2024 年度八王子数論セミナー補足資料 A

Selberg の篩の基本

鈴木雄太 （立教大学）

2024 年 8 月 15 日 版

概要

篩法とは, 与えられた整数の有限集合の中から, 小さい素数で割り切れてしまう数を取り除くことを考えたとき, 取り除かれずに残った数たちの個数を評価する技法のことである．この操作が, 粒度の大きい粒やダマが混じった粉を篩にかけて粒度の細かい粒だけをより分ける作業に似ていることが「篩法」という名前の由来であろう．篩法には様々な種類があるが, ここでは Maynard の手法 [5] や GPY の手法 [2, 3] の元となった Selberg の篩を, その基本的な形で紹介する.

目次

注: Landau の記号 $O(\bullet)$ や Vinogradov の記号 $\bullet \ll \bullet$ 等の漸近解析の記号については, 別紙の補足資料 C「基礎事項の補足」を参照のこと. また, この資料では, 主張に「ただしここで implicit constant は $a, b, \ldots, c$ に依存する」等の宣言があるとき, 対応する証明中の implicit constant も明記することなしに $a, b, \ldots, c$ に依存するものとする.

A.1 一般的な設定

A.1.1 篩データ

まずは, 「与えられた整数の有限集合の中から, 小さい素数で割り切れてしまう数を取り除くことを考えたとき, 取り除かれずに残った数たちの個数を評価する」と言ったときの「与えられた整数の有限集合の中から, 小さい素数で割り切れてしまう数を取り除く」という状況を, 一般的な名前ではないが「篩データ」という名前でまとめる.

Notation A.1.1.

- 整数 $a_1, \ldots, a_n$ の最大公約数を $(a_1, \ldots, a_n)$ で表す.
- 整数 $a_1, \ldots, a_n$ の最小公倍数を $[a_1, \ldots, a_n]$ で表す.

これらは普通, 文脈を用いることで, 整数の組と容易に区別できる.

Definition A.1.1 (数論的関数).

(1) 自然数全体 $\mathbb{N}$ を定義域とする複素数値関数を**数論的関数**と呼ぶ.

(2) 数論的関数 f が**乗法的**であるとは, $f(1)=1$ であり, 任意の自然数 m,n に対して

$$(m,n)=1 \implies f(mn)=f(m)f(n)$$

が成立することを言う.

(3) 数論的関数 f が**完全乗法的**であるとは, $f(1)=1$ であり, 任意の自然数 m,n に対して

$$f(mn)=f(m)f(n)$$

が成立することを言う.

Remark A.1.1. Definition A.1.1 で乗法的関数と完全乗法的関数に条件 $f(1)=1$ を課しているが, これは定数関数 $f(n)=0$ を排除するためである. この定数関数 $f(n)=0$ を除き, $f(1)=1$ は乗法性の定義の残りの「$(m,n)=1 \implies f(mn)=f(m)f(n)$」という条件の帰結である.

Notation A.1.2. この資料では文字 p は添字等のあるなしにかかわらず素数を表すものとする.

Definition A.1.2 (篩データ). 以下のものからなる組 $(\mathscr{A},\mathscr{P},\omega,X)$ を**篩データ**と呼ぶ：

- 篩をかけたい整数の有限多重集合 $\mathscr{A}$.
- 篩う際に着目したい素数の集合 $\mathscr{P}$.（素数全てでなくてもよい.）
- 乗法的関数 ω であって

$$0 \leq \omega(p) < p \quad \text{かつ} \quad p \notin \mathscr{P} \implies \omega(p)=0$$

を満たすもの. **局所密度**と呼ぶ. （その意味は Remark A.1.3 を参照のこと.）

- 整数の多重集合 $\mathscr{A}$ の要素数を近似するための実数 $X>0$.

篩データの簡単な例は多少の準備の下, Proposition A.1.3 と Proposition A.1.4 で取り扱う.

Remark A.1.2. 多重集合と言っているのは, 実際には整数の集合 I で添字付けられた

$$\mathscr{A}=(a_n)_{n\in I}$$

というような整数列のことである. 例えば, もし $a_n=1$ となることがちょうど 3 つの $n \in I$ で起これば $\mathscr{A}$ に 1 は重複度 3 で含まれていると理解する. 多重集合の要素数とは整数列としてみたときの項数のこと, つまり重複度込みの要素数であるとする. 以後, 多重集合に対して集合の用語や記号を流用する. 例えば, 部分多重集合とは整数列の部分列のことだと思う.

Definition A.1.3. 整数の多重集合 $\mathscr{A}$ と自然数 d に対して

$$\mathscr{A}_d := \{n \in \mathscr{A} \mid n \equiv 0 \pmod{d}\} \subseteq \mathscr{A}$$

と書く.

Notation A.1.3. 篩データ $(\mathscr{A}, \mathscr{P}, \omega, X)$ に対して, 以下の記法を用いる：

- 数論的関数 E を自然数 d に対して

$$\#\mathscr{A}_d = \frac{\omega(d)}{d} X + E(d) \tag{A.1.1}$$

  で定める. この等式 (A.1.1) を**局所条件**と呼ぼう. （通常, この誤差項は $R(d)$ だとか書かれるが, [5] と記号を合わせるために $E(d)$ と書いた.）
- 実数 $z > 0$ に対して

$$P(z) := \prod_{\substack{p \in \mathscr{P} \\ p < z}} p$$

  と書く.

Remark A.1.3. 局所条件 (A.1.1) は大雑把に言って

$$n \in \mathscr{A} \text{ が } d \text{ で割り切れる「確率」は } \frac{\omega(d)}{d} \text{ である}$$

ということを（誤差項 $E(d)$ 付きで）言っている.

A.1.2 局所条件の例

以下に, 多項式で作られる整数列の場合に局所条件とその誤差項評価の例を見てみよう.

Notation A.1.4. 以下, 整数 n, d に対して, 標準全射

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/d\mathbb{Z}$$

（つまり, d で割った余りを取る写像）による n の像のことを $n \pmod{d}$ と書くことにする.

Definition A.1.4. 多項式 $F \in \mathbb{Z}[X]$ に対して, 数論的関数 ω_F を

$$\omega_F(d) := \#\{x \pmod{d} \in \mathbb{Z}/d\mathbb{Z} \mid F(x) \equiv 0 \pmod{d}\}$$

で定める.

Proposition A.1.1. 多項式 $F \in \mathbb{Z}[X]$ に対して, ω_F は乗法的である.

Proof. 明らかに $\omega_F(1) = 1$ である. よって, 互いに素な自然数 (d, e) をとり, $\omega_F(de) = \omega_F(d)\omega_F(e)$ であることを示せば良い. 中国式剰余定理（Lemma C.3.1）より環同型

$$\mathbb{Z}/de\mathbb{Z} \to (\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/e\mathbb{Z});\ x \pmod{de} \mapsto (x \pmod{d}, x \pmod{e})$$

がある. この環同型を通して

$$F(x) \equiv 0 \pmod{de} \iff F(x) \equiv 0 \pmod{d} \text{ かつ } F(x) \equiv 0 \pmod{e}$$

であることから主張が従う. □

Definition A.1.5. 実数 x に対して,

$$[x] \coloneqq \max\{n \in \mathbb{Z} \mid n \le x\} \quad \text{および} \quad \{x\} \coloneqq x - [x]$$

とおき, それぞれ実数 x の**整数部分**および**小数部分**と呼ぶ.

Proposition A.1.2. 多項式 $F \in \mathbb{Z}[X]$ と実数 x, y であって $y > 0$ なるものに対し, 次を考える：

- 整数の有限列 $\mathscr{A} \coloneqq \{F(n) \mid n \in [x - y, x) \cap \mathbb{Z}\}$.
- 実数 $X = y > 0$.
- 乗法的関数 $\omega \coloneqq \omega_F$. （この数論的関数の乗法性については Proposition A.1.1 を参照.）

すると, 局所条件とその誤差項評価

$$\#\mathscr{A}_d = \frac{\omega(d)}{d}X + E(d) \quad \text{および} \quad |E(d)| \le \omega(d)$$

が成立する.

Proof. 部分列 $\mathscr{A}_d$ の定義（Definition A.1.3）より,

$$\#\mathscr{A}_d = \sum_{\substack{x-y \le n < x \\ F(n) \equiv 0 \pmod{d}}} 1$$

である. 右辺の項たちを $n \pmod{d}$ の値で分類すると

$$\#\mathscr{A}_d = \sum_{u \pmod{d}} \sum_{\substack{x-y \le n < x \\ F(n) \equiv 0 \pmod{d} \\ n \equiv u \pmod{d}}} 1$$

となるが, 条件 $F(n) \equiv 0 \pmod{d}$ は $n \pmod{d}$ の値にしか依存しないので

$$\#\mathscr{A}_d = \sum_{\substack{u \pmod{d} \\ F(u) \equiv 0 \pmod{d}}} \sum_{\substack{x-y \le n < x \\ n \equiv u \pmod{d}}} 1 \tag{A.1.2}$$

である. ここで $n \equiv u \pmod d$ なる整数を $n = u + dm$ とでもかけば

$$\sum_{\substack{x-y \le n < x \\ n \equiv u \pmod d}} 1 = \sum_{x-y \le u+dm < x} 1 = \sum_{\frac{x-y-u}{d} \le m < \frac{x-u}{d}} 1$$

である. 和を $m \rightsquigarrow -m$ で変数変換して

$$\sum_{\substack{x-y \le n < x \\ n \equiv u \pmod d}} 1 = \sum_{-\frac{x-u}{d} < m \le -\frac{x-y-u}{d}} 1 = \left[-\frac{x-y-u}{d} \right] - \left[-\frac{x-u}{d} \right] = \frac{y}{d} + E(u,d) \tag{A.1.3}$$

ただし

$$E(u,d) \coloneqq \left\{ -\frac{x-u}{d} \right\} - \left\{ -\frac{x-y-u}{d} \right\}$$

を得る. 特に, 任意の実数に対して $\{x\} \in [0,1)$ だから,

$$|E(u,d)| = \left| \left\{ -\frac{x-u}{d} \right\} - \left\{ -\frac{x-y-u}{d} \right\} \right| \le 1 \tag{A.1.4}$$

である. さて, (A.1.3) を (A.1.2) に代入し, ω_F の定義を思い出せば,

$$\#\mathscr{A}_d = \frac{y}{d} \sum_{\substack{u \pmod d \\ F(u) \equiv 0 \pmod d}} 1 + \sum_{\substack{u \pmod d \\ F(u) \equiv 0 \pmod d}} E(u,d) = \frac{\omega_F(d)}{d} y + E(d) \tag{A.1.5}$$

ただし

$$E(d) \coloneqq \sum_{\substack{u \pmod d \\ F(u) \equiv 0 \pmod d}} E(u,d)$$

を得る. あとは $E(d)$ を評価すればよいが, これは (A.1.4) より

$$|E(d)| \le \sum_{\substack{u \pmod d \\ F(u) \equiv 0 \pmod d}} |E(u,d)| \le \sum_{\substack{u \pmod d \\ F(u) \equiv 0 \pmod d}} 1 = \omega_F(d)$$

とすればよい. 最後に (A.1.5) にて, $X \coloneqq y$ および $\omega \coloneqq \omega_F$ を思い出せば主張を得る. □

A.1.3 篩関数

次に「与えられた整数の有限集合の中から, 小さい素数で割り切れてしまう数を取り除くことを考えたとき, 取り除かれずに残った数たちの個数を評価する」と言ったときの「取り除かれずに残った数たちの個数」を表す篩関数の定義とその使い方の例を見てみよう.

Definition A.1.6 (篩関数). 篩データ $(\mathscr{A}, \mathscr{P}, \omega, X)$ と実数 $z \ge 2$ に対して篩関数 $S(\mathscr{A}, \mathscr{P}, z)$ を

$$\mathcal{S}(\mathscr{A}, z) = \mathcal{S}(\mathscr{A}, \mathscr{P}, z) \coloneqq \{n \in \mathscr{A} \mid (n, P(z)) = 1\},$$

$$S(\mathscr{A}, z) = S(\mathscr{A}, \mathscr{P}, z) \coloneqq \#\mathcal{S}(\mathscr{A}, \mathscr{P}, z)$$

で定義する．ここで使う実数 z のことを, the level of sieve（篩水準）と呼ぶことがある.

Definition A.1.7. 素数の集合 $\mathscr{P}$ と自然数 n に対して, もし $n > 1$ ならば

$$p_{\min}(n) = p_{\min,\mathscr{P}}(n) \coloneqq \min\{p \in \mathscr{P} : p \mid n\}, \quad p_{\max}(n) = p_{\max,\mathscr{P}}(n) \coloneqq \max\{p \in \mathscr{P} : p \mid n\}$$

と定め, $n = 1$ に対しては

$$p_{\min}(1) \coloneqq +\infty, \quad p_{\max}(1) \coloneqq 1$$

と定める.

Remark A.1.4. 注意であるが, Definition A.1.6 において, 次の言い換えが成立する：

$$\begin{aligned}(n, P(z)) = 1 &\iff \text{任意の } p \in \mathscr{P} \cap [1, z) \text{ に対して } p \nmid n \\ &\iff p_{\min}(n) \geq z.\end{aligned}$$

つまり, $(n, P(z)) = 1$ は,「n が小さい素数で割り切れない」ということを意味する.

A.1.4 篩関数の利用例

これから篩関数の評価方法を与える篩法を展開するが, まず, 篩関数を評価できると素数や双子素数の個数を評価できることを確認しておこう．これから取り扱う Selberg の篩はそのままでは上からの評価しか与えないので, 双子素数の個数については上からの評価のみ考える.

Notation A.1.5. 素数すべての集合を $\mathbb{P}$ と書くことにする.

Definition A.1.8. 実数 $x \geq 1$ に対して,

$$\pi(x) \coloneqq \#\{p \leq x \mid p : \text{素数}\}$$

とする.

Definition A.1.9. 数論的関数 Ω と ν を, 自然数 n に対して

$$\begin{aligned}\Omega(n) &\coloneqq \sum_{p^v \mid n} 1 = (n \text{ の重複度を込めた素因数の個数}), \\ \nu(n) &\coloneqq \sum_{p \mid n} 1 = (n \text{ の重複度を除いた素因数の個数})\end{aligned}$$

で定める.

Proposition A.1.3. 実数 $x \geq 4$ に対して, 次のように与えられる篩データを考える：

- $\mathscr{A} \coloneqq [0, x) \cap \mathbb{Z}$.
- $\mathscr{P} \coloneqq \mathbb{P}$.
- $\omega(d) = 1$（定数関数）.
- $X \coloneqq x$.

このとき, 次が成り立つ：

(i) 任意の自然数 d に対して,

$$\#\mathscr{A}_d = \frac{\omega(d)}{d} X + E(d) \quad \text{および} \quad |E(d)| \leq 1$$

が成立する.（局所条件とその誤差評価）

(ii) 任意の実数 $z \geq 2$ に対して,

$$\pi(x) \leq S(\mathscr{A}, \mathscr{P}, z) + z$$

が成立する.

(iii)（セミナーでは飛ばす）任意の実数 $z \in [x^{\frac{1}{2}}, x)$ に対して

$$S(\mathscr{A}, \mathscr{P}, z) - 1 \leq \pi(x) \leq S(\mathscr{A}, \mathscr{P}, z) + z$$

が成立する.

Proof.

(i). これは Proposition A.1.2 を $F(X) \coloneqq X$, $x \coloneqq x$, $y \coloneqq x$ とともに用いれば従う.

(ii). 区間を分割することで（x が素数の場合も加味して 1 を加えて）

$$\pi(x) \leq \#\{n \in [z, x) \mid n : \text{素数}\} + \#\{n \in [2, z) \mid n : \text{素数}\} + 1$$

を得る. ただしここで素数は必ず 2 以上であることを第 2 項目で用いた. すると, 区間 $[2, z)$ の中の自然数の個数はそもそも $\leq [z] - 1 \leq z - 1$ であるから,

$$\begin{aligned} \pi(x) &\leq \#\{n \in [z, x) \mid n : \text{素数}\} + (z - 1) + 1 \\ &\leq \#\{n \in [z, x) \mid n : \text{素数}\} + z \end{aligned}$$

を得る. よって後は,（$\mathscr{A}$ の要素は重複度 1 しか持たないので）包含関係

$$\{n \in [z, x) \mid n : \text{素数}\} \subseteq \mathcal{S}(\mathscr{A}, \mathscr{P}, z) \tag{A.1.6}$$

を示せば良い. これは, Remark A.1.4 を思い出せば,

$$n \in \{n \in [z, x) \mid n : \text{素数}\} \implies p_{\min}(n) = n \geq z \implies (n, P(z)) = 1 \implies n \in \mathcal{S}(\mathscr{A}, \mathscr{P}, z)$$

と確認できる. よって, (A.1.6) が成り立つ.

(iii). 今, $x \geq 4$ かつ $z \in [x^{\frac{1}{2}}, x)$ なので $z \geq 2$ である. よって, 上からの評価は (ii) から従う. あとは下からの評価を示せばよい. これには包含関係

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, z) \subseteq \{n \in [0, x) \mid n : \text{素数}\} \cup \{1\} \tag{A.1.7}$$

を示せば

$$S(\mathcal{A}, \mathcal{P}, z) \leq \pi(x) + 1$$

を得るから良い. これは, $z \in [x^{\frac{1}{2}}, x)$ と Remark A.1.4 を思い出せば,

$$\begin{aligned} n \in \mathcal{S}(\mathcal{A}, \mathcal{P}, z) \implies p_{\min}(n) \geq z &\implies z^{\Omega(n)} \leq \prod_{p^v \| n} p^v = n < x \\ &\implies \Omega(n) < \frac{\log x}{\log z} \leq 2 \\ &\implies \Omega(n) = 0 \text{ or } 1 \\ &\implies n = 1 \text{ または } n : \text{素数} \end{aligned}$$

と確認できる. よって, (A.1.7) が成り立つ. □

Definition A.1.10. 実数 $x \geq 1$ に対して,

$$\pi_2(x) := \#\{p \leq x \mid p, p+2 : \text{素数}\}$$

とおく.

