MEMOS ON: CHAPTER 12. WOOLEY'S UPPER BOUND FOR $G(k)$ (AND LEMMA 5.3, LEMMA 5.4)

鈴木雄太

2019 年度八王子数論セミナー "Waring 問題" 冬の部でテキスト [2] の詳細を与えたノートです. セミナーに参加していただいた方々から誤植や改善のコメントをいただいていますので, 時間ができ次第修正・追記していく予定です. なにか不明な点等ありましたら鈴木雄太（suzuyu1729 [at] gmail.com）までご連絡ください.

12.1 Smooth numbers（セミナーでは証明は後回し）

Note 1 (p. 175)**.** 微分差分方程式

$$u\rho'(u) = -\rho(u-1) \quad (u > 1) \tag{1}$$

の初期値（議論を簡易化するために $u = 0$ の場合を含めています）

$$\rho(u) = 1 \quad (0 \leq u \leq 1) \tag{2}$$

を持つ解 $\rho\colon [0,\infty) \to \mathbb{R}$ であって $[0,\infty)$ 上連続かつ $(1,\infty)$ 上可微分であるもの（Dickman 関数と呼ばれる）の存在と一意性については, 最初の $u \in (1,2]$ あたりの部分が不安になりますが, これはもちろん次々と積分をすることで得られます：

微分差分方程式 (1) の初期値 (2) を持つ連続な解 $\rho\colon [0,n] \to \mathbb{R}$ （ただし $u = n$ における (1) の左辺は片側微分で解釈する）の存在と一意性を自然数 n に関する帰納法で示せば十分です.

まず, $n = 1$ のときは方程式 (1) の成立範囲外なので初期値条件 (2) を ρ の定義だと思えば存在性が従い, 一意性は同じく初期値条件より明らかです.

次に $N \geq 1$ とし, 解 $\rho\colon [0,N] \to \mathbb{R}$ の存在と一意性を仮定して解 $\rho\colon [0,N+1] \to \mathbb{R}$ の存在と一意性を示します. 一意性を示すために解 $\rho\colon [0,N+1] \to \mathbb{R}$ を任意に取り, この解はある特定の形で与えられなければいけないことを示します. 帰納法の仮定より $u \in [0,N]$ の範囲内では ρ はすでに一意的に定まることを見ているので $u \in (N,N+1]$ の範囲で考えれば十分です. すると, $u \in (N,N+1]$ のとき, $u > 1$ なので方程式 (1) より

$$\rho'(u) = -\frac{\rho(u-1)}{u} \tag{3}$$

とならなければいけません. ここで $u \in (N,N+1]$ のとき $u-1 \in (N-1,N] \subset [0,N]$ だから解 ρ の連続性の条件より (3) の右辺は $u \in (N,N+1]$ で連続なので微積分学

Date: March 16, 2020.

の基本定理より任意の $u, w \in (N, N+1]$ に対して

$$\rho(u) - \rho(w) = \int_w^u \rho'(v)dv = -\int_w^u \rho(v-1)\frac{dv}{v} = -\int_{w-1}^{u-1} \rho(v)\frac{dv}{v+1}$$

が成立します. ここで $w \to N$ の極限を取ることで

$$\rho(u) = \rho(N) - \int_{N-1}^{u-1} \rho(v)\frac{dv}{v+1} \tag{4}$$

を得ます. この右辺にはすでに帰納法の仮定により一意性が保証されている $\rho(u)$ の $u \in [N-1, N]$ での値しか出てこないので ρ は $u \in (N, N+1]$ の範囲でも一意的に与えられなければなりません. また解の存在性についても (4) によって $u \in (N, N+1]$ の範囲に延長された解を考えれば十分です. 実際, (4) の被積分関数の連続性（したがって有界）より ρ は $[N, N+1]$ においても連続であり, また $u \in (N, N+1]$ のとき (4) より (3) が導かれ (1) が成立します. 最後に $u = N$ における右側微分ですが, これは $\frac{\rho(v)}{v+1}$ の連続性により明らかに

$$\lim_{u \to N+0} \frac{\rho(u) - \rho(N)}{u - N} = -\lim_{u \to N+0} \frac{1}{u-N} \int_{N-1}^{u-1} \rho(v)\frac{dv}{v+1} = -\frac{\rho(N-1)}{N}$$

となり再び (3) を満たすので (1) が成立しています. 以上より Dickman 関数 $\rho(u)$ の存在と一意性が示されました.

Note 2 (Lemma 12.1-(ii))**.** 主張の右辺の $(\log 2X)^{-1}$ の 2 は単に $X = 1$ 付近で log が 0 に近づかないようにするためにつけられています.

Note 3 (Proof of Lemma 12.1-(i))**.** 等式

$$u\rho(u) = \int_{u-1}^{u} \rho(v)dv \quad (u \geq 1) \tag{5}$$

の証明は以下のとおりです： 両辺の差

$$\phi(u) \coloneqq u\rho(u) - \int_{u-1}^{u} \rho(v)dv$$

を $u > 1$ のときに微分すると方程式 (1) より

$$\phi'(u) = u\rho'(u) + \rho(u) - (\rho(u) - \rho(u-1)) = 0$$

となるので, 初期条件 (2) より $\phi(1) = 0$ であることを見ればよいです.

Note 4 (p. 175–176, Proof of Lemma 12.1 (ii))**.** ここの証明は標準的ですが, あまり細かく書かれていないので, 念の為詳細を残します：まず, 素数に関する初等的評価を 2 つ思い出しておきます. （これらの評価には素数定理は不要です. また, この 2 つの Lemma の証明はセミナーでは省略しましょう）

Lemma 1. 実数 $x \geq 1$ に対して

$$\pi(x) \coloneqq \sum_{p \leq x} 1 \ll \frac{x}{\log 2x}.$$

ただし implicit constant は絶対定数.

Proof. この評価は素数定理を弱めたものと見れますが, この弱い形の評価は Chebyshev が証明したのが初めてでしょう. 証明は例えば [1, Corollary 2.6] を参照のこと. □

Lemma 2. 実数 $x \geq 2$ に対して

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + b + O\left(\frac{1}{\log 2x}\right).$$

ただし定数 b と implicit constant は絶対定数.

Proof. 誤差項評価付きの素数定理からはもう少し強い主張が出ますが, この弱い形の主張は素数定理なしで示すことができます. Mertens の定理と呼ばれる一群の評価のひとつです. 証明は例えば [1, Theorem 2.7 (d)] を参照のこと. □

Lemma 3. 実数 x, y であって $2 \leq x \leq y$ なるものに対して

$$S(y,x) \coloneqq \sum_{x < p \leq y} \frac{1}{p} \quad \text{および} \quad S(y,x) = \log\frac{\log y}{\log x} + R(y,x)$$

とおくと

$$R(y,x) \ll \frac{1}{\log 2x}.$$

ただし定数 b と implicit constant は絶対定数.

Proof. 単に Lemma 2 の $x \coloneqq x$ のときと $x \coloneqq y$ のときの差を取れば従います. □

次に Buchstab 型の組合せ論的恒等式を示します：

Lemma 4 (p. 176, ℓ.5, formula (12.6))**.** 実数 $X \geq Z \geq Y \geq 1$ に対して,

$$A(X,Y) = A(X,Z) - \sum_{Y < p \leq Z} A\left(\frac{X}{p}, p\right)$$

が成立する.

Proof. まず $A(X,Z)$ の定義を思い出すと

$$A(X,Z) = \sum_{\substack{n \leq X \\ p_{\max}(n) \leq Z}} 1 \tag{6}$$

です. ただしここで

$$p_{\max}(n) \coloneqq \begin{cases} (p \text{ の最大素因子}) & (n > 1 \text{ のとき}), \\ 0 & (n = 1 \text{ のとき}) \end{cases}$$

とおきました. 上の和 (6) において $p_{\max}(n) \leq Y$ であるか否かに応じて和を分割し

$$A(X,Z) = \sum_{\substack{n \leq X \\ p_{\max}(n) \leq Y}} 1 + \sum_{\substack{n \leq X \\ Y < p_{\max}(n) \leq Z}} 1 = A(X,Y) + \sum_{\substack{n \leq X \\ Y < p_{\max}(n) \leq Z}} 1$$

を得ます. 最後の和の範囲内の n に対して, $p \coloneqq p_{\max}(n)$ とおき, p の値によって場合分けをします. すると

$$A(X,Z) = A(X,Y) + \sum_{Y < p \leq Z} \sum_{\substack{n \leq X \\ p_{\max}(n) = p}} 1$$

です. この右辺最後の和において, 与えられた p に対して n は $n = pm$ と一意的に書かれなければならず, さらに条件 $p_{\max}(n) = p$ は

$$p_{\max}(n) = p \iff p_{\max}(pm) = p \iff p_{\max}(m) \leq p$$

と書き直せます. よって,

$$\begin{aligned} A(X,Z) &= A(X,Y) + \sum_{Y<p\leq Z} \sum_{\substack{pm\leq X \\ p_{\max}(m)\leq p}} 1 \\ &= A(X,Y) + \sum_{Y<p\leq Z} \sum_{\substack{m\leq X/p \\ p_{\max}(m)\leq p}} 1 = A(X,Y) + \sum_{Y<p\leq Z} A\left(\frac{X}{p}, p\right) \end{aligned}$$

となり, 多少の項の移動の後に主張を得ます. □

Lemma 5. ある絶対定数 $B > 1$ が存在し, 任意の実数 $X \geq 1$ と $u > 0$ に対して,

$$|A(X, X^{\frac{1}{u}}) - X\rho(u)| \leq B^u X(\log 2X)^{-1}$$

が成り立つ.

Proof. 簡単のために $Y \coloneqq X^{\frac{1}{u}}$ とおきましょう. すると示すべき評価は

$$|A(X,Y) - X\rho(u)| \leq B^u X(\log 2X)^{-1}$$

と書き換えられます. 次にわかりやすいように準備として B の値を先に与えてしまいましょう. Lemma 1 および Lemma 3 より絶対定数 $C \geq 1$ が存在して任意の実数 x, y であって $2 \leq x \leq y$ なるものに対して

$$\sum_{p\leq x} 1 \leq Cx(\log 2x)^{-1} \quad \text{および} \quad \left| \sum_{x<p\leq y} \frac{1}{p} - \log\frac{\log y}{\log x} \right| \leq C(\log 2x)^{-1} \tag{7}$$

が成立します. そこで絶対定数 B として $B \coloneqq 36C \geq 36$ をとります.

さらに準備として簡単な評価を示しておきます. 関数 $\frac{X}{\log X}$ を考えると

$$\left(\frac{X}{\log X}\right)' = \frac{1}{\log X}\left(1 - \frac{1}{\log X}\right) \qquad (X \geq 2)$$

なので関数 $\frac{X}{\log X}$ は $2 \leq X \leq e$ のとき単調減少で $X \geq e$ のとき単調増加であったことを思い出します. 特にここから

$$\inf_{X\geq 1} \frac{X}{\log 2X} = \frac{1}{2} \inf_{X\geq 1} \frac{2X}{\log 2X} = \frac{1}{2} \inf_{X\geq 2} \frac{X}{\log X} = \frac{e}{2} \geq 1 \tag{8}$$

を得ます.

主張の証明に移ります. まず $u \in (0,1]$ のときを考えます. この場合は $Y = X^{\frac{1}{u}} \geq X$ かつ (2) より $\rho(u) = 1$ なので,

$$A(X,Y) - X\rho(u) = [X] - X = -\{X\}$$

となります. よって, (8) より

$$|A(X,Y) - X\rho(u)| \leq 1 \leq \frac{e}{2} \leq X(\log 2X)^{-1} \leq B^u X(\log 2X)^{-1}$$

を得ます. これで $u \in (0,1]$ のときが示せました.

次に $u \in (1,2]$ のときを考えます. Lemma 4 において $Z \coloneqq X$ とすることで

$$A(X,Y) = A(X,X) - \sum_{Y<p\le X} A\left(\frac{X}{p}, p\right) \tag{9}$$

を得ます. $A(X,Y)$ の定義より $A(X,X) = [X]$ です. また現在の範囲 $u \in (1,2]$ にては $Y = X^{\frac{1}{u}} \ge X^{\frac{1}{2}}$ なので (9) 右辺の和の範囲 $Y < p \le X$ にては

$$\frac{X}{p} \le X^{\frac{1}{2}} \le X^{\frac{1}{u}} < p$$

なので $A\left(\frac{X}{p}, p\right) = \left[\frac{X}{p}\right]$ もわかります. 以上より (9) は

$$\begin{aligned} A(X,Y) &= [X] - \sum_{Y<p\le X} \left[\frac{X}{p}\right] \\ &= X\left(1 - \sum_{Y<p\le X} \frac{1}{p}\right) - \left(\{X\} - \sum_{Y<p\le X} \left\{\frac{X}{p}\right\}\right) \end{aligned}$$

と書き直せます. よって

$$|A(X,Y) - X\rho(u)| \le R_{11} + R_{12} \tag{10}$$

とできます. ただし

$$R_{11} \coloneqq X\left|\left(1 - \sum_{Y<p\le X} \frac{1}{p}\right) - \rho(u)\right| \quad \text{および} \quad R_{12} \coloneqq \left|\{X\} - \sum_{Y<p\le X} \left\{\frac{X}{p}\right\}\right|$$

と置きました. 最初の R_{11} に対しては (7) を用いて

$$\begin{aligned} R_{11} &\le X\left|\left(1 - \log\frac{\log X}{\log Y}\right) - \rho(u)\right| + CX(\log 2Y)^{-1} \\ &\le X|(1-\log u) - \rho(u)| + uCX(\log 2X)^{-1} \\ &\le X|(1-\log u) - \rho(u)| + 2CX(\log 2X)^{-1} \end{aligned}$$

とできます. ここで (1) より現在の範囲 $u \in (1,2]$ において

$$\rho(u) = \rho(1) - \int_1^u \rho(t-1)\frac{dt}{t} = 1 - \int_1^u \frac{dt}{t} = 1 - \log u \tag{11}$$

を得るので（最初の等式は $1 < u' \le u$ なる u' をとり, $\rho(u) - \rho(u')$ を微積分の基本定理で計算した後に種々の連続性を用いて $u' \to 1$ とすることで得られます）, 結局

$$R_{11} \le 2CX(\log 2X)^{-1} \tag{12}$$

を得ます. 次に R_{12} については (7) より

$$-1 \le -\{X\} \le \sum_{Y<p\le X} \left\{\frac{X}{p}\right\} - \{X\} \le \sum_{Y<p\le X} \left\{\frac{X}{p}\right\} \le \sum_{p\le X} 1 \le CX(\log 2X)^{-1}$$

つまり

$$-1 \le \sum_{Y<p\le X} \left\{\frac{X}{p}\right\} - \{X\} \le CX(\log 2X)^{-1}$$

を得るので (8) より

$$R_{12} \le \max(1, CX(\log 2X)^{-1}) \le CX(\log 2X)^{-1} \tag{13}$$

を得ます. 以上の (12) と (13) を (10) に代入すれば $u \in (1,2]$ を思い出して

$$|A(X,Y) - X\rho(u)| \leq 3CX(\log 2X)^{-1} \leq BX(\log 2X)^{-1} \leq B^u X(\log 2X)^{-1}$$

を得ます. これで $u \in (1,2]$ のときが示せました.

最後に $u \in (2,\infty)$ の場合を考えます. まず小さな注意ですが, $u \in (2,\infty)$ の場合には $X \geq 2^u$ の場合を考えれば十分です. 実際, 反対に $X^{\frac{1}{u}} < 2$ の場合には $\log 2X \leq 2X$ であることと最初の定数 B の定義より $B \geq 4$ であることを使えば

$$B^u X(\log 2X)^{-1} \geq \frac{1}{2}B^u = \frac{B^{\frac{u}{2}}}{2}B^{\frac{u}{2}} \geq \frac{B}{2}2^u \geq 2^u > X$$

を得ます. よって $X^{\frac{1}{u}} < 2$ の場合には示すべき評価は自明な評価

$$-X \leq A(X,Y) - X\rho(u) \leq [X] \leq X \quad \text{つまり} \quad |A(X,Y) - X\rho(u)| \leq X$$

に帰着されます. (Lemma 12.1 (i) と (2) より $0 \leq \rho(u) \leq 1$ であることに注意します.) したがって, 現在の目的のためには主張

$\mathsf{P}(n)$:「任意の $u \in (0,n]$ と任意の $X \geq 2^u$ に対して

$$\left|A(X, X^{\frac{1}{u}}) - X\rho(u)\right| \leq B^u X(\log 2X)^{-1}$$

が成り立つ」

を $n = 2,3,\ldots$ に対して帰納的を用いて証明すれば十分です. 上までの議論で $n = 2$ の場合の証明が終わっていました. そこで $n \geq 3$ とし, 上の主張 $\mathsf{P}(n-1)$ を仮定し, 主張 $\mathsf{P}(n)$ を示しましょう. 任意に $u \in (0,n]$ を取りましょう. もし $u \in (0,n-1]$ ならば帰納法の仮定より示すべき評価が従うので

$$u \in (n-1,n] \tag{14}$$

と思って良いです. 任意に $X \geq 2^u$ を取りましょう. さて $v \coloneqq n - \frac{3}{2}$ とおき Lemma 4 において $Z \coloneqq X^{\frac{1}{v}}$ とおくことで (そのままですが)

$$A(X,Y) = A(X,Z) - \sum_{Y < p \leq Z} A\left(\frac{X}{p}, p\right) \tag{15}$$

を得ます. この右辺を評価していきます. まず, $Z = X^{\frac{1}{v}}$ であり, また $v = n - \frac{3}{2} \in (0,n-1]$ なので帰納法の仮定より (15) の右辺第 1 項に関して

$$|A(X,Z) - X\rho(v)| \leq B^v X(\log 2X)^{-1} = B^{n-\frac{3}{2}} X(\log 2X)^{-1}$$

を得ます. よって (14) と B の定義より

$$|A(X,Z) - X\rho(v)| \leq B^{u-\frac{1}{2}} X(\log 2X)^{-1} \leq \frac{1}{6}B^u X(\log 2X)^{-1} \tag{16}$$

を得ます. 次に (15) の右辺第 2 項に関して考えます. この和の範囲 $Y < p \leq Z$ において $w = w(p)$ を

$$p = \left(\frac{X}{p}\right)^{\frac{1}{w}} \quad \text{つまり} \quad w \coloneqq \frac{\log \frac{X}{p}}{\log p} = \frac{\log X}{\log p} - 1$$

で定めましょう. すると $Y = X^{\frac{1}{u}}$ および $Z = X^{\frac{1}{v}}$ だったので $Y < p \leq Z$ のとき

$$v - 1 = \frac{\log X}{\log Z} - 1 \leq w < \frac{\log X}{\log Y} - 1 = u - 1$$

つまり, $v = n - \frac{3}{2} \geq \frac{3}{2}$ を思い出せば

$$w \in [v-1, u-1) \subset (0, n-1]$$

を得ます. よって帰納法の仮定より $Y < p \leq Z$ のとき,

$$\begin{aligned}\left| A\left(\frac{X}{p}, p\right) - \frac{X}{p}\rho\left(\frac{\log X}{\log p} - 1\right)\right| &\leq B^w \frac{X}{p}\left(\log\frac{2X}{p}\right)^{-1} \\ &\leq B^{u-1}\frac{X}{p}\left(\log\frac{2X}{p}\right)^{-1}\end{aligned}$$

を得ます. 今 $v \geq \frac{3}{2}$ から $p \leq Z = X^{\frac{1}{v}} \leq X^{\frac{2}{3}}$ であることに注意すると,

$$\left(\log\frac{2X}{p}\right)^{-1} \leq (\log 2X^{\frac{1}{3}})^{-1} \leq 3(\log 2X)^{-1}$$

を得ます. よって

$$\left| A\left(\frac{X}{p}, p\right) - \frac{X}{p}\rho\left(\frac{\log X}{\log p} - 1\right)\right| \leq 3B^{u-1}X(\log 2X)^{-1}\frac{1}{p}$$

を得ます. この評価を足し上げ, (7) と B の定義を用いれば

$$\begin{aligned}&\left|\sum_{Y<p\leq Z}\left(A\left(\frac{X}{p}, p\right) - \frac{X}{p}\rho\left(\frac{\log X}{\log p} - 1\right)\right)\right| \\ &\leq \sum_{Y<p\leq Z}\left|A\left(\frac{X}{p}, p\right) - \frac{X}{p}\rho\left(\frac{\log X}{\log p} - 1\right)\right| \\ &\leq 3B^{u-1}X(\log 2X)^{-1}\sum_{Y<p\leq Z}\frac{1}{p} \\ &\leq \frac{1}{12C}\left(\log\frac{\log Z}{\log Y} + \frac{C}{\log 2Y}\right)B^u X(\log 2X)^{-1}\end{aligned}$$

を得ます. ここで

$$1 \leq \frac{\log Z}{\log Y} = \frac{u}{v} = \frac{u}{n-\frac{3}{2}} = \frac{2u}{2n-3} \leq \frac{2n}{2n-3} = 1 + \frac{3}{2n-3} \leq 2 \leq e \leq e^C$$

