liouville 函数, 则

$$|A_d^{(i)}| = \sum_{\substack{n\in A\\ d\mid n}} a_n^{(i)} = \frac{1}{2}\left(\sum_{\substack{n\in A\\ d\mid n}} 1 + (-1)^i \sum_{\substack{n\in A\\ d\mid n}} \lambda(n)\right) = \frac{1}{2}\left(|A_d| + (-1)^i \sum_{\substack{n\in A\\ d\mid n}} \lambda(n)\right),$$

$$\sum_{d\mid P(z)} \lambda^{\pm}(d)|A_d^{(i)}| = \frac{1}{2}\sum_{d\mid P(z)} \lambda^{\pm}(d)|A_d| + \frac{(-1)^i}{2}\sum_{d\mid P(z)}\sum_{\substack{n\in A\\ d\mid n}} \lambda^{\pm}(d)\lambda(n),$$

记

$$M^{\pm} = \frac{1}{2}\sum_{d\mid P(z)} \lambda^{\pm}(d)|A_d|, \qquad E^{\pm} = \frac{1}{2}\sum_{d\mid P(z)}\sum_{\substack{n\in A\\ d\mid n}} \lambda^{\pm}(d)\lambda(n)$$

分别为主项和误差项, 其中 $M^{\pm}$ 的估计就是筛法的任务, 而筛法本身无法提供 $E^{\pm}$ 中的 Liouville 函数 $\lambda(n)$ 的信息, 只能使用其他工具估计 (实际上, 实践表明即使假设了广义 Riemann 猜想, 在很多问题中也无法提供该和式的有效估计), 因此 $S^{(i)}$ 的上下界必然是

$$M^- - |E^-| \le S^{(i)} \le M^+ + |E^+|$$

的形式, 而上下界均与 i 无关, 即使用筛法得到的 $S^{(1)}$ 与 $S^{(0)}$ 的上界必然是相同的, 下界也必然是相同的. 现设 S 是一个正整数集合, 对于其中的任一元素 n, 都满足 $\Omega(n)$ 为奇数, 取 $A=S$, 则 $|S|\ge S^{(1)}$,

$S^{(0)}=0$, 若 $S^{(1)}$ 的下界估计是非平凡的, 即 $M^- - |E^-| > 0$, 则也有 $S^{(0)} > 0$, 这是不可能的, 因此必然 $M^- - |E^-| \le 0$, 当 S 中元素都满足 $\Omega(n)$ 为偶数时同理, 也就是说, 只使用筛法无法得到 $|S|$ 的非平凡下界估计.

例如, 取 $A=\{p_1 = N - p_2 : p_2 < N\}$, 此时 $|A| \ge S^{(1)}$, $S^{(0)}=0$. 取 $A=\{p_1p_2 : p_2 = N - p_1\}$, 此时 $|A| \ge S^{(0)}$, $S^{(1)}=0$.

附录 A　Siegel-Walfisz 定理

Siegel-Walfisz 定理的证明比较复杂, 这里就不写了, 仅作一些讨论. 近日 AI 关于 L 函数于 $\mathrm{Re}(s) > 7/8$ 半平面内无零点的证明可以直接推出 Siegel-Walfisz 定理, 而且结论更强. 此外, AI 还发现了一种更简单初等的方法来证明 Landau-Siegel 零点不存在, 这使得 Siegel-Walfisz 定理中的常数由非实效变为实效, 见本网站下一篇文章.

定理 25 (Siegel-Walfisz 定理)**.** *对任意实数 $A>1$, 若 $q \le (\log x)^A$, $(a,q)=1$, 则存在只依赖于 A 的正实数 $c(A)$, 有*

$$\pi(x;q,a) = \frac{\mathrm{Li}(x)}{\varphi(q)} + O\left(xe^{-c(A)\sqrt{\log x}}\right),$$
$$\theta(x;q,a) = \frac{x}{\varphi(q)} + O\left(xe^{-c(A)\sqrt{\log x}}\right),$$
$$\psi(x;q,a) = \frac{x}{\varphi(q)} + O\left(xe^{-c(A)\sqrt{\log x}}\right),$$

其中大 O 常数只与 A 有关.