Proposition A.1.4. 実数 $x \geq 1$ に対して, 次のように与えられる篩データを考える：

- $\mathcal{A} := \{n(n+2) \mid n \in [0, x) \cap \mathbb{Z}\}$.
- $\mathcal{P} := \mathbb{P}$.
- $\omega := \omega_F$. ただしここで $F(X) = X(X+2) \in \mathbb{Z}[X]$.（Definition A.1.4 を参照.）
- $X := x$.

このとき, 次が成り立つ：

(i) 素数 p に対して

$$\omega(p) = \begin{cases} 1 & (p = 2 \text{ のとき}), \\ 2 & (p > 2 \text{ のとき}) \end{cases}$$

が成立する.

(ii) 任意の自然数 d に対して,

$$\#\mathcal{A}_d = \frac{\omega(d)}{d} X + E(d) \quad \text{および} \quad |E(d)| \leq \omega(d)$$

が成立する.（局所条件とその誤差評価）

(iii) 任意の実数 $z \geq 2$ に対して,

$$\pi_2(x) \leq S(\mathcal{A}, \mathcal{P}, z) + z$$

が成立する．

Proof.

(i). Definition A.1.4 から

$$\omega(p) = \omega_F(p) = \#\{x \pmod p \mid x(x+2) \equiv 0 \pmod p\}$$

であるが, $\mathbb{Z}/p\mathbb{Z}$ は体だから

$$\omega(p) = \#\{0 \pmod p, -2 \pmod p\}$$

である．あとは $0 \equiv -2 \pmod p$ となるのが $p = 2$ のときであることに気をつければ主張を得る．

(ii). これは Proposition A.1.2 を $F(X) \coloneqq X(X+2)$, $x \coloneqq x$, $y \coloneqq x$ とともに用いれば従う．

(iii). 区間を分割することで（$x, x+2$ が素数の場合も加味して 1 を加えて）

$$\pi_2(x) \leq \#\{n \in [z, x) \mid n, n+2 : 素数\} + \#\{n \in [2, z) \mid n, n+2 : 素数\} + 1$$

を得る．ただしここで素数は必ず 2 以上であることを第 2 項目で用いた．すると, 区間 $[2, z)$ の中の自然数の個数はそもそも $\leq [z] - 1 \leq z - 1$ であるから,

$$\begin{aligned} \pi_2(x) &\leq \#\{n \in [z, x) \mid n, n+2 : 素数\} + (z-1) + 1 \\ &\leq \#\{n \in [z, x) \mid n, n+2 : 素数\} + z \end{aligned}$$

を得る．よって後は, （$\mathscr{A}$ の要素は重複度 1 しか持たないので）包含関係

$$\{n \in [z, x) \mid n, n+2 : 素数\} \subseteq \mathcal{S}(\mathscr{A}, \mathscr{P}, z) \tag{A.1.8}$$

を示せば良い．これは, Remark A.1.4 を思い出せば,

$$\begin{aligned} n \in \{n \in [z, x) \mid n, n+2 : 素数\} &\implies p_{\min}(n(n+2)) = \min(n, n+2) = n \geq z \\ &\implies (n(n+2), P(z)) = 1 \\ &\implies n \in \mathcal{S}(\mathscr{A}, \mathscr{P}, z) \end{aligned}$$

と確認できる．よって, (A.1.8) が成り立つ． □

A.2 Eratosthenes–Legendre の篩

A.2.1 乗法的関数に関する準備

Definition A.2.1. 自然数 d, n に対して

$$d \parallel n \overset{\text{def}}{\iff} d \mid n \text{ かつ } (d, n/d) = 1$$

と定める．

Remark A.2.1. 自然数 n, 素数 p, 非負整数 v に対して,

$$p^v \parallel n \iff p^v \mid n \text{ かつ } p^{v+1} \nmid n$$

つまり, $p^v \parallel n$ のとき n の素因数分解に現れる p のべきの指数は v である．（$v = 0$ を含める.）

Remark A.2.2. 以後, 空集合に渡る和と積（空和と空積）はそれぞれ 0 と 1 だと理解する.

Lemma A.2.1. 乗法的関数 f と自然数 n に対して,

$$\sum_{d|n} f(d) = \prod_{p^v \parallel n} \left(\sum_{e=0}^{v} f(p^e) \right) = \prod_{p^v \parallel n} (1 + f(p) + \cdots + f(p^v))$$

が成立する.（ここで右辺の積は素べき p^v であって $v \in \mathbb{N}$ なるものに渡る, つまり n を素因数分解したときに現れる素べき p^v に渡ることに注意.）

Proof. 最後の等号は f の乗法性から $f(1) = 1$ であるので明らか．最初の等号を示す.

まず, $n = 1$ のとき主張は自明なので, $n > 1$ と仮定してよい．自然数 n の素因数分解を

$$n = p_1^{v_1} \cdots p_r^{v_r}, \quad r \in \mathbb{Z}_{\geq 1},\ p_1, \ldots, p_r : \text{互いに異なる素数},\ v_1, \ldots, v_r \in \mathbb{N} \tag{A.2.9}$$

と書くことにする．すると, n の約数は

$$p_1^{e_1} \cdots p_r^{e_r} \quad \text{ただし} \quad e_i \in \{0, 1, \ldots, v_i\}$$

という形の自然数すべてである．よって,

$$\sum_{d|n} f(d) = \sum_{e_1=0}^{v_1} \cdots \sum_{e_r=0}^{v_r} f(p_1^{e_1} \cdots p_r^{e_r})$$

と書き直せる．すると, f の乗法性から

$$\sum_{d|n} f(d) = \sum_{e_1=0}^{v_1} \cdots \sum_{e_r=0}^{v_r} f(p_1^{e_1}) \cdots f(p_r^{e_r}) = \left(\sum_{e_1=0}^{v_1} f(p_1^{e_1}) \right) \times \cdots \times \left(\sum_{e_r=0}^{v_r} f(p_r^{e_r}) \right)$$

を得る．あとは $p_1, \ldots, p_r, v_1, \ldots, v_r$ が (A.2.9) で与えられていたことを思い出せば良い. □

A.2.2 Möbius 関数

Definition A.2.2 (平方無縁).
自然数 n がどの素数の平方でも割れないとき, n は**平方無縁**（square-free）であると言う.

Note A.2.1. 自然数 n が平方無縁であるとは, 言い換えてみれば, n を素因数分解したときに現れる素べきの指数がすべて 1 であることを意味する.

Definition A.2.3 (Möbius **関数**)**.** 数論的関数 μ を, 自然数 n に対して,

$$\mu(n) = \begin{cases} (-1)^r & n \text{ が } r \text{ 個の互いに異なる素数の積であるとき}\ (r \in \mathbb{Z}_{\geq 0}), \\ 0 & \text{それ以外} \end{cases}$$

で定める.

Notation A.2.1. 条件 P に対して, その**特性関数** $\mathbb{1}_{\mathsf{P}}$ を

$$\mathbb{1}_{\mathsf{P}} := \begin{cases} 1 & (\mathsf{P} \text{ が真のとき}), \\ 0 & (\mathsf{P} \text{ が偽のとき}) \end{cases}$$

と定める. (条件 P に現れる変数の関数とみなせる.)

Remark A.2.3. 注意であるが, 自然数 n に対して

$$\mu(n) \neq 0 \iff n : \text{square-free}$$

である. よって, Möbius 関数は $0, \pm 1$ しか値に持たないことに気をつければ

$$\mu(n)^2 = \mathbb{1}_{n:\text{square-free}}$$

であることが分かる.

Proposition A.2.1. Möbius 関数は乗法的である.

Proof. まず, 1 は 0 個の互いに異なる素数の積なので $\mu(1) = 1$ である. よって, 互いに素な自然数 m, n を任意にとり, $\mu(mn) = \mu(m)\mu(n)$ を示せばよい. 互いに素な自然数 m, n を任意にとる. もし, m, n のどちらかが平方無縁でなければ mn も平方無縁でないので

$$\mu(mn) = 0 = \mu(m)\mu(n)$$

となる. もし m, n がどちらも平方無縁であれば, m, n は互いに素だから

$$m = p_1 \cdots p_r, \quad n = p_{r+1} \cdots p_{r+s} \quad \text{ただし} \quad p_1, \ldots, p_r, p_{r+1}, \ldots, p_{r+s} : \text{互いに異なる素数}$$

と書けるので, Möbius 関数の定義より

$$\mu(mn) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(m)\mu(n)$$

を得る. これで, どの場合も $\mu(mn) = \mu(m)\mu(n)$ が示せた. □

Lemma A.2.2. 自然数 n に対して,

$$\sum_{d|n} \mu(d) = \mathbb{1}_{n=1}$$

が成立する.

Proof. Proposition A.2.1 より Möbius 関数は乗法的なので, Lemma A.2.1 を用いることができ,

$$\sum_{d|n} \mu(d) = \prod_{p^v \| n} (1 + \mu(p) + \cdots + \mu(p^v))$$

となる. ここで Möbius 関数の定義を思い出せば

$$\sum_{d|n} \mu(d) = \prod_{p|n} (1-1) = \mathbb{1}_{n=1}$$

と主張が得られる.（空積は 1 だと解釈すると約束していた.） □

A.2.3 Eratosthenes–Legendre の篩

いよいよ, この資料の最初の篩法である Eratosthenes–Legendre の篩について見てみる.

Theorem A.2.1 (Eratosthenes–Legendre **の篩**)**.** 篩データ $(\mathcal{A}, \mathcal{P}, \omega, X)$ と実数 $z \geq 2$ に対して,

$$S(\mathcal{A}, \mathcal{P}, z) = XV(z) + E$$

が

$$V(z) \coloneqq \sum_{d|P(z)} \frac{\mu(d)\omega(d)}{d} \quad \text{および} \quad E \coloneqq \sum_{d|P(z)} \mu(d)E(d)$$

とともに成立する.

Proof. 篩関数の定義より

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{\substack{n \in \mathcal{A} \\ (n, P(z))=1}} 1 = \sum_{n \in \mathcal{A}} \mathbb{1}_{(n, P(z))=1}$$

である. ここで Lemma A.2.2 を用いれば

$$\mathbb{1}_{(n,P(z))=1} = \sum_{d|(n,P(z))} \mu(d) = \sum_{\substack{d|P(z) \\ d|n}} \mu(d)$$

だから

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{n \in \mathcal{A}} \sum_{\substack{d|P(z) \\ d|n}} \mu(d)$$

である．ここで和を入れ替えて（Remark A.2.5 を参照のこと）

$$S(\mathscr{A}, \mathscr{P}, z) = \sum_{d|P(z)} \mu(d) \sum_{\substack{n \in \mathscr{A} \\ d|n}} 1 = \sum_{d|P(z)} \mu(d) \# \mathscr{A}_d$$

を得る．最後に局所条件

$$\#\mathscr{A}_d = \frac{\omega(d)}{d} X + E(d)$$

を代入すれば

$$S(\mathscr{A}, \mathscr{P}, z) = X \sum_{d|P(z)} \frac{\mu(d)\omega(d)}{d} + \sum_{d|P(z)} \mu(d) E(d) = XV(z) + E$$

を得る． □

Remark A.2.4. Section A.2.4 で詳しくのべる（セミナーでは飛ばす）が, Theorem A.2.1 は綺麗な等式を与える一方で誤差項

$$E = \sum_{d|P(z)} \mu(d) E(d)$$

に含まれる項数が多すぎて, 非常に小さい z を取らない限り, 誤差項の制御が不可能であり, 実用上はあまり強力ではない.

Remark A.2.5. Theorem A.2.1 の証明にあるような和の入れ替え

$$\sum_{n \in \mathscr{A}} \sum_{\substack{d|P(z) \\ d|n}} \mu(d) = \sum_{d|P(z)} \mu(d) \sum_{\substack{n \in \mathscr{A} \\ d|n}} 1$$

は次のように特性関数を用いると見やすい：条件 $d \mid n$ は外側の和の変数と内側の和の変数の両方が含まれる条件なので, このような条件を特性関数に置き換えて

$$\sum_{n \in \mathscr{A}} \sum_{\substack{d|P(z) \\ d|n}} \mu(d) = \sum_{n \in \mathscr{A}} \sum_{d|P(z)} \mu(d) \mathbb{1}_{d|n}$$

とする．こうしてしまえば内側の和と外側の和は独立になったので, 単に

$$\sum_{n \in \mathscr{A}} \sum_{\substack{d|P(z) \\ d|n}} \mu(d) = \sum_{d|P(z)} \sum_{n \in \mathscr{A}} \mu(d) \mathbb{1}_{d|n}$$

と和を入れ替えることができる．さらに特性関数を和の条件に戻してあげれば

$$\sum_{n \in \mathscr{A}} \sum_{\substack{d|P(z) \\ d|n}} \mu(d) = \sum_{d|P(z)} \sum_{\substack{n \in \mathscr{A} \\ d|n}} \mu(d) = \sum_{d|P(z)} \mu(d) \sum_{\substack{n \in \mathscr{A} \\ d|n}} 1$$

を得る．実際には特性関数を導入しなくても，「内側の和と外側の和の両方が出てくる条件は内側に残したまま和を入れ替える」と思ってしまったほうが計算が楽である．

Proposition A.2.2. Theorem A.2.1 の設定の下，

$$V(z) = \prod_{\substack{p\in\mathscr{P} \\ p<z}} \left(1 - \frac{\omega(p)}{p}\right)$$

が成立する．

Proof. 数論的関数

$$\mathbb{N} \to \mathbb{R};\, d \mapsto \frac{\mu(d)\omega(d)}{d}$$

は乗法的なので，Lemma A.2.1 が使えて

$$V(z) = \prod_{p^v \| P(z)} \left(\sum_{e=0}^{v} \frac{\mu(p^e)\omega(p^e)}{p^e}\right) \tag{A.2.10}$$

を得る．しかし，$P(z)$ は平方無縁なので，(A.2.10) の右辺に現れる素べきは $v = 1$ のもののみであり，

$$V(z) = \prod_{p|P(z)} \left(1 + \frac{\mu(p)\omega(p)}{p}\right) = \prod_{p|P(z)} \left(1 - \frac{\omega(p)}{p}\right) = \prod_{\substack{p\in\mathscr{P} \\ p<z}} \left(1 - \frac{\omega(p)}{p}\right)$$

を得る． □

A.2.4 Eratosthenes–Legendre の篩の弱点（セミナーでは飛ばす）

Eratosthenes–Legendre の篩（Theorem A.2.1）を見ると，篩関数 $S(\mathscr{A}, \mathscr{P}, z)$ は $XV(z)$ で近似できたように思えてくる．そこで，Eratosthenes–Legendre の篩を用いて，与えられた実数 x 以下の素数の個数 $\pi(x)$ を評価することを試みてみよう．

さて，Eratosthenes–Legendre の篩を用いて $\pi(x)$ の近似を試みてみよう．Proposition A.1.3 の状況を考える．篩水準 z を $z \in [x^{\frac{1}{2}}, x)$ の範囲にとれば，Proposition A.1.3 の (iii) より，

$$|\pi(x) - S(\mathscr{A}, \mathscr{P}, z)| \le z$$

である．さらに Theorem A.2.1 を用いれば

$$|\pi(x) - (XV(z) + E)| \le z \quad \text{ただし} \quad E \coloneqq \sum_{d|P(z)} \mu(d)E(d) \tag{A.2.11}$$

を得る．ここで E と z を誤差だとみなしてしまえば，Proposition A.2.2 より

$$\pi(x) \approx XV(z) = x \prod_{p<z} \left(1 - \frac{1}{p}\right) \tag{A.2.12}$$

という近似を得たことになる．（ここで $\approx$ という記号は,「とりあえずこの近似が成立すると思おう」程度の意味で用いている.）後に取り扱う Mertens の定理の証明法を用いれば

$$\prod_{p<z}\left(1-\frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log z} \quad (z \to \infty)$$

が分かる（今回のセミナーでは証明しない）．ただしここで γ は実は Euler–Mascheroni 定数

$$\gamma \coloneqq \lim_{N\to\infty}\left(\sum_{n\le N}\frac{1}{n} - \log N\right) = 0.57721566\cdots$$

と等しい．よって, (A.2.12) より, $z \coloneqq x^{\frac{1}{2}}$ とでも取れば

$$\pi(x) \approx e^{-\gamma}\frac{x}{\log z} \approx 2e^{-\gamma}\frac{x}{\log x} \tag{A.2.13}$$

を得られたように見える．これは次の周知の素数定理に似ている：

Theorem A.2.2 (素数定理 (Hadamard (1896), de la Vallée Poussin (1896))**).**

$$\pi(x) \sim \frac{x}{\log x} \quad (x \to \infty).$$

しかし, **おわかりいただけただろうか**… 実は

$$2e^{-\gamma} = 1.12291896\cdots$$

なので, 上に得た (A.2.13) は素数定理と（定数倍だけ）食い違っているのである！（そもそも, 篩水準 z は $z \coloneqq x^{\frac{1}{2}}$ と選んだわけだが, $z \in [x^{\frac{1}{2}}, x(\log x)^{-2})$ の範囲内ならどんな z でも上の議論は成立してしまい, z の任意性の分だけ近似 (A.2.13) の値をずらすことができたのも何やら怪しい.）一体どこで間違えたのであろうか.

実は, (A.2.11) に現れる誤差

$$E = \sum_{d\mid P(z)} \mu(d)E(d)$$

が大きすぎるのである！実際, Proposition A.1.3 の (i) を用いても, Lemma A.2.1 から

$$|E| \le \sum_{d\mid P(z)} \mu(d)^2 = \prod_{p\mid P(z)} 2 = 2^{\pi(z)}$$

となるが, この評価は $z > x^{\frac{1}{2}}$ を思い出せば, 素数定理から十分大の x で, 少なくとも

$$2^{\pi(z)} \ge 2^{x^{\frac{1}{3}}}$$

となり, $x/\log x$ 程度の大きさの主要項は凌駕してしまう！振り返れば, 局所条件である Proposition A.1.3 の (i) では $E(d)$ は主要項に比べて小さく, 正当に「誤差項」と呼べたが, Eratosthenes–Legendre の篩に含まれる組合せ論的構造から膨大な量の誤差項 $E(d)$ が積もる一方で, 主要項には綺麗な打ち消し合いが起こったため, 誤差項が「塵も積もれば山となる」といった感じに主要項を凌駕

した, というわけである．20 世紀以降の篩法のテーマは,「如何にしてこの Eratosthenes–Legendre の篩の欠点を乗り越えるか」, つまり,「残余項 E の制御を如何にして可能にするか」ということにある．

A.3　Selberg の篩

Eratosthenes–Legendre の篩の欠点を乗り越えるための基本的なアイデアは「（篩関数の漸近式を諦めて上や下からの評価に甘んじてもよいとして）Möbius 関数をより都合の良い関数『偽 Möbius 関数』に置き換えてしまう」というものである．特に,『偽 Möbius 関数』の台（値が 0 でない範囲）を制限することで, 誤差項

$$E = \sum_{d \mid P(z)} \mu(d) E(d)$$

の d の範囲を無理やり小さい範囲に制限し, 誤差項の増大を抑えたいということになる．これは一方で Eratosthenes–Legendre の篩の主要項である $XV(z)$ を壊してしまうので, 主要項の制御も考えなければならない.