および $Y = X^{\frac{1}{u}} \geq 2$ から

$$\frac{C}{\log 2Y} \leq \frac{C}{\log 4} \leq C$$

となることより, 先の評価は

$$\left|\sum_{Y<p\leq Z}\left(A\left(\frac{X}{p}, p\right) - \frac{X}{p}\rho\left(\frac{\log X}{\log p} - 1\right)\right)\right| \leq \frac{1}{6}B^u X(\log 2X)^{-1} \tag{17}$$

となります. さて (15) に (16) と (17) を使えば

$$|A(X,Y) - X\rho(u)| \leq R_2 + \frac{1}{3}B^u X(\log 2X)^{-1} \tag{18}$$

を得ます. ただしここで

$$R_2 \coloneqq X\left|\left(\rho(v) - \sum_{Y<p\leq Z}\frac{1}{p}\rho\left(\frac{\log X}{\log p} - 1\right)\right) - \rho(u)\right| \tag{19}$$

とおきました. この R_2 を評価するために左辺の和を計算します. まず

$$v_1 \coloneqq \max(v,2) \quad \text{および} \quad Z_1 \coloneqq X^{\frac{1}{v_1}} \in (Y,Z]$$

とおき,

$$\sum_{Y<p\leq Z} \frac{1}{p}\rho\left(\frac{\log X}{\log p}-1\right) = \sum_{Y<p\leq Z_1} + \sum_{Z_1<p\leq Z} = \sum\nolimits_1 + \sum\nolimits_2 \tag{20}$$

と分割します. 和 $\sum_1$ について考えましょう. 和 $\sum_1$ の範囲 $Y<p\leq Z_1$ においては

$$\frac{\log X}{\log p}-1 \geq \frac{\log X}{\log Z_1}-1 = v_1-1 \geq 1$$

なので微積分学の基本定理から

$$\rho\left(\frac{\log X}{\log p}-1\right) = \int_{v_1}^{\frac{\log X}{\log p}} \rho'(t-1)dt + \rho(v_1-1)$$

を得ます. よって, Lemma 3 の記号を思い出し

$$S(t) \coloneqq S(t,Y) \quad \text{および} \quad R(t) \coloneqq R(t,Y) \tag{21}$$

おけば

$$\begin{aligned}
\sum\nolimits_1 &= \sum_{Y<p\leq Z_1} \frac{1}{p}\int_{v_1}^{\frac{\log X}{\log p}} \rho'(t-1)dt + \rho(v_1-1)\sum_{Y<p\leq Z_1}\frac{1}{p} \\
&= \int_{v_1}^{u} \rho'(t-1)S(X^{\frac{1}{t}})dt + \rho(v_1-1)S(Z_1) \\
&= \int_{v_1}^{u} \rho'(t-1)\log\frac{u}{t}dt + \rho(v_1-1)\log\frac{u}{v_1} \\
&\qquad + \int_{v_1}^{u} \rho'(t-1)R(X^{\frac{1}{t}})dt + \rho(v_1-1)R(Z_1)
\end{aligned}$$

と書き直せます. ここで部分積分を用いた後に (1) を使えば

$$\begin{aligned}
\sum\nolimits_1 &= \int_{v_1}^{u} \rho(t-1)\frac{dt}{t} + \int_{v_1}^{u} \rho'(t-1)R(X^{\frac{1}{t}})dt + \rho(v_1-1)R(Z_1) \\
&= \rho(v_1) - \rho(u) + \int_{v_1}^{u} \rho'(t-1)R(X^{\frac{1}{t}})dt + \rho(v_1-1)R(Z_1)
\end{aligned} \tag{22}$$

を得ます. 次に和 $\sum_2$ を考えましょう. まず, $v<2$ のときつまり $v_1=2$ となったときを考えると, 和の範囲 $Z_1<p\leq Z$ では

$$\frac{1}{2} \leq v-1 = \frac{\log X}{\log Z_1}-1 \leq \frac{\log X}{\log p}-1 < \frac{\log X}{\log Z_1}-1 = v_1-1 = 1$$

です. よって (2) より記号 (21) の下,

$$\sum\nolimits_2 = \sum_{Z_1<p\leq Z}\frac{1}{p} = S(Z)-S(Z_1) = \log\frac{v_1}{v} + R(Z) - R(Z_1)$$

です. 特にこのときは $v, v_1 \in (\frac{3}{2}, 2]$ なので (2) と (11) より

$$\rho(v) = 1-\log v, \quad \rho(v_1) = 1-\log v_1 \quad \text{および} \quad \rho(v-1) = \rho(v_1-1) = 1$$

であり, したがって上の式は

$$\sum\nolimits_2 = \rho(v) - \rho(v_1) + \rho(v-1)R(Z) - \rho(v_1-1)R(Z_1) \tag{23}$$

と書き直せます. 一方 $v \geq 2$ のときは $v = v_1$ つまり $Z = Z_1$ なので

$$\sum\nolimits_2 = 0 = \rho(v) - \rho(v_1) + \rho(v-1)R(Z) - \rho(v_1-1)R(Z_1)$$

です. どちらにせよ (23) がいつも成り立つことがわかりました. したがって, (22) と (23) を (20) に代入して

$$\sum_{Y<p\leq Z} \frac{1}{p}\rho\left(\frac{\log X}{\log p} - 1\right) = \rho(v) - \rho(u) + \int_{v_1}^{u} \rho'(t-1)R(X^{\frac{1}{t}})dt + \rho(v-1)R(Z)$$

を得ます. これをさらに R_2 の定義 (19) に代入し, Lemma 3 を使えば

$$\begin{aligned} R_2 &\leq \int_{v_1}^{u} |\rho'(t-1)R(X^{\frac{1}{t}})|dt + |\rho(v-1)R(Z)| \\ &\leq C(\log 2X^{\frac{1}{u}})^{-1}\left(\int_{v_1}^{u} |\rho'(t-1)|dt + \rho(v-1)\right) \end{aligned}$$

をえます. また Lemma 12.1 (i) より ρ は単調減少つまり $u > 1$ に対して $\rho'(u) \leq 0$ なのでさらに

$$\begin{aligned} R_2 &\leq C(\log 2X^{\frac{1}{u}})^{-1}\left(\rho(v-1) - \int_{v_1}^{u} \rho'(t-1)dt\right) \\ &= C(\log 2X^{\frac{1}{u}})^{-1}\left(\rho(v-1) - \rho(u) + \rho(v_1-1)\right) \\ &\leq 2C(\log 2X^{\frac{1}{u}})^{-1}\rho(v-1) \\ &\leq 2C(\log 2X)^{-1}u\rho(v-1) \end{aligned}$$

となりますが,

$$u \leq n = v - 1 + \frac{5}{2} \leq 6(v-1)$$

なので, (5) と $\rho(u) \leq 1$ より

$$\begin{aligned} R_2 &\leq 12C(\log 2X)^{-1}(v-1)\rho(v-1) \\ &\leq 12C(\log 2X)^{-1} \leq \frac{1}{3}B(\log 2X)^{-1} \leq \frac{1}{3}B^u(\log 2X)^{-1} \end{aligned}$$

を得ます. この評価を (18) に代入すれば,

$$|A(X,Y) - X\rho(u)| \leq B^u X(\log 2X)^{-1}$$

を得ます. これで主張 $\mathsf{P}(n)$ が示され, 証明が完了しました. □

Note 5 (p.177, l.1–12)**.** ここの notation は多少ややこしいですが, 以下のようにまとめておきます. 次のものを用意します：

- 自然数 k, s, t ただし $k \geq 2$, $s, t \geq 0$.
- 変数 Z に関して 1 次以上の多項式 $\Psi(Z, U_1, \ldots, U_t) \in \mathbb{Z}[Z, U_1, \ldots, U_t]$ (ただし以後 $\boldsymbol{U} = (U_1, \ldots, U_t)$ 等, 後半の t 変数はまとめて書く事が多い),
- 多項式 $\Psi(Z, \boldsymbol{U})$ の変数 Z の動く範囲を指定する実数 $P \geq 1$,
- 自然数の組 $\boldsymbol{x}, \boldsymbol{y}$ の動く範囲を指定する実数 $Q, R \geq 1$ (実数 R は smoothness の尺度. 主に $\boldsymbol{x}, \boldsymbol{y} \in \mathscr{A}(Q,R)^s$ という状況を考える)

- 多項式 $\Psi(Z, \boldsymbol{U})$ の変数の組 $\boldsymbol{U}$ の範囲を指定する有限集合 $\mathscr{U} \subset \mathbb{N}^t$ $(U \coloneqq \#U)$. ただし $t = 0$ のときは $\mathbb{N}^t = \{\varnothing\}$ と解釈する.

さらに次のような変数・記号の使い方をします：

- 多項式 $\Psi(Z, \boldsymbol{U})$ の Z に代入される自然数を動く変数 z, w
- 多項式 $\Psi(Z, \boldsymbol{U})$ の $\boldsymbol{U}$ に代入される自然数の組を動く変数 $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}^t$ (組の成分は $\boldsymbol{u} = (u_i)_{i=1}^t$ と $\boldsymbol{v} = (v_i)_{i=1}^t$ 等と書く)
- 変数の組 $\boldsymbol{X} = (X_i)_{i=1}^s$ に対して (いわゆる power sum)

$$p(\boldsymbol{X}) = p_k(\boldsymbol{X}) \coloneqq \sum_{i=1}^{s} X_i^k.$$

- $p_k(\boldsymbol{X})$ の $\boldsymbol{X}$ に代入される自然数の組を動く変数 $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{N}^s$ (組の成分は $\boldsymbol{x} = (x_i)_{i=1}^s$ と $\boldsymbol{y} = (y_i)_{i=1}^s$ 等と書く).

この状況で $S_s(P, Q, R; \Psi) = S_s(P, Q, R; \Psi; \mathscr{U})$ は

$$S_s(P, Q, R; \Psi; \mathscr{U}) \coloneqq \#\left\{ \begin{matrix} 1 \le z, w \le P,\ \boldsymbol{u}, \boldsymbol{v} \in \mathscr{U} \\ \boldsymbol{x}, \boldsymbol{y} \in \mathscr{A}(Q, R)^s \end{matrix} \;\middle|\; \Psi(z, \boldsymbol{u}) + p_k(\boldsymbol{x}) = \Psi(w, \boldsymbol{v}) + p_k(\boldsymbol{y}) \right\}$$

と定義されています. （あまり良い内包的記法ではありませんが, 右辺の集合は組 $(z, w, \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{x}, \boldsymbol{y})$ の集まりです. 以後同様の省略をします.） また対応する集合を

$$\mathscr{S}_s(P, Q, R; \Psi; \mathscr{U}) \coloneqq \left\{ \begin{matrix} 1 \le z, w \le P,\ \boldsymbol{u}, \boldsymbol{v} \in \mathscr{U} \\ \boldsymbol{x}, \boldsymbol{y} \in \mathscr{A}(Q, R)^s \end{matrix} \;\middle|\; \Psi(z, \boldsymbol{u}) + p_k(\boldsymbol{x}) = \Psi(w, \boldsymbol{v}) + p_k(\boldsymbol{y}) \right\}$$

と花文字で表すことにしましょう. 注意ですが方程式

$$\Psi(z, \boldsymbol{u}) + p_k(\boldsymbol{x}) = \Psi(w, \boldsymbol{v}) + p_k(\boldsymbol{y})$$

は $p(\boldsymbol{X})$ の定義を思い出せばテキストに書いてある方程式 (12.9)

$$\Psi(z, \boldsymbol{u}) + x_1^k + \cdots + x_s^k = \Psi(w, \boldsymbol{v}) + y_1^k + \cdots + y_s^k \tag{24}$$

と全く同じものです. またこの方程式 (24)（の与える条件）には

- 変数たち $x_1, \ldots, x_s$ の置換に対しての不変性
- 変数たち $y_1, \ldots, y_s$ の置換に対しての不変性
- 組 $(z, \boldsymbol{u}, \boldsymbol{x})$ と組 $(w, \boldsymbol{v}, \boldsymbol{y})$ の入れ替えに対しての不変性

という対称性があることに注意します. 便宜のため, 上の記号に誤解の恐れが無い限り

$$S_s(P, Q, R; \Psi) \coloneqq S_s(P, Q, R; \Psi; \mathscr{U}), \quad \mathscr{S}_s(P, Q, R) \coloneqq \mathscr{S}_s(P, Q, R; \Psi; \mathscr{U}), \ \ldots$$

といったような省略を行い, また $\mathscr{S}_s(P, Q, R)$ の元 $(z, w, \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{x}, \boldsymbol{y})$ を

$$\begin{pmatrix} z, \boldsymbol{u}, \boldsymbol{x} \\ w, \boldsymbol{v}, \boldsymbol{y} \end{pmatrix}$$

等と表しましょう.

後の操作のためにいくつか Lemma を示します.

Lemma 6. 有限集合（この補題では上記変数の使い方を踏襲しない）

$$\mathscr{X}_1, \ldots, \mathscr{X}_s, \mathscr{Y}_1, \ldots, \mathscr{Y}_t$$

と写像

$$\phi_i \colon \mathscr{X}_i \to \mathbb{Z} \quad (i = 1, \ldots, s) \quad \text{および} \quad \psi_i \colon \mathscr{Y}_i \to \mathbb{Z} \quad (i = 1, \ldots, t)$$

対して

$$f_i(\alpha) \coloneqq \sum_{x \in \mathscr{X}_i} e(\alpha \phi_i(x)) \quad (i = 1, \dots, s)$$

および

$$g_i(\alpha) \coloneqq \sum_{x \in \mathscr{Y}_i} e(\alpha \psi_i(y)) \quad (i = 1, \dots, t)$$

を考える. このとき,

$$\begin{aligned} &\# \left\{ \boldsymbol{x} \in \prod_{i=1}^{s} \mathscr{X}_i,\ \boldsymbol{y} \in \prod_{i=1}^{t} \mathscr{Y}_i \;\middle|\; \phi_1(x_1) + \cdots + \phi_s(x_s) = \psi_1(y_1) + \cdots + \psi_t(y_t) \right\} \\ &= \int_0^1 \left(\prod_{i=1}^{s} f_i(\alpha) \right) \overline{\left(\prod_{i=1}^{t} g_i(\alpha) \right)} d\alpha \end{aligned}$$

が成り立つ. （この Lemma はこのノートでは毎回律儀に適用しますが, 実際のセミナーでは聴講者が全員納得できれば適用方法を明示的に宣言しなくてもいいでしょう.）

Proof. 上記 f_i や g_i の定義中の和において和を取る変数を x_i や y_i に変更すれば

$$\prod_{i=1}^{s} f_i(\alpha) = \sum_{\boldsymbol{x} \in \prod_{i=1}^{s} \mathscr{X}_i} e(\alpha(\phi_1(x_1) + \cdots + \phi_s(x_s)))$$

および

$$\begin{aligned} \overline{\prod_{i=1}^{t} g_i(\alpha)} &= \overline{\sum_{\boldsymbol{y} \in \prod_{i=1}^{t} \mathscr{Y}_i} e(\alpha(\psi_1(y_1) + \cdots + \psi_t(y_t)))} \\ &= \sum_{\boldsymbol{y} \in \prod_{i=1}^{t} \mathscr{Y}_i} e(-\alpha(\psi_1(y_1) + \cdots + \psi_t(y_t))) \end{aligned}$$

を得ます. したがって指数関数の直交性より

$$\begin{aligned} &\int_0^1 \left(\prod_{i=1}^{s} f_i(\alpha) \right) \overline{\left(\prod_{i=1}^{t} g_i(\alpha) \right)} d\alpha \\ &= \sum_{\substack{\boldsymbol{x} \in \prod_{i=1}^{s} \mathscr{X}_i \\ \boldsymbol{y} \in \prod_{i=1}^{t} \mathscr{Y}_i}} \int_0^1 e(\alpha((\phi_1(x_1) + \cdots + \phi_s(x_s)) - (\psi_1(y_1) + \cdots + \psi_t(y_t)))) d\alpha \\ &= \# \left\{ \boldsymbol{x} \in \prod_{i=1}^{s} \mathscr{X}_i,\ \boldsymbol{y} \in \prod_{i=1}^{t} \mathscr{Y}_i \;\middle|\; \phi_1(x_1) + \cdots + \phi_s(x_s) = \psi_1(y_1) + \cdots + \psi_t(y_t) \right\} \end{aligned}$$

を得るので証明を終わります. □

Lemma 7. 先の記号の下で, テキストの p.179 と同様に

$$f(\alpha) = f(\alpha, P) = f(\alpha, P, R) \coloneqq \sum_{x \in \mathscr{A}(P,R)} e(\alpha x^k)$$

とおくと

$$S_s(P, R) = \int_0^1 |f(\alpha, P, R)|^{2s} d\alpha$$

が成立する.

Proof. Lemma 6 を

$$\mathscr{X}_i, \mathscr{Y}_i \coloneqq \mathscr{A}(P,R), \quad \phi_i, \psi_i \colon \mathscr{X}_i, \mathscr{Y}_i \to \mathbb{Z};\, x \mapsto x^k \quad (i=1,\dots,s)$$

に適用すれば

$$f_i(\alpha) = g_i(\alpha) = f(\alpha,P,R) \quad (i=1,\dots,s)$$

となるので Lemma を得る. □

Lemma 8. 先の記号の下で, テキストの p.179 と同様に

$$F(\alpha) = F(\alpha,P,\Psi,\mathscr{U}) \coloneqq \sum_{\substack{1\le z\le P\\ \boldsymbol{u}\in\mathscr{U}}} e(\alpha\Psi(z,\boldsymbol{u}))$$

とおくと, Lemma 7 と同じ記号の下,

$$S_s(P,Q,R;\Psi;\mathscr{U}) = \int_0^1 |F(\alpha,P,\Psi,\mathscr{U})|^2 |f(\alpha,Q,R)|^{2s} d\alpha$$

が成立する.

Proof. Lemma 6 を

$$\begin{gathered}
\mathscr{X}_1, \mathscr{Y}_1 \coloneqq \{(z,\boldsymbol{u}) \mid z\in[1,P]\cap\mathbb{Z},\ \boldsymbol{u}\in\mathscr{U}\},\\
\mathscr{X}_i, \mathscr{Y}_i \coloneqq \mathscr{A}(Q,R) \quad (i=2,\dots,s+1),\\
\phi_1, \psi_1 \colon \mathscr{X}_1, \mathscr{Y}_1 \to \mathbb{Z};\, (z,\boldsymbol{u}) \mapsto \Psi(z,\boldsymbol{u})\\
\phi_i, \psi_i \colon \mathscr{X}_i, \mathscr{Y}_i \to \mathbb{Z};\, x \mapsto x^k \quad (i=2,\dots,s+1)
\end{gathered}$$

に適用すれば

$$\begin{aligned}
f_1(\alpha) = g_1(\alpha) &= F(\alpha,P,\Psi,\mathscr{U}),\\
f_i(\alpha) = g_i(\alpha) &= f(\alpha,Q,R) \quad (i\ge 2)
\end{aligned}$$

となるので Lemma を得る. □

12.2 The fundamental lemma

Note 6 (Theorem 12.1)**.** 省略された変数は以下の通り：

Theorem 1. いままでの記号の下, 実数 M,Q,P であって $1<M<Q\le P$ なるものに対して,

$$\begin{aligned}
S_s(P,Q,R;\Psi;\mathscr{U}) \ll S_s(P,M,R;\Psi;\mathscr{U}) &+ N + P^{\varepsilon}QMS_{s-1}(P,Q,R;\Psi;\mathscr{U})\\
&+ P^{\varepsilon}U(MR)^{2s-1}T_s(P,Q,R,M;\Psi;\mathscr{U})
\end{aligned}$$

が成立する. ただしここで, N は

$$N \coloneqq \#\{(z,w,\boldsymbol{u},\boldsymbol{v},\boldsymbol{x},\boldsymbol{y}) \in \mathscr{S}_s(P,Q,R;\Psi;\mathscr{U}) \mid \Psi'(z,\boldsymbol{u}) = \Psi'(w,\boldsymbol{v}) = 0\}$$

で与えられる.