现假设 $q \le (\log N)^A$, $x \le N$, 当 $x \le \sqrt{N}$ 时,

$$\left|\pi(x;q,a) - \frac{\mathrm{Li}(x)}{\varphi(q)}\right| \le \pi(x;q,a) + \frac{\mathrm{Li}(x)}{\varphi(q)} \le 2x \le 2\sqrt{N} \ll \frac{N}{(\log N)^C}$$

对任意 $C>0$ 成立, 当 $x \ge \sqrt{N}$ 时, $N \le x^2$, 则 $q \le (\log N)^{2A}$, 所以

$$\pi(x;q,a) = \frac{\mathrm{Li}(x)}{\varphi(q)} + O\left(xe^{-c(A)\sqrt{\log x}}\right) = \frac{\mathrm{Li}(x)}{\varphi(q)} + O\left(Ne^{-(c(A)/\sqrt{2})\sqrt{\log N}}\right) = \frac{\mathrm{Li}(x)}{\varphi(q)} + O\left(\frac{N}{(\log N)^C}\right)$$

对任意 $C>0$ 成立, 这样就得到了 1.2.2 节中的 Siegel-Walfisz 定理.

此外, 还有一种推论.

定理 26. *设 $q \le (\log x)^A$, χ 是模 q 的非主特征, 则对于任意的 $y \in (1,x]$, 都有*

$$|\psi(y,\chi)| \ll \frac{x}{(\log x)^A}.$$

证明. 由 Dirichlet 特征的正交性得

$$\psi(y,\chi) = \sum_{\substack{a=1\\(a,q)=1}}^{q} \chi(a)\psi(y;q,a),$$

由于 $\chi \neq \chi_0$ 时有

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} \chi(a) = 0,$$

所以

$$\psi(y,\chi) = \sum_{\substack{a=1\\(a,q)=1}}^{q} \chi(a)\psi(y;q,a) - \frac{y}{\varphi(q)} \sum_{\substack{a=1\\(a,q)=1}}^{q} \chi(a) = \sum_{\substack{a=1\\(a,q)=1}}^{q} \chi(a)\left(\psi(y;q,a) - \frac{y}{\varphi(q)}\right).$$

当 $y \leq \sqrt{x}$ 时,

$$|\psi(y,\chi)| \ll y \leq \sqrt{x} \ll \frac{x}{(\log x)^A}.$$

当 $y > \sqrt{x}$ 时, $2\log y > \log x$, 所以 $q \leq (\log x)^A \ll (\log y)^A$, 由 Siegel-Walfisz 定理得

$$|\psi(y,\chi)| \leq \sum_{\substack{a=1\\(a,q)=1}}^{q} \left|\psi(y;q,a) - \frac{y}{\varphi(q)}\right| \ll \varphi(q) y e^{-c(A)\sqrt{\log y}} \ll (\log x)^A y e^{-c(A)\sqrt{\log y}},$$

再由 $y \leq x$, 可得

$$|\psi(y,\chi)| \ll (\log x)^A x e^{-(c(A)/\sqrt{2})\sqrt{\log x}} \ll \frac{x}{(\log x)^A}.$$

因此对所有的 $y \leq x$ 都有

$$|\psi(y,\chi)| \ll \frac{x}{(\log x)^A},$$

定理成立. □

附录 B Bombieri-Vinogradov 定理

本节我们使用 Vaughan 的方法, 证明如下形式的 Bombieri-Vinogradov 定理, 本节参考自 [1].

定理 27 (Bombieri-Vinogradov 定理)**.** *对任意正实数 $A > 0$, 都有*

$$\sum_{q \leq Q} \max_{y \leq x} \max_{(a,q)=1} \left|\psi(y;q,a) - \frac{y}{\varphi(q)}\right| \ll x^{1/2} Q (\log x)^5,$$

对任意实数 $x > 1$ 成立, 其中

$$\frac{x^{1/2}}{(\log x)^A} \leq Q \leq x^{1/2},$$

$\ll$ 常数只依赖于 A.