A.3.1　Selberg の篩のアイデア

Selberg の篩での『偽 Möbius 関数』の作り方は次の非常に単純な観察に基づく：

Lemma A.3.1. 次のものを考える：

- 素数のある集合 $\mathscr{P}$.
- 実数 $z \geq 2$.

このとき, 実数列 $(\lambda_d)_{d \mid P(z)}$ であって,

$$\lambda_1 = 1 \tag{A.3.14}$$

なるものを考える．このとき, 自然数 $N \mid P(z)$ に対して,

$$\sum_{d \mid N} \mu(d) \leq \left(\sum_{d \mid N} \lambda_d \right)^2 \tag{A.3.15}$$

である.

Proof. $N = 1$ であるか否かで場合分けをする．$N = 1$ のときは (A.3.14) より

$$\sum_{d \mid N} \mu(d) = 1 \quad \text{かつ} \quad \left(\sum_{d \mid N} \lambda_d \right)^2 = \lambda_1^2 = 1$$

なので主張は成立する．$N > 1$ のときは Lemma A.2.2 と λ_d が実数値であることから

$$\sum_{d \mid N} \mu(d) = 0 \leq \left(\sum_{d \mid N} \lambda_d \right)^2$$

を得る. $\square$

この Lemma A.3.1 より, 篩関数の上からの評価を考えるだけなら, Möbius 関数の約数に渡る和

$$\sum_{d|N} \mu(d)$$

を不等式 (A.3.15) の右辺

$$\left(\sum_{d|N} \lambda_d\right)^2$$

つまり「偽 Möbius 関数」の約数に渡る和に置き換えることができる.

しかし, Lemma A.3.1 は非常に単純である. 鍵となっているのは実数の平方が必ず非負であるというだけのことである. これだけで意味ある upper bound sieve が作れるのは驚きであるが, もちろんこれから行わなければならないのは適切な (λ_d) の構成である. まずはひとまず Lemma A.3.1 で得られた結果を篩関数に用いて得られる評価を見てみる：

Proposition A.3.1. 次のものを考える：

- 篩データ $(\mathscr{A}, \mathscr{P}, \omega, X)$.
- 実数 $R, z \geq 2$.
- 実数列 $(\lambda_d)_{d|P(z)}$ であって

$$\lambda_1 = 1 \tag{A.3.16}$$

  かつ

$$d \geq R \implies \lambda_d = 0 \tag{A.3.17}$$

  なるもの.

このとき,

$$S(\mathscr{A}, \mathscr{P}, z) \leq XV + E$$

が

$$V := \sum_{\substack{d_1, d_2 | P(z) \\ d_1, d_2 < R}} \lambda_{d_1} \lambda_{d_2} \frac{\omega([d_1, d_2])}{[d_1, d_2]} \quad \text{および} \quad E := \sum_{\substack{d_1, d_2 | P(z) \\ d_1, d_2 < R}} \lambda_{d_1} \lambda_{d_2} E([d_1, d_2])$$

とともに成り立つ.

Proof. Lemma A.2.2 と Lemma A.3.1 より,

$$S(\mathscr{A}, \mathscr{P}, z) = \sum_{n \in \mathscr{A}} \mathbb{1}_{(n, P(z))=1} = \sum_{n \in \mathscr{A}} \sum_{d|(n, P(z))} \mu(d) \leq \sum_{n \in \mathscr{A}} \left(\sum_{d|(n, P(z))} \lambda_d \right)^2$$

を得る. ここで 2 乗を開けば（和の交換の仕方については Remark A.2.5 を参照）

$$S(\mathscr{A}, \mathscr{P}, z) \leq \sum_{n \in \mathscr{A}} \sum_{\substack{d_1 | P(z) \\ d_1 | n}} \sum_{\substack{d_2 | P(z) \\ d_2 | n}} \lambda_{d_1} \lambda_{d_2} = \sum_{d_1, d_2 | P(z)} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{n \in \mathscr{A} \\ d_1, d_2 | n}} 1 \tag{A.3.18}$$

となる. ここで $d_1, d_2 \mid n \iff [d_1, d_2] \mid n$ だから, 局所条件を用いれば, (A.3.18) から

$$\begin{aligned} S(\mathscr{A}, \mathscr{P}, z) &\le \sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} \# \mathscr{A}_{[d_1, d_2]} \\ &= X \sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} \frac{\omega([d_1, d_2])}{[d_1, d_2]} + \sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} E([d_1, d_2]) \end{aligned}$$

を得る. 最後に (A.3.17) に気をつければ主張を得る. □

A.3.2 主要項の対角化

さて, 今は upper bound sieve を構成しているため, Proposition A.3.1 での upper bound の主要項 XV をなるべく小さくしたい. ここで, Proposition A.3.1 にあるように

$$V = \sum_{\substack{d_1, d_2 \mid P(z) \\ d_1, d_2 \le R}} \lambda_{d_1} \lambda_{d_2} \frac{\omega([d_1, d_2])}{[d_1, d_2]} \tag{A.3.19}$$

であるが, これは λ_d たちを変数とする二次形式である. よって, 我々がすべきことは, 制約条件 (A.3.16) の下で二次形式 (A.3.19) を最小化することである. この最小化のために, まずは (A.3.19) を「対角化」してみよう.

Lemma A.3.2. 乗法的関数 f と自然数 m, n に対して

$$f(m)f(n) = f([m, n])f((m, n))$$

が成立する.

Proof. 素数 p と自然数 N に対して, 非負整数 $v_p(N)$ を

$$p^{v_p(N)} \parallel N$$

で定める. すると, 素因数分解を考えることで

$$\begin{aligned} f(m)f(n) &= \prod_p f(p^{v_p(m)}) \prod_p f(p^{v_p(n)}) \\ &= \prod_p f(p^{\max(v_p(m), v_p(n))}) \prod_p f(p^{\min(v_p(m), v_p(n))})) \\ &= f([m, n])f((m, n)) \end{aligned}$$

を得る. □

定義 (A.3.19) の中で d_1, d_2 のどちらかが $\omega(p) = 0$ となる素因数 p を持つような項は 0 なので,

$$\mathscr{P}^* \coloneqq \{p \in \mathscr{P} \mid \omega(p) > 0\} \quad \text{および} \quad P^*(z) \coloneqq \prod_{\substack{p \in \mathscr{P}^* \\ p < z}} p$$

と書くことにすれば

$$V = \sum_{\substack{d_1,d_2 \mid P^*(z) \\ d_1,d_2 \le R}} \lambda_{d_1}\lambda_{d_2} \frac{\omega([d_1,d_2])}{[d_1,d_2]}$$

となることに注意する.

一般的ではないが, 次の用語を用意しておく：

Definition A.3.1. 数論的関数 g が**平方無縁数を台とする**とは,

$$n \in \mathbb{N} \text{ が平方無縁でない} \implies g(n) = 0$$

となることを言う.（注：一般的な用語ではない.）

Remark A.3.1. 平方無縁数を台とする乗法的関数 g を定義するには素数での値

$$g(p) \quad (p\text{: 素数})$$

のみを指定すればよい.（素因数分解の存在と一意性の帰結.）

Proposition A.3.2. Proposition A.3.1 と同じ状況の下, 平方無縁数に台を持つ乗法的関数 g を

$$g(p) \coloneqq \frac{\omega(p)}{p - \omega(p)} \tag{A.3.20}$$

で定義する（**相対密度**と呼ばれる）.（なお, $0 \le \omega(p) < p$ という条件が Definition A.1.2 で仮定されていたので (A.3.20) の右辺の分母は 0 ではない.）このとき,

$$V \coloneqq \sum_{\substack{d_1,d_2 \mid P^*(z) \\ d_1,d_2 < R}} \lambda_{d_1}\lambda_{d_2} \frac{\omega([d_1,d_2])}{[d_1,d_2]}$$

に対して

$$V = \sum_{\substack{r \mid P^*(z) \\ r < R}} g(r) y_r^2$$

が変数変換

$$y_r \coloneqq \begin{cases} \dfrac{\mu(r)}{g(r)} \displaystyle\sum_{\substack{d \mid P^*(z) \\ d < R \\ r \mid d}} \frac{\lambda_d \omega(d)}{d} & r \mid P^*(z) \text{ のとき}, \\ 0 & \text{それ以外} \end{cases} \tag{A.3.21}$$

で与えられる $(y_r)_{r \in \mathbb{N}}$ とともに成立する.

Proof. Lemma A.3.2 と $\mathscr{P}^*$ の定義より

$$V = \sum_{\substack{d_1,d_2 | P^*(z) \\ d_1,d_2<R}} \frac{\lambda_{d_1}\omega(d_1)}{d_1} \frac{\lambda_{d_2}\omega(d_2)}{d_2} \frac{(d_1,d_2)}{\omega((d_1,d_2))} \tag{A.3.22}$$

を得る．ここで Lemma A.2.1 より, 平方無縁数 $d \mid P^*(z)$ に対して

$$\frac{d}{\omega(d)} = \prod_{p|d} \frac{p}{\omega(p)} = \prod_{p|d}\left(1 + \frac{p-\omega(p)}{\omega(p)}\right) = \prod_{p|d}\left(1 + \frac{\mu^2(p)}{g(p)}\right) = \sum_{r|d} \frac{\mu(r)^2}{g(r)}$$

を得る．これを (A.3.22) に代入して

$$\begin{aligned} V &= \sum_{\substack{d_1,d_2 | P^*(z) \\ d_1,d_2<R}} \frac{\lambda_{d_1}\omega(d_1)}{d_1} \frac{\lambda_{d_2}\omega(d_2)}{d_2} \sum_{r|(d_1,d_2)} \frac{\mu(r)^2}{g(r)} \\ &= \sum_{\substack{r | P^*(z) \\ r<R}} \frac{\mu(r)^2}{g(r)} \sum_{\substack{d_1,d_2 | P^*(z) \\ d_1,d_2<R \\ r|d_1,d_2}} \frac{\lambda_{d_1}\omega(d_1)}{d_1} \frac{\lambda_{d_2}\omega(d_2)}{d_2} \\ &= \sum_{\substack{r | P^*(z) \\ r<R}} g(r)\left(\frac{\mu(r)}{g(r)} \sum_{\substack{d | P^*(z) \\ d<R \\ r|d}} \frac{\lambda_d\omega(d)}{d}\right)^2 = \sum_{\substack{r | P^*(z) \\ r<R}} g(r)y_r^2 \end{aligned}$$

と主張を得る．ここで最後の和は条件 $r \mid P^*(z)$ から平方無縁数のみに渡ることを用いた． □

Remark A.3.2. Halberstam–Richert [4, 式 (1.5), p. 99] と比べると, Proposition A.3.2 では y_r の定義の仕方が少々ヘンテコである．これは Maynard [5] の notation と合わせたことに由来する．また, Proposition A.3.2 での数論的関数 g は Maynard [5] の Lemma 5.2 の g とは異なる（逆数の関係になっている）ことに注意する．むしろ, Maynard [5] の Lemma 6.1 の g が Proposition A.3.2 の g に対応する．

A.3.3 逆変換の計算

さて, Proposition A.3.2 で与えられた等式

$$V = \sum_{\substack{r | P^*(z) \\ r<R}} g(r)y_r^2$$

が元々の V の対角化であるためには, Proposition A.3.2 で用いた変数変換

$$y_r \coloneqq \frac{\mu(r)}{g(r)} \sum_{\substack{d | P^*(z) \\ d<R \\ r|d}} \frac{\lambda_d\omega(d)}{d}$$

が可逆な必要があるが, これは次の形の Möbius 反転公式により与えることができる（あとで Maynard の論文 [5] で使うために多変数版を示します）：

Lemma A.3.3 (Möbius **反転公式**)**.** 自然数 k と多変数の数論的関数

$$\Lambda, Y\colon \mathbb{N}^k \to \mathbb{C}$$

であって, 次の条件を満たすものを考える：

(1) 数論的関数 Λ, Y は各変数ごとに見て平方無縁数に台を持つ. つまり

$$n_1, \ldots, n_k \text{ のどれかが平方無縁でない} \implies \Lambda(d_1, \ldots, d_k), Y(r_1, \ldots, r_k) = 0$$

が成り立つ.

(2) 数論的関数 Λ, Y の台は有限である. つまり

$$\#\{(d_1, \ldots, d_k) \in \mathbb{N}^k \mid \Lambda(d_1, \ldots, d_k) \neq 0\} < +\infty,$$
$$\#\{(r_1, \ldots, r_k) \in \mathbb{N}^k \mid Y(r_1, \ldots, r_k) \neq 0\} < +\infty$$

が成り立つ.

このとき, 次の 2 つは同値：

(i) 任意の平方無縁数 $r_1, \ldots, r_k$ に対して

$$Y(r_1, \ldots, r_k) = \left(\prod_{i=1}^{k} \mu(r_i)\right) \sum_{\substack{d_1, \ldots, d_k \\ r_i \mid d_i\ (\forall i)}} \Lambda(d_1, \ldots, d_k)$$

が成立する.

(ii) 任意の平方無縁数 $d_1, \ldots, d_k$ に対して

$$\Lambda(d_1, \ldots, d_k) = \left(\prod_{i=1}^{k} \mu(d_i)\right) \sum_{\substack{r_1, \ldots, r_k \\ d_i \mid r_i\ (\forall i)}} Y(r_1, \ldots, r_k)$$

が成立する.

Proof. 対称性より (i) $\implies$ (ii) を示せば十分なので, これのみを示す. 実際に (i) が成立したと仮定する. すると, 平方無縁数たち $d_1, \ldots, d_k$ に対し, (ii) に現れる和は

$$\begin{aligned}
\sum_{d_i \mid r_i\ (\forall i)} Y(r_1, \ldots, r_k) &= \sum_{m_1, \ldots, m_k} Y(d_1 m_1, \ldots, d_k m_k) \\
&= \sum_{m_1, \ldots, m_k} \left(\prod_{i=1}^{k} \mu(d_i m_i)\right) \sum_{d_i m_i \mid e_i\ (\forall i)} \Lambda(e_1, \ldots, e_k) \\
&= \sum_{m_1, \ldots, m_k} \left(\prod_{i=1}^{k} \mu(d_i m_i)\right) \sum_{n_1, \ldots, n_k} \Lambda(d_1 m_1 n_1, \ldots, d_k m_k n_k)
\end{aligned}$$

と書き直せる. ここで Λ は各変数ごと平方無縁数を台に持つので, 和の変数に $(d_i, m_i) = 1$ という条

件を課しても良い．すると, $d_1,\dots,d_k$ は平方無縁だから, Möbius 関数の乗法性より

$$\left(\prod_{i=1}^{k}\mu(d_i)\right)\sum_{d_i|r_i\ (\forall i)}Y(r_1,\dots,r_k)=\sum_{m_1,\dots,m_k}\sum_{n_1,\dots,n_k}\left(\prod_{i=1}^{k}\mu(m_i)\right)\Lambda(d_1m_1n_1,\dots,d_km_kn_k)$$

を得る．後は $u_i=m_in_i$ の値で項を分類してから Lemma A.2.2 を使えば

$$\begin{aligned}\left(\prod_{i=1}^{k}\mu(d_i)\right)\sum_{d_i|r_i\ (\forall i)}Y(r_1,\dots,r_k)&=\sum_{u_1,\dots,u_k}\Lambda(d_1u_1,\dots,d_ku_k)\sum_{\substack{m_1,\dots,m_k\\ n_1,\dots,n_k\\ m_in_i=u_i\ (\forall i)}}\left(\prod_{i=1}^{k}\mu(m_i)\right)\\&=\sum_{u_1,\dots,u_k}\Lambda(d_1u_1,\dots,d_ku_k)\left(\prod_{i=1}^{k}\sum_{m_in_i=u_i}\mu(m_i)\right)\\&=\Lambda(d_1,\dots,d_k)\end{aligned}$$

となる．これで (ii) が示された． □

Proposition A.3.3. Proposition A.3.2 と同じ状況の下, (A.3.21) の逆変換

$$\lambda_d=\frac{\mu(d)d}{\omega(d)}\sum_{\substack{r|P^*(z)\\ r<R\\ d|r}}g(r)y_r$$

が $d\mid P^*(z)$ かつ $d<R$ のとき成立する．

Proof. 変数変換 (A.3.21) は, $r\mid P^*(z)$ のとき

$$g(r)y_r=\mu(r)\sum_{r|d}\frac{\lambda_d\omega(d)}{d}\mathbb{1}_{\substack{d|P^*(z)\\ d<R}}$$

と Lemma A.3.3 の (i) の形に書ける．そこで, Lemma A.3.3 の $k=1$ の場合を

$$\Lambda(d)\coloneqq\frac{\lambda_d\omega(d)}{d}\mathbb{1}_{\substack{d|P^*(z)\\ d<R}}\quad\text{および}\quad Y(r)\coloneqq g(r)y_r$$

とともに用いたい．それには, Lemma A.3.3 の条件 (1) と (2) を確かめる必要がある．まず, Λ について考えると, 条件 (1) は特性関数の条件 $d\mid P^*(z)$ から明らかに成立し, 条件 (2) は特性関数の条件 $d<R$ から明らかに成立する．また, Y に対しては y_r の定義 (A.3.21) から

$$r\nmid P^*(z)\quad\text{または}\quad r\geq R\implies y_r=0\tag{A.3.23}$$

だから条件 (1), (2) は成立する．よって, $d\mid P^*(z)$ かつ $d<R$ のとき, Lemma A.3.3 の (ii) から

$$\lambda_d=\frac{d}{\omega(d)}\frac{\lambda_d\omega(d)}{d}\mathbb{1}_{\substack{d|P^*(z)\\ d<R}}=\frac{\mu(d)d}{\omega(d)}\sum_{d|r}g(r)y_r$$

を得る．最後に, 右辺の和の範囲を (A.3.23) を用いて整理すれば主張を得る． □

A.3.4　最小化問題

以上で, 我々の主要項の最小化問題は次のように解決できる：

Proposition A.3.4. Proposition A.3.2 と同じ状況の下,

$$G_d(x,z) \coloneqq \sum_{\substack{r \mid P^*(z) \\ r<x \\ (r,d)=1}} g(r) \quad (d \mid P(z)) \quad \text{および} \quad G \coloneqq G_1(R,z)$$

とおく. すると, 二次形式

$$V \coloneqq \sum_{\substack{d_1,d_2 \mid P(z) \\ d_1,d_2<R}} \lambda_{d_1}\lambda_{d_2}\frac{\omega([d_1,d_2])}{[d_1,d_2]} = \sum_{\substack{d_1,d_2 \mid P^*(z) \\ d_1,d_2<R}} \lambda_{d_1}\lambda_{d_2}\frac{\omega([d_1,d_2])}{[d_1,d_2]}$$

を制約条件

$$\lambda_1 = 1$$

の下で最小化する $(\lambda_d)_{\substack{d \mid P^*(z) \\ d<R}}$ は

$$\lambda_d \coloneqq \frac{\mu(d)}{\displaystyle\prod_{p \mid d}\left(1-\frac{\omega(p)}{p}\right)}\frac{G_d(R/d,z)}{G} \quad (d \mid P^*(z),\ d<R) \tag{A.3.24}$$

で与えられ, この (A.3.24) の下で V は

$$V = \frac{1}{G}$$

という値を取る.