Note 7 (Lemma 12.2)**.** もしかすると証明が読みにくいかもしれないので詳細を与えます（特に最後の v の選び方における ε は最終的な主張の ε と揃わなかったりします汗）. まずは Chapter 1 の Exercise 1.5.1 になっている Lemma を示します（2 通りの手法を記します）:

Lemma 9. 整数 M, s であって $1 \leq s \leq M$ であるものに対して,

$$\#\{(x_1, \dots, x_s) \in \mathbb{N}^s \mid x_1 + \cdots + x_s \leq M\} = \binom{M}{s}.$$

Proof. **(ひとつめの証明)** 生成関数を用います. 自然数を指数として持つべき級数は

$$\frac{T}{1-T} = \sum_{x \geq 1} T^x$$

です. よって s 乗した後に変数 x を $x_1, \dots, x_s$ などに名前を変えてあげることで

$$\left(\frac{T}{1-T}\right)^s = \sum_{x_1, \dots, x_s \geq 1} T^{x_1 + \cdots + x_s} = \sum_{x \geq 0} \left(\sum_{\substack{x_1 + \cdots + x_s = x \\ x_1, \dots, x_s \geq 1}} 1 \right) T^x$$

を得ます. ここにさらに

$$\frac{1}{1-T} = \sum_{y \geq 0} T^y$$

をかけると

$$\begin{aligned} T^s (1-T)^{-s-1} &= \sum_{x,y \geq 0} \left(\sum_{\substack{x_1 + \cdots + x_s = x \\ x_1, \dots, x_s \geq 1}} 1 \right) T^{x+y} \\ &= \sum_{m \geq 0} \left(\sum_{\substack{x+y=m \\ x,y \geq 0}} \sum_{\substack{x_1 + \cdots + x_s = x \\ x_1, \dots, x_s \geq 1}} 1 \right) T^m = \sum_{m \geq 0} \left(\sum_{\substack{x_1 + \cdots + x_s \leq m \\ x_1, \dots, x_s \geq 1}} 1 \right) T^m \end{aligned} \tag{25}$$

を得ます. 一方, 最左辺を見れば拡張された 2 項定理より

$$\begin{aligned} T^s (1-T)^{-s-1} &= T^s \sum_{m=0}^{\infty} \binom{-s-1}{m} (-T)^m \\ &= \sum_{m=s}^{\infty} (-1)^{m-s} \binom{-s-1}{m-s} T^m. \end{aligned} \tag{26}$$

ここで (25) と (26) の係数を比較して

$$\sum_{\substack{x_1 + \cdots + x_s \leq M \\ x_1, \dots, x_s \geq 1}} 1 = (-1)^{M-s} \binom{-s-1}{M-s} = \frac{(-1)^{M-s} \prod_{i=1}^{M-s} (-s-i)}{(M-s)!} = \frac{\prod_{i=1}^{M-s} (i+s)}{(M-s)!}$$

最後の積で $j := M - s - i$ と変数変換して

$$\sum_{\substack{x_1 + \cdots + x_s \leq M \\ x_1, \dots, x_s \geq 1}} 1 = \frac{\prod_{j=0}^{M-s-1} (M-j)}{(M-s)!} = \binom{M}{M-s} = \binom{M}{s}$$

を得て証明が終わります.

(ふたつめの証明) 集合

$$X \coloneqq \{(x_1, \dots, x_s) \in \mathbb{N}^s \mid x_1 + \cdots + x_s \leq M\}$$
$$Y \coloneqq \{(y_1, \dots, y_s) \in \mathbb{N}^s \mid y_1 < \cdots < y_s \leq M\}$$

を考えると写像

$$\phi \colon X \to Y\,;\, (x_1, \dots, x_s) \mapsto (x_1, x_1 + x_2, x_1 + x_2 + x_3, \dots, x_1 + \cdots + x_s)$$
$$\psi \colon Y \to X\,;\, (y_1, \dots, y_s) \mapsto (y_1, y_2 - y_1, y_3 - y_2, \dots, y_s - y_{s-1})$$

は互いの逆写像になっているので, どちらも全単射であり, よって $\#X = \#Y$ ですが, $\#Y$ は M 以下の自然数を順序の違いを除いて s 個選び出す選び方の個数に等しいので $\#X = \#Y = \binom{M}{s}$ です. □

では Lemma 12.2 を示しましょう.

Lemma 10. 自然数 r と実数 $X \geq 1$ と $\varepsilon > 0$ に対して

$$\#\{n \leq X \mid s_0(n) = s_0(r)\} \ll X^{\varepsilon}.$$

ただし "$\ll$" に含まれる implicit constant は ε に依存する.

Proof. まず, $r = 1$ の場合は $s_0(n) = s_0(r)$ となるのは $n = 1$ の場合のみなので主張は自明に従います. したがって, 以下 $r \geq 2$ と仮定します. すると, もはや $s_0(1) \neq s_0(r)$ なので $X \geq 2$ であると仮定して良いです. さらに $0 < \varepsilon \leq 1$ のときのみ考えれば十分です. 次に $s_0(r)$ は定義より square-free（素因数分解に現れる指数がすべて 1）なので,

$$s_0(r) = p_1 \cdots p_t \quad (p_1 < \cdots < p_t \colon \text{素数})$$

という形に素因数分解できます. 自然数 n が $s_0(n) = s_0(r)$ を満たすというのは n が

$$n = p_1^{u_1} \cdots p_t^{u_t} \quad (u_1, \dots, u_t \geq 1)$$

と素因数分解されることと同じなので, 自然数の組 $\boldsymbol{u} = (u_1, \dots, u_t)$ であって

$$p_1^{u_1} \cdots p_t^{u_t} \leq X$$

なるものの個数 U を評価すればよいです. 特にこのとき任意の $i = 1, \dots, t$ に対して

$$2^{u_i} \leq p_i^{u_i} \leq p_1^{u_1} \cdots p_t^{u_t} \leq X$$

だから最両辺の対数をとり,

$$1 \leq u_i \leq \frac{\log X}{\log 2} \tag{27}$$

を得ます. さらに $v = [\exp(\frac{2}{\varepsilon})]$ とおきましょう.

まず $t \leq v$ の場合には主張はただちに従うことを示します. このときは (27) より, 各 $u_1, \dots, u_t$ のとりうる値をばらばらに数えて組 $\boldsymbol{u}$ の個数 U は

$$U \leq \left(\frac{\log X}{\log 2}\right)^t$$

です. ここで $X \geq 2$, $t \leq v$ と $\log X \leq X$ を用いれば

$$U \leq \left(\frac{\log X}{\log 2}\right)^v = \left(\frac{v \log X^{\frac{\varepsilon}{v}}}{\varepsilon \log 2}\right)^v \leq \left(\frac{v}{\varepsilon \log 2}\right)^v X^{\varepsilon} \leq \left(\frac{\exp(\frac{2}{\varepsilon})}{\varepsilon \log 2}\right)^{\exp(\frac{2}{\varepsilon})} X^{\varepsilon}$$

を得るので主張が従います. よって以後 $t > v$ のときのみ考察すれば十分です.

残りの $t > v$ のときは組 $\boldsymbol{u}$ を前半の $\boldsymbol{u}_1 = (u_1, \ldots, u_v)$ の取りうる値の個数 U_1 と後半の $\boldsymbol{u}_2 = (u_{v+1}, \ldots, u_t)$ の取りうる値の個数 U_2 とを別々に評価してこの U_1 と U_2 の評価の積をとります. まず, 前半の $\boldsymbol{u}_1$ のとりうる値の個数 U_1 に対しては先と同様に単に各 $u_1, \ldots, u_v$ の場合の数をばらばらに数えることで

$$\begin{aligned} U_1 &\leq \left(\frac{\log X}{\log 2}\right)^v = \left(\frac{2v \log X^{\frac{\varepsilon}{2v}}}{\varepsilon \log 2}\right)^v \\ &\leq \left(\frac{2v}{\varepsilon \log 2}\right)^v X^{\frac{\varepsilon}{2}} \leq \left(\frac{2\exp(\frac{2}{\varepsilon})}{\varepsilon \log 2}\right)^{\exp(\frac{2}{\varepsilon})} X^{\frac{\varepsilon}{2}} \end{aligned} \tag{28}$$

を得ます. 次に後半の $\boldsymbol{u}_2$ のとりうる値の個数 U_2 を評価しましょう. ひとつ $\boldsymbol{u}_2$ を取り出してくると $\boldsymbol{u}$ の条件と p_i の単調性より（p_i は単調なので $p_{v+1} \geq v+1$ であることに注意します）

$$(v+1)^{u_{v+1}+\cdots+u_t} \leq p_{v+1}^{u_{v+1}+\cdots+u_t} \leq p_{v+1}^{u_{v+1}} \cdots p_t^{u_t} \leq p_1^{u_1} \cdots p_t^{u_t} \leq X$$

です. よって最両辺の対数をとり

$$u_{v+1} + \cdots + u_t \leq M := \left[\frac{\log X}{\log(v+1)}\right]$$

を得ます. このような自然数の組 $\boldsymbol{u}_2 = (u_{v+1}, \ldots, u_t)$ の個数 U_2 は Lemma 9 より

$$U_2 \leq \binom{M}{t-v} \leq 2^M \leq e^M \leq \exp\left(\frac{\log X}{\log(v+1)}\right)$$

と評価できます. ここでさらに $v = [\exp(\frac{2}{\varepsilon})]$ も思い出せば $v+1 > \exp(\frac{2}{\varepsilon})$ より

$$U_2 \leq \exp\left(\frac{\log X}{\log(\exp(\frac{2}{\varepsilon}))}\right) = \exp\left(\frac{\varepsilon}{2}\log X\right) = X^{\frac{\varepsilon}{2}} \tag{29}$$

を得ます. 以上の (28) と (29) より最終的に

$$U \leq U_1 U_2 \leq \left(\frac{2\exp(\frac{2}{\varepsilon})}{\varepsilon \log 2}\right)^{\exp(\frac{2}{\varepsilon})} X^{\varepsilon}$$

を得て証明を終わります. □

Note 8 (p.179 の l.3–4)**.** 明らかですがこの評価は

$$S_s(P,Q,R) \leq S^{(1)} + S^{(2)} + S^{(3)} + S^{(4)} \leq 4 \max_j S^{(j)} \tag{30}$$

であることから従います.（左辺で数えられているものを被りも許して 4 つの部分に分類しているのでこの評価は明らかです.）

Note 9 (p.179, Theorem 12.1 の証明の (i))**.** 詳細は以下の通り：まず

$$\mathscr{S}^{(1)} := \left\{ \binom{z, \boldsymbol{u}, \boldsymbol{x}}{w, \boldsymbol{v}, \boldsymbol{y}} \in \mathscr{S}_s(P,Q,R) \;\middle|\; \text{ある } j \text{ で } \min\{x_j, y_j\} \leq M \right\}$$

とおくと $S^{(1)} = \#\mathscr{S}^{(1)}$ です. この集合 $\mathscr{S}^{(1)}$ は

$$\mathscr{S}^{(1)} = \left\{ \begin{pmatrix} z, \boldsymbol{u}, \boldsymbol{x} \\ w, \boldsymbol{v}, \boldsymbol{y} \end{pmatrix} \in \mathscr{S}_s(P,Q,R) \;\middle|\; \min\{x_1, \dots, x_s, y_1, \dots, y_s\} \le M \right\}$$

とも書き換えられます. よって

$$\mathscr{S}_X^{(1,j)} \coloneqq \left\{ \begin{pmatrix} z, \boldsymbol{u}, \boldsymbol{x} \\ w, \boldsymbol{v}, \boldsymbol{y} \end{pmatrix} \in \mathscr{S}_s(P,Q,R) \;\middle|\; x_j \le M \right\}$$
$$\mathscr{S}_Y^{(1,j)} \coloneqq \left\{ \begin{pmatrix} z, \boldsymbol{u}, \boldsymbol{x} \\ w, \boldsymbol{v}, \boldsymbol{y} \end{pmatrix} \in \mathscr{S}_s(P,Q,R) \;\middle|\; y_j \le M \right\}$$

とおけば

$$\mathscr{S}^{(1)} \subset \bigcup_{i=1}^{s} \mathscr{S}_X^{(1,j)} \cup \bigcup_{i=1}^{s} \mathscr{S}_Y^{(1,j)}$$

なので被りも含めて数えて

$$S^{(1)} \le \sum_{i=1}^{s} \#\mathscr{S}_X^{(1,j)} + \sum_{i=1}^{s} \#\mathscr{S}_Y^{(1,j)} \tag{31}$$

です. ここで, $\mathscr{S}_s(P,Q,R;\Psi,\mathscr{U})$ を定義する方程式 (24) の対称性を用いれば,

$$\#\mathscr{S}_X^{(1,j)} = \#\mathscr{S}_Y^{(1,j)} = \#\mathscr{S}_X^{(1,1)}$$

が任意の j に対して成立することがわかります. よって (31) より

$$S^{(1)} \le 2s \cdot \#\mathscr{S}_X^{(1,1)} \tag{32}$$

を得ます. ここで $\mathscr{S}_X^{(1,1)}$ の定義を開いてみると $M < Q$ に気をつけて

$$\mathscr{S}_X^{(1,1)} = \left\{ \begin{matrix} 1 \le z,w \le P,\ \boldsymbol{u},\boldsymbol{v} \in \mathscr{U} \\ \boldsymbol{x} \in \mathscr{A}(M,R) \times \mathscr{A}(Q,R)^{s-1} \\ \boldsymbol{y} \in \mathscr{A}(Q,R)^{s} \end{matrix} \;\middle|\; \Psi(z,\boldsymbol{u}) + \sum_{i=1}^{s} x_i^k = \Psi(w,\boldsymbol{v}) + \sum_{i=1}^{s} y_i^k \right\}$$

であり, Lemma 6 を

$$\mathscr{X}_1, \mathscr{Y}_1 \coloneqq \{(z,\boldsymbol{u}) \mid z \in [1,P] \cap \mathbb{Z},\ \boldsymbol{u} \in \mathscr{U}\}$$
$$\mathscr{X}_2 \coloneqq \mathscr{A}(M,R), \quad \mathscr{Y}_2 \coloneqq \mathscr{A}(Q,R)$$
$$\mathscr{X}_i, \mathscr{Y}_i \coloneqq \mathscr{A}(Q,R) \quad (i = 3, \dots, s+1)$$
$$\phi_1, \psi_1 \colon \mathscr{X}_1, \mathscr{Y}_1 \to \mathbb{Z};\ (z,\boldsymbol{u}) \mapsto \Psi(z,\boldsymbol{u})$$
$$\phi_i, \psi_i \colon \mathscr{X}_i, \mathscr{Y}_i \to \mathbb{Z};\ x \mapsto x^k \quad (i = 2, \dots, s+1)$$

に適用すれば

$$f_1(\alpha) = g_1(\alpha) = F(\alpha, P, \Psi, \mathscr{U}),$$
$$f_2(\alpha) = f(\alpha, M, R), \quad g_2(\alpha) = f(\alpha, Q, R),$$
$$f_i(\alpha) = g_i(\alpha) = f(\alpha, Q, R) \quad (i \ge 3)$$

となるので, (Lemma 8 の記号を用いれば)

$$\begin{aligned} \mathscr{S}_X^{(1,1)} &= \int_0^1 |F(\alpha)|^2 f(\alpha,M,R) \overline{f(\alpha,Q,R)} |f(\alpha,Q,R)|^{2(s-1)} d\alpha \\ &\le \int_0^1 |F(\alpha)|^2 |f(\alpha,M,R)| |f(\alpha,Q,R)|^{2s-1} d\alpha \end{aligned}$$

です. 指数 $(p,q)=(2s,\frac{2s}{2s-1})$（これは $\frac{1}{p}+\frac{1}{q}=1$ を満たす）で Hölder の不等式を

$$\begin{aligned}&|F(\alpha)|^2|f(\alpha,M,R)||f(\alpha,Q,R)|^{2s-1}\\&=|F(\alpha)|^{\frac{2}{p}}|f(\alpha,M,R)|\times|F(\alpha)|^{\frac{2}{q}}|f(\alpha,Q,R)|^{2s-1}\end{aligned}$$

という分解に用いれば,

$$\mathscr{S}_X^{(1,1)}\le\left(\int_0^1|F(\alpha)|^2|f(\alpha,M,R)|^{2s}d\alpha\right)^{\frac{1}{2s}}\left(\int_0^1|F(\alpha)|^2|f(\alpha,Q,R)|^{2s}d\alpha\right)^{\frac{2s-1}{2s}}$$

を得ます. さらに (32) と Lemma 8 よりこれは

$$S^{(1)}\le 2sS_s(P,M,R,\Psi;\mathscr{U})^{\frac{1}{2s}}S_s(P,Q,R,\Psi;\mathscr{U})^{1-\frac{1}{2s}}$$

を意味します. よって $\max_j S^{(j)}=S^{(1)}$ のときは (30) より

$$S_s(P,Q,R,\Psi;\mathscr{U})\le 8sS_s(P,M,R,\Psi;\mathscr{U})^{\frac{1}{2s}}S_s(P,Q,R,\Psi;\mathscr{U})^{1-\frac{1}{2s}}$$

です. 左辺が 0 のときは示すべきことはないので左辺は 0 でないとしてよく, 両辺を

$$S_s(P,Q,R,\Psi;\mathscr{U})^{1-\frac{1}{2s}}$$

で割ってから $2s$ 乗すると

$$S_s(P,Q,R,\Psi;\mathscr{U})\le(8s)^{2s}S_s(P,M,R,\Psi;\mathscr{U})$$

となりこの場合は Theorem 12.1 の主張が成立します. （このテキストでは implicit constant は s に依存してよかったことに注意します.)

Note 10 (p.179, Theorem 12.1 の証明の (ii))**.** 詳細は以下の通り：まず

$$\mathscr{S}^{(2)}\coloneqq\left\{\begin{pmatrix}z,\boldsymbol{u},\boldsymbol{x}\\w,\boldsymbol{v},\boldsymbol{y}\end{pmatrix}\in\mathscr{S}_s(P,Q,R)\;\middle|\;\Psi'(z,\boldsymbol{u})=0\text{ or }\Psi'(w,\boldsymbol{v})=0\right\}$$

とおくと $S^{(2)}=\#\mathscr{S}^{(2)}$ です. 集合 $\mathscr{S}^{(2)}$ を定める条件は

$\Psi'(z,\boldsymbol{u})=\Psi'(w,\boldsymbol{v})=0$ ではなく $\Psi'(z,\boldsymbol{u})$ と $\Psi'(w,\boldsymbol{v})$ のどちらかが 0 というだけだということに注意します. また

$$\begin{aligned}\mathscr{S}_{Z,U}^{(2)}&\coloneqq\left\{\begin{pmatrix}z,\boldsymbol{u},\boldsymbol{x}\\w,\boldsymbol{v},\boldsymbol{y}\end{pmatrix}\in\mathscr{S}_s(P,Q,R)\;\middle|\;\Psi'(z,\boldsymbol{u})=0\right\}\\\mathscr{S}_{W,V}^{(2)}&\coloneqq\left\{\begin{pmatrix}z,\boldsymbol{u},\boldsymbol{x}\\w,\boldsymbol{v},\boldsymbol{y}\end{pmatrix}\in\mathscr{S}_s(P,Q,R)\;\middle|\;\Psi'(w,\boldsymbol{v})=0\right\}\end{aligned}$$

とおくと,

$$\mathscr{S}^{(2)}\subset\mathscr{S}_{Z,U}^{(2)}\cup\mathscr{S}_{W,V}^{(2)}$$

なので被りも含めて

$$S^{(2)}\le\#\mathscr{S}_{Z,U}^{(2)}+\#\mathscr{S}_{W,V}^{(2)}$$

を得ます. ここで $\mathscr{S}_s(P,Q,R;\Psi,\mathscr{U})$ を定義する方程式 (24) の対称性を用いれば,

$$\#\mathscr{S}_{Z,U}^{(2)}=\#\mathscr{S}_{W,V}^{(2)}$$

と知れるので, さらに

$$S^{(2)}\le 2\cdot\#\mathscr{S}_{Z,U}^{(2)}\tag{33}$$

を得ます. さてテキストと同様に

$$G(\alpha)=G(\alpha,P,\Psi,\mathscr{U}):=\sum_{\substack{1\le z\le P\\ \boldsymbol{u}\in\mathscr{U}\\ \Psi'(z,\boldsymbol{u})=0}}e(\alpha\Psi(z,\boldsymbol{u}))$$

とおき, Note 9 のときと同様に Lemma 6 を

$$\begin{gathered}\mathscr{X}_1:=\{(z,\boldsymbol{u})\mid z\in[1,P]\cap\mathbb{Z},\ \boldsymbol{u}\in\mathscr{U},\ \Psi'(z,\boldsymbol{u})=0\},\\ \mathscr{Y}_1:=\{(w,\boldsymbol{v})\mid w\in[1,P]\cap\mathbb{Z},\ \boldsymbol{v}\in\mathscr{U}\}\\ \mathscr{X}_i,\mathscr{Y}_i:=\mathscr{A}(Q,R)\quad(i=2,\dots,s+1)\\ \phi_1,\psi_1\colon\mathscr{X}_1,\mathscr{Y}_1\to\mathbb{Z};\ (z,\boldsymbol{u})\mapsto\Psi(z,\boldsymbol{u})\\ \phi_i,\psi_i\colon\mathscr{X}_i,\mathscr{Y}_i\to\mathbb{Z};\ x\mapsto x^k\quad(i=2,\dots,s+1)\end{gathered}$$

に適用すれば

$$\begin{gathered}f_1(\alpha)=G(\alpha,P,\Psi,\mathscr{U}),\quad g_1(\alpha)=F(\alpha,P,\Psi,\mathscr{U}),\\ f_i(\alpha)=g_i(\alpha)=f(\alpha,Q,R)\quad(i\ge2)\end{gathered}$$