特别的, 取 $Q = x^{1/2}/(\log x)^A$, $A > 5$ 即得

$$\sum_{q \leq Q} \max_{y \leq x} \max_{(a,q)=1} \left|\psi(y;q,a) - \frac{y}{\varphi(q)}\right| \ll x(\log x)^{5-A},$$

将 $5 - A$ 重写为 $-A$, 令 $B(A) = A + 5$ 就得到, 对任意正实数 $A > 0$, 总存在一个依赖 A 的正数 $B(A)$ 使得

$$\sum_{q \leq Q} \max_{y \leq x} \max_{(a,q)=1} \left|\psi(y;q,a) - \frac{y}{\varphi(q)}\right| \ll \frac{x}{(\log x)^A}$$

对任意实数 $x>1$ 成立, 其中

$$Q=\frac{x^{1/2}}{(\log x)^{B(A)}},$$

再由函数 ψ 和 π 之间的关系就得到了 2.7.3 节中的 Bombieri-Vinogradov 定理.

Bombieri-Vinogradov 定理的证明主要用到了大筛法不等式, Vaughan 恒等式以及 Siegel-Walfisz 定理.

引理 48. 设 $\{a_m\}_{m=1}^M$ 和 $\{b_n\}_{n=1}^N$ 是任意的复数列, $Q\geq 1$, 则

$$\begin{aligned}&\sum_{q\leq Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{1\leq y\leq MN}\left|\sum_{\substack{m=1\\ mn\leq y}}^{M}\sum_{n=1}^{N}a_m b_n\chi(mn)\right|\\ &\ll \log(2MN)\left((M+Q^2)(N+Q^2)\left(\sum_{m=1}^{M}|a_m|^2\right)\left(\sum_{n=1}^{N}|b_n|^2\right)\right)^{1/2},\end{aligned}$$

其中 $\sum_{\chi \bmod q}^*$ 表示对模 q 的所有原特征求和.

证明. 定义函数

$$\delta(u,x)=\begin{cases}1, & |u|<x,\\ 1/2, & |u|=x,\\ 0, & |u|>x,\end{cases}$$

则由 Fourier 反演可知

$$\hat{\delta}(t,x)=\int_{-\infty}^{\infty}\delta(u,x)e^{-itu}\,\mathrm{d}u=\int_{-x}^{x}e^{-itu}\,\mathrm{d}u=\begin{cases}2x, & t=0,\\ \dfrac{2\sin(tx)}{t}, & t\neq 0,\end{cases}$$

$$\delta(u,x)=\int_{-\infty}^{\infty}e^{iut}\frac{\sin(xt)}{\pi t}\,\mathrm{d}t,$$

则对任意 $0\leq u\neq x$, $T\geq 1$, 有

$$\begin{aligned}\delta(u,x)&=\int_{-T}^{T}e^{iut}\frac{\sin(xt)}{\pi t}\,\mathrm{d}t+O\left(\int_{T}^{\infty}\frac{e^{iut}\sin(xt)}{t}\,\mathrm{d}t+\int_{-\infty}^{-T}\frac{e^{iut}\sin(xt)}{t}\,\mathrm{d}t\right)\\ &=\int_{-T}^{T}e^{iut}\frac{\sin(xt)}{\pi t}\,\mathrm{d}t+O\left(\int_{T}^{\infty}\frac{(e^{iut}+e^{-iut})\sin(xt)}{t}\,\mathrm{d}t\right)\\ &=\int_{-T}^{T}e^{iut}\frac{\sin(xt)}{\pi t}\,\mathrm{d}t+O\left(\int_{T}^{\infty}\frac{\cos(ut)\sin(xt)}{t}\,\mathrm{d}t\right),\end{aligned}$$

由 $\sin(xt)\cos(ut)=(\sin((x+u)t)+\sin((x-u)t))/2$ 和

$$\int_{T}^{\infty}\frac{\sin(at)}{t}\,\mathrm{d}t=O\left(\frac{1}{T|a|}\right),\qquad a\neq 0$$

可得

$$\delta(u,x)=\int_{-T}^{T}e^{iut}\frac{\sin(xt)}{\pi t}\,\mathrm{d}t+O\left(\frac{1}{T|x-u|}\right).$$

取 $x=\log([y]+1/2)$, 则对任何正整数 m 和 n, $\log(mn)\neq x$, 再结合

$$\frac{1}{|x-\log(mn)|}=\left|\int_{mn}^{[y]+1/2}\frac{\mathrm{d}t}{t}\right|^{-1}\leq\frac{\max\{[y]+1/2,mn\}}{|[y]+1/2-mn|}\leq 2\max\{[y]+1/2,mn\}\ll MN,$$