Proof. Lagrange の未定乗数法も使えるが, ここでは Cauchy–Schwarz の不等式とその等号成立条件を用いた方法を使う. 変数変換 (A.3.21) の逆変換は Proposition A.3.3 で与えられた. 特に

$$\lambda_1 = \frac{\mu(1)}{\omega(1)}\sum_{\substack{r \mid P^*(z) \\ r<R}} g(r)y_r = \sum_{\substack{r \mid P^*(z) \\ r<R}} g(r)y_r$$

である. よって, 対角化を与える Proposition A.3.2 を思い出せば,

$$V = \sum_{\substack{r \mid P^*(z) \\ r<R}} g(r)y_r^2$$

を制約条件

$$\sum_{\substack{r \mid P^*(z) \\ r<R}} g(r)y_r = 1 \tag{A.3.25}$$

の下で最小化することを考えれば良い．このとき

$$r \mid P^*(z) \implies g(r) = \prod_{p \mid r} \frac{\omega(p)}{p - \omega(p)} > 0$$

に注意すれば, Cauchy–Schwarz の不等式から

$$1 = \Bigg(\sum_{\substack{r \mid P^*(z) \\ r < R}} \sqrt{g(r)} y_r \cdot \sqrt{g(r)}\Bigg)^2 \le \Bigg(\sum_{\substack{r \mid P^*(z) \\ r < R}} g(r) y_r^2\Bigg)\Bigg(\sum_{\substack{r \mid P^*(z) \\ r < R}} g(r)\Bigg) \tag{A.3.26}$$

を得る．よって,

$$V = \sum_{\substack{r \mid P^*(z) \\ r < R}} g(r) y_r^2 \ge \frac{1}{G} \tag{A.3.27}$$

を得る．この等号は (A.3.26) で用いた Cauchy–Schwarz 不等式の等号成立条件が成り立つときに達成される．Cauchy–Schwarz 不等式の等号は考えている関数（ベクトル）が平行なときに達成される．つまり, ある定数 c によって

$$\sqrt{g(r)} y_r = c\sqrt{g(r)} \iff y_r = c$$

がすべての $r \mid P^*(z)$ かつ $r < R$ なる自然数 r に対して成り立つとき, (A.3.27) の等号が成立する．これを制約条件 (A.3.25) の中に入れれば

$$1 = \sum_{\substack{r \mid P^*(z) \\ r < R}} g(r) y_r = c \sum_{\substack{r \mid P^*(z) \\ r < R}} g(r) = c \cdot G \rightsquigarrow c = \frac{1}{G}$$

となる．つまり, (A.3.27) は

$$y_r = \frac{1}{G} \quad (r \mid P^*(z),\ r < R)$$

のとき達成される．ここに Proposition A.3.3 を用いれば, $d \mid P^*(z)$ かつ $d < R$ なる d に対して,

$$\lambda_d = \frac{\mu(d) d}{\omega(d)} \sum_{\substack{r \mid P^*(z) \\ r < R \\ d \mid r}} g(r) y_r = \frac{1}{G} \frac{\mu(d) d}{\omega(d)} \sum_{\substack{r \mid P^*(z) \\ r < R \\ d \mid r}} g(r)$$

を得る．この最後の和にて r を dr に置き換えれば

$$\lambda_d = \frac{1}{G} \frac{\mu(d) d}{\omega(d)} \sum_{\substack{dr \mid P^*(z) \\ r < R/d}} g(dr)$$

だが g は平方無縁数を台に持つので

$$\lambda_d = \frac{1}{G} \frac{\mu(d) d g(d)}{\omega(d)} \sum_{\substack{r \mid P^*(z) \\ r < R/d \\ (r,d)=1}} g(r) = \frac{\mu(d)}{\prod_{p \mid d} \left(1 - \frac{\omega(p)}{p}\right)} \frac{G_d(R/d, z)}{G}$$

を得る．以上で主張が得られた． □

A.3.5　係数 λ_d の評価

さらに Proposition A.3.1 での誤差評価を行うために, Proposition A.3.4 で得られた最適な λ_d の評価を与えておく：

Proposition A.3.5. Proposition A.3.4 の状況の下, (A.3.24) で与えられた λ_d に対して,

$$|\lambda_d| \le 1$$

が $d \mid P^*(z)$ かつ $d < R$ のとき成立する.

Proof. Proposition A.3.4 で与えられた和

$$G = \sum_{\substack{n \mid P^*(z) \\ n < R}} g(n)$$

について考える. この和の項を $e \coloneqq (n, d)$ の値で分類すると

$$G = \sum_{e \mid d} \sum_{\substack{n \mid P^*(z) \\ n < R \\ (n,d)=e}} g(n) = \sum_{e \mid d} \sum_{\substack{en \mid P^*(z) \\ n < R/e \\ (n,d/e)=1}} g(en)$$

となるが, この和では g が平方無縁数を台に持つので, g の乗法性も思い出して

$$G = \sum_{e \mid d} g(e) \sum_{\substack{en \mid P^*(z) \\ n < R/e \\ (n,d/e)=1 \\ (n,e)=1}} g(n) = \sum_{e \mid d} g(e) \sum_{\substack{en \mid P^*(z) \\ n < R/e \\ (n,d)=1}} g(n) = \sum_{e \mid d} g(e) \sum_{\substack{n \mid P^*(z) \\ n < R/e \\ (n,d)=1}} g(n)$$

を得る. 今, 各項は非負なので

$$G \ge \sum_{e \mid d} g(e) \sum_{\substack{n \mid P^*(z) \\ n < R/d \\ (n,d)=1}} g(n) = \left(\sum_{e \mid d} g(e) \right) G_d(R/d, z).$$

最後に $d \mid P^*(z)$ から d が平方無縁であることに注意して Lemma A.2.1 を使えば

$$G \ge \prod_{p \mid d} (1 + g(p)) G_d(R/d, z) = \prod_{p \mid d} \left(\frac{p}{p - \omega(p)} \right) G_d(R/d, z) = \frac{1}{\displaystyle\prod_{p \mid d} \left(1 - \frac{\omega(p)}{p} \right)} G_d(R/d, z).$$

よって, (A.3.24) より

$$|\lambda_d| \le \frac{\mu(d)^2}{\displaystyle\prod_{p \mid d} \left(1 - \frac{\omega(p)}{p} \right)} \frac{G_d(R/d, z)}{G} \le 1$$

を得る. □

A.3.6　結果のまとめ

以上の議論をまとめて, 次の結果を得る：

Theorem A.3.1 (基本的な Selberg の篩). 次のものを考える：

- 篩データ $(\mathscr{A}, \mathscr{P}, \omega, X)$. また

$$\mathscr{P}^* := \{p \in \mathscr{P} \mid \omega(p) > 0\} \quad \text{および} \quad P^*(z) := \prod_{\substack{p \in \mathscr{P}^* \\ p < z}} p$$

  と書くことにする.
- 実数 $R, z \geq 2$.
- 平方無縁数に台を持つ乗法的関数

$$g(p) := \frac{\omega(p)}{p - \omega(p)}.$$

- 実数列 $(\lambda_d)_{d \mid P(z)}$ であって

$$\lambda_d := \begin{cases} \dfrac{\mu(d)}{\displaystyle\prod_{p \mid d}\left(1 - \dfrac{\omega(p)}{p}\right)} \dfrac{G_d(R/d, z)}{G} & (d \mid P^*(z) \text{ かつ } d < R \text{ のとき}), \\ \\ 0 & (\text{それ以外}) \end{cases}$$

  で定義されるもの. ただしここで

$$G_d(x, z) := \sum_{\substack{r \mid P^*(z) \\ r < x \\ (r,d)=1}} g(r) \quad (d \mid P(z)) \quad \text{および} \quad G := G_1(R, z). \tag{A.3.28}$$

このとき, 次が成り立つ：

(i) 篩関数の上からの評価

$$S(\mathscr{A}, \mathscr{P}, z) \leq \frac{X}{G} + E$$

が残余項

$$E := \sum_{\substack{d_1, d_2 \mid P(z) \\ d_1, d_2 < R}} \lambda_{d_1} \lambda_{d_2} E([d_1, d_2])$$

とともに成り立つ.

(ii) 任意の $d \mid P(z)$ に対して, $|\lambda_d| \leq 1$ である.

Proof. 評価 (i) については, Proposition A.3.1 に Proposition A.3.4 を用いれば良い. (ii) は Proposition A.3.5 で示された. □

A.4 基本的な Selberg の篩の応用 I — 素数の個数評価

Selberg の篩の応用として, まずは x 以下の素数の個数 $\pi(x)$ の評価を得てみよう.

次の補題を準備する：

Lemma A.4.1. 実数 $x > 1$ に対して

$$\sum_{n<x} \frac{1}{n} \geq \log x$$

が成立する.

Proof. 関数 $u \mapsto \frac{1}{u}$ は $u > 0$ で単調に減少するので,

$$\sum_{n<x} \frac{1}{n} = \sum_{n<x} \int_n^{n+1} \frac{du}{n} \geq \sum_{n<x} \int_n^{n+1} \frac{du}{u}$$

である. ここで, $n < x$ なる自然数は $1, \ldots, \lceil x \rceil - 1$ ですべてなので, 積分区間をつなげて

$$\sum_{n<x} \frac{1}{n} \geq \int_1^{\lceil x \rceil} \frac{du}{u} = \log\lceil x \rceil \geq \log x$$

を得る.（ただしここで, $\lceil x \rceil$ は $\lceil x \rceil \coloneqq \min\{n \in \mathbb{Z} \mid n \geq x\}$ で定義される天井関数である.） □

では実際に $\pi(x)$ を評価してみよう. 次の結果は, 定数倍を除き, 素数定理

$$\pi(x) \sim \frac{x}{\log x} \quad (x \to \infty)$$

と同等の評価を上からだけではあるが, 示すことに成功している：

Theorem A.4.1 (Chebyshev)**.** 定数 $C \geq 1$ が存在して, 実数 $x \geq 2$ に対して,

$$\pi(x) \leq C \frac{x}{\log x}$$

が成立する.

Proof. Proposition A.1.3 の篩データ $(\mathscr{A}, \mathscr{P}, \omega, X)$ を用いる. すると, Proposition A.1.3 の (ii) より

$$\pi(x) \leq S(\mathscr{A}, \mathscr{P}, z) + z \tag{A.4.29}$$

である. よって, 篩関数 $S(\mathscr{A}, \mathscr{P}, z)$ を上から評価したい.

Selberg の篩（Theorem A.3.1）を用いる. パラメター $R \geq 2$ を取れば, Theorem A.3.1 より

$$S(\mathscr{A}, \mathscr{P}, z) \leq \frac{X}{G} + E = \frac{x}{G} + E \tag{A.4.30}$$

が成立する．ただしここで, 和 G は

$$G \coloneqq \sum_{\substack{r \mid P^*(z) \\ r<R}} g(r) \quad \text{ただし} \quad g(p) \coloneqq \frac{\omega(p)}{p-\omega(p)} \tag{A.4.31}$$

と定義され, 残余項 E は

$$E \coloneqq \sum_{\substack{d_1,d_2 \mid P(z) \\ d_1,d_2<R}} \lambda_{d_1}\lambda_{d_2} E([d_1,d_2]) \quad \text{ただし} \quad |\lambda_d| \leq 1 \tag{A.4.32}$$

で定義される．次に, (A.4.30) の右辺を評価すべく, G と E の評価を行う．

まず, 和 G について考える．和 (A.4.31) の条件 $r \mid P^*(z)$ は取り扱いづらいので

$$R \coloneqq z \tag{A.4.33}$$

ととり, $g(p)=0 \iff \omega(p)=0$ に注意して,

$$G = \sum_{\substack{r \mid P^*(z) \\ r<z}} g(r) = \sum_{r<z} g(r) \tag{A.4.34}$$

と単純化しておく．今, 局所密度は $\omega(p)=1$ で定義されているので, (A.4.31) より

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

が成立する．ここで, 自然数 n に対して, その素因数分解の指数をすべて 1 にしたものを

$$k(n) \coloneqq \prod_{p \mid n} p$$

と書けば, 平方無縁数 r に対して, 等比級数の展開と素因数分解の一意性より,

$$g(r) = \prod_{p \mid r}\left(\frac{1}{p-1}\right) = \prod_{p \mid r}\left(\frac{1}{p}+\frac{1}{p^2}+\cdots\right) = \sum_{\substack{n \\ p \mid n \iff p \mid r}} \frac{1}{n} = \sum_{\substack{n \\ k(n)=r}} \frac{1}{u}$$

を得る．これを足し上げれば, (A.4.34) は Lemma A.4.1 を用いて

$$G = \sum_{r<z} \mu(r)^2 g(r) = \sum_{\substack{n \\ k(n)<z}} \frac{1}{n} \geq \sum_{n<z} \frac{1}{n} \geq \log z \tag{A.4.35}$$

と下から評価できる．

次に, 誤差項 E であるが, Proposition A.1.3 の (i) と $|\lambda_d| \leq 1$ を (A.4.32) に用いれば,

$$|E| \leq \sum_{\substack{d_1,d_2 \mid P(z) \\ d_1,d_2<R}} 1 \leq \sum_{d_1,d_2<R} 1 \leq R^2$$

と評価できる．今 (A.4.33) で決めたように $R \coloneqq z$ と選んでいるから

$$|E| \leq z^2 \tag{A.4.36}$$

を得る．

以上の (A.4.35) と (A.4.36) を (A.4.30) に用いれば

$$S(\mathscr{A},\mathscr{P},z) \leq \frac{x}{\log z} + z^2$$

を得る．これをさらに (A.4.29) に用いれば

$$\pi(x) \leq \frac{x}{\log z} + z^2 + z$$

を得る．一旦, x は十分大, 特に $x \geq 8$ として

$$z \coloneqq x^{\frac{1}{3}} \geq 2 \tag{A.4.37}$$

と取ってみる．実数 $X > 0$ に対し, $\log X \leq X$ を用いれば $\frac{1}{3}\log X = \log X^{\frac{1}{3}} \leq X^{\frac{1}{3}}$ が分かるから

$$z^2 + z \leq 2z^2 = 2x^{\frac{2}{3}} = \frac{2x}{x^{\frac{1}{3}}} \leq \frac{6x}{\log x}$$

を得る．よって, $x \geq 8$ のとき, (A.4.37) から

$$\pi(x) \leq \frac{3x}{\log x} + \frac{6x}{\log x} \leq \frac{9x}{\log x} \quad (x \geq 8) \tag{A.4.38}$$

が得られる．一方, 増減表を書けば得られる評価

$$\min_{x \geq 2} \frac{x}{\log x} = \left(\frac{x}{\log x}\right)\bigg|_{x=e} = e$$

を用いれば,

$$\pi(x) \leq 8 \leq \frac{8}{e}\frac{x}{\log x} \leq \frac{9x}{\log x} \quad (2 \leq x \leq 8) \tag{A.4.39}$$

である．よって, (A.4.38) と (A.4.39) より, $C \coloneqq 9$ と取れば主張が成立することが分かる． □

上記の Theorem A.4.1 の証明では, Eratosthenes–Legendre の篩が失敗した残余項の制御を Selberg のアイデアが見事に成し遂げていることが見て取れる．

A.5 Mertens の定理

A.5.1 von Mangoldt 関数

前節では, 篩法を用いて $\pi(x)$ の上からの評価に成功した．しかし, このままでは素数に関する漸近公式を示すのは無理なので, 他の方法を考えてみよう．素数というのは自然数に素因数分解が成り立つように定義したものである．そこで自然数 n に対して, その素因数分解を書いてみる：

$$n = \prod_{p^v \| n} p^v.$$

これからやりたいのは素数に渡る和の取り扱いである．しかし, 上の素因数分解は和と相性が悪そうに見える．そこで, 積を和に直すべく log を取ってみると

$$\log n = \sum_{p^v \| n} v \log p$$

という等式を得る．ここで $\log p$ の前の因子 v は p が n を割る回数だから, この等式を

$$\log n = \sum_{p^v | n} \log p \tag{A.5.40}$$

とも書ける．この等式は次のように定義される von Mangoldt 関数を使うとより簡潔に書ける．

Definition A.5.1 (von Mangoldt **関数**). **von Mangoldt 関数**と呼ばれる数論的関数 Λ を

$$\Lambda(n) := \begin{cases} \log p & n\text{ が素数 }p\text{ の 1 次以上のべき乗のとき}, \\ 0 & \text{それ以外} \end{cases}$$

で定める．

Proposition A.5.1. 自然数 n に対して

$$\log n = \sum_{d|n} \Lambda(d) = \sum_{dm=n} \Lambda(d).$$

Proof. これは (A.5.40) を書き換えただけの等式である． □

A.5.2 Mertens の定理

Proposition A.5.1 の等式によって, 我々のよく知っている対数関数と素数が結びついた．この等式を Möbius 反転を用いて $\Lambda(n)$ に関して「解く」ことも可能であるが, 今回考えたいのは素数に渡る和なので, 先に Proposition A.5.1 で得た等式を足し上げよう．次を準備しておく．

Lemma A.5.1. 実数 $x \geq 2$ に対して

$$\sum_{n \leq x} \log n = x \log x - x + O(\log x)$$

が成立する．

Proof. 微積分学の基本定理より

$$\log n = \log x - \int_n^x \frac{du}{u}$$

である．これを代入すれば, 積分と和の交換は Remark A.2.5 を参考にして

$$\sum_{n \leq x} \log n = \log x \sum_{n \leq x} 1 - \sum_{n \leq x} \int_n^x \frac{du}{u} = [x] \log x - \sum_{n \leq x} \int_1^x \mathbb{1}_{n \leq u} \frac{du}{u}$$

$$
\begin{aligned}
&= [x]\log x - \int_1^x \left(\sum_{n\le x} \mathbb{1}_{n\le u}\right)\frac{du}{u} \\
&= [x]\log x - \int_1^x \left(\sum_{n\le u} 1\right)\frac{du}{u} \\
&= [x]\log x - \int_1^x \frac{[u]}{u}du \\
&= x\log x - \int_1^x du - \{x\}\log x + \int_1^x \frac{\{u\}}{u}du \\
&= x\log x - x - \{x\}\log x + \int_1^x \frac{\{u\}}{u}du + 1
\end{aligned}
$$

だが

$$
-\{x\}\log x + \int_1^x \frac{\{u\}}{u}du + 1 \ll \log x + \int_1^x \frac{du}{u} + 1 \ll \log x
$$

だから主張を得る. □

すると, 和を取った後に Proposition A.5.1 の等式を「解く」と次が得られる：

Theorem A.5.1 (Mertens **の定理**)**.** 実数 $x \ge 1$ に対して,

$$
\sum_{n\le x} \frac{\Lambda(n)}{n} = \log x + O(1) \quad \text{および} \quad \sum_{p\le x} \frac{\log p}{p} = \log x + O(1)
$$

が成立する.