となるので,

$$\begin{aligned}\#\mathscr{S}^{(2)}_{Z,U}&=\int_0^1G(\alpha,P,\Psi,\mathscr{U})\overline{F(\alpha,P,\Psi,\mathscr{U})}|f(\alpha,Q,R)|^{2s}d\alpha\\ &\le\int_0^1|G(\alpha,P,\Psi,\mathscr{U})||F(\alpha,P,\Psi,\mathscr{U})||f(\alpha,Q,R)|^{2s}d\alpha\end{aligned}$$

を得ます. ここで

$$\begin{aligned}&|G(\alpha,P,\Psi,\mathscr{U})||F(\alpha,P,\Psi,\mathscr{U})||f(\alpha,Q,R)|^{2s}\\ &=|G(\alpha,P,\Psi,\mathscr{U})||f(\alpha,Q,R)|^s\times|F(\alpha,P,\Psi,\mathscr{U})||f(\alpha,Q,R)|^s\end{aligned}$$

という分解に Cauchy–Schwarz の不等式を用いれば

$$\#\mathscr{S}^{(2)}_{Z,U}\le\left(\int_0^1|G(\alpha)|^2|f(\alpha)|^{2s}d\alpha\right)^{\frac12}\left(\int_0^1|F(\alpha)|^2|f(\alpha)|^{2s}d\alpha\right)^{\frac12}\tag{34}$$

となります. ここで Lemma 6 を

$$\begin{gathered}\mathscr{X}_1,\mathscr{Y}_1:=\{(z,\boldsymbol{u})\mid z\in[1,P]\cap\mathbb{Z},\ \boldsymbol{u}\in\mathscr{U},\ \Psi'(z,\boldsymbol{u})=0\},\\ \mathscr{X}_i,\mathscr{Y}_i:=\mathscr{A}(Q,R)\quad(i=2,\dots,s+1)\\ \phi_1,\psi_1\colon\mathscr{X}_1,\mathscr{Y}_1\to\mathbb{Z};\ (z,\boldsymbol{u})\mapsto\Psi(z,\boldsymbol{u})\\ \phi_i,\psi_i\colon\mathscr{X}_i,\mathscr{Y}_i\to\mathbb{Z};\ x\mapsto x^k\quad(i=2,\dots,s+1)\end{gathered}$$

に適用すれば

$$\begin{gathered}f_1(\alpha)=g_1(\alpha)=G(\alpha,P,\Psi,\mathscr{U}),\\ f_i(\alpha)=g_i(\alpha)=f(\alpha,Q,R)\quad(i\ge2)\end{gathered}$$

となるので,

$$N=\#\left\{(z,w,\boldsymbol{u},\boldsymbol{v},\boldsymbol{x},\boldsymbol{y})\in\mathscr{S}_s(P,Q,R)\mid\Psi'(z,\boldsymbol{u})=\Psi'(w,\boldsymbol{v})=0\right\}$$

$$= \# \left\{ \begin{matrix} (z,\boldsymbol{u})\in\mathscr{X}_1,(w,\boldsymbol{v})\in\mathscr{Y}_1 \\ \boldsymbol{x},\boldsymbol{y}\in\mathscr{A}(Q,R)^s \end{matrix} \;\middle|\; \Psi(z,\boldsymbol{u}) + \sum_{i=1}^{s} x_i^k = \Psi(w,\boldsymbol{v}) + \sum_{i=1}^{s} y_i^k \right\}$$
$$= \int_0^1 |G(\alpha)|^2 |f(\alpha)^s|^2 d\alpha$$

です. これと Lemma 8 を (34) に代入すれば

$$\#\mathscr{S}_{Z,U}^{(2)} \le N^{\frac{1}{2}} (S_s(P,Q,R;\Psi,\mathscr{U}))^{\frac{1}{2}}$$

です. さらに (33) と組み合わせて

$$S^{(2)} \le 2N^{\frac{1}{2}} (S_s(P,Q,R;\Psi,\mathscr{U}))^{\frac{1}{2}}$$

を得ます. よって $\max_j S^{(j)} = S^{(2)}$ のときは (30) より

$$S_s(P,Q,R,\Psi;\mathscr{U}) \le 8N^{\frac{1}{2}} (S_s(P,Q,R;\Psi,\mathscr{U}))^{\frac{1}{2}}$$

です. 左辺が 0 のときは示すべきことはないので左辺は 0 でないとしてよく, 両辺を

$$S_s(P,Q,R,\Psi;\mathscr{U})^{\frac{1}{2}}$$

で割ってから 2 乗すると

$$S_s(P,Q,R,\Psi;\mathscr{U}) \le 64N$$

となり, この場合は Theorem 12.1 の主張が成立します.

Note 11 (p.179, Theorem 12.1 の証明の (iii) の冒頭–p.180, 式 (12.17) の直前まで)**.** 注意ですが, $\mathscr{X}(z,\boldsymbol{u})$ では特に smoothness の条件はついていません. 単に

$$\mathscr{X}(z,\boldsymbol{u}) := \{x \in \mathbb{Z} \mid x \in [1,Q],\ x\,\mathscr{D}(M)\,\Psi'(z,\boldsymbol{u})\}$$

というだけです. (注:このノートでは $\mathscr{X}(z,\boldsymbol{u})$ を使いません.) 次に

$$\mathscr{S}^{(3)} := \Big\{ \begin{pmatrix} z,\boldsymbol{u},\boldsymbol{x} \\ w,\boldsymbol{v},\boldsymbol{y} \end{pmatrix} \in \mathscr{S}_s(P,Q,R) \mid \Psi'(z,\boldsymbol{u}), \Psi'(w,\boldsymbol{v}) \ne 0,$$
$$\text{ある } j \text{ に対して } x_j\,\mathscr{D}(M)\,\Psi'(z,\boldsymbol{u}) \text{ または } y_j\,\mathscr{D}(M)\,\Psi'(w,\boldsymbol{v}) \Big\}$$

とおくと $S^{(3)} \le \#\mathscr{S}^{(3)}$ です. また

$$\mathscr{S}_X^{(3,j)} := \left\{ \begin{matrix} 1\le z,w\le P,\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U} \\ x_j\in[1,Q]\cap\mathbb{Z},\ x_i\in\mathscr{A}(Q,R)\ (i\in\{1,\dots,s\}\setminus\{j\}) \\ y_1,\dots,y_s\in\mathscr{A}(Q,R) \end{matrix} \;\middle|\; \begin{matrix} \Psi(z,\boldsymbol{u})+p_k(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+p_k(\boldsymbol{y}) \\ \Psi'(z,\boldsymbol{u})\ne 0,\ x_j\mathscr{D}(M)\Psi'(z,\boldsymbol{u}) \end{matrix} \right\}$$
$$\mathscr{S}_Y^{(3,j)} := \left\{ \begin{matrix} 1\le z,w\le P,\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U} \\ x_1,\dots,x_s\in\mathscr{A}(Q,R) \\ y_j\in[1,Q]\cap\mathbb{Z},\ y_i\in\mathscr{A}(Q,R)\ (i\in\{1,\dots,s\}\setminus\{j\}) \end{matrix} \;\middle|\; \begin{matrix} \Psi(z,\boldsymbol{u})+p_k(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+p_k(\boldsymbol{y}) \\ \Psi'(w,\boldsymbol{v})\ne 0,\ y_j\mathscr{D}(M)\Psi'(w,\boldsymbol{v}) \end{matrix} \right\}$$

とおくと (注:x_j や y_j の smoothness を無視しても条件は弱くなるだけです),

$$\mathscr{S}^{(3)} \subset \bigcup_{j=1}^{s} \mathscr{S}_X^{(3,j)} \cup \bigcup_{j=1}^{s} \mathscr{S}_Y^{(3,j)}$$

なので被りも含めて

$$S^{(3)} \le \sum_{j=1}^{s} \#\mathscr{S}_X^{(3,j)} + \sum_{j=1}^{s} \#\mathscr{S}_Y^{(3,j)}$$

を得ます. ここで $\mathscr{S}_s(P,Q,R;\Psi;\mathscr{U})$ を定義する方程式 (24) の対称性を用いれば,

$$\#\mathscr{S}_X^{(3,j)} = \#\mathscr{S}_Y^{(3,j)} = \#\mathscr{S}_X^{(3,1)}$$

と知れるので, さらに

$$S^{(3)} \le 2s \cdot \#\mathscr{S}_X^{(3,1)} \tag{35}$$

を得ます. さてテキストと同様に

$$H(\alpha) = H(\alpha,P,M,\Psi,\mathscr{U}) \coloneqq \sum_{\substack{1\le z\le P\\ \boldsymbol{u}\in\overline{\mathscr{U}}\\ \Psi'(z,\boldsymbol{u})\neq 0}} \sum_{\substack{1\le x\le Q\\ x\mathscr{D}(M)\Psi'(z,\boldsymbol{u})}} e(\alpha(\Psi(z,\boldsymbol{u})+x^k))$$

とおき, Lemma 6 を

$$\begin{aligned}
\mathscr{X}_1 &\coloneqq \{(z,\boldsymbol{u},x) \mid z\in[1,P]\cap\mathbb{Z},\ \boldsymbol{u}\in\mathscr{U},\ \Psi'(z,\boldsymbol{u})\neq 0,\ x\,\mathscr{D}(M)\,\Psi'(z,\boldsymbol{u})\}\\
\mathscr{Y}_1 &\coloneqq \{(w,\boldsymbol{v}) \mid w\in[1,P]\cap\mathbb{Z},\ \boldsymbol{v}\in\mathscr{U}\}\\
\mathscr{X}_i,\mathscr{Y}_i &\coloneqq \mathscr{A}(Q,R)\quad (i=2,\dots,s),\quad \mathscr{Y}_{s+1}\coloneqq\mathscr{A}(Q,R)
\end{aligned}$$

および

$$\begin{aligned}
\phi_1\colon \mathscr{X}_1\to\mathbb{Z};\ (z,\boldsymbol{u},x)\mapsto\Psi(z,\boldsymbol{u})+x^k,\quad \psi_1\colon\mathscr{Y}_1\to\mathbb{Z};\ (w,\boldsymbol{v})\mapsto\Psi(w,\boldsymbol{v})\\
\phi_i,\psi_i\colon \mathscr{X}_i,\mathscr{Y}_i\to\mathbb{Z};\ x\mapsto x^k\quad (i=2,\dots,s),\quad \psi_{s+1}\colon\mathscr{Y}_{s+1}\to\mathbb{Z};\ y\mapsto y^k
\end{aligned}$$

に適用すれば

$$\begin{aligned}
f_1(\alpha)=H(\alpha,P,M,\Psi,\mathscr{U}),\quad g_1(\alpha)=F(\alpha,P,\Psi,\mathscr{U}),\\
f_i(\alpha)=g_i(\alpha)=f(\alpha,Q,R)\quad (i=2,\dots,s),\quad g_{s+1}(\alpha)=f(\alpha,Q,R)
\end{aligned}$$

となるので,

$$\begin{aligned}
\#\mathscr{S}_X^{(3,1)} &= \int_0^1 H(\alpha)\overline{F(\alpha)}|f(\alpha,Q,R)|^{2(s-1)}\overline{f(\alpha,Q,R)}d\alpha\\
&\le \int_0^1 |H(\alpha)||F(\alpha)||f(\alpha,Q,R)|^{2s-1}d\alpha
\end{aligned}$$

を得ます. ここで

$$|H(\alpha)||F(\alpha)||f(\alpha,Q,R)|^{2s-1} = |H(\alpha)||f(\alpha,Q,R)|^{s-1}\times|F(\alpha)||f(\alpha,Q,R)|^{s}$$

という分解に Cauchy–Schwarz の不等式を用いれば

$$\#\mathscr{S}_X^{(3,1)} \le \left(\int_0^1 |H(\alpha)|^2|f(\alpha)|^{2(s-1)}d\alpha\right)^{\frac12}\left(\int_0^1 |F(\alpha)|^2|f(\alpha)|^{2s}d\alpha\right)^{\frac12} \tag{36}$$

となります.

Note 12 (p.179, Theorem 12.1 の証明の (iii), 式 (12.17) より p.181 の l.2 まで)**.** 先の Note 11 に引き続き, 次に積分

$$\int_0^1 |H(\alpha)|^2|f(\alpha)|^{2(s-1)}d\alpha$$

について考えます. まず

$$\tilde{\mathscr{S}}^{(3)} \coloneqq \left\{ \begin{matrix} 1\le z,w\le P,\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U} \\ x_1\in[1,Q]\cap\mathbb{Z},\ x_2,\dots,x_s\in\mathscr{A}(Q,R) \\ y_1\in[1,Q]\cap\mathbb{Z},\ y_2,\dots,y_s\in\mathscr{A}(Q,R) \end{matrix} \middle| \begin{matrix} \Psi(z,\boldsymbol{u})+p_k(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+p_k(\boldsymbol{y}) \\ \Psi'(z,\boldsymbol{u})\neq 0,\ x_1\mathscr{D}(M)\Psi'(z,\boldsymbol{u}) \\ \Psi'(w,\boldsymbol{v})\neq 0,\ y_1\mathscr{D}(M)\Psi'(w,\boldsymbol{v}) \end{matrix} \right\} \tag{37}$$

とおきます. 次に Lemma 6 を

$$\mathscr{X}_1,\mathscr{Y}_1 \coloneqq \{(z,\boldsymbol{u},x) \mid z\in[1,P]\cap\mathbb{Z},\ \boldsymbol{u}\in\mathscr{U},\ \Psi'(z,\boldsymbol{u})\neq 0,\ x\,\mathscr{D}(M)\,\Psi'(z,\boldsymbol{u})\}$$
$$\mathscr{X}_i,\mathscr{Y}_i \coloneqq \mathscr{A}(Q,R) \quad (i=2,\dots,s)$$

に適用すれば

$$f_1(\alpha)=g_1(\alpha)=H(\alpha,P,M,\Psi,\mathscr{U}),$$
$$f_i(\alpha)=g_i(\alpha)=f(\alpha,Q,R) \quad (i\ge 2)$$

となるので,

$$\#\tilde{\mathscr{S}}^{(3)} \coloneqq \int_0^1 |H(\alpha)|^2|f(\alpha)|^{2(s-1)}d\alpha$$

です. さらに $\tilde{\mathscr{S}}^{(3)}$ の定義 (37) にある条件 $x_1\,\mathscr{D}(M)\,\Psi'(z,\boldsymbol{u})$ が成り立てば

$$x_1=dx\le Q,\quad d\le M,\quad s_0(x)\mid\Psi'(z,\boldsymbol{u})$$

なる d,x の存在がわかります. 同様に条件 $y_1\,\mathscr{D}(M)\,\Psi'(w,\boldsymbol{v})$ が成り立てば

$$y_1=ey\le Q,\quad e\le M,\quad s_0(y)\mid\Psi'(w,\boldsymbol{v})$$

なる e,y の存在がわかります. もちろん $x_1=dx$ や $y_1=ey$ と上のように書く書き表し方は一意的ではないことが多いでしょうけれど, その表し方の個数まで含めて数えれば個数は大きくなるだけです. よって, これら変数 d,e,x,y の導入と

$$x_2\rightsquigarrow x_1,\ \dots,\ x_s\rightsquigarrow x_{s-1},\quad y_2\rightsquigarrow y_1,\ \dots,\ y_s\rightsquigarrow y_{s-1}$$

という変数の名前の書き換えの下, 方程式 (24) は

$$\Psi(z,\boldsymbol{u})+d^kx^k+\sum_{i=1}^{s-1}x_i^k=\Psi(w,\boldsymbol{v})+e^ky^k+\sum_{i=1}^{s-1}y_i^k$$

と書き換わるので,

$$\mathscr{V} \coloneqq \left\{ \begin{matrix} 1\le z,w\le P,\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U} \\ d,e\in[1,M]\cap\mathbb{Z},\ x,y\in[1,Q]\cap\mathbb{Z}, \\ \boldsymbol{x},\boldsymbol{y}\in\mathscr{A}(Q,R)^{s-1} \end{matrix} \middle| \begin{matrix} \Psi(z,\boldsymbol{u})+d^kx^k+p_k(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+e^ky^k+p_k(\boldsymbol{y}) \\ \Psi'(z,\boldsymbol{u})\neq 0,\ dx\le Q,\ s_0(x)\mid\Psi'(z,\boldsymbol{u}) \\ \Psi'(w,\boldsymbol{v})\neq 0,\ ey\le Q,\ s_0(y)\mid\Psi'(w,\boldsymbol{v}) \end{matrix} \right\} \tag{38}$$

とおけば

$$\#\tilde{\mathscr{S}}^{(3)}\le\#\mathscr{V} \tag{39}$$

です. さて $\mathscr{V}$ の定義 (38) において $s_0(x)$ と $s_0(y)$ の値で元を分類することで (本当はここの "$\le$" は等号ですが)

$$\#\mathscr{V}\le\sum_{q,r\le Q}{}^{\flat}\#\mathscr{V}(q,r) \tag{40}$$

を得ます. ただしここで, 記号 $\sum^{\flat}$ は平方無縁数に渡る和を表し,

$$\mathscr{V}(q,r) \coloneqq \left\{ \begin{pmatrix} z,\boldsymbol{u},d,x,\boldsymbol{x} \\ w,\boldsymbol{v},e,y,\boldsymbol{y} \end{pmatrix}\in\mathscr{V} \;\middle|\; s_0(x)=q,\ s_0(y)=r \right\}$$

とおき, 評価

$$q = s_0(x) \le x \le Q \quad \text{および} \quad r = s_0(y) \le y \le Q$$

を用いました. 注意ですが

$$\mathscr{V}(q,r) \coloneqq \left\{ \begin{array}{c} 1\le z,w\le P,\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U} \\ d,e\in[1,M]\cap\mathbb{Z},\ x,y\in[1,Q]\cap\mathbb{Z}, \\ \boldsymbol{x},\boldsymbol{y}\in\mathscr{A}(Q,R)^{s-1} \end{array} \middle| \begin{array}{c} \Psi(z,\boldsymbol{u})+d^kx^k+p_k(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+e^ky^k+p_k(\boldsymbol{y}) \\ \Psi'(z,\boldsymbol{u})\neq 0,\ dx\le Q,\ s_0(x)=q,\ q\mid\Psi'(z,\boldsymbol{u}) \\ \Psi'(w,\boldsymbol{v})\neq 0,\ ey\le Q,\ s_0(y)=r,\ r\mid\Psi'(w,\boldsymbol{v}) \end{array} \right\}$$

と書けます. テキストと同様に

$$\begin{aligned} G_q(\alpha) = G_q(\alpha,P,\Psi,\mathscr{U}) &\coloneqq \sum_{\substack{1\le z\le P \\ \boldsymbol{u}\in\mathscr{U} \\ \Psi'(z,\boldsymbol{u})\neq 0 \\ q\mid\Psi'(z,\boldsymbol{u})}} e(\alpha\Psi(z,\boldsymbol{u})), \\ F_q(\alpha) = F_q(Q,M) &\coloneqq \sum_{\substack{1\le dx\le Q \\ d\le M \\ s_0(x)=q}} e(\alpha(d^kx^k)) \\ I(\alpha) = I(\alpha,P,Q,M,\Psi,\mathscr{U}) &\coloneqq \sum_{q\le Q}{}^{\flat} G_q(\alpha)F_q(\alpha) \\ &= \sum_{q\le Q}{}^{\flat} G_q(\alpha) \sum_{\substack{1\le dx\le Q \\ d\le M \\ s_0(x)=q}} e(\alpha(d^kx^k)) \end{aligned}$$

とおき, 与えられた square-free numbers q,r に対して Lemma 6 を

$$\begin{aligned} \mathscr{X}_1 &\coloneqq \{(z,\boldsymbol{u}) \mid z\in[1,P]\cap\mathbb{Z},\ \boldsymbol{u}\in\mathscr{U},\ q \mid s_0(\Psi'(z,\boldsymbol{u}))\} \\ \mathscr{Y}_1 &\coloneqq \{(w,\boldsymbol{v}) \mid w\in[1,P]\cap\mathbb{Z},\ \boldsymbol{v}\in\mathscr{U},\ r \mid s_0(\Psi'(w,\boldsymbol{v}))\} \\ \mathscr{X}_2 &\coloneqq \{(d,x)\in\mathbb{N}^2 \mid d\le M,\ dx\le Q,\ s_0(x)=q\} \\ \mathscr{Y}_2 &\coloneqq \{(e,y)\in\mathbb{N}^2 \mid e\le M,\ ey\le Q,\ s_0(y)=r\} \\ \mathscr{X}_i,\mathscr{Y}_i &\coloneqq \mathscr{A}(Q,R) \quad (i=3,\dots,s+1) \end{aligned}$$

および

$$\begin{gathered} \phi_1,\psi_1\colon \mathscr{X}_1,\mathscr{Y}_1\to\mathbb{Z};\ (z,\boldsymbol{u})\mapsto\Psi(z,\boldsymbol{u}), \\ \phi_2,\psi_2\colon \mathscr{X}_2,\mathscr{Y}_2\to\mathbb{Z};\ (d,x)\mapsto d^kx^k \\ \phi_i,\psi_i\colon \mathscr{X}_i,\mathscr{Y}_i\to\mathbb{Z};\ x\mapsto x^k \quad (i=3,\dots,s+1) \end{gathered}$$

に適用すれば

$$\begin{gathered} f_1(\alpha)=G_q(\alpha,P,\Psi,\mathscr{U}), \quad g_1(\alpha)=G_r(\alpha,P,\Psi,\mathscr{U}) \\ f_2(\alpha)=F_q(\alpha,Q,M), \quad g_2(\alpha)=F_r(\alpha,Q,M), \\ f_i(\alpha)=g_i(\alpha)=f(\alpha,Q,R) \quad (i=3,\dots,s) \end{gathered}$$

となるので

$$\#\mathscr{V}(q,r)=\int_0^1 G_q(\alpha)F_q(\alpha)\overline{G_r(\alpha)F_r(\alpha)}|f(\alpha)|^{2(s-1)}d\alpha$$

を得ます. これを q, r に渡って足し上げ, (40) を用いることで

$$\begin{aligned}
\#\mathscr{V} &\le \sum_{q,r\le Q}^{\flat}\int_0^1 G_q(\alpha)F_q(\alpha)\overline{G_r(\alpha)F_r(\alpha)}|f(\alpha)|^{2(s-1)}d\alpha \\
&= \int_0^1 \Big(\sum_{q\le Q}^{\flat} G_q(\alpha)F_q(\alpha)\Big)\overline{\Big(\sum_{r\le Q}^{\flat} G_r(\alpha)F_r(\alpha)\Big)}|f(\alpha)|^{2(s-1)}d\alpha \qquad (41)\\
&= \int_0^1 |I(\alpha)|^2|f(\alpha)|^{2(s-1)}d\alpha
\end{aligned}$$

を得ます.