可得

$$\begin{aligned}\sum_{\substack{m=1\\mn\leq y}}^{M}\sum_{n=1}^{N}a_mb_n\chi(mn)&=\sum_{m=1}^{M}\sum_{n=1}^{N}a_mb_n\chi(mn)\delta(\log(mn),x)\\&=\int_{-T}^{T}\left(\sum_{m=1}^{M}\sum_{n=1}^{N}a_mb_n\chi(mn)(mn)^{it}\right)\frac{\sin(xt)}{\pi t}\,\mathrm{d}t+O\left(T^{-1}MN\sum_{m=1}^{M}|a_m|\sum_{n=1}^{N}|b_n|\right),\end{aligned}$$

则

$$\begin{aligned}&\sum_{q\leq Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi\bmod q}\max_{1\leq y\leq MN}\left|\sum_{\substack{m=1\\mn\leq y}}^{M}\sum_{n=1}^{N}a_mb_n\chi(mn)\right|\\&\leq\left(\int_{-T}^{T}\max_{1\leq y\leq MN}\left|\frac{\sin xt}{\pi t}\right|\,\mathrm{d}t\right)\max_{|t|\leqslant T}\left(\sum_{q\leq Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi\bmod q}\left|\sum_{m=1}^{M}\sum_{n=1}^{N}a_mb_n\chi(mn)(mn)^{it}\right|\right)\\&\quad+T^{-1}Q^2MN\sum_{m=1}^{M}|a_m|\sum_{n=1}^{N}|b_n|,\end{aligned}$$

以下取 $T=(MN)^{3/2}$, 由 Cauchy-Schwarz 不等式得

$$T^{-1}Q^2MN\sum_{m=1}^{M}|a_m|\sum_{n=1}^{N}|b_n|\ll Q^2\left(\sum_{m=1}^{M}|a_m|^2\right)^{1/2}\left(\sum_{n=1}^{N}|b_n|^2\right)^{1/2},$$

由 Cauchy-Schwarz 不等式和大筛法不等式得

$$\begin{aligned}&\sum_{q\leq Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi\bmod q}\left|\sum_{m=1}^{M}\sum_{n=1}^{N}a_mb_n\chi(mn)(mn)^{it}\right|\\&\ll\left(\sum_{q\leq Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi\bmod q}\left|\sum_{m=1}^{M}a_m\chi(m)m^{it}\right|^2\right)^{1/2}\left(\sum_{q\leq Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi\bmod q}\left|\sum_{n=1}^{N}b_n\chi(n)n^{it}\right|^2\right)^{1/2}\\&\ll\left((M+Q^2)\sum_{m=1}^{M}|a_m|^2\right)^{1/2}\left((N+Q^2)\sum_{n=1}^{N}|b_n|^2\right)^{1/2},\end{aligned}$$

由 $|\sin(xt)|\leq\min\{1,|xt|\}$ 知

$$\begin{aligned}\int_{-T}^{T}\max_{1\leq y\leq MN}\left|\frac{\sin xt}{\pi t}\right|\,\mathrm{d}t&\ll\int_{-T}^{T}\max_{1\leq y\leq MN}\min\left\{\frac{1}{|t|},\log\left([y]+\frac{1}{2}\right)\right\}\,\mathrm{d}t\\&\ll\int_{-T}^{T}\min\left\{\frac{1}{|t|},\log\left(MN+\frac{1}{2}\right)\right\}\,\mathrm{d}t\end{aligned}$$

$$\ll \int_0^1 \log\left(MN+\frac{1}{2}\right)\mathrm{d}t+\int_1^T \frac{1}{t}\,\mathrm{d}t$$
$$\ll \log 2MN,$$

此处写为 $2MN$ 是防止 $MN=1$ 时对数变成 0, 综上可得

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{1\le y\le MN}\left|\sum_{\substack{m=1\\ mn\le y}}^{M}\sum_{n=1}^{N}a_m b_n\chi(mn)\right|$$
$$\ll \log(2MN)\left((M+Q^2)(N+Q^2)\left(\sum_{m=1}^{M}|a_m|^2\right)\left(\sum_{n=1}^{N}|b_n|^2\right)\right)^{1/2},$$

引理得证. □

引理 49. 设 $Q\ge 1$, $x>1$, 则有

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{y\le x}|\psi(y,\chi)|\ll (x+x^{5/6}Q+x^{1/2}Q^2)(\log x)^4.$$

证明. 当 $Q^2\ge x$ 时, 在上一个引理中取 $M=1$, $a_1=1$, $N=[x]$, $b_n=\Lambda(n)$ 即得

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{y\le x}|\psi(y,\chi)|\ll \log x\left((1+Q^2)(x+Q^2)(x(\log x)^2)\right)^{1/2}\ll Q^2x^{1/2}(\log x)^2,$$

右边显然 $\ll (x+x^{5/6}Q+x^{1/2}Q^2)(\log x)^4$, 因此以下均设 $Q^2<x$.