Proof. 範囲 $x \ge 2$ で証明すれば良い.

まずは von Mangoldt 関数に関する和から考える. Proposition A.5.1 より

$$
\sum_{n\le x} \log n = \sum_{n\le x}\sum_{dm=n} \Lambda(d) = \sum_{dm\le x} \Lambda(d) = \sum_{d\le x} \Lambda(d) \sum_{m\le x/d} 1 = \sum_{d\le x} \Lambda(d)\left[\frac{x}{d}\right]
$$

だが, 最後の整数部分を近似し,

$$
\sum_{n\le x} \log n = x\sum_{d\le x} \frac{\Lambda(d)}{d} + O\left(\sum_{d\le x} \Lambda(d)\right) \tag{A.5.41}
$$

を得る. 次に, この誤差項を抑えたい. von Mangoldt 関数の定義を思い出すと

$$
\sum_{d\le x} \Lambda(d) = \sum_{v\ge 1}\sum_{p^v\le x} \log p
$$

であるが, 素数は常に 2 以上なので, $p^v \le x$ から $v \le \frac{\log x}{\log 2}$ が分かるから

$$
\sum_{d\le x} \Lambda(d) = \sum_{1\le v\le \frac{\log x}{\log 2}} \sum_{p^v\le x} \log p \le (\log x) \sum_{1\le v\le \frac{\log x}{\log 2}} \pi(x^{\frac{1}{v}})
$$

とできる．ここで $v=1$ のときだけ特別視して, $v\geq 2$ のときは $\pi(X)\leq X$ を用いることで

$$\sum_{d\leq x}\Lambda(d)\leq \pi(x)\log x+(\log x)\sum_{2\leq v\leq \frac{\log x}{\log 2}}x^{\frac{1}{v}}\ll \pi(x)\log x+x^{\frac{1}{2}}(\log x)^2$$

となる．さらに, $\pi(x)$ の上からの評価 Theorem A.4.1 を用いれば

$$\sum_{d\leq x}\Lambda(d)\ll x+x^{\frac{1}{2}}(\log x)^2\ll x$$

が分かる．これを (A.5.41) に代入すれば

$$\sum_{n\leq x}\log n=x\sum_{d\leq x}\frac{\Lambda(d)}{d}+O(x) \tag{A.5.42}$$

を得る．一方, Lemma A.5.1 より

$$\sum_{n\leq x}\log n=x\log x+O(x) \tag{A.5.43}$$

が成立する．以上の (A.5.42) と (A.5.43) を合わせると

$$x\sum_{d\leq x}\frac{\Lambda(d)}{d}=x\log x+O(x)$$

を得る．これを von Mangoldt 関数の和について「解け」ば

$$\sum_{d\leq x}\frac{\Lambda(d)}{d}=\log x+O(1)$$

と von Mangoldt 関数に対する主張を得る．

次に素数に渡る和に関する主張であるが,

$$\sum_{n\leq x}\frac{\Lambda(n)}{n}=\sum_{p^v\leq x}\frac{\log p}{p^v}$$

だから $v=1$ の部分だけ特別視すれば

$$\sum_{p\leq x}\frac{\log p}{p}=\sum_{n\leq x}\frac{\Lambda(n)}{n}-\sum_{v\geq 2}\sum_{p^v\leq x}\frac{\log p}{p^v}$$

を得る．ここに上に示した von Mangoldt 関数に関する主張を用いて

$$\sum_{p\leq x}\frac{\log p}{p}=\log x-\sum_{v\geq 2}\sum_{p^v\leq x}\frac{\log p}{p^v}+O(1)$$

を得る．よって, 示すべきは

$$\sum_{v\geq 2}\sum_{p^v\leq x}\frac{\log p}{p^v}\ll 1 \tag{A.5.44}$$

である．これは

$$\sum_{v\ge 2}\sum_{p^v\le x}\frac{\log p}{p^v}\le\sum_p\log p\sum_{v\ge 2}\frac{1}{p^v}=\sum_p\frac{\log p}{p(p-1)}$$

だが $p\ge 2$ のとき $p-1\ge\frac{p}{2}$ であり, また $\log p=2\log p^{\frac12}\le 2p^{\frac12}$ なので

$$\sum_{v\ge 2}\sum_{p^v\le x}\frac{\log p}{p^v}\le 2\sum_p\frac{\log p}{p^2}\le 4\sum_{n=1}^{\infty}n^{-\frac32}$$

を得る．最後の和は積分と比較するか

$$\sum_{n=1}^{\infty}n^{-\frac32}=\frac32\sum_{n=1}^{\infty}\int_n^{\infty}u^{-\frac52}du=\frac32\int_1^{\infty}\left(\sum_{n\le u}1\right)u^{-\frac52}du\le\frac32\int_1^{\infty}u^{-\frac32}du=3$$

とすれば収束性が分かるので, (A.5.44) が示せた． □

A.6 相対密度の平均値

Selberg の篩は

$$S(\mathscr{A},\mathscr{P},z)\le\frac{X}{G}+E\quad ただし\quad G:=\sum_{\substack{r|P^*(z)\\ r<R}}g(r)$$

という形の評価を与える．よって, これを実際に使うときには相対密度 g の和 G の下からの評価が必要になる．Theorem A.4.1 で ad hoc な方法で G の下からの評価を得たが, ここではより systematic に和 G を取り扱う方法を考える．相変わらず簡単のために $R:=z$ と取ることにすると, $r<z$ なる自然数 r の素因子は z より小さいので, Definition A.1.2 で $p\notin\mathscr{P}$ のとき $\omega(p)=0$ と仮定していたことも思い出せば

$$G=\sum_{r<z}g(r)$$

となる．そこで, 実数 $x\ge 1$ に対して相対密度 g の平均値を

$$M(x)=M_g(x):=\sum_{n<x}g(n)$$

と書き（注：解析数論ではしばしばただの総和のことを平均値と呼んで $\frac{1}{x}$ のような正規化の因子を省く事が多い）, この平均値の漸近公式を与える一般的な定理を準備しよう．この定理は Maynard [5] の Lemma 6.1 に対応する．Maynard [5] は Halberstam–Richert [4] を引用しているが, ここでは Iwaniec–Friedlander の Opera de Cribro [1] の Appendix A.2 を参考にした議論を用いる．（この議論はさらに [6] に基づくということである.）

A.6.1　数論的関数の平均値の簡単な評価

まず, 本格的に相対密度の平均値について考える前に, 非負値の乗法的関数一般に対して簡単な評価を準備しておく（この評価は Maynard の論文 [5] でもあちこちで便利である）：

Lemma A.6.1. 平方無縁数を台に持つ非負値の乗法的関数 g で, 実数 $\kappa > 0$ と $A \geq 1$ に対して

$$\sum_{w \leq p < z} g(p) \leq \kappa \log \frac{\log z}{\log w} + \frac{A}{\log w} \quad (2 \leq \forall w \leq \forall z) \tag{A.6.45}$$

が成立するものを考える.（応用時は Lemma A.6.4 を参照のこと.）このとき,

$$\sum_{n < x} g(n) \ll (\log x)^{\kappa}$$

が成立する. ただしここで implicit constant は κ, A に依存する.

Proof. 数論的関数 g は平方無縁数を台に持つので, Lemma A.2.1 と実数 X に対して成り立つ不等式

$$1 + X \leq e^{X}$$

より,

$$\sum_{n<x} g(n) \leq \prod_{p<x} (1 + g(p)) \leq \exp\left(\sum_{p<x} g(p)\right)$$

を得る. ここに (A.6.45) を $w \coloneqq 2$ と $z \coloneqq x$ とともに用い,

$$\sum_{n<x} g(n) \leq \exp\left(\kappa \log\log x - \kappa \log\log 2 + \frac{A}{\log 2}\right) = e^{\frac{A}{\log 2}} (\log 2)^{-\kappa} (\log x)^{\kappa}$$

を得る. これで主張が示された. □

A.6.2　局所密度に関する仮定

以後, この Section A.6 では, 以下の設定・条件を用いる：

- 非負値の乗法的関数 γ. 前節までの局所密度 ω に対応するので, 同じく局所密度と呼ぼう.
  （一旦, Definition A.1.2 より一般的な状況で考える.）
- 定数 $\kappa > 0$. 篩次元と呼ぶ. 以後, implicit constant は κ に依存して良いものとする.
- 定数 $A_1, A_2 \geq 1$. 以後, implicit constant は A_1, A_2, κ に依存して良いものとする.
- 定数 $L \geq 1$. 以後, implicit constant は L に**依存してはいけない**とする.
- 次の局所密度の素数での値に関する条件：

$$0 \leq \frac{\gamma(p)}{p} \leq 1 - \frac{1}{A_1}. \tag{Γ_1}$$

- 次の局所密度の篩次元に関する条件：

$$-L \le \sum_{w \le p < z} \frac{\gamma(p)\log p}{p} - \kappa \log\frac{z}{w} \le A_2 \quad (2 \le \forall w \le \forall z). \tag{Γ_2}$$

この条件が成立することを, 「γ は篩次元 κ を持つ」という.

- 平方無縁数を台に持つ乗法的関数 g を

$$g(p) \coloneqq \frac{\gamma(p)}{p-\gamma(p)} \tag{A.6.46}$$

で定める. 仮定 (Γ_1) より右辺の分母は 0 でない. 注意であるが

$$g(p) = \frac{\gamma(p)}{p} + \frac{\gamma(p)}{p}g(p) \tag{A.6.47}$$

と書くこともできる. γ として局所密度 ω が取られたとき, g は**相対密度**と呼ばれることがある.

- 総和関数

$$M(x) = M_g(x) \coloneqq \sum_{n<x} g(n).$$

A.6.3 局所密度に関する仮定の帰結

以下, 条件 (Γ_1), (Γ_2) の帰結のうち必要なものをいくつか証明する：

Lemma A.6.2. 条件 (Γ_2) を仮定する. 非負値かつ広義単調減少な C^1 級関数

$$\Phi\colon [w,z] \to \mathbb{R} \quad ただし \quad 2 \le w \le z$$

に対して,

$$\kappa\int_w^z \Phi(u)\frac{du}{u} - L\Phi(w) \le \sum_{w\le p<z}\frac{\gamma(p)\log p}{p}\Phi(p) \le \kappa\int_w^z \Phi(u)\frac{du}{u} + A_2\Phi(w)$$

が成立する.

Proof. 微積分学の基本定理より

$$\Phi(p) = \int_p^z (-\Phi'(u))du + \Phi(z)$$

だから, Lemma A.5.1 の証明での Remark A.2.5 に基づいた変形を参考にして

$$\begin{aligned}\sum_{w\le p<z}\frac{\gamma(p)\log p}{p}\Phi(p) &= \sum_{w\le p<z}\frac{\gamma(p)\log p}{p}\int_p^z(-\Phi'(u))du + \Phi(z)\sum_{w\le p<z}\frac{\gamma(p)\log p}{p} \\ &= \int_w^z\Biggl(\sum_{w\le p<u}\frac{\gamma(p)\log p}{p}\Biggr)(-\Phi'(u))du + \Phi(z)\sum_{w\le p<z}\frac{\gamma(p)\log p}{p}\end{aligned} \tag{A.6.48}$$

を得る．ここで $2 \le w \le z$ に対して

$$\sum_{w \le p < z} \frac{\gamma(p)\log p}{p} = \kappa \log \frac{z}{w} + \delta(w,z) \tag{A.6.49}$$

と書くことにする．すると (Γ_2) より, 任意の $2 \le w \le z$ に対して

$$-L \le \delta(w,z) \le A_2 \tag{A.6.50}$$

が成立する．さて, (A.6.49) を (A.6.48) に代入したあと, $(-\Phi'(u))$ を積分するように部分積分を行い,

$$\begin{aligned}\sum_{w \le p < z} \frac{\gamma(p)\log p}{p}\Phi(p) &= \kappa \int_w^z \left(\log \frac{u}{w}\right)(-\Phi'(u))du + \kappa\left(\log \frac{z}{w}\right)\Phi(z) \\ &\qquad + \int_w^z \delta(w,u)(-\Phi'(u))du + \Phi(z)\delta(w,z) \\ &= \kappa \int_w^z \frac{\Phi(u)}{u}du + \int_w^z \delta(w,u)(-\Phi'(u))du + \Phi(z)\delta(w,z)\end{aligned} \tag{A.6.51}$$

を得る．あとは $\Phi(z), -\Phi'(u) \ge 0$ なので, (A.6.50) から

$$\begin{aligned}\int_w^z \delta(w,u)(-\Phi'(u))du + \Phi(z)\delta(w,z) &\le A_2 \int_w^z (-\Phi'(u))du + A_2\Phi(z) = A_2\Phi(w), \\ \int_w^z \delta(w,u)(-\Phi'(u))du + \Phi(z)\delta(w,z) &\ge -L \int_w^z (-\Phi'(u))du - L\Phi(z) = -L\Phi(w),\end{aligned}$$

を得る．この誤差評価を (A.6.51) に用いて主張を得る． □

Lemma A.6.3. 条件 (Γ_2) を仮定する．範囲 $2 \le w \le z$ で

$$-\frac{L}{\log w} \le \sum_{w \le p < z} \frac{\gamma(p)}{p} - \kappa \log \frac{\log z}{\log w} \le \frac{A_2}{\log w}$$

および

$$\sum_{w \le p < z} \frac{\gamma(p)}{p \log p} \le \frac{1}{\log w}\left(\kappa + \frac{A_2}{\log w}\right)$$

が成立する．

Proof. それぞれ, Lemma A.6.2 において

$$\Phi(u) \coloneqq \frac{1}{\log u} \quad \text{および} \quad \Phi(u) \coloneqq \frac{1}{(\log u)^2}$$

とすればよい．なお, 主要項は

$$\int_w^z \frac{du}{u \log u} = \log \frac{\log z}{\log w} \quad \text{および} \quad \int_w^z \frac{du}{u(\log u)^2} = \frac{1}{\log w} - \frac{1}{\log z} \le \frac{1}{\log w}$$

と計算および評価される． □

Lemma A.6.4 (**Mertens の定理**). 範囲 $2 \le w \le z$ で

$$\sum_{w \le p < z} \frac{1}{p} = \log \frac{\log z}{\log w} + O\left(\frac{1}{\log w}\right)$$

が成立する.

Proof. Mertens の定理（Theorem A.5.1）を使えば, 定数関数 $\gamma(p) = 1$ に対して, 条件 (Γ_2) が $\kappa = 1$ と $A, L = O(1)$ で成立する. よって, Lemma A.6.3 から主張が従う. □

Lemma A.6.5. 条件 (Γ_2) を仮定する. 任意の素数 p に対して

$$\frac{\gamma(p)}{p} \le \frac{A_2}{\log p}$$

が成立する.

Proof. 実数 $\varepsilon \in (0,1)$ をとる. 条件 (Γ_2) において, $w \coloneqq p$, $z \coloneqq p + \varepsilon$ とすれば, 今, $\varepsilon \in (0,1)$ だから区間 $[w, z)$ 内の素数は p のみになるので, ϖ を素数を渡る変数とすれば

$$\frac{\gamma(p) \log p}{p} = \sum_{w \le \varpi < z} \frac{\gamma(\varpi) \log \varpi}{\varpi} \le \kappa \log \frac{p + \varepsilon}{p} + \frac{A_2}{\log p}$$

を得る. あとは極限 $\varepsilon \searrow 0$ をとればよい. □

Lemma A.6.6. 条件 (Γ_1) と (Γ_2) を仮定する. 任意の素数 p に対して

$$g(p) \le A_1 \frac{\gamma(p)}{p} \le \frac{A_1 A_2}{\log p}$$

が成立する.

Proof. 数論的関数 g の定義 (A.6.46) と (Γ_1) より

$$g(p) = \frac{\gamma(p)}{p - \gamma(p)} = \frac{1}{1 - \frac{\gamma(p)}{p}} \frac{\gamma(p)}{p} \le A_1 \frac{\gamma(p)}{p}$$

を得る. あとは Lemma A.6.5 を使えば後半の評価を得る. □

Lemma A.6.7. 条件 (Γ_1), (Γ_2) を仮定する. 範囲 $2 \le w \le z$ で

$$\sum_{w \le p < z} g(p)^2 \ll \sum_{w \le p < z} \frac{\gamma(p)}{p} g(p) \ll \frac{1}{\log w}$$

が成立する. ただし implicit constant は κ, A_1, A_2 のみに依存する.