Note 13 (p.179, Theorem 12.1 の証明の (iii), p.181 の l.3 以後)**.** まず最初の Cauchy–Schwarz 不等式の適用ですがテキストの評価は

$$\begin{aligned}
|I(\alpha)|^2 &\le \sum_{q\le Q}^{\flat}|G_q(\alpha)|^2\sum_{q\le Q}^{\flat}|F_q(\alpha)|^2 \\
&= \sum_{q\le Q}^{\flat}|G_q(\alpha)|^2\sum_{q\le Q}^{\flat}\Big|\sum_{\substack{dx\le Q\\ d\le M\\ s_0(x)=q}} e(\alpha(d^kx^k))\Big|^2
\end{aligned}$$

の誤植です.（右辺の 3 つ目の和のあとの 2 乗が抜け落ちています. また q の範囲はテキストとは異なるものを用いています.）さて右辺の後半の和

$$\sum\nolimits_1 := \sum_{q\le Q}^{\flat}\Big|\sum_{\substack{dx\le Q\\ d\le M\\ s_0(x)=q}} e(\alpha(d^kx^k))\Big|^2$$

を評価します. 指数関数は 1 で抑え, 内側の和を 2 重和に書き換え, この和は

$$\sum\nolimits_1 \le \sum_{q\le Q}^{\flat}\Big(\sum_{\substack{x\le Q\\ s_0(x)=q}}\sum_{\substack{d\le Q/x\\ d\le M}} 1\Big)^2$$

となります. 内側の和に Cauchy–Schwarz 不等式を用いれば

$$\sum\nolimits_1 \le \sum_{q\le Q}^{\flat}\Big(\sum_{\substack{x\le Q\\ s_0(x)=q}} 1\Big)\sum_{\substack{x\le Q\\ s_0(x)=q}}\Big(\sum_{\substack{d\le Q/x\\ d\le M}} 1\Big)^2.$$

ここで Lemma 12.2 より（この Lemma の評価は q に関して一様でした）

$$\sum_{\substack{x\le Q\\ s_0(x)=q}} 1 \ll Q^{\frac{\varepsilon}{2}}$$

なのでさらに

$$\begin{aligned}
\sum\nolimits_1 &\le Q^{\frac{\varepsilon}{2}}\sum_{q\le Q}^{\flat}\sum_{\substack{x\le Q\\ s_0(x)=q}}\Big(\sum_{\substack{d\le Q/x\\ d\le M}} 1\Big)^2 \le Q^{\frac{\varepsilon}{2}}\sum_{x\le Q}\min\Big(\frac{Q^2}{x^2}, M^2\Big) \\
&= Q^{\frac{\varepsilon}{2}}\Big(\sum_{x\le Q/M} M^2 + \sum_{Q/M<x\le Q}\frac{Q^2}{x^2}\Big) \ll Q^{\frac{\varepsilon}{2}}\Big(\frac{Q}{M}\cdot M^2 + Q^2\cdot\frac{1}{Q/M}\Big) \le QMP^{\frac{\varepsilon}{2}}
\end{aligned}$$

と抑える事ができます.（テキストとは少し違う方法をとりました.）以上より,

$$|I(\alpha)|^2 \ll QMP^{\frac{\varepsilon}{2}} \sum_{q\leq Q}^{\flat} |G_q(\alpha)|^2$$

です. したがって, (41) より

$$\#\mathscr{V} \leq QMP^{\frac{\varepsilon}{2}} \sum_{q\leq Q}^{\flat} \int_0^1 |G_q(\alpha)|^2 |f(\alpha)|^{2(s-1)} d\alpha \tag{42}$$

を得ます. 最後に右辺の

$$\sum\nolimits_2 \coloneqq \sum_{q\leq Q}^{\flat} \int_0^1 |G_q(\alpha)|^2 |f(\alpha)|^{2(s-1)} d\alpha$$

の部分を考察しましょう. まず和を開いて直交性を用いると

$$\sum\nolimits_2 = \sum_{q\leq Q}^{\flat} \sum_{\substack{1\leq z,w\leq P \\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U} \\ \Psi'(z,\boldsymbol{u}),\Psi'(w,\boldsymbol{v})\neq 0 \\ q|\Psi'(z,\boldsymbol{u}),\ q|\Psi'(w,\boldsymbol{v})}} \sum_{\substack{\boldsymbol{x},\boldsymbol{y}\in\mathscr{A}(Q,R)^{s-1} \\ \Psi(z,\boldsymbol{u})+p(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+p(\boldsymbol{y})}} 1$$

となります. ここで外側 2 つの和を入れ替えて

$$\sum\nolimits_2 = \sum_{\substack{1\leq z,w\leq P \\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U} \\ \Psi'(z,\boldsymbol{u}),\Psi'(w,\boldsymbol{v})\neq 0}} \left(\sum_{\substack{q\leq Q \\ q|(\Psi'(z,\boldsymbol{u}),\Psi'(w,\boldsymbol{v}))}}^{\flat} 1 \right) \sum_{\substack{\boldsymbol{x},\boldsymbol{y}\in\mathscr{A}(Q,R)^{s-1} \\ \Psi(z,\boldsymbol{u})+p(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+p(\boldsymbol{y})}} 1 \tag{43}$$

を得ます. 内側の括弧内の和は約数関数 $\tau(n)$ を用いて

$$\sum_{\substack{q\leq Q \\ q|(\Psi'(z,\boldsymbol{u}),\Psi'(w,\boldsymbol{v}))}}^{\flat} 1 \leq \tau((\Psi'(z,\boldsymbol{u}),\Psi'(w,\boldsymbol{v}))) \ll_{\varepsilon,D} \left(\max_{\substack{1\leq z\leq P \\ \boldsymbol{u}\in\mathscr{U}}} |\Psi'(z,\boldsymbol{u})| \right)^{\frac{\varepsilon}{2D}} \tag{44}$$

と評価されます. ただしここで D は $\Psi(Z,\boldsymbol{U})$ の total degree です. そこで

$$\Psi(Z,\boldsymbol{U}) = \sum_{\substack{i,j_1,\dots,j_k\geq 0 \\ i+j_1+\cdots+j_k\leq D}} c_{i,j_1,\dots,j_k} Z^i U_1^{j_1}\cdots U_k^{j_k}$$

とおけば,

$$\Psi'(Z,\boldsymbol{U}) = \sum_{\substack{i\geq 1,\, j_1,\dots,j_k\geq 0 \\ i+j_1+\cdots+j_k\leq D}} i c_{i,j_1,\dots,j_k} Z^{i-1} U_1^{j_1}\cdots U_k^{j_k}$$

なので $\mathscr{U}\subset[1,CP]^t$ の仮定と記号

$$c_{\max} \coloneqq \max_{\substack{i,j_1,\dots,j_k\geq 0 \\ i+j_1+\cdots+j_k\leq D-1}} |c_{i+1,j_1,\dots,j_k}|$$

のもと,

$$\max_{\substack{1\leq z\leq P \\ \boldsymbol{u}\in\mathscr{U}}} |\Psi'(z,\boldsymbol{u})| \leq c_{\max} C^D D P^D \sum_{\substack{i,j_1,\dots,j_k\geq 0 \\ i+j_1+\cdots+j_k\leq D-1}} 1 \ll_{c_{\max},C,D} P^D$$

です. よって (44) より

$$\sum_{\substack{q\le Q\\ q\mid(\Psi'(z,\boldsymbol{u}),\Psi'(w,\boldsymbol{v}))}}^{\flat} 1 \ll_{c_{\max},C,D} P^{\frac{\varepsilon}{2}}$$

であり, これを (43) に代入すれば

$$\begin{aligned}\sum\nolimits_2 &\ll_{c_{\max},C,D} P^{\frac{\varepsilon}{2}} \sum_{\substack{1\le z,w\le P\\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U}\\ \Psi'(z,\boldsymbol{u}),\Psi'(w,\boldsymbol{v})\neq 0}} \sum_{\substack{\boldsymbol{x},\boldsymbol{y}\in\mathscr{A}(Q,R)^{s-1}\\ \Psi(z,\boldsymbol{u})+p(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+p(\boldsymbol{y})}} 1\\ &\le P^{\frac{\varepsilon}{2}} S_{s-1}(P,Q,R;\Psi;\mathscr{U})\end{aligned}$$

が成立して (39) と (42) より

$$\#\tilde{\mathscr{S}}^{(3)} \ll_{c_{\max},C,D} QMP^{\varepsilon} S_{s-1}(P,Q,R;\Psi;\mathscr{U})$$

を得ます. テキストと同様に $\max_j S^{(j)} = S^{(3)}$ のときは (30), (35) と (36) より

$$S_s(P,Q,R) \ll_{s,c_{\max},C,D} (QMP^{\varepsilon} S_{s-1}(P,Q,R))^{\frac{1}{2}} S_s(P,Q,R)^{\frac{1}{2}}$$

です. 左辺が 0 のときは示すべきことはないので左辺は 0 でないとしてよく, 両辺を

$$S_s(P,Q,R)^{\frac{1}{2}}$$

で割ってから 2 乗すると

$$S_s(P,Q,R) \ll_{s,c_{\max},C,D} QMP^{\varepsilon} S_{s-1}(P,Q,R)$$

となりこの場合は Theorem 12.1 の主張が成立します. (Theorem 12.1 では implicit constant は $s, c_{\max}, C, D$ に依存してよいです.)

Note 14 (p.181, Theorem 12.1 の証明の (iv), p.183 の l.11 まで)**.** 集合

$$\mathscr{S}^{(4)} \coloneqq \left\{ \begin{pmatrix} z,\boldsymbol{u},\boldsymbol{x}\\ w,\boldsymbol{v},\boldsymbol{y}\end{pmatrix} \in \mathscr{S}_s(P,Q,R) \;\middle|\; \begin{array}{c} x_1,\dots,x_s,y_1,\dots,y_s>M\\ \Psi'(z,\boldsymbol{u}),\Psi'(w,\boldsymbol{v})\neq 0\\ \forall j,\ x_j\ \mathscr{D}(M)\ \Psi'(z,\boldsymbol{u})\ \text{と}\ y_j\ \mathscr{D}(M)\ \Psi'(w,\boldsymbol{v})\ \text{は成立しない}\end{array} \right\}$$

を考えましょう. もちろん $S^{(4)} = \#\mathscr{S}^{(4)}$ です. この $\mathscr{S}^{(4)}$ の任意の元と任意の $i = 1,\dots,s$ に対し

$$x_i = m_i\xi_i, \quad (m_i, \Psi'(z,\boldsymbol{u})) = 1, \quad m_i \in (M, MR]\cap\mathbb{Z}, \quad \xi_i \in \mathscr{A}(Q/M,R) \tag{45}$$

なる自然数 m_i, ξ_i が少なくとも 1 つ存在することを示します. まず,

$$\mu_i \coloneqq \prod_{\substack{p^v\| x_i\\ p\nmid\Psi'(z,\boldsymbol{u})}} p^v$$

とおきましょう. すると

$$x_i/\mu_i = \prod_{\substack{p^v\| x_i\\ p\mid\Psi'(z,\boldsymbol{u})}} p^v$$

なので x_i/μ_i の素因数はすべて $\Psi'(z,\boldsymbol{u})$ の約数です. ここで $\mathscr{S}^{(4)}$ の定義の条件より $x_i\,\mathscr{D}(M)\,\Psi'(z,\boldsymbol{u})$ ではないので, $\mu_i > M$ でなければいけません. また x_i は R-smooth だったので μ_i も R-smooth です. ここで素数 $p_1,\cdots,p_r \le R$ によって

$$\mu_i = p_1\cdots p_r$$

と書きましょう. すると $\mu_j > M$ だったのである $t \in \{1,\dots,r\}$ が存在して,

$$p_1 \cdots p_{t-1} \le M < p_1 \cdots p_t$$

とできます. もちろん $p_t \le R$ だったので, この不等式から

$$M < p_1 \cdots p_t \le p_1 \cdots p_{t-1} R \le MR$$

がわかります. そこで $m_i \coloneqq p_1 \cdots p_t$, $\xi_i \coloneqq p_{t+1} \cdots p_r$ とおきます. 定義より $(\mu_i, \Psi'(z,\boldsymbol{u})) = 1$ だったことと $\xi_i = x_i/m_i \le Q/M$ より, この μ_i, ξ_i は条件 (45) を満たしています. 同様に $\mathscr{S}^{(4)}$ の任意の元に対し

$$y_i = \ell_i \eta_i, \quad (\ell_i, \Psi'(w,\boldsymbol{v})) = 1, \quad \ell_i \in (M, MR] \cap \mathbb{Z}, \quad \eta_i \in \mathscr{A}(Q/M, R)$$

なる自然数 ℓ_i, η_i の存在もわかります. もちろんこのような m_i, ξ_i や ℓ_i, η_i は一意的には定まりませんが, それらをすべて数えてしまえば個数は大きくなります. よって再度

$$\xi_1 \rightsquigarrow x_1,\ \dots,\ \xi_s \rightsquigarrow x_s,\ \eta_1 \rightsquigarrow y_1,\ \dots,\ \eta_s \rightsquigarrow y_s$$

等と変数の名前をつけ直せば

$$S^{(4)} \le \#\mathscr{W} \tag{46}$$

ただし $a \coloneqq m_1 \cdots m_s$ および $b \coloneqq \ell_1 \cdots \ell_s$ と書いて

$$\mathscr{W} \coloneqq \left\{ \begin{matrix} 1 \le z,w \le P,\ \boldsymbol{u},\boldsymbol{v} \in \mathscr{U} \\ \boldsymbol{m},\boldsymbol{\ell} \in ((M,MR] \cap \mathbb{Z})^s \\ \boldsymbol{x},\boldsymbol{y} \in \mathscr{A}(Q/M,R)^s \end{matrix} \;\middle|\; \begin{matrix} \Psi(z,\boldsymbol{u}) + \sum_{i=1}^s m_i^k x_i^k = \Psi(w,\boldsymbol{v}) + \sum_{i=1}^s \ell_i^k y_i^k \\ (a, \Psi'(z,\boldsymbol{u})) = (b, \Psi'(w,\boldsymbol{v})) = 1 \end{matrix} \right\},$$

とおきました. ここで $\boldsymbol{m}$ と $\boldsymbol{\ell}$ の値で分類すべく

$$\mathscr{W}(\boldsymbol{m},\boldsymbol{\ell}) \coloneqq \left\{ \begin{matrix} 1 \le z,w \le P,\ \boldsymbol{u},\boldsymbol{v} \in \mathscr{U} \\ \boldsymbol{x},\boldsymbol{y} \in \mathscr{A}(Q/M,R)^s \end{matrix} \;\middle|\; \begin{matrix} \Psi(z,\boldsymbol{u}) + \sum_{i=1}^s m_i^k x_i^k = \Psi(w,\boldsymbol{v}) + \sum_{i=1}^s \ell_i^k y_i^k \\ (a, \Psi'(z,\boldsymbol{u})) = (b, \Psi'(w,\boldsymbol{v})) = 1 \end{matrix} \right\}$$

とおけば,

$$S^{(4)} \le \sum_{\substack{M < m_1,\dots,m_s \le MR \\ M < \ell_1,\dots,\ell_s \le MR}} \#\mathscr{W}(\boldsymbol{m},\boldsymbol{\ell})$$

となります. さてテキストと同様に

$$F(\alpha,a) = F(\alpha,a,P,\Psi,\mathscr{U}) \coloneqq \sum_{\substack{1 \le z \le P \\ \boldsymbol{u} \in \mathscr{U} \\ (a,\Psi'(z,\boldsymbol{u}))=1}} e(\alpha \Psi(z,\boldsymbol{u}))$$

$$f(\alpha,m) = f(\alpha,m,Q,M,R) \coloneqq \sum_{x \in \mathscr{A}(Q/M,R)} e(\alpha m^k x^k)$$

とおき, Lemma 6 を

$$\begin{aligned} \mathscr{X}_1 &\coloneqq \{(z,\boldsymbol{u}) \mid z \in [1,P] \cap \mathbb{Z},\ \boldsymbol{u} \in \mathscr{U},\ (a, \Psi'(z,\boldsymbol{u})) = 1\} \\ \mathscr{Y}_1 &\coloneqq \{(w,\boldsymbol{v}) \mid w \in [1,P] \cap \mathbb{Z},\ \boldsymbol{v} \in \mathscr{U},\ (b, \Psi'(w,\boldsymbol{v})) = 1\} \\ \mathscr{X}_i, \mathscr{Y}_i &\coloneqq \mathscr{A}(Q/M,R) \quad (i = 2,\dots,s+1) \end{aligned}$$

および

$$\begin{aligned} \phi_1, \psi_1 &\colon \mathscr{X}_1, \mathscr{Y}_1 \to \mathbb{Z};\ (z,\boldsymbol{u}) \mapsto \Psi(z,\boldsymbol{u}) \\ \phi_i &\colon \mathscr{X}_i \to \mathbb{Z};\ x \mapsto m_i^k x^k \quad (i = 2,\dots,s+1) \end{aligned}$$

$$\psi_i\colon \mathscr{Y}_i \to \mathbb{Z};\ x \mapsto \ell_i^k x^k \quad (i = 2, \dots, s+1)$$

に適用すれば

$$f_1(\alpha) = F(\alpha, a, P, M, \Psi, \mathscr{U}), \quad g_1(\alpha) = F(\alpha, b, P, M, \Psi, \mathscr{U}),$$
$$f_i(\alpha) = f(\alpha, m_i, Q, R), \quad g_i(\alpha) = f(\alpha, \ell_i, Q, R) \quad (i = 2, \dots, s+1)$$

となるので,

$$\begin{aligned}\#\mathscr{W}(\boldsymbol{m}, \boldsymbol{\ell}) &= \int_0^1 F(\alpha, a)\overline{F(\alpha, b)} \prod_{i=1}^{s} (f(\alpha, m_i)\overline{f(\alpha, \ell_i)}) d\alpha \\ &\leq \int_0^1 |F(\alpha, a)||F(\alpha, b)| \prod_{i=1}^{s} (|f(\alpha, m_i)||f(\alpha, \ell_i)|) d\alpha\end{aligned}$$

を得ます. これを (46) に代入すれば

$$S^{(4)} \leq \sum_{\substack{M < m_1, \dots, m_s \leq MR \\ M < \ell_1, \dots, \ell_s \leq MR}} \int_0^1 |F(\alpha, a)||F(\alpha, b)| \prod_{i=1}^{s} (|f(\alpha, m_i)||f(\alpha, \ell_i)|) d\alpha$$

ここに Hölder の不等式を指数

$$(p_1, \dots, p_{2s}) = (2s, \dots, 2s)$$

と分解

$$\begin{aligned}&|F(\alpha, a)||F(\alpha, b)| \prod_{i=1}^{s} (|f(\alpha, m_i)||f(\alpha, \ell_i)|) \\ &= \left(\prod_{i=1}^{s} |F(\alpha, a)|^{\frac{1}{s}} |f(\alpha, m_i)| \right) \left(\prod_{i=1}^{s} |F(\alpha, b)|^{\frac{1}{s}} |f(\alpha, \ell_i)| \right)\end{aligned}$$

に用いれば,

$$\begin{aligned}S^{(4)} \leq \prod_{i=1}^{s} \Bigg(&\sum_{\substack{M < m_1, \dots, m_s \leq MR \\ M < \ell_1, \dots, \ell_s \leq MR}} \int_0^1 |F(\alpha, a)|^2 |f(\alpha, m_i)|^{2s} d\alpha \Bigg)^{\frac{1}{2s}} \\ &\times \prod_{i=1}^{s} \Bigg(\sum_{\substack{M < m_1, \dots, m_s \leq MR \\ M < \ell_1, \dots, \ell_s \leq MR}} \int_0^1 |F(\alpha, b)|^2 |f(\alpha, \ell_i)|^{2s} d\alpha \Bigg)^{\frac{1}{2s}}\end{aligned}$$