对每个模 q 的原特征 χ, 在 Vaughan 恒等式中取 $\Psi(m,n)=\Lambda(n)\chi(mn)$ 即得

$$\sum_{u<\ell\le y}\Lambda(\ell)\chi(\ell)=\sum_{d\le u}\sum_{u<\ell\le y/d}\sum_{m\le y/(\ell d)}\mu(d)\Lambda(\ell)\chi(dm\ell)-\sum_{u<k\le y}\sum_{u<\ell\le y/k}\sum_{\substack{d\mid k\\ d\le u}}\mu(d)\Lambda(\ell)\chi(k\ell),$$

当 $y<u$ 时显然 $|\psi(y,\chi)|\ll y<u$, 当 $y\ge u$ 时则有

$$\psi(y,\chi)=\sum_{\ell\le u}\Lambda(\ell)\chi(\ell)+\sum_{d\le u}\sum_{u<\ell\le y/d}\sum_{m\le y/(\ell d)}\mu(d)\Lambda(\ell)\chi(dm\ell)-\sum_{u<k\le y}\sum_{u<\ell\le y/k}\sum_{\substack{d\mid k\\ d\le u}}\mu(d)\Lambda(\ell)\chi(k\ell),$$

对于第一项, 显然

$$\left|\sum_{\ell\le u}\Lambda(\ell)\chi(\ell)\right|\le\sum_{\ell\le u}\Lambda(\ell)\ll u,$$

对于第二项, 设 $m\ell=r$, 则

$$\begin{aligned}\sum_{d\le u}\sum_{u<\ell\le y/d}\sum_{m\le y/(\ell d)}\mu(d)\Lambda(\ell)\chi(dm\ell)&=\sum_{d\le u}\mu(d)\sum_{r\le y/d}\chi(dr)\sum_{\substack{\ell>u\\ \ell\mid r}}\Lambda(\ell)\\&=\sum_{d\le u}\mu(d)\sum_{r\le y/d}\chi(dr)\sum_{\ell\mid r}\Lambda(\ell)-\sum_{d\le u}\mu(d)\sum_{r\le y/d}\chi(dr)\sum_{\substack{\ell\le u\\ \ell\mid r}}\Lambda(\ell)\end{aligned}$$

$$= \sum_{d\le u}\mu(d)\sum_{r\le y/d}\chi(dr)\log r - \sum_{d\le u}\mu(d)\sum_{r\le y/d}\chi(dr)\sum_{\substack{\ell\le u\\ \ell\mid r}}\Lambda(\ell),$$

设

$$S_2 = -\sum_{d\le u}\mu(d)\sum_{r\le y/d}\chi(dr)\sum_{\substack{\ell\le u\\ \ell\mid r}}\Lambda(\ell),$$

$$S_3 = \sum_{d\le u}\mu(d)\sum_{r\le y/d}\chi(dr)\log r,$$

$$S_4 = -\sum_{u<k\le y}\sum_{u<\ell\le y/k}\sum_{\substack{d\mid k\\ d\le u}}\mu(d)\Lambda(\ell)\chi(k\ell),$$

则有

$$\psi(y,\chi) = O(u) + S_2 + S_3 + S_4,$$

两边取 max 求和即得

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{y\le x}|\psi(y,\chi)| \le O(uQ^2) + T_2 + T_3 + T_4,$$

其中

$$T_i = \sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{y\le x}|S_i|, \qquad i = 2,3,4.$$

先估计 T_3, 当 χ 是主特征即 $q=1$ 时,

$$|S_3| \le \sum_{d\le u}\sum_{r\le y/d}\log r \le \sum_{r\le y}\frac{y}{r}\log r \ll y(\log y)^2,$$