Proof. 前半の評価は Lemma A.6.6 から

$$\sum_{w\le p<z} g(p)^2 \le A_1 \sum_{w\le p<z} \frac{\gamma(p)}{p} g(p)$$

と従う．後半の評価は Lemma A.6.3 と Lemma A.6.6 より

$$\sum_{w\le p<z} \frac{\gamma(p)}{p} g(p) \le A_1A_2 \sum_{w\le p<z} \frac{\gamma(p)}{p\log p} \le \frac{A_1A_2}{\log w}\left(\kappa + \frac{A_2}{\log w}\right) \le \frac{A_1A_2}{\log w}\left(\kappa + \frac{A_2}{\log 2}\right)$$

と従う． □

Lemma A.6.8. 条件 (Γ_1), (Γ_2) を仮定する．範囲 $2\le w\le z$ で

$$-\frac{L}{\log w} \le \sum_{w\le p<z} g(p) - \kappa \log\frac{\log z}{\log w} \le O\!\left(\frac{1}{\log w}\right)$$

が成立する．特に Lemma A.6.1 を用いれば

$$\sum_{n<x} g(n) \ll (\log x)^{\kappa} \tag{A.6.52}$$

が分かる．ただし上記評価の implicit constant たちは κ, A_1, A_2 のみに依存する．

Proof. まず, (A.6.47) から

$$\sum_{w\le p<z} g(p) = \sum_{w\le p<z} \frac{\gamma(p)}{p} + \sum_{w\le p<z} \frac{\gamma(p)}{p} g(p) \tag{A.6.53}$$

である．すると, Lemma A.6.3 から

$$\sum_{w\le p<z} g(p) \ge \sum_{w\le p<z} \frac{\gamma(p)}{p} \ge \kappa\log\frac{\log z}{\log w} - \frac{L}{\log w}$$

だから, 下からの評価を得る．よって, 上からの評価

$$\sum_{w\le p<z} g(p) - \kappa\log\frac{\log z}{\log w} \le O\!\left(\frac{1}{\log w}\right)$$

のみ示せばよい．先に得た分解 (A.6.53) の右辺の最初の和は Lemma A.6.3 より

$$\sum_{w\le p<z} \frac{\gamma(p)}{p} \le \kappa\log\frac{\log z}{\log w} + \frac{A_2}{\log w}$$

と評価でき, ふたつめの和は Lemma A.6.7 で評価でき, 主張が従う． □

A.6.4 積分方程式の導出

Lemma A.6.9. 仮定 (Γ_1), (Γ_2) の下, 実数 $x \geq 2$ に対して

$$M(x)\log x = (\kappa+1)\int_2^x \frac{M(u)}{u}du + \Delta(x) \tag{A.6.54}$$

が成立し, 誤差項 $\Delta(x)$ は $x \geq 2$ に対して

$$\Delta(x) \ll L(\log x)^\kappa \tag{A.6.55}$$

と評価できる. ただしここで implicit constant は κ, A_1, A_2 のみに依存する.

Proof. 平方無縁数 n に対して

$$\log n = \sum_{p|n}\log p = \sum_{pm=n}\log p \tag{A.6.56}$$

であることを用いるべく, 一旦, $g(n)\log n$ の総和関数

$$\sum_{n<x} g(n)\log n$$

について考える. 数論的関数 g は平方無縁数に台を持つから (A.6.56) より

$$\sum_{n<x} g(n)\log n = \sum_{mp<x} g(mp)\log p = \sum_{np<x} g(np)\log p$$

である. すると, g が平方無縁数に台を持つから $(n,p)=1$ という条件を課せて, g は乗法的なので

$$\sum_{n<x} g(n)\log n = \sum_{\substack{np<x\\(n,p)=1}} g(n)g(p)\log p \tag{A.6.57}$$

を得る. ここで g の代わりにもともとの γ を用いるべく (A.6.47) を思い出し, (A.6.57) を

$$\begin{aligned}\sum_{n<x} g(n)\log n &= \sum_{\substack{np<x\\(n,p)=1}} g(n)\frac{\gamma(p)\log p}{p} + \sum_{\substack{np<x\\(n,p)=1}} g(n)\frac{\gamma(p)\log p}{p}g(p)\\ &= \sum_{\substack{np<x\\(n,p)=1}} g(n)\frac{\gamma(p)\log p}{p} + \sum_{n<x} g(n)\sum_{\substack{p<x/n\\(p,n)=1}}\frac{\gamma(p)\log p}{p}g(p)\end{aligned} \tag{A.6.58}$$

と書いておく. 条件 $(n,p)=1$ とは $p \nmid n$ のことだから, (A.6.58) の右辺第 1 項目はさらに

$$\begin{aligned}\sum_{\substack{np<x\\(n,p)=1}} g(n)\frac{\gamma(p)\log p}{p} &= \sum_{np<x} g(n)\frac{\gamma(p)\log p}{p} - \sum_{\substack{np<x\\p|n}} g(n)\frac{\gamma(p)\log p}{p}\\ &= \sum_{np<x} g(n)\frac{\gamma(p)\log p}{p} - \sum_{np^2<x} g(np)\frac{\gamma(p)\log p}{p}\end{aligned}$$

とできる．この最右辺第 2 項目は g が平方無縁数に台を持つから, g の乗法性より

$$\begin{aligned}\sum_{\substack{np<x\\(n,p)=1}} g(n)\frac{\gamma(p)\log p}{p} &= \sum_{np<x} g(n)\frac{\gamma(p)\log p}{p} - \sum_{\substack{np^2<x\\(n,p)=1}} g(n)\frac{\gamma(p)\log p}{p}g(p)\\ &= \sum_{np<x} g(n)\frac{\gamma(p)\log p}{p} - \sum_{n<x} g(n)\sum_{\substack{p<(x/n)^{\frac{1}{2}}\\(p,n)=1}} \frac{\gamma(p)\log p}{p}g(p)\end{aligned}$$

と書き直せる．これを (A.6.58) に代入して

$$\begin{aligned}&-\sum_{n<x} g(n)\sum_{\substack{p<(x/n)^{\frac{1}{2}}\\(p,n)=1}} \frac{\gamma(p)\log p}{p}g(p) + \sum_{n<x} g(n)\sum_{\substack{p<x/n\\(p,n)=1}} \frac{\gamma(p)\log p}{p}g(p)\\ &= \sum_{n<x} g(n)\sum_{\substack{(x/n)^{\frac{1}{2}}\le p<x/n\\(p,n)=1}} \frac{\gamma(p)\log p}{p}g(p)\end{aligned}$$

に気をつければ

$$\sum_{n<x} g(n)\log n = \sum_{np<x} g(n)\frac{\gamma(p)\log p}{p} + \sum_{n<x} g(n)\sum_{\substack{(x/n)^{\frac{1}{2}}\le p<x/n\\(p,n)=1}} \frac{\gamma(p)\log p}{p}g(p) \tag{A.6.59}$$

と 2 つの和への分解を得る．一旦, 実数 $u \ge 1$ に対して

$$\sum_{p<u} \frac{\gamma(p)\log p}{p} = \kappa\log u + \delta(u) \tag{A.6.60}$$

と書くと,

$$\delta(u) = \sum_{p<u} \frac{\gamma(p)\log p}{p} - \kappa\log u = \sum_{2\le p<u} \frac{\gamma(p)\log p}{p} - \kappa\log\frac{u}{2} - \kappa\log 2$$

なので, (Γ_2) から, 実数 $u \ge 2$ に対して

$$-L - \kappa\log 2 \le \delta(u) \le A_2 - \kappa\log 2 \quad 従って \quad \delta(u) \ll L$$

を得る．また, $1 \le u < 2$ の範囲でも $p < u$ なる素数 p が存在しないので

$$1 \le u < 2 \implies \delta(u) = \sum_{p<u} \frac{\gamma(p)\log p}{p} - \kappa\log u = -\kappa\log u \quad 従って \quad \delta(u) \ll L$$

となる．よって, いずれにせよ

$$\delta(u) \ll L \qquad (u \ge 1) \tag{A.6.61}$$

である．そこで, (A.6.59) を

$$\sum_{n<x} g(n)\log n = \sum_{n<x} g(n)\sum_{p<x/n} \frac{\gamma(p)\log p}{p} + \sum_{n<x} g(n)\sum_{\substack{(x/n)^{\frac{1}{2}}\le p<x/n\\(p,n)=1}} \frac{\gamma(p)\log p}{p}g(p)$$

と書き, ここに (A.6.60) を代入すれば

$$\sum_{n<x} g(n)\log n = \kappa\sum_{n<x} g(n)\log\frac{x}{n} + \widetilde{\Delta}(x) \tag{A.6.62}$$

ただし

$$\widetilde{\Delta}(x) \coloneqq \sum_{n<x} g(n)\delta\left(\frac{x}{n}\right) + \sum_{n<x} g(n) \sum_{\substack{(x/n)^{\frac{1}{2}}\le p<x/n \\ (p,n)=1}} \frac{\gamma(p)\log p}{p} g(p) \tag{A.6.63}$$

を得る. さらに, (A.6.62) の両辺に

$$\sum_{n<x} g(n)\log\frac{x}{n}$$

を足せば,

$$M(x)\log x = (\kappa+1)\sum_{n<x} g(n)\log\frac{x}{n} + \widetilde{\Delta}(x) \tag{A.6.64}$$

を得る. ここで

$$\sum_{n<x} g(n)\log\frac{x}{n} = \sum_{n<x} g(n)\int_n^x \frac{du}{u} = \int_1^x \frac{M(u)}{u}du$$

であるが, g の乗法性から $g(1)=1$ なので, $x\ge 2$ のとき

$$(\kappa+1)\sum_{n<x} g(n)\log\frac{x}{n} = (\kappa+1)\int_2^x \frac{M(u)}{u}du + (\kappa+1)\log 2$$

を得る. これを (A.6.64) に代入すれば, 主張されている等式 (A.6.54) が

$$\Delta(x) \coloneqq \widetilde{\Delta}(x) + (\kappa+1)\log 2$$

とともに成立していることがわかる. あとは,

$$(\kappa+1)\log 2 \ll L(\log x)^\kappa$$

だから, (A.6.63) で与えられた $\widetilde{\Delta}(x)$ に対して

$$\widetilde{\Delta}(x) \ll L(\log x)^\kappa \tag{A.6.65}$$

を示せば良い.

まず, (A.6.63) の右辺第 1 項については, (A.6.61) から

$$\sum_{n<x} g(n)\delta\left(\frac{x}{m}\right) \ll L\sum_{n<x} g(n) = LM(x) \tag{A.6.66}$$

を得る. さらに, (A.6.63) の右辺第 2 項

$$\sum_{n<x} g(n) \sum_{\substack{(x/n)^{\frac{1}{2}}\le p<x/n \\ (p,n)=1}} \frac{\gamma(p)\log p}{p} g(p)$$

については, 内側の和が空でなければ, 対応する p に対して $2 \le p < x/n$ が成り立つので,

$$\sum_{n<x} g(n) \sum_{\substack{(x/n)^{\frac{1}{2}} \le p < x/n \\ (p,n)=1}} \frac{\gamma(p)\log p}{p} g(p) \ll \sum_{n<x/2} g(n) \sum_{\max((x/n)^{\frac{1}{2}},2) \le p < x/n} \frac{\gamma(p)\log p}{p} g(p)$$

とできる（外側の和の範囲も $n < x/2$ にまで狭めていることに注意）. すると, Lemma A.6.6 より

$$\sum_{n<x} g(n) \sum_{\substack{(x/n)^{\frac{1}{2}} \le p < x/n \\ (p,n)=1}} \frac{\gamma(p)\log p}{p} g(p) \ll \sum_{n<x/2} g(n) \sum_{\max((x/n)^{\frac{1}{2}},2) \le p < x/n} \frac{\gamma(p)}{p}$$

となるが,

$$n < x/2 \implies 2 \le \max((x/n)^{\frac{1}{2}}, 2) \le x/n$$

だから, さらに Lemma A.6.3 から

$$\begin{aligned}
&\sum_{n<x} g(n) \sum_{\substack{(x/n)^{\frac{1}{2}} \le p < x/n \\ (p,n)=1}} \frac{\gamma(p)\log p}{p} g(p) \\
&\le \sum_{n<x/2} g(n) \left(\kappa \log \frac{\log(x/n)}{\log\max((x/n)^{\frac{1}{2}}, 2)} + \frac{A_2}{\log\max((x/n)^{\frac{1}{2}}, 2)} \right) \qquad \text{(A.6.67)} \\
&\ll \sum_{n<x} g(n) = M(x).
\end{aligned}$$

以上の (A.6.66) と (A.6.67) を (A.6.63) に代入すれば

$$\widetilde{\Delta}(x) \ll LM(x)$$

を得る. あとはここに Lemma A.6.1 を用いて $M(x)$ を評価すれば (A.6.65) が得られる. □

A.6.5 漸近式の導出

Lemma A.6.10. 仮定 (Γ_1), (Γ_2) の下, ある定数 c_g が存在して, 実数 $x \ge 2$ に対して

$$M(x) = c_g (\log x)^{\kappa} + O(L(\log x)^{\kappa-1})$$

が成り立つ. ただしここで implicit constant は κ, A_1, A_2 のみに依存する.

Proof. まずは, Lemma A.6.9 の誤差評価 (A.6.55) により, 積分

$$c_g \coloneqq (\kappa+1) \int_2^{\infty} \Delta(u)(\log u)^{-(\kappa+2)} \frac{du}{u} \qquad \text{(A.6.68)}$$

が絶対収束することに注意する. 特に, $x \ge 2$ に対して

$$\int_x^{\infty} \Delta(u)(\log u)^{-(\kappa+2)} \frac{du}{u} \ll L \int_x^{\infty} (\log u)^{-2} \frac{du}{u} \ll L(\log x)^{-1} \qquad \text{(A.6.69)}$$

という tail estimate が成立する．そこで, Lemma A.6.9 で得た積分方程式 (A.6.54) の変数 x を t に置き換え, 両辺に $t^{-1}(\log t)^{-(\kappa+2)}$ をかけて $t \in [2, x]$ に渡って積分すれば

$$\begin{aligned}
&\int_2^x M(t)(\log t)^{-(\kappa+1)}\frac{dt}{t} \\
&= (\kappa+1)\int_2^x \left(\int_2^t \frac{M(u)}{u}du\right)(\log t)^{-(\kappa+2)}\frac{dt}{t} + \int_2^x \Delta(t)(\log t)^{-(\kappa+2)}\frac{dt}{t}
\end{aligned} \tag{A.6.70}$$

となる．この右辺第 1 項目の積分は順序を入れ替えれば

$$\begin{aligned}
&(\kappa+1)\int_2^x \left(\int_2^t \frac{M(u)}{u}du\right)(\log t)^{-(\kappa+2)}\frac{dt}{t} \\
&= (\kappa+1)\int_2^x \frac{M(u)}{u}\left(\int_u^x (\log t)^{-(\kappa+2)}\frac{dt}{t}\right)du \\
&= \int_2^x \frac{M(u)}{u}((\log u)^{-(\kappa+1)} - (\log x)^{-(\kappa+1)})du \\
&= \int_2^x M(t)(\log t)^{-(\kappa+1)}\frac{dt}{t} - (\log x)^{-(\kappa+1)}\int_2^x \frac{M(u)}{u}du
\end{aligned}$$

と計算できる．これを (A.6.70) に代入すると, ちょうど左辺が消えて

$$(\log x)^{-(\kappa+1)}\int_2^x \frac{M(u)}{u}du = \int_2^x \Delta(t)(\log t)^{-(\kappa+2)}\frac{dt}{t}$$

となる．この右辺に (A.6.68) と (A.6.69) を用いてから両辺に $(\log x)^{\kappa+1}$ をかければ

$$\int_2^x \frac{M(u)}{u}du = \frac{c_g}{\kappa+1}(\log x)^{\kappa+1} + O(L(\log x)^{\kappa})$$

を得る．あとは, この漸近式を Lemma A.6.9 の (A.6.54) の右辺に代入すれば主張を得る． □

A.6.6 主要項の係数の決定

Definition A.6.1 (Riemann zeta **関数**)**.** 実数 $s > 1$ に対して

$$\zeta(s) \coloneqq \sum_{n=1}^{\infty} \frac{1}{n^s}$$

と定める．この関数 ζ を Riemann zeta 関数と呼ぶ.