を得ます. ここで $\boldsymbol{m}$ と $\boldsymbol{\ell}$ の間の対称性より

$$\begin{aligned}&\sum_{\substack{M < m_1, \dots, m_s \leq MR \\ M < \ell_1, \dots, \ell_s \leq MR}} \int_0^1 |F(\alpha, a)|^2 |f(\alpha, m_i)|^{2s} d\alpha \\ &= \sum_{\substack{M < m_1, \dots, m_s \leq MR \\ M < \ell_1, \dots, \ell_s \leq MR}} \int_0^1 |F(\alpha, b)|^2 |f(\alpha, \ell_i)|^{2s} d\alpha\end{aligned}$$

となり $m_1,\dots,m_s$ の間の対称性より

$$\sum_{\substack{M<m_1,\dots,m_s\le MR\\ M<\ell_1,\dots,\ell_s\le MR}}\int_0^1 |F(\alpha,a)|^2|f(\alpha,m_i)|^{2s}d\alpha$$
$$=\sum_{\substack{M<m_1,\dots,m_s\le MR\\ M<\ell_1,\dots,\ell_s\le MR}}\int_0^1 |F(\alpha,a)|^2|f(\alpha,m_1)|^{2s}d\alpha$$

ので, さらに

$$\begin{aligned} S^{(4)} &\le \prod_{i=1}^{s}\Bigg(\sum_{\substack{M<m_1,\dots,m_s\le MR\\ M<\ell_1,\dots,\ell_s\le MR}}\int_0^1 |F(\alpha,a)|^2|f(\alpha,m_1)|^{2s}d\alpha\Bigg)^{\frac{1}{s}}\\ &=\sum_{\substack{M<m_1,\dots,m_s\le MR\\ M<\ell_1,\dots,\ell_s\le MR}}\int_0^1 |F(\alpha,a)|^2|f(\alpha,m_1)|^{2s}d\alpha =: I \end{aligned}\tag{47}$$

を得ます. この右辺 I について考えましょう. まず整数 a,m に対して, Lemma 6 を

$$\mathscr{X}_1,\mathscr{Y}_1 \coloneqq \{(z,\boldsymbol{u}) \mid z\in[1,P]\cap\mathbb{Z},\ \boldsymbol{u}\in\mathscr{U},\ (a,\Psi'(z,\boldsymbol{u}))=1\}$$
$$\mathscr{X}_i,\mathscr{Y}_i \coloneqq \mathscr{A}(Q/M,R)\quad (i=2,\dots,s+1)$$

および

$$\phi_1,\psi_1\colon \mathscr{X}_1,\mathscr{Y}_1\to\mathbb{Z};\ (z,\boldsymbol{u})\mapsto\Psi(z,\boldsymbol{u})$$
$$\phi_i,\psi_i\colon \mathscr{X}_i,\mathscr{Y}_i\to\mathbb{Z};\ x\mapsto m^k x^k\quad (i=2,\dots,s+1)$$

に適用すれば

$$f_1(\alpha)=g_1(\alpha)=F(\alpha,a)$$
$$f_i(\alpha)=g_i(\alpha)=f(\alpha,m)\quad (i=2,\dots,s+1)$$

となるので,

$$\int_0^1 |F(\alpha,a)|^2|f(\alpha,m)|^{2s}d\alpha$$
$$=\#\left\{\begin{matrix}1\le z,w\le P,\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U}\\ \boldsymbol{x},\boldsymbol{y}\in\mathscr{A}(Q/M,R)\end{matrix}\ \middle|\ \begin{matrix}\Psi(z,\boldsymbol{u})+m^k p_k(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+m^k p_k(\boldsymbol{y})\\ (a,\Psi'(z,\boldsymbol{u}))=(a,\Psi'(w,\boldsymbol{v}))=1\end{matrix}\right\}$$

を得ます. ここで $m\mid a$ の仮定のもと, 条件

$$(a,\Psi'(z,\boldsymbol{u}))=(a,\Psi'(w,\boldsymbol{v}))=1$$

を条件

$$(m,\Psi'(z,\boldsymbol{u}))=(m,\Psi'(w,\boldsymbol{v}))=1$$

に弱めれば

$$\int_0^1 |F(\alpha,a)|^2|f(\alpha,m)|^{2s}d\alpha\le \#\tilde{\mathscr{W}}(m)$$

ただし

$$\tilde{\mathscr{W}}(m)\coloneqq\left\{\begin{matrix}1\le z,w\le P,\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U}\\ \boldsymbol{x},\boldsymbol{y}\in\mathscr{A}(Q/M,R)\end{matrix}\ \middle|\ \begin{matrix}\Psi(z,\boldsymbol{u})+m^k p_k(\boldsymbol{x})=\Psi(w,\boldsymbol{v})+m^k p_k(\boldsymbol{y})\\ (m,\Psi'(z,\boldsymbol{u}))=(m,\Psi'(w,\boldsymbol{v}))=1\end{matrix}\right\}$$

を得ます. よって,

$$I \leq \sum_{\substack{M<m_1,\dots,m_s\leq MR \\ M<\ell_1,\dots,\ell_s\leq MR}} \#\tilde{\mathscr{W}}(m_1)$$

ですが, もはや右辺の各項は $m_2,\dots,m_s,\ell_1,\dots,\ell_s$ に依存しないので, これらの個数 $(=(MR)^{2s-1})$ を数え上げて (47) を思い出し,

$$S^{(4)} \leq (MR)^{2s-1} \sum_{M<m\leq MR} \#\tilde{\mathscr{W}}(m) \tag{48}$$

を得ます.

Note 15 (p.183 の l.12 から l.20)**.** 引用されている補題は次のようにまとめることができます (いわゆる Hensel の補題の一例です):

Lemma 11. 素数 p, 自然数 σ と整数係数多項式 $f(X)$ に対して, 合同方程式

$$f(X) \equiv 0 \pmod{p^\sigma} \tag{49}$$

の根 $x \pmod{p^\sigma}$ であって

$$(p, f'(x)) = 1 \tag{50}$$

なるものの個数は $\deg f$ を超えない. つまり

$$\#\{x \pmod{p^\sigma} \in \mathbb{Z}/p^\sigma\mathbb{Z} \mid f(x) \equiv 0 \pmod{p^\sigma},\ (p, f'(x)) = 1\} \leq \deg f$$

が成り立つ.

Proof. まず, 与えられた多項式 $f(X)$ がそもそも $f(X) \equiv 0 \pmod{p}$ であれば (50) を満たす解は存在しないので, 多項式として $f(X) \not\equiv 0 \pmod{p}$ と仮定してよいです. さらに, 方程式 (49) の条件 (50) を満たす根全体の集合を X_σ と書きましょう:

$$X_\sigma \coloneqq \{x \pmod{p^\sigma} \mid f(x) \equiv 0 \pmod{p^\sigma},\ (f'(x), p) = 1\}.$$

指数 σ に関する帰納法で示します.

まず, $\sigma = 1$ の場合は合同方程式 (49) は体 $\mathbb{F}_p$ 上の自明でない $\deg f$ 次方程式なのでそもそも高々$\deg f$ 個しか根を持ち得ず主張が成立します.

次に, $\tau \geq 1$ とし, $\sigma = \tau$ の場合に主張が成立したとして $\sigma = \tau + 1$ の場合を示します. まず, 任意の $x \pmod{p^{\tau+1}} \in X_{\tau+1}$ に対して, (49) と (50) の $(\bmod p^\tau)$-reduction をとれば

$$X_{\tau+1} \to X_\tau\,;\, x \pmod{p^{\tau+1}} \mapsto x \pmod{p^\tau} \tag{51}$$

という写像が定まります. 帰納法の仮定より $\#X_\tau \leq \deg f$ なので, あとは ϕ が単射であることを示せば十分です. そこで整数 x, y であって

$$\begin{cases} x \pmod{p^{\tau+1}}, y \pmod{p^{\tau+1}} \in X_{\tau+1} \text{ および} \\ \phi(x \pmod{p^{\tau+1}}) = \phi(y \pmod{p^{\tau+1}}) \end{cases} \tag{52}$$

なるものを任意に取ります. このとき $x \equiv y \pmod{p^{\tau+1}}$ を示せば十分です. まず, (52) の後半は $x \equiv y \pmod{p^\tau}$ ということにほかなりません. よって, ある $z \in \mathbb{Z}$ に

よって $y = x + p^\tau z$ と書くことができます. さて

$$f(X) = \sum_{i=0}^{d} a_i X^i$$

と書くと,

$$\begin{aligned} f(X+H) &= \sum_{n=0}^{d} a_n (X+H)^n = \sum_{n=0}^{d} a_n \sum_{i=0}^{n} \binom{n}{i} X^{n-i} H^i = \sum_{i=0}^{d} H^i \sum_{n=i}^{d} a_n \binom{n}{i} X^{n-i} \\ &= \sum_{n=0}^{d} a_n X^n + H \sum_{n=1}^{d} n a_n X^{n-1} + H^2 \sum_{i=2}^{d} H^{i-2} \sum_{n=i}^{d} a_n \binom{n}{i} X^{n-i} \\ &= f(X) + f'(X)H + H^2 \sum_{i=0}^{d-2} H^i \sum_{n=i+2}^{d} a_n \binom{n}{i+2} X^{n-i-2} \end{aligned}$$

なので $X = x$ および $H = p^\tau z$ とおいて, $2\tau \geq \tau + 1$ に注意して

$$f(y) = f(x + p^\tau z) \equiv f(x) + f'(x) p^\tau z \pmod{p^{\tau+1}}$$

を得ます. また (52) の前半より $f(x) \equiv f(y) \equiv 0 \pmod{p^{\tau+1}}$ なので

$$f'(x) p^\tau z \equiv 0 \pmod{p^{\tau+1}}$$

を得ます. これはつまり $p^{\tau+1} \mid f'(x) p^\tau z$ またはさらに $p \mid f'(x) z$ を意味します. 再び (52) の前半より $(f'(x), p) = 1$ なので, 最終的に $p \mid z$ を得ます. したがって

$$y = x + p^\tau z \equiv x \pmod{p^{\tau+1}}$$

を得て (51) の単射性を得ました. これで証明を終わります. □

Note 16 (p.183, l.(−5)–Theorem 12.1 の場合 (iv) の終わりまで)**.** まず, Note 14 で導入した $\tilde{\mathscr{W}}(m)$ の条件

$$\Psi(z, \boldsymbol{u}) + m^k p_k(\boldsymbol{x}) = \Psi(w, \boldsymbol{v}) + m^k p_k(\boldsymbol{y})$$

より $\Psi(z, \boldsymbol{u}) \equiv \Psi(w, \boldsymbol{v}) \pmod{m^k}$ が成立するので, $\tilde{\mathscr{W}}(m)$ は

$$\tilde{\mathscr{W}}(m) \coloneqq \left\{ \begin{matrix} 1 \leq z, w \leq P,\ \boldsymbol{u}, \boldsymbol{v} \in \mathscr{U} \\ \boldsymbol{x}, \boldsymbol{y} \in \mathscr{A}(Q/M, R)^s \end{matrix} \;\middle|\; \begin{matrix} \Psi(z,\boldsymbol{u}) + m^k p_k(\boldsymbol{x}) = \Psi(w,\boldsymbol{v}) + m^k p_k(\boldsymbol{y}) \\ \Psi(z,\boldsymbol{u}) \equiv \Psi(w,\boldsymbol{v}) \pmod{m^k} \\ (m, \Psi'(z,\boldsymbol{u})) = (m, \Psi'(w,\boldsymbol{v})) = 1 \end{matrix} \right\}$$

と書いても良いことに注意します. そこでこの剰余 $\Psi(z, \boldsymbol{u}) \equiv \Psi(w, \boldsymbol{v}) \pmod{m^k}$ の値によって分類すべく整数 $h = 1, \ldots, m^k$ に対して

$$\tilde{\mathscr{W}}(m, h) \coloneqq \left\{ \begin{matrix} 1 \leq z, w \leq P,\ \boldsymbol{u}, \boldsymbol{v} \in \mathscr{U} \\ \boldsymbol{x}, \boldsymbol{y} \in \mathscr{A}(Q/M, R)^s \end{matrix} \;\middle|\; \begin{matrix} \Psi(z,\boldsymbol{u}) + m^k p_k(\boldsymbol{x}) = \Psi(w,\boldsymbol{v}) + m^k p_k(\boldsymbol{y}) \\ (m, \Psi'(z,\boldsymbol{u})) = (m, \Psi'(w,\boldsymbol{v})) = 1 \\ \Psi(z,\boldsymbol{u}) \equiv \Psi(w,\boldsymbol{v}) \equiv h \pmod{m^k} \end{matrix} \right\}$$

とおきましょう. すると

$$\#\tilde{\mathscr{W}}(m) = \sum_{h=1}^{m^k} \#\tilde{\mathscr{W}}(m, h) \tag{53}$$

となります. そこで

$$\tilde{g}(\alpha,h,m)=\tilde{g}(\alpha,h,m,P,\Psi,\mathscr{U}):=\sum_{\substack{1\le z\le P\\ \boldsymbol{u}\in\mathscr{U}\\ (m,\Psi'(z,\boldsymbol{u}))=1\\ \Psi(z,\boldsymbol{u})\equiv h\ (\mathrm{mod}\ m^k)}}e(\alpha\Psi(z,\boldsymbol{u}))$$

とおいて, Lemma 6 を

$$\begin{aligned}\mathscr{X}_1,\mathscr{Y}_1&:=\{(z,\boldsymbol{u})\mid z\in[1,P]\cap\mathbb{Z},\ \boldsymbol{u}\in\mathscr{U},\\ &\qquad (m,\Psi'(z,\boldsymbol{u}))=1,\ \Psi(z,\boldsymbol{u})\equiv h\ (\mathrm{mod}\ m^k)\}\\ \mathscr{X}_i,\mathscr{Y}_i&:=\mathscr{A}(Q/M,R)\quad (i=2,\dots,s+1)\end{aligned}$$

および

$$\begin{gathered}\phi_1,\psi_1\colon \mathscr{X}_1,\mathscr{Y}_1\to\mathbb{Z};\ (z,\boldsymbol{u})\mapsto\Psi(z,\boldsymbol{u})\\ \phi_i,\psi_i\colon \mathscr{X}_i,\mathscr{Y}_i\to\mathbb{Z};\ x\mapsto m^kx^k\quad (i=2,\dots,s+1)\end{gathered}$$

に適用すれば

$$\begin{aligned}f_1(\alpha)=g_1(\alpha)&=\tilde{g}(\alpha,h,m)\\ f_i(\alpha)=g_i(\alpha)&=f(\alpha,m)\quad (i=2,\dots,s+1)\end{aligned}$$

となるので,

$$\#\tilde{\mathscr{W}}(m,h)=\int_0^1|\tilde{g}(\alpha,h,m)|^2|f(\alpha,m)|^{2s}d\alpha$$

を得ます. または (53) とテキストで定義された

$$G(\alpha,m):=\sum_{h=1}^{m^k}|\tilde{g}(\alpha,h,m)|^2$$

を用いれば

$$\begin{aligned}\#\tilde{\mathscr{W}}(m)&=\sum_{h=1}^{m^k}\int_0^1|\tilde{g}(\alpha,h,m)|^2|f(\alpha,m)|^{2s}d\alpha\\ &=\int_0^1G(\alpha,m)|f(\alpha,m)|^{2s}d\alpha\end{aligned}\tag{54}$$

です. さてテキストで定義された集合

$$\mathscr{B}(h,\boldsymbol{u}):=\{x\ (\mathrm{mod}\ m^k)\mid\Psi(x,\boldsymbol{u})\equiv h\ (\mathrm{mod}\ m^k),\ (m,\Psi'(x,\boldsymbol{u}))=1\}$$

のことを思い出し, $\tilde{g}(\alpha,h,m)$ の定義式に現れる和において z の値を $(\mathrm{mod}\ m^k)$ で分類してあげれば

$$\begin{aligned}\tilde{g}(\alpha,h,m)&=\sum_{\boldsymbol{u}\in\mathscr{U}}\sum_{\substack{1\le z\le P\\ (m,\Psi'(z,\boldsymbol{u}))=1\\ \Psi(z,\boldsymbol{u})\equiv h\ (\mathrm{mod}\ m^k)}}e(\alpha\Psi(z,\boldsymbol{u}))\\ &=\sum_{\boldsymbol{u}\in\mathscr{U}}\sum_{x\in\mathscr{B}(h,\boldsymbol{u})}\sum_{\substack{1\le z\le P\\ z\equiv x\ (\mathrm{mod}\ m^k)}}e(\alpha\Psi(z,\boldsymbol{u}))\end{aligned}$$

$$= \sum_{\boldsymbol{u}\in\mathscr{U}} \sum_{x\in\mathscr{B}(h,\boldsymbol{u})} g(\alpha, x, \boldsymbol{u}; m)$$

を得ます. ただしテキストと同じように

$$g(\alpha, x, \boldsymbol{u}; m) \coloneqq \sum_{\substack{1\le z\le P \\ z\equiv x \pmod{m^k}}} e(\alpha\Psi(z, \boldsymbol{u}))$$

とおきました. したがって Cauchy–Schwarz 不等式より

$$\begin{aligned} G(\alpha, m) &= \sum_{h=1}^{m^k} \Big| \sum_{\boldsymbol{u}\in\mathscr{U}} \sum_{x\in\mathscr{B}(h,\boldsymbol{u})} g(\alpha, x, \boldsymbol{u}; m)\Big|^2 \\ &\le (\#\mathscr{U})(\#\mathscr{B}(h,\boldsymbol{u})) \sum_{h=1}^{m^k} \sum_{\boldsymbol{u}\in\mathscr{U}} \sum_{x\in\mathscr{B}(h,\boldsymbol{u})} |g(\alpha, x, \boldsymbol{u}; m)|^2, \end{aligned}$$

ここで $U \coloneqq \#\mathscr{U}$ とおいたこととテキストの (12.22) を思い出せば

$$G(\alpha, m) \ll m^{\frac{\varepsilon}{2}} U \sum_{h=1}^{m^k} \sum_{\boldsymbol{u}\in\mathscr{U}} \sum_{x\in\mathscr{B}(h,\boldsymbol{u})} |g(\alpha, x, \boldsymbol{u}; m)|^2$$

となります. Theorem 12.1 の最終的な主張において $R > Q$ の場合は $R = Q$ と置き換えても主張は変わらないので $R \le Q$ と仮定して一般性を失いません. したがって $m \le MR \le Q^2 \le P^2$ なので,

$$G(\alpha, m) \ll P^{\varepsilon} U \sum_{h=1}^{m^k} \sum_{\boldsymbol{u}\in\mathscr{U}} \sum_{x\in\mathscr{B}(h,\boldsymbol{u})} |g(\alpha, x, \boldsymbol{u}; m)|^2$$

また

$$\mathbb{Z}/m^k\mathbb{Z} \supset \bigsqcup_{h=1}^{m^k} \mathscr{B}(h, \boldsymbol{u})$$

であることを考えれば h に渡る和と x に渡る和をあわせ

$$G(\alpha, m) \ll P^{\varepsilon} U \sum_{\boldsymbol{u}\in\mathscr{U}} \sum_{x=1}^{m^k} |g(\alpha, x, \boldsymbol{u}; m)|^2$$

を得ます. これを (54) に代入して (48) を思い出すことで

$$S^{(4)} \ll P^{\varepsilon} U (MR)^{2s-1} \sum_{M<m\le MR} \sum_{\boldsymbol{u}\in\mathscr{U}} \sum_{x=1}^{m^k} \int_0^1 |g(\alpha, x, \boldsymbol{u}; m)|^2 |f(\alpha, m)|^{2s} d\alpha \tag{55}$$

を得ます. この左辺の積分に対して Lemma 6 を

$$\begin{aligned} \mathscr{X}_1, \mathscr{Y}_1 &\coloneqq \{z \in [1, P] \cap \mathbb{Z} \mid z \equiv x \pmod{m^k}\} \\ \mathscr{X}_i, \mathscr{Y}_i &\coloneqq \mathscr{A}(Q/M, R) \quad (i = 2, \dots, s+1) \end{aligned}$$

および

$$\begin{aligned} \phi_1, \psi_1 &\colon \mathscr{X}_1, \mathscr{Y}_1 \to \mathbb{Z};\ z \mapsto \Psi(z, \boldsymbol{u}) \\ \phi_i, \psi_i &\colon \mathscr{X}_i, \mathscr{Y}_i \to \mathbb{Z};\ x \mapsto m^k x^k \quad (i = 2, \dots, s+1) \end{aligned}$$

に適用すれば

$$f_1(\alpha) = g_1(\alpha) = g(\alpha, x, \boldsymbol{u}, m)$$
$$f_i(\alpha) = g_i(\alpha) = f(\alpha, m) \quad (i = 2, \dots, s+1)$$

となるので,

$$\int_0^1 |g(\alpha, x, \boldsymbol{u}; m)|^2 |f(\alpha, m)|^{2s} d\alpha = \#\mathscr{T}(x, \boldsymbol{u}, m) \tag{56}$$

ただし

$$\mathscr{T}(x, \boldsymbol{u}, m) = \left\{ \begin{matrix} 1 \le z, w \le P \\ \boldsymbol{x}, \boldsymbol{y} \in \mathscr{A}(Q/M, R)^s \end{matrix} \;\middle|\; \begin{matrix} \Psi(z, \boldsymbol{u}) + m^k p_k(\boldsymbol{x}) = \Psi(w, \boldsymbol{u}) + m^k p_k(\boldsymbol{y}) \\ z \equiv w \equiv x \pmod{m^k} \end{matrix} \right\}$$

となります. ここで

$$\mathscr{T} = \left\{ \begin{matrix} 1 \le z, w \le P,\ \boldsymbol{u} \in \mathscr{U} \\ \boldsymbol{x}, \boldsymbol{y} \in \mathscr{A}(Q/M, R)^s \\ M < m \le MR \end{matrix} \;\middle|\; \begin{matrix} \Psi(z, \boldsymbol{u}) + m^k p_k(\boldsymbol{x}) = \Psi(w, \boldsymbol{u}) + m^k p_k(\boldsymbol{y}) \\ z \equiv w \pmod{m^k} \end{matrix} \right\}$$

とおけば,

$$\#\mathscr{T} = T_s(P, Q, R, M; \Psi; \mathscr{U})$$

ですが, m, $\boldsymbol{u}$ および $z \equiv w \pmod{m^k}$ の値で分類することにより

$$T_s(P, Q, R, M; \Psi, \mathscr{U}) = \#\mathscr{T} = \sum_{M < m \le MR} \sum_{\boldsymbol{u} \in \mathscr{U}} \sum_{x=1}^{m^k} \#\mathscr{T}(x, \boldsymbol{u}, m)$$

となります. ここに (56) と (55) を用いれば

$$S^{(4)} \ll P^{\varepsilon} U (MR)^{2s-1} T_s(P, Q, R, M; \Psi, \mathscr{U})$$

を得て $\max_j S^{(j)} = S^{(4)}$ の場合も Theorem 12.1 が成立することがわかります.