当 χ 是非主特征时, 由 Pólya-Vinogradov 不等式有

$$\begin{aligned} S_3 &= \sum_{d\le u}\mu(d)\chi(d)\sum_{r\le y/d}\chi(r)\int_1^r t^{-1}\,\mathrm{d}t \\ &= \int_1^y t^{-1}\left(\sum_{d\le \min(u,yt^{-1})}\mu(d)\chi(d)\sum_{t\le r\le y/d}\chi(r)\right)\mathrm{d}t \\ &\ll u\sqrt{q}\log q\log y, \end{aligned}$$

所以利用 $Q^2 < x$ 即得

$$T_3 \ll (x + uQ^{5/2})(\log x)^2.$$

再估计 T_2, 对 S_2 换元, 令 $r = \ell m$, $k = d\ell$ 则有

$$S_2 = -\sum_{k\le u^2}\sum_{\substack{d\ell = k\\ d\le u,\,\ell\le u}}\mu(d)\Lambda(\ell)\sum_{km\le y}\chi(km),$$

再设

$$a_k = \sum_{\substack{d\ell=k\\ d\le u,\,\ell\le u}} \mu(d)\Lambda(\ell),$$

将 S_2 分为两部分

$$S_2 = S_{21} + S_{22},$$

$$S_{21} = -\sum_{k\le u}\sum_{km\le y} a_k\chi(km),$$
$$S_{22} = -\sum_{u<k\le u^2}\sum_{km\le y} a_k\chi(km),$$

相应的有

$$T_2 \le T_{21} + T_{22},$$

其中

$$T_{2i} = \sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{y\le x}|S_{2i}|, \qquad i = 1, 2.$$

对于 T_{21}, 当 χ 为非主特征时, 由 $|a_k| \le \log k$ 及 Pólya-Vinogradov 不等式得

$$|S_{21}| \le \sum_{k\le u}\log k\left|\sum_{km\le y}\chi(m)\right| \ll u\sqrt{q}\log q\log u.$$

当 χ 为主特征时, 有

$$|S_{21}| \le \sum_{k\le u}\log k\left|\sum_{km\le y}1\right| \ll \sum_{k\le u}\frac{y}{k}\log k \ll y(\log u)^2,$$

因此与 T_3 类似, 有

$$T_{21} \ll (x + uQ^{5/2})(\log x)^2.$$

对于 T_{22}, 对 k 分段, 设 M 和 M' 满足

$$u \le M < u^2, \qquad M < M' \le 2M,$$

由前一引理得,

$$\begin{aligned}
&\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{y\le x}\left|\sum_{M<k\le M'}\sum_{\substack{1\le m\le y/M\\ km\le y}} a_k\chi(k)\chi(m)\right|\\
&\ll (M+Q^2)^{1/2}(xM^{-1}+Q^2)^{1/2}x^{1/2}(\log x)^2\\
&\ll \left(x + QxM^{-1/2} + Qx^{1/2}M^{1/2} + Q^2x^{1/2}\right)(\log x)^2,
\end{aligned}$$

对所有这些分段求和, 段数为 $O(\log u)$, 由 $u \le x$ 得

$$T_{22} \ll \left(x + Qxu^{-1/2} + Qx^{1/2}u + Q^2x^{1/2}\right)(\log x)^3,$$

所以

$$T_2 \ll (x+uQ^{5/2})(\log x)^2 + \left(x + Qxu^{-1/2} + Qx^{1/2}u + Q^2x^{1/2}\right)(\log x)^3.$$

最后估计 T_4, 设

$$b_k = \sum_{\substack{d\mid k\\ d\le u}} \mu(d),$$

显然 $|b_k| \le d(k)$, 对 ℓ 分段, 设

$$u \le N < x/u, \qquad N < N' \le 2N,$$

则由上一引理得

$$\begin{aligned}
&\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{y\le x}\left|\sum_{\substack{N<\ell\le N'\\ k\ell\le y}}\sum_{u\le k\le y/N}\Lambda(\ell)\chi(\ell)b_k\chi(k)\right|\\
&\ll (N+Q^2)^{1/2}(xN^{-1}+Q^2)^{1/2}\left(\sum_{\ell=1}^{N'}(\Lambda(\ell))^2\right)^{1/2}\left(\sum_{k=1}^{x/N}(d(k))^2\right)^{1/2}\log x\\
&\ll (N+Q^2)^{1/2}(xN^{-1}+Q^2)^{1/2}N^{1/2}\left(\log N\right)^{1/2}(x/N)^{1/2}(\log x)^{5/2}\\
&\ll \left(x+QxN^{-1/2}+Qx^{1/2}N^{1/2}+Q^2x^{1/2}\right)(\log x)^3,
\end{aligned}$$