Lemma A.6.11. 実数 $s \in (1, 2]$ に対して

$$\zeta(s) = \frac{1}{s-1} + O(1)$$

が成立する．特に

$$\lim_{s \searrow 0}\bigl(s\zeta(s+1)\bigr) = 1$$

である．

Proof. 微積分学の基本定理から, $s>0$ に対して

$$\frac{1}{n^s}=s\int_n^\infty\frac{du}{u^{s+1}}$$

である．よって,

$$\begin{aligned}\zeta(s)=s\sum_{n=1}^\infty\int_n^\infty\frac{du}{u^{s+1}}=s\int_1^\infty\frac{[u]}{u^{s+1}}du=s\int_1^\infty\frac{du}{u^s}-s\int_1^\infty\frac{\{u\}}{u^{s+1}}du\\=\frac{1}{s-1}+1-s\int_1^\infty\frac{\{u\}}{u^s}du\end{aligned}$$

である．ここで $s\in(1,2]$ のとき

$$0\le s\int_1^\infty\frac{\{u\}}{u^{s+1}}du\le s\int_1^\infty\frac{du}{u^{s+1}}=1$$

であることを用いれば主張が得られる． □

Lemma A.6.12. 仮定 (Γ_1), (Γ_2) の下, Lemma A.6.10 で導入された定数 c_g に対して

$$c_g=\frac{1}{\Gamma(\kappa+1)}\prod_p\left(1-\frac{\gamma(p)}{p}\right)^{-1}\left(1-\frac{1}{p}\right)^\kappa$$

が成立する．特に $c_g>0$ であることが分かる．

Proof. まずは定数 c_g を決定するためのアイデアを述べる．Dirichlet 級数

$$Z_g(s)\coloneqq\sum_{n=1}^\infty\frac{g(n)}{n^s}=\prod_p\left(1+\frac{g(p)}{p^s}\right)\quad\text{for } s>0 \tag{A.6.71}$$

を考える．この Dirichlet 級数の収束性は後に Lemma A.6.10 を用いて確認する．この $Z_g(s)$ の $s\searrow 0$ の下での挙動は Lemma A.6.10 で得た漸近式を通して c_g を用いて書き下すことができる．一方で, $Z_g(s)$ を $\zeta(s+1)$ と比較しても $Z_g(s)$ の $s\searrow 0$ の下での挙動を書き下せる．実際に, $Z_g(s)$ を $\zeta(s+1)$ のべき乗で近似することを考えると, Lemma A.6.8 を Mertens の定理と比較すれば平均的には

$$g(p)\approx\frac{\kappa}{p}$$

であることが期待できる．すると, Euler 積の因子の「2 次以降」の項を無視すれば

$$\begin{aligned}Z_g(s)&=\prod_p\left(1+\frac{g(p)}{p^s}\right)\\&\approx\prod_p\left(1+\frac{\kappa}{p^{s+1}}\right)\approx\prod_p\left(1+\frac{1}{p^{s+1}}\right)^\kappa\approx\prod_p\left(1-\frac{1}{p^{s+1}}\right)^{-\kappa}=\zeta(s+1)^\kappa\end{aligned}$$

という近似が期待できる．最後の $\zeta(s+1)$ のべき乗は Lemma A.6.11 を使えば $s \searrow 0$ のときの挙動を調べることができる．これら 2 通りに得られた $Z_g(s)$ の $s \searrow 0$ の下での漸近展開を比較して c_g の表示を得たい．

この証明中の implicit constant はすべて g に依存して良いものとする．まずは, $s>0$ に対して, 微積分学の基本定理から

$$\frac{1}{n^s} = s\int_n^\infty \frac{du}{u^{s+1}}$$

である．よって,

$$Z_g(s) = s\sum_{n=1}^\infty g(n)\int_n^\infty \frac{du}{u^{s+1}} = s\int_1^\infty \left(\sum_{n\le u} g(n)\right)\frac{du}{u^{s+1}} = s\int_1^\infty M(u)\frac{du}{u^{s+1}} \tag{A.6.72}$$

を得る．Lemma A.6.10 を

$$M(u) = c_g(\log u)^\kappa + E(u) \quad \text{ただし} \quad E(u) \ll L(\log u)^{\kappa-1} \quad (u\ge 2) \tag{A.6.73}$$

と書けば,

$$1 < u \le 2 \implies M(u) = g(1) = 1$$

に気をつけて, (A.6.72) は

$$\begin{aligned} Z_g(s) &= s\int_2^\infty M(u)\frac{du}{u^{s+1}} + s\int_1^2 \frac{du}{u^{s+1}} \\ &= c_g s\int_2^\infty (\log u)^\kappa \frac{du}{u^{s+1}} + s\int_2^\infty E(u)\frac{du}{u^{s+1}} + O(1) \\ &= c_g s\int_1^\infty (\log u)^\kappa \frac{du}{u^{s+1}} + s\int_2^\infty E(u)\frac{du}{u^{s+1}} + O(1) \end{aligned} \tag{A.6.74}$$

となる．ここで (A.6.74) の右辺第 1 項目は $u = e^{\frac{x}{s}}$ と変数変換すれば

$$c_g s\int_1^\infty (\log u)^\kappa \frac{du}{u^{s+1}} = c_g s^{-\kappa}\int_0^\infty e^{-x}x^\kappa dx = c_g\Gamma(\kappa+1)s^{-\kappa} \tag{A.6.75}$$

とできる．同様に, (A.6.74) の右辺第 2 項目は (A.6.73) を用いることで

$$s\int_2^\infty E(u)\frac{du}{u^{s+1}} \ll Ls\int_1^\infty (\log u)^{\kappa-1}\frac{du}{u^{s+1}} = Ls^{-(\kappa-1)}\Gamma(\kappa) \tag{A.6.76}$$

とできる．以上の (A.6.75) と (A.6.76) より, (A.6.71) が $s>0$ のとき収束していることがわかる．また, これら (A.6.75) と (A.6.76) を (A.6.74) に代入すれば, $s\in(0,1]$ で

$$Z_g(s) = c_g\Gamma(\kappa+1)s^{-\kappa} + O(Ls^{-(\kappa-1)}+1)$$

を得るので,

$$\lim_{s\searrow 0}\bigl(s^\kappa Z_g(s)\bigr) = c_g\Gamma(\kappa+1) \tag{A.6.77}$$

である．

一方, $s>0$ に対して, Riemann zeta 関数の Euler 積表示

$$\zeta(s+1)=\prod_p\left(1-\frac{1}{p^{s+1}}\right)^{-1}$$

を用いれば

$$Z_g(s)=\Pi(s)\zeta(s+1)^\kappa \quad ただし \quad \Pi(s):=\prod_p\left(1+\frac{g(p)}{p^s}\right)\left(1-\frac{1}{p^{s+1}}\right)^\kappa \tag{A.6.78}$$

である．ここで無限積 $\Pi(s)$ に注目する．Lemma A.6.8 を Mertens の定理と組み合わせれば

$$\sum_{w\le p<z}\left(g(p)-\frac{\kappa}{p}\right)\ll\frac{L}{\log w}\quad(2\le w\le z)$$

を得る．ここに, $s\in[0,1]$ に対して

$$\frac{1}{p^s}=s\int_p^z\frac{du}{u^{s+1}}+\frac{1}{z^s}$$

を用いれば

$$\begin{aligned}\sum_{w\le p<z}\left(\frac{g(p)}{p^s}-\frac{\kappa}{p^{s+1}}\right)&=\sum_{w\le p<z}\left(g(p)-\frac{\kappa}{p}\right)\frac{1}{p^s}\\&=s\sum_{w\le p<z}\left(g(p)-\frac{\kappa}{p}\right)\int_p^z\frac{du}{u^{s+1}}+\frac{1}{z^s}\sum_{w\le p<z}\left(g(p)-\frac{\kappa}{p}\right)\\&=s\int_w^z\left(\sum_{w\le p<u}\left(g(p)-\frac{\kappa}{p}\right)\right)\frac{du}{u^{s+1}}+\frac{1}{z^s}\sum_{w\le p<z}\left(g(p)-\frac{\kappa}{p}\right)\\&\ll\frac{L}{\log w}\int_w^z\frac{du}{u^{s+1}}+\frac{L}{\log w}\frac{1}{z^s}=\frac{L}{\log w}\frac{1}{w^s}\end{aligned}$$

したがって

$$\sum_{w\le p<z}\left(\frac{g(p)}{p^s}-\frac{\kappa}{p^{s+1}}\right)\ll\frac{L}{\log w} \tag{A.6.79}$$

を得る．さらに Lemma A.6.6 から

$$\begin{aligned}\log\left(1+\frac{g(p)}{p^s}\right)&=\frac{g(p)}{p^s}+O\left(\frac{g(p)^2}{p^{2s}}\right)=\frac{g(p)}{p^s}+O(g(p)^2),\\ \log\left(1-\frac{1}{p^{s+1}}\right)&=-\frac{1}{p^{s+1}}+O\left(\frac{1}{p^{2(s+1)}}\right)=-\frac{1}{p^{s+1}}+O\left(\frac{1}{p^2}\right)\end{aligned}$$

を得る．これらと (A.6.79), Lemma A.6.7 を組み合わせれば, $s\in[0,1]$ と $2\le w\le z$ に対して,

$$\log\prod_{w\le p<z}\left(1+\frac{g(p)}{p^s}\right)\left(1-\frac{1}{p^{s+1}}\right)^\kappa=\sum_{w\le p<z}\left(\log\left(1+\frac{g(p)}{p^s}\right)+\kappa\log\left(1-\frac{1}{p^{s+1}}\right)\right)$$

$$
\begin{aligned}
&= \sum_{w \le p < z} \left(\frac{g(p)}{p^s} - \frac{\kappa}{p^{s+1}} \right) + O\biggl(\sum_{w \le p < z} g(p)^2 + \sum_{w \le p < z} \frac{1}{p^2} \biggr) \\
&\ll \frac{L}{\log w} + \frac{1}{w} \ll \frac{L}{\log w}
\end{aligned}
$$

を得る．この評価は $w \to \infty$ のとき $s \in [0,1]$ に関して一様に 0 に収束する．つまり, (A.6.78) で与えられた無限積 $\Pi(s)$ は $s \in [0,1]$ に関して一様に収束している．無限積 $\Pi(s)$ の各因子はもちろん $s \in [0,1]$ に関して連続関数なので, それら連続な因子の一様収束する無限積である $\Pi(s)$ 自体も $s \in [0,1]$ に関する連続関数である．よって,

$$
\begin{aligned}
\lim_{s \searrow 0} \Pi(s) = \Pi(0) &= \prod_p (1 + g(p)) \left(1 - \frac{1}{p} \right)^{\kappa} \\
&= \prod_p \left(\frac{p}{p - \gamma(p)} \right) \left(1 - \frac{1}{p} \right)^{\kappa} = \prod_p \left(1 - \frac{\gamma(p)}{p} \right)^{-1} \left(1 - \frac{1}{p} \right)^{\kappa}
\end{aligned}
$$

である．これを (A.6.78), Lemma A.6.11 と組み合わせれば

$$
\lim_{s \searrow 0} \bigl(s^{\kappa} Z_g(s) \bigr) = \lim_{s \searrow 0} \bigl(\Pi(s) (s \zeta(s+1))^{\kappa} \bigr) = \prod_p \left(1 - \frac{\gamma(p)}{p} \right)^{-1} \left(1 - \frac{1}{p} \right)^{\kappa} \tag{A.6.80}
$$

を得る．

あとは (A.6.77) と (A.6.80) を合わせて

$$
c_g \Gamma(\kappa + 1) = \prod_p \left(1 - \frac{\gamma(p)}{p} \right)^{-1} \left(1 - \frac{1}{p} \right)^{\kappa}
$$

を得るので, 主張を得る． □

A.6.7 結果のまとめ

以上の Lemma A.6.10 と Lemma A.6.12 と組み合わせれば, 次を得る：

Theorem A.6.1. 仮定 (Γ_1), (Γ_2) の下, 実数 $x \ge 2$ に対して

$$
M(x) = c_g (\log x)^{\kappa} + O(L (\log x)^{\kappa - 1})
$$

が成り立つ．ただしここで,

$$
c_g \coloneqq \frac{1}{\Gamma(\kappa + 1)} \prod_p \left(1 - \frac{\gamma(p)}{p} \right)^{-1} \left(1 - \frac{1}{p} \right)^{\kappa}
$$

であり, implicit constant は κ, A_1, A_2 のみに依存する．

Proof. Lemma A.6.10 と Lemma A.6.12 から直ちに従う． □

さらに部分総和法を用いれば Maynard の論文 [5] の p. 400 にある Lemma 6.1 が得られる（多少 Maynard の論文 [5] と記法が異なるが, 対応は Remark A.6.1 を参照のこと）. まず, 係数 c_g の評価を準備しておく：

Proposition A.6.1. 仮定 (Γ_1), (Γ_2) の下, Lemma A.6.10 で導入された定数 c_g に対して

$$c_g \ll 1$$

が成立する. ただしここで implicit constant は κ, A_1, A_2 のみに依存し, L には依存しない.

Proof. Lemma A.6.10 と Lemma A.6.8 の (A.6.52) から, $x \geq 2$ に対して,

$$M(x) \ll (\log x)^\kappa \quad \text{および} \quad M(x) = c_g(\log x)^\kappa + O(L(\log x)^{\kappa-1}),$$

を得る. よって, κ, A_1, A_2 のみに依存する定数 $C_1, C_2 \geq 0$ が存在して, $x \geq 2$ に対して,

$$|M(x)| \leq C_1(\log x)^\kappa \quad \text{および} \quad |M(x) - c_g(\log x)^\kappa| \leq C_2 L(\log x)^{\kappa-1}$$

が得られる. したがって,

$$\begin{aligned} |c_g|(\log x)^\kappa &= |M(x) - (M(x) - c_g(\log x)^\kappa)| \\ &\leq |M(x)| + |M(x) - c_g(\log x)^\kappa| \leq C_1(\log x)^\kappa + C_2 L(\log x)^{\kappa-1} \end{aligned}$$

を得る. 全体を $(\log x)^\kappa$ で割ると

$$|c_g| \leq C_1 + C_2 L(\log x)^{-1}$$

となるが, $x \to \infty$ の極限を取ることで L を含む項は消えてしまい,

$$|c_g| \leq C_1$$

が分かり, 主張を得る. □

すると, Maynard の論文 [5] の Lemma 6.1 は次の形で示せる：

Theorem A.6.2. 仮定 (Γ_1), (Γ_2) の下, 実数 $z \geq 2$ と C^1 級関数 $G\colon [0,1] \to \mathbb{R}$ に対して

$$\sum_{d<z} g(d) G\left(\frac{\log d}{\log z}\right) = \kappa c_g (\log z)^\kappa \int_0^1 G(x) x^{\kappa-1} dx + O(G_{\max} L(\log z)^{\kappa-1})$$

が成り立つ. ただしここで,

$$c_g \coloneqq \frac{1}{\Gamma(\kappa+1)} \prod_p \left(1 - \frac{\gamma(p)}{p}\right)^{-1} \left(1 - \frac{1}{p}\right)^\kappa \quad \text{および} \quad G_{\max} \coloneqq \max_{t\in[0,1]} (|G(t)| + |G'(t)|)$$

であり, implicit constant は κ, A_1, A_2 のみに依存する.

Proof. 微積分学の基本定理から

$$G\left(\frac{\log d}{\log z}\right) = G(1) - \int_{\frac{\log d}{\log z}}^{1} G'(x)dx$$

だから, これを主張の左辺に代入して

$$\sum_{d<z} g(d)G\left(\frac{\log d}{\log z}\right) = G(1)M(z) - \sum_{d<z} g(d) \int_{\frac{\log d}{\log z}}^{1} G'(x)dx$$

を得る．ここで

$$\frac{\log d}{\log z} < x \iff d < z^x$$

に気をつけて和と積分を交換すれば

$$\begin{aligned}\sum_{d<z} g(d)G\left(\frac{\log d}{\log z}\right) &= G(1)\sum_{d<z} g(d) - \int_0^1 \left(\sum_{d<z^x} g(d)\right)G'(x)dx \\ &= G(1)M(z) - \int_0^1 M(z^x)G'(x)dx\end{aligned}$$

を得る．ここで

$$0 < x \leq \frac{\log 2}{\log z} \implies 1 < z^x \leq 2 \implies M(z^x) = g(1) = 1$$

だから, $z \geq 2$ より積分の $x = 0$ 周りの部分を分けて

$$\begin{aligned}\sum_{d<z} g(d)G\left(\frac{\log d}{\log z}\right) &= G(1)M(z) - \int_{\frac{\log 2}{\log z}}^{1} M(z^x)G'(x)dx - \int_0^{\frac{\log 2}{\log z}} G'(x)dx \\ &= G(1)M(z) - \int_{\frac{\log 2}{\log z}}^{1} M(z^x)G'(x)dx + O(G_{\max}(\log z)^{-1})\end{aligned} \tag{A.6.81}$$

とできる．右辺の残りの部分には Proposition A.6.1 と Theorem A.6.1 が適用でき, $\kappa > 0$ だから

$$\begin{aligned}&G(1)M(z) - \int_{\frac{\log 2}{\log z}}^{1} M(z^x)G'(x)dx \\ &= c_g(\log z)^\kappa\left(G(1) - \int_{\frac{\log 2}{\log z}}^{1} G'(x)x^\kappa dx\right) + O\left(G_{\max}L(\log z)^{\kappa-1}\left(1 + \int_0^1 x^{\kappa-1}dx\right)\right) \\ &= c_g(\log z)^\kappa\left(G(1) - \int_{\frac{\log 2}{\log z}}^{1} G'(x)x^\kappa dx\right) + O(G_{\max}L(\log z)^{\kappa-1})\end{aligned}$$

となる．さらに残った積分を $[0,1]$ にまで広げた後に部分積分すれば

$$\begin{aligned}&G(1)M(z) - \int_{\frac{\log 2}{\log z}}^{1} M(z^x)G'(x)dx \\ &= c_g(\log z)^\kappa\left(G(1) - \int_0^1 G'(x)x^\kappa dx + O\left(\int_0^{\frac{\log 2}{\log z}} |G'(x)|x^\kappa dx\right)\right) + O(G_{\max}L(\log z)^{\kappa-1})\end{aligned}$$

$$= \kappa c_g (\log z)^\kappa \int_0^1 G(x) x^{\kappa-1} dx + O(G_{\max} L (\log z)^{\kappa-1})$$

となる．これを (A.6.81) に用いて主張を得る． □

Remark A.6.1. Theorem A.6.2 と Maynard の論文 [5] の Lemma 6.1 では, 以下の点が異なる：

- Maynard の論文 [5] の Lemma 6.1 では g を完全乗法的関数として定義して, 和に $\mu(d)^2$ という係数をつけている．しかし, これは g を平方無縁数に台を持つ乗法的関数として定義して和に $\mu(d)^2$ という係数をつけないことと同じである．
- Maynard の論文 [5] は Theorem A.6.2 の $\kappa = 1$ の場合である．

A.7 基本的な Selberg の篩の応用 II — 双子素数の個数評価

Maynard の論文に移る前の最後の話題として, Selberg の篩を用いて, x 以下の双子素数の個数 $\pi_2(x)$ の評価を行ってみよう．次の結果は, 定数倍を除き, Hardy–Littlewood の漸近公式

$$\pi_2(x) \sim 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \frac{x}{(\log x)^2} \quad (x \to \infty)$$

と同等の評価を上からだけではあるが, 示すことに成功している：

Theorem A.7.1 (Brun)**.** 実数 $x \geq 2$ に対して,

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

が成立する．

Proof. Theorem A.4.1 のときと同様に, 十分大の x について示せば十分である．Proposition A.1.4 の篩データ $(\mathscr{A}, \mathscr{P}, \omega, X)$ を用いる．すると, Proposition A.1.4 の (iii) より

$$\pi_2(x) \leq S(\mathscr{A}, \mathscr{P}, z) + z \tag{A.7.82}$$

である．よって, 篩関数 $S(\mathscr{A}, \mathscr{P}, z)$ を上から評価したい．

ここで, Selberg の篩（Theorem A.3.1）を用いる．パラメター $R \geq 2$ を取れば, Theorem A.3.1 より

$$S(\mathscr{A}, \mathscr{P}, z) \leq \frac{X}{G} + E = \frac{x}{G} + E \tag{A.7.83}$$

が成立する．ただしここで, 和 G は

$$G \coloneqq \sum_{\substack{r \mid P^*(z) \\ r < R}} g(r) \quad ただし \quad g(p) \coloneqq \frac{\omega(p)}{p - \omega(p)} \tag{A.7.84}$$

と定義され, 残余項 E は

$$E := \sum_{\substack{d_1,d_2|P(z)\\ d_1,d_2<R}} \lambda_{d_1}\lambda_{d_2}E([d_1,d_2]) \quad \text{ただし} \quad |\lambda_d| \leq 1 \tag{A.7.85}$$

で定義される. 次に, (A.7.83) の右辺を評価すべく, G と E の評価を行う.