Note 17 (p.184, l.12 以降)**.** 注意ですが, 式 (12.24) において考えている多項式 $f(X)$ が整数係数（$f(X) \in \mathbb{Z}[X]$）であり, $h \in \mathbb{Z}$, $m \in \mathbb{Z} \setminus \{0\}$ のとき

$$\Delta_1(f(X); h, m) \in \mathbb{Z}[X, h, m]$$

です. 実際整数係数多項式は X^n（$n \ge 0$）の整数係数線形結合でかけるので $\Delta(*; h, m)$ の線形性より

$$\Delta_1(X^n; h, m) \in \mathbb{Z}[X, h, m]$$

のみ示せば十分ですが,

$$\begin{aligned} \Delta_1(X^n; h, m) &= m^{-k}((X + hm^k)^n - X^n) \\ &= m^{-k}(X + hm^k - X)((X + hm^k)^{n-1} + \cdots + X^{n-1}) \\ &= h((X + hm^k)^{n-1} + \cdots + X^{n-1}) \in \mathbb{Z}[X, h, m] \end{aligned}$$

です. また

$$\deg_X \Delta_1(f(X); h, m) = \deg_X f - 1$$

にも注意します. （右辺を X^n の整数係数線形結合で書いた後に最高次項の寄与を考えてそれが低次の項によって打ち消されないことを見れば十分です.）

Note 18 (p.184, l.(−1)–p.185, l.7)**.** いくつか注意です:
1. $\mathscr{U}_0 \coloneqq \{\varnothing\}$ と解釈します.
2. $k \geq 2$ であることを思い出すと, $\eta \in (0, \frac{1}{2}]$ 程度にとれば $\phi_j \leq \frac{1}{k}$ となるようにするので

$$h_j \leq H_j = PM_j^{-k} \leq P \quad \text{および } m_i \leq M_j R = P^{\phi_j} R \leq P$$

が成立します. よって p.177 の l.11 にある $\mathscr{U}$ の super set

$$(\mathbb{Z} \cap [1, CP])^t$$

としては実際には $C = 1$ の

$$(\mathbb{Z} \cap [1, P])^t$$

が取れます.
3. $\phi_j \in (0, \frac{1}{k}]$ と $\Phi_j = \phi_1 + \cdots + \phi_j$ より $0 \leq j \leq k-1$ のとき

$$1 = \frac{1}{k} + \cdots + \frac{1}{k} \geq \phi_1 + \cdots + \phi_k \geq \phi_1 + \cdots + \phi_{j+1} = \Phi_j + \phi_{j+1}$$

なので

$$Q_j = P^{1-\Phi_j} \geq P^{\phi_{j+1}} = M_{j+1}$$

が成立しています.
4. パラメータ Q_{j+1} は $j = 0, \ldots, k-1$ に対して

$$Q_{j+1} = P^{1-\Phi_{j+1}} = P^{1-\Phi_j} P^{-\phi_{j+1}} = Q_j / M_{j+1}$$

となるように定められています.
5. 明らかですが

$$\#\mathscr{U}_j = \prod_{i=1}^{j} \#\{1 \leq h_i \leq H_i\} \times \#\{1 \leq m_i \leq M_i R\} \leq \prod_{i=1}^{j} H_i M_i R$$

が成立します.
6. 基本的には以後, 2 つの量

$$S_s(P, Q, R; \Psi; \mathscr{U}), \quad T_s(P, Q, R, M; \Psi; \mathscr{U})$$

としては

$$S_s(P, Q_j, R; \Psi_j; \mathscr{U}_j) \quad (0 \leq j \leq k),$$

および

$$T_s(P, Q_j, R, M_{j+1}; \Psi_j; \mathscr{U}_j) \quad (0 \leq j \leq k-1)$$

という形で用います.

Note 19 (p.185, Theorem 12.2 の主張)**.** 省略された変数は以下の通り :

Theorem 2. いままでの記号の下, $j = 0, \ldots, k-1$ に対して

$$\begin{aligned} &S_s(P, Q_j, R; \Psi_j; \mathscr{U}_j) \\ &\ll P^{\varepsilon} \Bigg(\prod_{i=1}^{j} H_i M_i R_i \Bigg) (M_{j+1} R)^{2s-1} T_s(P, Q_j, R, M_{j+1}; \Psi_j; \mathscr{U}_j) \end{aligned}$$

が成立する.

Note 20 (p.185, Theorem 12.2 の証明の l.1–3)**.** 証明の最初に "The inequality $\Psi_j'(z;\boldsymbol{h},\boldsymbol{m}) > 0$ holds for all choices of the variables under consideration." とありますがこれは次のようにしてわかります：まず, 主張されているのは「任意の $1 \le z \le P$, $\boldsymbol{h} \in \prod_{i=1}^{j}[1,H_i]$, $\boldsymbol{m} \in \prod_{i=1}^{j}(M_i, M_iR]$ に対して $\Psi_j'(z;\boldsymbol{h},\boldsymbol{m}) > 0$」ということです. 次この証明ですが, 次の補題を準備します（これは実質夏に行った p.25 の Exercises 2.8.1 の系です）：

Lemma 12. いままでの記号の下, $j = 0, \dots, k-1$ に関して,

$$\Psi_j(X;\boldsymbol{H},\boldsymbol{M}) = \Delta_j(X^k;\boldsymbol{H},\boldsymbol{M}) = \sum_{\substack{\ell_0\ge 0,\ell_1,\dots,\ell_j\ge 1\\ \ell_0+\cdots+\ell_j=k}} \frac{k!}{\ell_0!\ell_1!\cdots\ell_j!} X^{\ell_0}\prod_{i=1}^{j} M_i^{-k}(H_iM_i^k)^{\ell_i}$$

が成立する. ただし

$$\boldsymbol{H} = (H_1,\dots,H_j), \quad \boldsymbol{M} = (M_1,\dots,M_j)$$

とした.

Proof. 変数 j に関する帰納法で示します. まず $j = 0$ のときは右辺が単に

$$\sum_{\substack{\ell_0\ge 0\\ \ell_0=k}} \frac{k!}{\ell_0!} X^{\ell_0} = X^k$$

となり, 左辺は

$$\Delta_0(X^k;\varnothing,\varnothing) = X^k$$

なので明らかに主張が成立します. 次に $1 \le J \le k-1$ として, $j = J-1$ のとき主張が成立すると仮定して $j = J$ のときを示します. 帰納法の仮定と Δ_j の定義より, もし

$$\tilde{\boldsymbol{H}} = (H_i)_{i=1}^{J-1}, \quad \tilde{\boldsymbol{M}} = (M_i)_{i=1}^{J-1}$$

とかくならば,

$$\begin{aligned}
&\Delta_J(X^k;\boldsymbol{H},\boldsymbol{M})\\
&= M_J^{-k}\left(\Delta_{J-1}((X+H_JM_J^k)^k;\tilde{\boldsymbol{H}},\tilde{\boldsymbol{M}}) - \Delta_{J-1}(X^k;\tilde{\boldsymbol{H}},\tilde{\boldsymbol{M}})\right)\\
&= M_J^{-k}\sum_{\substack{\tilde{\ell}_0\ge 0,\ell_1,\dots,\ell_{J-1}\ge 1\\ \tilde{\ell}_0+\cdots+\ell_{J-1}=k}} \frac{k!}{\tilde{\ell}_0!\ell_1!\cdots\ell_j!}((X+H_JM_J^k)^{\tilde{\ell}_0} - X^{\tilde{\ell}_0})\prod_{i=1}^{J-1} M_i^{-k}(H_iM_i^k)^{\ell_i}
\end{aligned}$$

を得ます. ここに二項展開より得られる

$$M_J^{-k}\left((X+H_JM_J^k)^{\tilde{\ell}_0} - X^{\tilde{\ell}_0}\right) = \sum_{\substack{\ell_0\ge 0,\ell_J\ge 1\\ \ell_0+\ell_J=\tilde{\ell}_0}} \frac{\tilde{\ell}_0!}{\ell_0!\ell_J!} X^{\ell_0}M_J^{-k}(H_JM_J^k)^{\ell_J}$$

を代入すれば

$$\Delta_J(X^k;\boldsymbol{H},\boldsymbol{M}) = \sum_{\substack{\ell_0\ge 0,\ell_1,\dots,\ell_J\ge 1\\ \ell_0+\cdots+\ell_J=k}} \frac{k!}{\ell_0!\ell_1!\cdots\ell_j!} X^{\ell_0}\prod_{i=1}^{J} M_i^{-k}(H_iM_i^k)^{\ell_i}$$

となり主張を得ます. これで証明を終わります. □

さて, Lemma 12 より

$$\Psi'_j(X;\boldsymbol{H},\boldsymbol{M})=\sum_{\substack{\ell_0,\ell_1,\dots,\ell_j\geq 1\\ \ell_0+\cdots+\ell_j=k}}\frac{k!}{\ell_0!\ell_1!\cdots\ell_j!}\ell_0X^{\ell_0-1}\prod_{i=1}^{j}M_i^{-k}(H_iM_i^k)^{\ell_i}$$

です. ここに $X=z,\boldsymbol{H}=\boldsymbol{h},\boldsymbol{M}=\boldsymbol{m}$ を代入すればこれら変数たちはすべて自然数なので各項も自然数になります. よって, $\ell_0=k-j,\ell_1=\cdots=\ell_j=1$ の項が少なくとも存在するので上記和は空和でないことを確認して $\Psi'_j(z;\boldsymbol{h},\boldsymbol{m})>0$ を得ます.

Note 21 (p.185, Theorem 12.2 の証明の l.4–7)**.** 最初の評価

$$S_s(P,M_{j+1},R;\Psi_j;\mathscr{U}_j)\leq M_{j+1}^2S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)$$

ですが, これはまず Lemma 8 を用いて

$$S_s(P,M_{j+1},R;\Psi_j;\mathscr{U}_j)=\int_0^1|F(\alpha,P,\Psi_j,\mathscr{U}_j)|^2|f(\alpha,M_{j+1},R)|^{2s}d\alpha$$

とした後, 右辺の $|f(\alpha,M_{j+1},R)|^2$ ひとつに自明な評価

$$|f(\alpha,M_{j+1},R)|^2\leq\#\mathscr{A}(M_{j+1},R)^2\leq M_{j+1}^2$$

を用いて

$$S_s(P,M_{j+1},R;\Psi_j;\mathscr{U}_j)\leq M_{j+1}^2\int_0^1|F(\alpha,P,\Psi_j,\mathscr{U}_j)|^2|f(\alpha,M_{j+1},R)|^{2(s-1)}d\alpha$$

を得ます. ここで再度 Lemma 8 を右辺に用いて

$$S_s(P,M_{j+1},R;\Psi_j;\mathscr{U}_j)\leq M_{j+1}^2S_{s-1}(P,M_{j+1},R;\Psi_j;\mathscr{U}_j)$$

を得ます. その後で評価

$$S_{s-1}(P,M_{j+1},R;\Psi_j;\mathscr{U}_j)\leq S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)$$

は単に方程式

$$\Psi(z,\boldsymbol{u})+x_1^k+\cdots+x_{s-1}^k=\Psi(w,\boldsymbol{v})+y_1^k+\cdots+y_{s-1}^k$$

中の x_i や y_i たちの範囲を $\mathscr{A}(M_{j+1},R)$ から $\mathscr{A}(Q_j,R)$ に広げる事により得られます. ここで Note 18 の 3 より $Q_j\geq M_{j+1}$ が成立していることに注意しましょう. 2 つ目の評価

$$M_{j+1}^2S_{s-1}(P,M_{j+1},R;\Psi_j;\mathscr{U}_j)\leq Q_jM_{j+1}S_{s-1}(P,M_{j+1},R;\Psi_j;\mathscr{U}_j)$$

も単に $Q_j\geq M_{j+1}$ より従います.

Note 22 (p.185, l.(−4)–(-3))**.** この部分ですが, 直前の評価の "$\ll$" の implicit constant $B\geq 1$ を

$$S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)\leq B\Bigg(P^{\varepsilon}Q_jM_{j+1}S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)$$
$$+P^{\varepsilon}\Bigg(\prod_{i=1}^{j}H_iM_iR\Bigg)(M_{j+1}R)^{2s-1}T_s(P,Q_j,R,M_{j+1};\Psi_j;\mathscr{U}_j)\Bigg)$$

と明示的に書いておけば

$$\begin{aligned}&S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)-BP^{\varepsilon}Q_jM_{j+1}S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)\\&\le BP^{\varepsilon}\Big(\prod_{i=1}^{j}H_iM_iR\Big)(M_{j+1}R)^{2s-1}T_s(P,Q_j,R,M_{j+1};\Psi_j;\mathscr{U}_j)\end{aligned}$$

なので $c=\frac{1}{2B}$ とおいて

$$P^{\varepsilon}Q_jM_{j+1}S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)\le\frac{1}{2B}S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)$$

のとき

$$\begin{aligned}&\frac{1}{2}S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)\\&\le S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)-BP^{\varepsilon}Q_jM_{j+1}S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)\\&\le BP^{\varepsilon}\Big(\prod_{i=1}^{j}H_iM_iR\Big)(M_{j+1}R)^{2s-1}T_s(P,Q_j,R,M_{j+1};\Psi_j;\mathscr{U}_j)\end{aligned}$$

となることより従います.

Note 23 (p.186, l.1–3)**.** この部分の評価

$$S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)\le S_0(P,Q_j,R;\Psi_j;\mathscr{U}_j)^{\frac{1}{s}}S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)^{\frac{s-1}{s}}$$

ですが, Lemma 8 を用いて

$$S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)=\int_0^1|F(\alpha,P,\Psi_j,\mathscr{U}_j)|^2|f(\alpha,Q_j,R)|^{2(s-1)}d\alpha$$

と書いた後に分解

$$\begin{aligned}&|F(\alpha,P,\Psi_j,\mathscr{U}_j)|^2|f(\alpha,Q_j,R)|^{2(s-1)}\\&=|F(\alpha,P,\Psi_j,\mathscr{U}_j)|^{\frac{2}{s}}\times|F(\alpha,P,\Psi_j,\mathscr{U}_j)|^{2\frac{s-1}{s}}|f(\alpha,Q_j,R)|^{2(s-1)}\end{aligned}$$

と指数 $(s,\frac{s}{s-1})$ を用いて Hölder の不等式を適用して Lemma 8 を用いれば

$$\begin{aligned}&S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)\\&\le\Big(\int_0^1|F(\alpha,P,\Psi_j,\mathscr{U}_j)|^2d\alpha\Big)^{\frac{1}{s}}\Big(\int_0^1|F(\alpha,P,\Psi_j,\mathscr{U}_j)|^2|f(\alpha,Q_j,R)|^{2s}d\alpha\Big)^{\frac{s-1}{s}}\\&=S_0(P,Q_j,R;\Psi_j;\mathscr{U}_j)^{\frac{1}{s}}S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)^{\frac{s-1}{s}}\end{aligned}$$

となることで得られます.

Note 24 (p.186, l.4–6)**.** ここの評価の詳細は以下の通り：まず, 直前の評価

$$S_{s-1}(P,Q_j,R;\Psi_j;\mathscr{U}_j)\le S_0(P,Q_j,R;\Psi_j;\mathscr{U}_j)^{\frac{1}{s}}S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)^{\frac{s-1}{s}}$$

と p.185 最後に与えられた仮定

$$P^{\varepsilon}Q_jM_{j+1}S_{s-1}(P,Q_j,R;\Psi_j,\mathscr{U}_j)>cS_s(P,Q_j,R;\Psi_j,\mathscr{U}_j)$$

を組み合わせると

$$S_s(P,Q_j,R;\Psi_j,\mathscr{U}_j)\ll P^{\varepsilon}Q_jM_{j+1}S_0(P,Q_j,R;\Psi_j;\mathscr{U}_j)^{\frac{1}{s}}S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)^{\frac{s-1}{s}}$$

となりますが, 両辺を

$$S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)^{\frac{s-1}{s}}$$

で割って s 乗することで最初の評価

$$S_s(P,Q_j,R;\Psi_j,\mathscr{U}_j)\ll (P^{\varepsilon}Q_jM_{j+1})^sS_0(P,Q_j,R;\Psi_j;\mathscr{U}_j)$$

を得ます. そのあと $S_s(P,Q,R;\Psi;\mathscr{U})$ の定義を思い出せば

$$S_0(P,Q_j,R;\Psi_j;\mathscr{U}_j)=\sum_{\substack{1\le z,w\le P\\ \boldsymbol{u},\boldsymbol{v}\in\mathscr{U}_j\\ \Psi_j(z,\boldsymbol{u})=\Psi_j(w,\boldsymbol{v})}}1=\sum_{\boldsymbol{u},\boldsymbol{v}\in\mathscr{U}_j}\sum_{1\le z\le P}\sum_{\substack{1\le w\le P\\ \Psi_j(z,\boldsymbol{u})=\Psi_j(w,\boldsymbol{v})}}1 \tag{57}$$

を得ます. 今 $j=0,\dots,k-1$ なので, Lemma 12 より $\Psi_j(X;\boldsymbol{H},\boldsymbol{M})$ は X に関して少なくとも 1 次以上 k 次以下です. よって与えられた $\boldsymbol{u},\boldsymbol{v},z$ に対して,

$$1\le \#\{w\in\mathbb{N}\mid \Psi_j(w,\boldsymbol{v})=\Psi_j(z,\boldsymbol{u})\}\le k$$

を得るので, (57) より

$$S_0(P,Q_j,R;\Psi_j;\mathscr{U}_j)\le k\sum_{\boldsymbol{u},\boldsymbol{v}\in\mathscr{U}}\sum_{1\le z\le P}1\ll P(\#\mathscr{U}_j)^2=P\Big(\prod_{i=1}^{j}H_iM_iR\Big)^2$$

を得ます. これを用いれば 2 つ目の評価も従います.