同理, 求和得

$$T_4 \ll \left(x + Qxu^{-1/2} + Q^2x^{1/2}\right)(\log x)^4.$$

综上,

$$\begin{aligned}
&\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{y\le x}|\psi(y,\chi)| \ll uQ^2 + T_{21} + T_{22} + T_3 + T_4\\
&\ll uQ^2 + (x+uQ^{5/2})(\log x)^2 + \left(x + Qxu^{-1/2} + Qx^{1/2}u + Q^2x^{1/2}\right)(\log x)^4,
\end{aligned}$$

现取

$$u = \begin{cases} x^{1/3}, & 1 \le Q \le x^{1/3},\\ Q^{-1}x^{2/3}, & x^{1/3} < Q \le x^{1/2}, \end{cases}$$

可以推出当 $Q^2 < x$ 时

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\max_{y\le x}|\psi(y,\chi)| \ll (x + x^{5/6}Q + x^{1/2}Q^2)(\log x)^4,$$

引理得证. □

Bombieri-Vinogradov 定理的证明. 由

$$\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\overline{\chi(a)}\chi(n) = \begin{cases} 1, & n \equiv a \pmod q,\\ 0, & n \not\equiv a \pmod q \end{cases}$$

知

$$\psi(y;q,a)=\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\overline{\chi(a)}\psi(y,\chi),$$

设

$$\psi'(y,\chi)=\begin{cases}\psi(y,\chi), & \chi\neq\chi_0,\\ \psi(y,\chi)-y, & \chi=\chi_0,\end{cases}$$

则有

$$\psi(y;q,a)-\frac{y}{\varphi(q)}=\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\overline{\chi(a)}\psi'(y,\chi),$$

$$\left|\psi(y;q,a)-\frac{y}{\varphi(q)}\right|\leq\frac{1}{\varphi(q)}\sum_{\chi \bmod q}|\psi'(y,\chi)|,$$

右侧与 a 无关.

现设 χ 是一个非原特征, 其对应的原特征为 $\chi^*\pmod{q^*}$, 则

$$\begin{aligned}\psi'(y,\chi^*)-\psi'(y,\chi)&=\sum_{\substack{p^k\leq y\\ p\mid q}}\chi^*(p^k)\log p\\ &\ll\sum_{p\mid q}\left[\frac{\log y}{\log p}\right]\log p\\ &\ll(\log y)\sum_{p\mid q}\log p\\ &\ll\log q\log y,\end{aligned}$$

所以

$$\left|\psi(y;q,a)-\frac{y}{\varphi(q)}\right|\ll\log q\log y+\frac{1}{\varphi(q)}\sum_{d\mid q}{\sum_{\chi \bmod d}}^{*}|\psi'(y,\chi)|,$$

$$\max_{y\leq x}\max_{(a,q)=1}\left|\psi(y;q,a)-\frac{y}{\varphi(q)}\right|\ll\log q\log x+\frac{1}{\varphi(q)}\sum_{d\mid q}{\sum_{\chi \bmod d}}^{*}\max_{y\leq x}|\psi'(y,\chi)|,$$

$$\sum_{q\leq Q}\max_{y\leq x}\max_{(a,q)=1}\left|\psi(y;q,a)-\frac{y}{\varphi(q)}\right|\ll Q\log Q\log x+\sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{d\mid q}{\sum_{\chi \bmod d}}^{*}\max_{y\leq x}|\psi'(y,\chi)|,$$

上式右侧第二项为

$$\begin{aligned}\sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{d\mid q}{\sum_{\chi \bmod d}}^{*}\max_{y\leq x}|\psi'(y,\chi)|&=\sum_{d\leq Q}\sum_{k\leq Q/d}\frac{1}{\varphi(kd)}{\sum_{\chi \bmod d}}^{*}\max_{y\leq x}|\psi'(y,\chi)|\\ &\leq\left(\sum_{k\leq Q/d}\frac{1}{\varphi(k)}\right)\sum_{d\leq Q}\frac{1}{\varphi(d)}{\sum_{\chi \bmod d}}^{*}\max_{y\leq x}|\psi'(y,\chi)|\\ &\ll\log Q\sum_{d\leq Q}\frac{1}{\varphi(d)}{\sum_{\chi \bmod d}}^{*}\max_{y\leq x}|\psi'(y,\chi)|.\end{aligned}$$