まず, 和 G について考える. 和 (A.7.84) の条件 $r \mid P^*(z)$ は取り扱いづらいので

$$R := z \tag{A.7.86}$$

ととり, $g(p) = 0 \iff \omega(p) = 0$ に注意して,

$$G = \sum_{\substack{r|P^*(z)\\ r<z}} g(r) = \sum_{r<z} g(r) \tag{A.7.87}$$

と単純化しておく. ここで相対密度 g は Section A.6 と同じように

$$g(p) = \frac{\gamma(p)}{p-\gamma(p)} \quad \text{ただし} \quad \gamma(p) := \omega(p)$$

で与えられているので, Theorem A.6.1 を使えば, (A.7.87) の漸近式が得られそうである. そこで, 今考えている局所密度 $\gamma = \omega$ に対して, 条件 (Γ_1), (Γ_2) を確かめたい. 今, 局所密度は Proposition A.1.4 の (i) のように

$$\omega(p) = \begin{cases} 1 & (p = 2 \text{ のとき}), \\ 2 & (p > 2 \text{ のとき}) \end{cases} \tag{A.7.88}$$

を満たす. よって, $p = 2$ であれば

$$0 \leq \frac{\omega(2)}{2} = \frac{1}{2} \leq 1 - \frac{1}{3}$$

であり, $p > 2$ であれば

$$0 \leq \frac{\omega(p)}{p} = \frac{2}{p} \leq \frac{2}{3} = 1 - \frac{1}{3}$$

だから, 条件 (Γ_1) が $A_1 = 3$ とともに成立している. また, (A.7.88) と Theorem A.5.1 より

$$\sum_{n<x} \frac{\omega(p)\log p}{p} = 2\sum_{n<x} \frac{\log p}{p} + O(1) = 2\log x + O(1)$$

が成り立つ. この漸近公式の差を取れば, $2 \leq w \leq z$ に対して

$$\sum_{w\leq n<z} \frac{\omega(p)\log p}{p} = 2\log\frac{z}{w} + O(1)$$

を得るので, 条件 (Γ_2) が $\kappa = 2,\ A_2, L = O(1)$ とともに成立している. よって, Theorem A.6.1 より

$$G \gg (\log z)^2 \tag{A.7.89}$$

という下からの評価を得る．

次に, 誤差項 E であるが, Proposition A.1.4 の (ii) と $|\lambda_d| \le 1$ を (A.7.85) に用いれば, Definition A.1.9 で定義したように n の重複度を除いた素因数の個数を $\nu(n)$ と書くことを思い出すと

$$|E| \le \sum_{\substack{d_1,d_2|P(z)\\ d_1,d_2<R}} \omega([d_1,d_2]) \le \sum_{d_1,d_2<R} 2^{\nu([d_1,d_2])} \le \sum_{d_1,d_2<R} 2^{\nu(d_1)+\nu(d_2)} = \left(\sum_{d<R} 2^{\nu(d)}\right)^2$$

とできる．ここで $d<R$ であれば $R/d>1$ であることを用いると（Rankin's trick と呼ぶ）

$$\sum_{d<R} 2^{\nu(d)} \le R \sum_{d<R} \frac{2^{\nu(d)}}{d}$$

とできるので, Lemma A.6.1 と Mertens の定理（Lemma A.6.4）を用いれば

$$\sum_{d<R} 2^{\nu(d)} \ll R(\log R)^2$$

を得る．よって, 今 (A.7.86) で決めたように $R \coloneqq z$ と選んでいるから

$$|E| \ll z^2(\log z)^4 \tag{A.7.90}$$

を得る．

以上の (A.7.89) と (A.7.90) を (A.7.83) に用いれば

$$S(\mathscr{A},\mathscr{P},z) \ll \frac{x}{(\log z)^2} + z^2(\log z)^4$$

を得る．これをさらに (A.7.82) に用いれば

$$\pi_2(x) \le \frac{x}{(\log z)^2} + z^2(\log z)^4$$

を得る．あとは x を十分大とし, $z \coloneqq x^{\frac{1}{4}} \ge 2$ とでも取ってみれば, 主張を得る． □

Theorem A.7.1 を用いれば, 双子素数の逆数和の収束性がわかる．

Theorem A.7.2 (Brun)**.** 級数

$$\sum_{p,p+2:\ \text{素数}} \frac{1}{p}$$

は収束する．

Proof. 双子素数が有限個しかなかった場合は考えている級数は有限和なので証明すべきことはない．よって, 双子素数が無限個存在した場合を考えれば良い．微積分学の基本定理より

$$\frac{1}{p} = \int_p^\infty \frac{du}{u^2}$$

だから

$$\sum_{p,p+2:\ \text{素数}} \frac{1}{p} = \sum_{p,p+2:\ \text{素数}} \int_p^\infty \frac{du}{u^2} = \int_2^\infty \Bigg(\sum_{\substack{p \le u \\ p,p+2:\ \text{素数}}} 1 \Bigg) \frac{du}{u^2} = \int_2^\infty \frac{\pi_2(u)}{u^2} du$$

と書き直せる．ここで, Theorem A.7.1 を用いれば

$$\sum_{p,p+2:\ \text{素数}} \frac{1}{p} \ll \int_2^\infty \frac{1}{u(\log u)^2} du < +\infty$$

が分かる． □

A.8 Maynard の論文での数論的関数の評価についての補足

Maynard の論文 [5] では数カ所数論的関数の評価が説明なしに行われている部分がある．この節ではこれら評価を systematic に行う方法について取り扱う．

例えば, Maynard の論文 [5] の (5.3) 式で代わりに使える評価

$$\sum_{d<R} \mu(d)^2 \tau_k(d) \ll R(\log R)^k \tag{A.8.91}$$

は $d < R$ のとき $R/d > 1$ なので, R/d を無理やりかけると（Rankin's trick と呼ぶ）

$$\sum_{d<R} \mu(d)^2 \tau_k(d) \le R \sum_{d<R} \frac{\mu(d)^2 \tau_k(d)}{d} \tag{A.8.92}$$

となる．ここで, Lemma A.6.4 より, 範囲 $2 \le w \le z$ で

$$\sum_{w \le p < z} \frac{\mu(p)^2 \tau_k(p)}{p} = k \sum_{w \le p < z} \frac{1}{p} = k \log \frac{\log z}{\log w} + O\bigg(\frac{k}{\log w}\bigg)$$

であるから, Lemma A.6.1 の条件 (A.6.45) は $\kappa = k$, $A = O(k)$ で成立する．よって, (A.8.92) と Lemma A.6.1 より (A.8.91) を得る．本当は, (A.8.91) の右辺の log べきは $(\log R)^{k-1}$ にまで改善できる．この $\log R$ 一個分の損失は Rankin's trick の使用によって生じてしまっている．この Rankin's trick の弱点の象徴的な例は, x 以下の自然数の個数を数えるときにわざわざ Rankin's trick を用いた

$$x \asymp \sum_{n<x} 1 \le x \sum_{n<x} \frac{1}{n} \asymp x \log x$$

であろう．一方, Maynard の論文 [5] の (5.9) 式のように Rankin's trick を使う必要のない場合は最良の log の指数が得られることが多い．

実は上に述べた Rankin's trick の弱点は補うことができる．これには, 次に紹介する Lemma A.8.1 のように, Lemma A.6.9 で用いたのと同じトリックを用いると良い：

Lemma A.8.1. 平方無縁数に台を持つ非負値の乗法的関数 f を考える．また, 数論的関数 g を

$$g(n) \coloneqq \frac{f(n)}{n}$$

で定める．さらに次の 2 条件を仮定する：

(1) Lemma A.6.1 の (A.6.45) が成り立つ．つまり, 実数 $\kappa > 0$ と $A \geq 1$ に対して

$$\sum_{w \leq p < z} g(p) \leq \kappa \log \frac{\log z}{\log w} + \frac{A}{\log w} \quad (2 \leq \forall w \leq \forall z)$$

が成立する．（応用時は Lemma A.6.4 を参照のこと.）

(2) ある実数 $C \geq 0$ が存在して, 実数 $x \geq 1$ に対して

$$\sum_{p<x} f(p) \log p \leq Cx$$

が成立する．

すると, $x \geq 2$ に対して

$$\sum_{n<x} g(n) \ll (\log x)^{\kappa}, \quad \sum_{n<x} f(n) \ll x(\log x)^{\kappa-1}, \quad \sum_{n \geq x} \frac{f(n)}{n^2} \ll x^{-1}(\log x)^{\kappa-1}$$

が成立する．ただしここで implicit constant は κ, A, C のみに依存する．

Proof. 最初の $g(n)$ の和の評価は Lemma A.6.1 そのものなので, 残りの 2 つの評価を証明する．

平方無縁数に対して,

$$\log n = \sum_{p|n} \log p = \sum_{mp=n} \log p$$

が成り立つという素因数分解の帰結を用いたい．そのため, $f(n)$ の和の代わりに

$$\sum_{n<x} f(n) \log n$$

を考える．すると,

$$\sum_{n<x} f(n) \log n = \sum_{n<x} f(n) \sum_{mp=n} \log p = \sum_{mp<x} f(mp) \log p = \sum_{np<x} f(np) \log p$$

を得る．f は平方無縁数に台を持つ乗法的関数なので, $(n,p) > 1$ ならば $f(np) = 0$ であり

$$\sum_{n<x} f(n) \log n = \sum_{\substack{np<x \\ (n,p)=1}} f(np) \log p = \sum_{n<x} f(n) \sum_{\substack{p<x/n \\ (p,n)=1}} f(p) \log p$$

を得る．ここで, f は非負値だから $(p,n) = 1$ という条件を外して

$$\sum_{n<x} f(n) \log n \leq \sum_{n<x} f(n) \sum_{p<x/n} f(p) \log p$$

とできる．ここで (2) を用いれば

$$\sum_{n<x} f(n)\log n \le Cx\sum_{n<x}\frac{f(n)}{n} = Cx\sum_{n<x} g(n) \tag{A.8.93}$$

を得る．一方で, 実数 x に対して $\log x \le x$ だから f が非負値であることより

$$\sum_{n<x} f(n)\log\frac{x}{n} \le x\sum_{n<x}\frac{f(n)}{n} = x\sum_{n<x} g(n) \tag{A.8.94}$$

も分かる．よって, (A.8.93) と (A.8.94) を足して $\log x$ で割れば

$$\sum_{n<x} f(n) = \frac{1}{\log x}\sum_{n<x} f(n)\log x = \frac{1}{\log x}\left(\sum_{n<x} f(n)\log n + \sum_{n<x} f(n)\log\frac{x}{n}\right) \ll \frac{x}{\log x}\sum_{n<x} g(n)$$

を得る．あとは g の和に Lemma A.6.1 を適用すれば, 評価

$$\sum_{n<x} f(n) \ll x(\log x)^{\kappa-1} \tag{A.8.95}$$

を得る．

最後の和については,

$$\frac{1}{n^2} = 2\int_n^\infty \frac{du}{u^3}$$

を用いると, f が非負値であることを思い出し

$$\sum_{n\ge x}\frac{f(n)}{n^2} = 2\sum_{n\ge x} f(n)\int_n^\infty\frac{du}{u^3} = 2\int_x^\infty\left(\sum_{x\le n<u} f(n)\right)\frac{du}{u^3} \le 2\int_x^\infty\left(\sum_{n<u} f(n)\right)\frac{du}{u^3}$$

とできる．ここに上で示した (A.8.95) を用いれば

$$\sum_{n\ge x}\frac{f(n)}{n^2} \ll \int_x^\infty \frac{(\log u)^{\kappa-1}}{u^2}du$$

を得る．十分大の実数 x_0 に対して, $x^{-\frac{1}{2}}(\log x)^{\kappa-1}$ は $[x_0,\infty)$ 上で単調減少するから,

$$\sum_{n\ge x}\frac{f(n)}{n^2} \ll x^{-\frac{1}{2}}(\log x)^{\kappa-1}\int_x^\infty\frac{du}{u^{\frac{3}{2}}} \ll x^{-1}(\log x)^{\kappa-1}$$

となり, 最後の和の評価も得られる． □

Remark A.8.1. 実際にはもう少し議論を挟めば, Lemma A.6.1 と Lemma A.8.1 での「平方無縁数に台を持つ」という条件は取り除くことができる．ここでは Maynard の論文 [5] を読むのに十分な範囲で証明を簡単にするためこの条件を課した．

Corollary A.8.1. 平方無縁数に台を持つ非負値の乗法的関数 f を考える. また, 数論的関数 g を

$$g(n) \coloneqq \frac{f(n)}{n}$$

で定める. さらに, 数論的関数 f が実数 $\kappa > 0$ と $A \geq 1$ に対して,

$$f(p) \leq \kappa + \frac{A}{p} \tag{A.8.96}$$

を満たしたとする. すると, $x \geq 2$ に対して

$$\sum_{n<x} g(n) \ll (\log x)^{\kappa}, \quad \sum_{n<x} f(n) \ll x(\log x)^{\kappa-1}, \quad \sum_{n \geq x} \frac{f(n)}{n^2} \ll x^{-1}(\log x)^{\kappa-1}$$

が成立する. ただしここで implicit constant は κ, A のみに依存する.

Proof. Lemma A.8.1 の条件 (1) と (2) を確かめれば良い.

まず, 条件 (1) を確認する. 範囲 $2 \leq w \leq z$ で (A.8.96) より

$$\sum_{w \leq p < z} g(p) = \sum_{w \leq p < z} f(p) \leq \kappa \sum_{w \leq p < z} \frac{1}{p} + A \sum_{w \leq p < z} \frac{1}{p^2} = \kappa \sum_{w \leq p < z} \frac{1}{p} + O\left(\frac{1}{w}\right)$$

とできる. さらに Lemma A.6.4 を用いれば

$$\sum_{w \leq p < z} g(p) \leq \kappa \log \frac{\log z}{\log w} + O\left(\frac{1}{\log w}\right)$$

となる. よって, 条件 (1) が満たされることが分かった.

次に, 条件 (2) を確かめる. (A.8.96) から

$$f(p) \ll 1$$

が分かるので, $x \geq 1$ に対して, Theorem A.4.1 を用いれば

$$\sum_{p<x} f(p) \log p \ll \sum_{p<x} \log p \ll \pi(x) \log x \ll x$$

となり, 条件 (2) も満たされることが分かった.

以上より, Lemma A.8.1 が適用でき, 主張が得られる. $\square$

Example A.8.1. Maynard の論文 [5] の (5.25) で使われている評価

$$\sum_{\substack{s > D_0 \\ (s,W)=1}} \frac{\mu(s)^2}{g(s)^2} \ll \frac{1}{D_0}$$

を示してみよう. (和の中では条件 $(s, W) = 1$ がおそらく implicit に仮定されています (そうじゃないと偶数の s で項が無限大になる). これは, 式 (5.22) で $\lambda_{d_1,\ldots,d_k}$ の台の条件 $(d, W) = 1$

から $s_{i,j}$ たちに $(s_{i,j}, W) = 1$ という制約を課しても和が変わらないことによります.）ただしここで $D_0 \geq 3$, $W = \prod_{p<D_0} p$ であり, 完全乗法的関数 g は

$$g(p) = p - 2$$

で定義される.（Corollary A.8.1 の g とは意味が異なる.）平方無縁数に台を持つ数論的関数 f を

$$f(p) \coloneqq \begin{cases} \left(\dfrac{p}{p-2}\right)^2 & (p > D_0 \text{ のとき}), \\ 0 & p \leq D_0 \end{cases} \tag{A.8.97}$$

で定めると

$$\sum_{\substack{s>D_0 \\ (s,W)=1}} \frac{\mu(s)^2}{g(s)^2} = \sum_{s>D_0} \frac{f(n)}{n^2}$$

である. ここで $p > D_0$ のときは $p \geq 3$ なので, f の定義 (A.8.97) から

$$f(p) = \left(\frac{p}{p-2}\right)^2 = \left(1 + \frac{2}{p-2}\right)^2 \leq \left(1 + \frac{6}{p}\right)^2 = 1 + \frac{12}{p} + \frac{36}{p^2} \leq 1 + \frac{24}{p}$$

を得る. 一方, $p \leq D_0$ のときは, f の定義 (A.8.97) から自明に

$$f(p) = 0 \leq 1 + \frac{24}{p}$$

である. よって, Corollary A.8.1 の条件 (A.8.96) が $\kappa = 1$, $A = 24$ とともに成立しているので, Corollary A.8.1 の一番最後の評価から

$$\sum_{\substack{s>D_0 \\ (s,W)=1}} \frac{\mu(s)^2}{g(s)^2} = \sum_{s>D_0} \frac{f(n)}{n^2} \ll \frac{1}{D_0}$$

を得る.

参考文献

[1] J. B. Friedlander and H. Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications, vol. 57, American Mathematical Society, 2010.

[2] D. Goldston, J. Pintz, and C. Y. Yıldırım, *Primes in tuples I*, Ann. of Math. **170** (2009), 819–862.

[3] ———, *Primes in tuples II*, Acta Math. **204** (2010), 1–47.

[4] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, 1974.

[5] J. Maynard, *Small gaps between primes*, Ann. of Math. **181** (2015), 383–413.

[6] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, Math. Ann. **143** (1961), 75–102.