现设 $Q_1=(\log x)^A>1$, $Q_1\le U<Q$, $U<U'\le 2U$, 则当 $d>Q_1$ 时模 d 的原特征一定不是主特征, 由前一引理得

$$\sum_{U<d\le U'}\frac{1}{\varphi(d)}\sideset{}{^*}\sum_{\chi \bmod d}\max_{y\le x}|\psi'(y,\chi)|\ll\left(\frac{x}{U}+x^{5/6}+x^{1/2}U\right)(\log x)^4,$$

取 $U=2^kQ_1, k=0,1,\dots,$ 求和, 由于 $k\ll\log Q$, 有

$$\sum_{Q_1<d\le Q}\frac{1}{\varphi(d)}\sideset{}{^*}\sum_{\chi \bmod d}\max_{y\le x}|\psi'(y,\chi)|\ll\left(\frac{x}{Q_1}+x^{5/6}\log Q+x^{1/2}Q\right)(\log x)^4.$$

当 $1<d\le Q_1=(\log x)^A$ 时, 由 Siegel-Walfisz 定理得

$$|\psi(y,\chi)|\ll\frac{x}{(\log x)^{2A}},\qquad \chi\ne\chi_0,$$

$$\sum_{1<d\le Q_1}\frac{1}{\varphi(d)}\sideset{}{^*}\sum_{\chi \bmod d}\max_{y\le x}|\psi'(y,\chi)|\ll\frac{x}{(\log x)^A},$$

当 $d=1$ 时, 由素数定理得

$$\sum_{d=1}\frac{1}{\varphi(d)}\sideset{}{^*}\sum_{\chi \bmod d}\max_{y\le x}|\psi'(y,\chi)|=\max_{y\le x}|\psi(y)-y|\ll\frac{x}{(\log x)^A},$$

所以由 $x^{1/2}(\log x)^{-A}\le Q\le x^{1/2}$ 得

$$\begin{aligned}\sum_{q\le Q}\max_{y\le x}\max_{(a,q)=1}\left|\psi(y;q,a)-\frac{y}{\varphi(q)}\right|&\ll Q\log Q\log x+\left(\frac{x}{(\log x)^A}+x^{5/6}\log Q+x^{1/2}Q\right)(\log x)^4\log Q\\&\ll x^{1/2}Q(\log x)^5,\end{aligned}$$

定理得证. □

参考文献

[1] Harold Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000, Revised by Hugh L. Montgomery.

[2] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, no. 4, Academic Press, London and New York, 1974. MR 0347761

[3] Henryk Iwaniec, *Sieve methods*, Graduate course lecture notes, Rutgers University, Spring 1996, 1996.

[4] Graham J. O. Jameson, *Notes on the large sieve*, Lecture notes, Lancaster University, October 2017.

[5] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory I: Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2006.

[6] ———, *Multiplicative number theory II: Primes and sieves*, Cambridge Studies in Advanced Mathematics, vol. 218, Cambridge University Press, Cambridge, 2026.

[7] Melvyn B. Nathanson, *Additive number theory: The classical bases*, Graduate Texts in Mathematics, no. 164, Springer, New York, 1996.

[8] Atle Selberg, *The general sieve-method and its place in prime number theory*, Proceedings of the International Congress of Mathematicians (Cambridge, MA), vol. 1, American Mathematical Society, 1950, pp. 286–292. MR 0033296

[9] Gérald Tenenbaum, *Introduction to analytic and probabilistic number theory*, 3rd ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, Rhode Island, 2015.

[10] R. C. Vaughan, *An elementary method in prime number theory*, Acta Arithmetica **37** (1980), no. 1, 111–115.

[11] ———, *The hardy–littlewood method*, Cambridge Tracts in Mathematics, no. 80, Cambridge University Press, Cambridge, 1981.

[12] 潘承洞, 潘承彪, 解析数论基础, 现代数学基础丛书, 科学出版社, 北京, 1991.