Note 25 (p.186, l.7–11)**.** ここは少し暗算が厳しいですが, ひとつめの評価は

$$\begin{aligned}
&T_s(P,Q_j,R,M_{j+1};\Psi_j,\mathscr{U}_j)\\
&\ge \#\{(z,w)\mid z=w\in[1,P]\}\times\#\{\boldsymbol{u}\in\mathscr{U}_j\}\\
&\quad\times\#\{m\in(M_{j+1},M_{j+1}R]\}\times\#\{(\boldsymbol{x},\boldsymbol{y})\mid \boldsymbol{x}=\boldsymbol{y}\in\mathscr{A}(Q_j/M_{j+1},R)^s\}\\
&\gg P(\#\mathscr{U})M_{j+1}RA(Q_j/M_{j+1},R)^s\gg P\Big(\prod_{i=1}^{j}H_iM_iR\Big)M_{j+1}R(Q_j/M_{j+1})^s
\end{aligned}$$

より従います. 2 つ目の評価は少しずつ計算すると

$$\begin{aligned}
&\Big(\prod_{i=1}^{j}H_iM_iR\Big)(M_{j+1}R)^{2s-1}P\Big(\prod_{i=1}^{j}H_iM_iR\Big)M_{j+1}R(Q_j/M_{j+1})^s\\
&=(M_{j+1}R)^{2s-1}PM_{j+1}R(Q_j/M_{j+1})^s\Big(\prod_{i=1}^{j}H_iM_iR\Big)^2\\
&=R^{2s}(M_{j+1})^{2s-1}PM_{j+1}(Q_j/M_{j+1})^s\Big(\prod_{i=1}^{j}H_iM_iR\Big)^2\\
&=R^{2s}P(M_{j+1})^{2s}(Q_j/M_{j+1})^s\Big(\prod_{i=1}^{j}H_iM_iR\Big)^2\\
&=R^{2s}P(M_{j+1}^2)^s(Q_j/M_{j+1})^s\Big(\prod_{i=1}^{j}H_iM_iR\Big)^2
\end{aligned}$$

$$= R^{2s}P(Q_jM_{j+1})^s\Big(\prod_{i=1}^{j}H_iM_iR\Big)^2$$

より

$$P^{\varepsilon s}\Big(\prod_{i=1}^{j}H_iM_iR\Big)(M_{j+1}R)^{2s-1}T_s(P,Q_j,R,M_{j+1};\Psi_j,\mathscr{U}_j)$$
$$\gg P(P^{\varepsilon}Q_jM_{j+1})^s\Big(\prod_{i=1}^{j}H_iM_iR\Big)^2 \gg S_s(P,Q_j,R;\Psi_j,\mathscr{U}_j)$$

を得ます.

12.3 Successive efficient differences

Note 26 (Lemma12.3 の主張)**.** 省略された変数は以下の通り. 記号

$$S_s(P,R) \coloneqq \#\mathscr{S}_s(P,R)$$

ただし

$$\mathscr{S}_s(P,R) = \{\boldsymbol{x},\boldsymbol{y} \in \mathscr{A}(P,R)^s \mid p(\boldsymbol{x}) = p(\boldsymbol{y})\}$$

を思い出しておきましょう:

Lemma 13. いままでの記号の下, $j = 0,\dots,k-1$ に対して

$$T_s(P,Q_j,R,M_{j+1};\Psi_{j+1},\mathscr{U}_j) \ll P\Big(\prod_{i=1}^{j}H_iM_iR\Big)M_{j+1}RS_s(Q_{j+1},R)$$
$$+ S_s(Q_{j+1},R)^{\frac{1}{2}}S_s(P,Q_{j+1},R;\Psi_{j+1},\mathscr{U}_{j+1})^{\frac{1}{2}}$$

が成立する.

Note 27 (p.187, l.7)**.** ここの評価ですが, $z = w$ の場合には条件

$$z \equiv w \pmod{m^k}$$

が常に成り立つのでこの条件を取り除いてよいのと, 方程式 (12.12) の現在の形

$$\Psi_{j+1}(z;\boldsymbol{h},\boldsymbol{m}) + m^kp(\boldsymbol{x}) = \Psi_{j+1}(w;\boldsymbol{h},\boldsymbol{m}) + m^kp(\boldsymbol{x})$$

が両辺から $\Psi_{j+1}(z;\boldsymbol{h},\boldsymbol{m}) = \Psi_{j+1}(w;\boldsymbol{h},\boldsymbol{m})$ を引いて m^k で割ることで

$$p(\boldsymbol{x}) = p(\boldsymbol{y})$$

と同値になることから

$$U_0 = \#\{(z,w) \mid z = w \le P\} \times \#\mathscr{U}_j \times \#\{M_{j+1} < m \le M_{j+1}R\}$$
$$\times \#\{\boldsymbol{x},\boldsymbol{y} \in \mathscr{A}(Q_j/M_{j+1},R)^s \mid p(\boldsymbol{x}) = p(\boldsymbol{y})\}$$
$$\le P\Big(\prod_{i=1}^{j}H_iM_iR\Big)M_{j+1}RS_s(Q_j/M_{j+1},R)$$

となり, あとは $Q_{j+1} = Q_j/M_{j+1}$ であったことを思い出せば

$$U_0 \le P\Big(\prod_{i=1}^{j}H_iM_iR\Big)M_{j+1}RS_s(Q_{j+1},R)$$

を得ます.

Note 28 (p.187, l.9)**.** 冒頭の

$$1 \le h \le M_{j+1} \quad \text{は} \quad 1 \le h \le H_{j+1} \quad \text{の誤植}$$

であろうと思われます. この後者の $1 \le h \le H_{j+1}$ は

$$hm^k \le z + hm^k = w \le P$$

と $m > M_{j+1}$ より

$$h \le Pm^{-k} \le PM_{j+1}^{-k} = H_{j+1}$$

から得られます. （というよりは, こうなるように H_{j+1} を定義しています.)

Note 29 (p.187, l.14–19)**.** ここで "Now it is a simple matter to use and integral..." とありますが, 詳細は以下のとおりです：まずテキストのここまでの議論より U_1 は

$$U_1 \coloneqq \#\left\{ \begin{matrix} 1 \le z \le P, (\boldsymbol{h}, \boldsymbol{m}) \in \mathscr{U}_{j+1} \\ \boldsymbol{x}, \boldsymbol{y} \in \mathscr{A}(Q_{j+1}, R)^s \end{matrix} \;\middle|\; \sum_{i=1}^{s} x_i^k = \Psi_{j+1}(z; \boldsymbol{h}, \boldsymbol{m}) + \sum_{i=1}^{s} y_i^k \right\}$$

という形だったので Lemma 6 を

$$\mathscr{X}_i, \mathscr{Y}_i \coloneqq \mathscr{A}(Q_{j+1}, R) \quad (i = 1, \dots, s)$$
$$\mathscr{Y}_{s+1} \coloneqq \{(z, \boldsymbol{h}, \boldsymbol{m}) \mid 1 \le z \le P, (\boldsymbol{h}, \boldsymbol{m}) \in \mathscr{U}_{j+1}\}$$

および

$$\phi_i, \psi_i \colon \mathscr{X}_i, \mathscr{Y}_i \to \mathbb{Z};\ x \mapsto x^k \quad (i = 1, \dots, s)$$
$$\psi_{s+1} \colon \mathscr{Y}_{s+1} \to \mathbb{Z};\ (z, \boldsymbol{h}, \boldsymbol{m}) \mapsto \Psi_{j+1}(z; \boldsymbol{h}, \boldsymbol{m})$$

に適用すれば, Lemma 8 の記号の下,

$$f_i(\alpha) = g_i(\alpha) = f(\alpha, Q_{j+1}, R) \quad (i = 1, \dots, s)$$
$$g_{s+1}(\alpha) = F(\alpha, P, \Psi_{j+1}, \mathscr{U}_{j+1})$$

となるので,

$$U_1 = \int_0^1 |f(\alpha, Q_{j+1}, R)|^{2s} \overline{F(\alpha, P, \Psi_{j+1}, \mathscr{U}_{j+1})} d\alpha$$

と書けます. ここで Cauchy–Schwarz 不等式を分解

$$\begin{aligned} &|f(\alpha, Q_{j+1}, R)|^{2s} \overline{F(\alpha, P, \Psi_{j+1}, \mathscr{U}_{j+1})} \\ &= |f(\alpha, Q_{j+1}, R)|^{s} \times |f(\alpha, Q_{j+1}, R)|^{s} \overline{F(\alpha, P, \Psi_{j+1}, \mathscr{U}_{j+1})} \end{aligned}$$

に対して用いれば

$$\begin{aligned} U_1 \le &\left(\int_0^1 |f(\alpha, Q_{j+1}, R)|^{2s} d\alpha \right)^{\frac{1}{2}} \\ &\times \left(\int_0^1 |F(\alpha, P, \Psi_{j+1}, \mathscr{U}_{j+1})|^2 |f(\alpha, Q_{j+1}, R)|^{2s} d\alpha \right)^{\frac{1}{2}} \end{aligned}$$

を得ます. ここで Lemma 7 と Lemma 8 を右辺に用いれば

$$U_2 \le S_s(Q_{j+1}, R)^{\frac{1}{2}} S_s(P, Q_{j+1}, R; \Psi_{j+1}; \mathscr{U}_{j+1})^{\frac{1}{2}}$$

を得ます.

12.4 A mean value theorem

Note 30 (Section 12.4 冒頭から Lemma 12.4)**.** ここの Lemma 12.4 の証明ですが, ϕ_k の選び方が唐突なので以下の議論を用いた方がわかりやすいかもしれません.

まず, 予備の観察を行います. 我々の目標は

$$S_s(P,R) \coloneqq \#\left\{ \boldsymbol{x},\boldsymbol{y} \in \mathscr{A}(P,R)^s \;\middle|\; \sum_{i=1}^{s} x_i^k = \sum_{i=1}^{s} y_i^k \right\}$$

を評価することでした. そこで任意の $\varepsilon > 0$ に対して十分小さい $\eta > 0$ で

$$S_s(P,R) \ll P^{\lambda+\varepsilon} \tag{58}$$

という評価が示せたとしましょう. まず, 自明な評価

$$S_s(P,R) \le \#(\mathscr{A}(P,R)^{2s}) \le P^{2s}$$

があるので, λ としては $\lambda \le 2s$ の範囲だけ考えれば十分です. (つまり $\lambda > 2s$ なるときは (58) は意味がないというわけです.) また一方で整数 n に対して

$$S_s(P,R,n) \coloneqq \#\left\{ \boldsymbol{x},\boldsymbol{y} \in \mathscr{A}(P,R)^s \;\middle|\; \sum_{i=1}^{s} x_i^k = \sum_{i=1}^{s} y_i^k + n \right\}$$

を考えると, Lemma 6 を

$$\mathscr{X}_i, \mathscr{Y}_i \coloneqq \mathscr{A}(P,R) \quad (i = 1,\dots,s), \quad \mathscr{Y}_{s+1} \coloneqq \{n\}$$

および

$$\phi_i, \psi_i \colon \mathscr{X}_i, \mathscr{Y}_i \to \mathbb{Z};\ x \mapsto x^k \quad (i = 1,\dots,s), \quad \psi_{s+1} \colon \mathscr{Y}_i \to \mathbb{Z};\ n \mapsto n$$

に適用すれば

$$f_i(\alpha) = g_i(\alpha) = f(\alpha,P,R) \quad (i = 1,\dots,s), \quad g_{s+1}(\alpha) = e(n\alpha)$$

となるので, Lemma 7 も合わせて

$$S_s(P,R,n) = \int_0^1 |f(\alpha,P,R)|^{2s} e(-n\alpha)\,d\alpha \le \int_0^1 |f(\alpha,P,R)|^{2s}\,d\alpha = S_s(P,R)$$

を得ます. そこで $\boldsymbol{x},\boldsymbol{y} \in \mathscr{A}(P,R)$ たちを $p(\boldsymbol{x}) - p(\boldsymbol{y})$ の値で分類すれば

$$\boldsymbol{x},\boldsymbol{y} \in \mathscr{A}(P,R) \implies |p(\boldsymbol{x}) - p(\boldsymbol{y})| \le sP^k$$

に気をつけて,

$$\#(\mathscr{A}(P,R)^{2s}) = \sum_{|n| \le sP^k} S_s(P,R,n) \le sP^k S_s(P,R).$$

さらに Lemma 12.1 の (ii) より $R = P^\eta$ ならば

$$P^{2s} \ll_{\eta,s} P^k S_s(P,R) \quad \text{よって} \quad P^{2s-k} \ll_{\eta,s} S_s(P,R) \tag{59}$$

です. したがって (58) の λ は, 必ず $\lambda \ge 2s - k - \varepsilon$ よって $\varepsilon \to 0$ とすることで $\lambda \ge 2s - k$ を満たしていなければいけません. 以上をまとめて評価 (58) の指数 λ としては

$$2s - k \le \lambda \le 2s \tag{60}$$

なるものだけ考えることになります. ここで (59) の評価の別証明を与えておきます. Lemma 7 で与えられる積分を思い出しておきます. さて, $|\alpha| \leq \frac{1}{6}P^{-k}$ とすると, $1 \leq x \leq P$ のとき

$$\mathrm{Re}\left(e(\alpha x^k)\right) = \cos(2\pi\alpha x^k) \geq \cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$$

なので Lemma 12.1 の (ii) より

$$|\alpha| \leq \frac{1}{6}P^{-k} \implies |f(\alpha, P, R)| \geq \sum_{x \in \mathscr{A}(P,R)} \mathrm{Re}(e(\alpha x^k)) \geq \frac{1}{2}\#\mathscr{A}(P,R) \gg_\eta P$$

です. したがって Lemma 7 より

$$\begin{aligned} S_s(P,R) &= \int_{-\frac{1}{2}}^{\frac{1}{2}} |f(\alpha,P,R)|^{2s} d\alpha \\ &\geq \int_{|\alpha| \leq \frac{1}{6}P^{-k}} |f(\alpha,P,R)|^{2s} d\alpha \gg_{\eta,s} P^{2s} \int_{|\alpha| \leq \frac{1}{6}P^{-k}} d\alpha \gg P^{2s-k} \end{aligned}$$

を得て, 評価 (59) に再びたどり着きます.

本題に戻ります. Lemma 12.4 で行いたいことは, 任意の $\varepsilon > 0$ に対する評価

$$S_{s+1}(P,R) \ll_\varepsilon P^{\lambda_{s+1}+\varepsilon} \tag{61}$$

を評価

$$S_s(P,R) \ll_\varepsilon P^{\lambda_s+\varepsilon} \tag{62}$$

を仮定して導くことです. 注意ですが, 評価 (62) と言っているのは, 「任意の $\varepsilon > 0$ に対して, ある $\eta > 0$ が存在して $R \leq P^\eta$ のときに評価 (62) が s, k, ε, η に依存しうる implicit constant とともに成立する」ということです. 評価 (61) を導く際には ε はもっと小さいもので置き換えて適用するかもしれません. また, (60) より

$$2s - k \leq \lambda_s \leq 2s \tag{63}$$

と仮定して一般性を失いません. さて, 評価 (62) を満たすような与えられた指数 λ_s に対してなるべく小さな λ_{s+1} で (61) を示したいです. まず,

$$\Psi_0(X) = X^k, \quad \mathscr{U}_0 = \{\varnothing\}, \quad Q_0 = P$$

であったことを思い出すと（$\#\mathscr{U}_0 = 1$ です）, (61) の左辺は

$$\begin{aligned} S_{s+1}(P,R) &= S_s(P,P,R;\Psi_0;\mathscr{U}_0) \\ &= S_s(P,Q_0,R;\Psi_0;\mathscr{U}_0) \end{aligned}$$

とかけることに注意します. そこで $S_{s+1}(P,R)$ をいきなり評価するのではなく

$$S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j) \tag{64}$$

を j に関して帰納的に評価していきましょう. すでに列 ϕ_j は最適に与えられていたと思い ϕ_j を決定していきます. この ϕ_j に対して, M_j, H_j, Q_j, Ψ_j, $\mathscr{U}_j$ を $j = 1, \ldots, k$ に対して p.184 の最後の行から p.185 の 4 行目までのように定めましょう. 便宜的に

$$U_j \coloneqq \#\mathscr{U}_j = \prod_{i=1}^{j} H_i M_i R$$

とおきます. 順序としては $j=k$ から初めて,

$$\begin{aligned} &S_s(Q_j,R) \text{ と } S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)\\ &\rightsquigarrow T_s(P,Q_{j-1},R,M_j;\Psi_{j-1},\mathscr{U}_{j-1}) \quad \text{(via Lemma 12.3)}\\ &\rightsquigarrow S_s(P,Q_{j-1},R;\Psi_{j-1};\mathscr{U}_{j-1}) \quad \text{(via Theorem 12.2)} \end{aligned} \tag{65}$$

の順に帰納的に評価をしていきます. 注意ですが, ϕ_j を決めるというのは $M_j=P^{\phi_j}$ を思い出せば, (65) の中でどのような M_j を用いて Theorem 12.2 を適用するか決めることに対応しています.

まず, $j=k$ の場合には, k 次多項式の k 回差分を取ってしまえば定数になってしまうので, 自明な評価

$$|F(\alpha,P,\Psi_k,\mathscr{U}_k)| \le PU_k$$

と Lemma 7 と Lemma 8 を用いて

$$\begin{aligned} S_s(P,Q_k,R;\Psi_k;\mathscr{U}_k) &= \int_0^1 |F(\alpha,P,\Psi_k,\mathscr{U}_k)|^2 |f(\alpha,Q_k,R)|^{2s} d\alpha\\ &\le (PU_k)^2 \int_0^1 |f(\alpha,Q_k,R)|^{2s} d\alpha = (PU_k)^2 S_s(Q_k,R) \end{aligned}$$

としてしまいます. ここで, 仮定 (62) を思い出し

$$S_s(P,Q_k,R;\Psi_k;\mathscr{U}_k) \ll P^{\varepsilon}(PU_k)^2 Q_k^{\lambda_s} \tag{66}$$

を得ます. これで $j=k$ の場合の (64) の評価を終わります.

次に $j=k-1$ の場合を見てみましょう. まず, 先に (65) の通り Theorem 12.2 から

$$\begin{aligned} &S_s(P,Q_{k-1},R;\Psi_{k-1};\mathscr{U}_{k-1})\\ &\ll P^{\varepsilon}U_{k-1}(M_kR)^{2s-1} T_s(P,Q_{k-1},R,M_k;\Psi_{k-1},\mathscr{U}_{k-1}) \end{aligned}$$

とします. 続いて (65) の通り Lemma 12.3 から

$$\begin{aligned} &S_s(P,Q_{k-1},R;\Psi_{k-1};\mathscr{U}_{k-1})\\ &\ll P^{\varepsilon}U_{k-1}(M_kR)^{2s-1}\\ &\quad \times (PU_{k-1}M_kRS_s(Q_k,R) + (S_s(Q_k,R)S_s(P,Q_k,R;\Psi_k,\mathscr{U}_k))^{\frac{1}{2}}) \end{aligned}$$

として $S_s(Q_k,R)$ と $S_s(P,Q_k,R;\Psi_k,\mathscr{U}_k)$ の評価に帰着させます. そこで $S_s(Q_k,R)$ には (62) を用い, $S_s(P,Q_k,R;\Psi_k,\mathscr{U}_k)$ には (66) を用いることで

$$\begin{aligned} &S_s(P,Q_{k-1},R;\Psi_{k-1};\mathscr{U}_{k-1})\\ &\ll P^{\varepsilon}U_{k-1}(M_kR)^{2s-1}(P^{\varepsilon}PU_{k-1}M_kRQ_k^{\lambda_s} + (P^{2\varepsilon}(PU_k)^2Q_k^{2\lambda_s})^{\frac{1}{2}})\\ &\ll P^{\varepsilon}U_{k-1}(M_kR)^{2s-1}(P^{\varepsilon}PU_{k-1}M_kRQ_k^{\lambda_s} + P^{\varepsilon}PU_kQ_k^{\lambda_s})\\ &\ll P^{2\varepsilon}U_{k-1}(M_kR)^{2s-1}PQ_k^{\lambda_s}(U_{k-1}M_kR+U_k) \end{aligned}$$

を得ます. ここで

$$U_k = \prod_{i=1}^{k} H_iM_iR = H_kM_kR\prod_{i=1}^{k-1} H_iM_iR = U_{k-1}H_kM_kR$$

を思い出すと

$$S_s(P,Q_{k-1},R;\Psi_{k-1};\mathscr{U}_{k-1})$$

$$\ll P^{2\varepsilon}U_{k-1}(M_kR)^{2s-1}PQ_k^{\lambda_s}(U_{k-1}M_kR+U_{k-1}H_kM_kR)$$
$$\ll P^{2\varepsilon}U_{k-1}^2(M_kR)^{2s}PQ_k^{\lambda_s}(1+H_k)$$

ですが, さらに

$$H_k=PM_k^{-k},\quad Q_k=Q_{k-1}M_k^{-1}$$

も思い出すと

$$S_s(P,Q_{k-1},R;\Psi_{k-1};\mathscr{U}_{k-1})\ll P^{2\varepsilon}R^{2s}U_{k-1}^2PQ_{k-1}^{\lambda_s}M_k^{2s-\lambda_s}(1+PM_k^{-k}) \tag{67}$$

を得ます. ここで注意ですが, R は ε に依存して良い定数 $\eta>0$ により $R=P^{\eta}$ と定められているので, R は P^{ε} のように無視できてしまう因子と思うことができるので右辺前半に P^{ε} とまとめて書いています. さて右辺が最小になるように ϕ_k つまり M_k を決めましょう. P,R,U_{k-1},Q_{k-1} は ϕ_k つまり M_k に依存しないので残りの

$$M_k^{2s-\lambda_s}(1+PM_k^{-k})=M_k^{2s-\lambda_s}+PM_k^{2s-k-\lambda_s}$$

という部分を考えます. ここで (63) を思い出せば, 右辺の第 1 項目は M_k に関して単調増加で第 2 項目は M_k に関して単調減少なのでこの両項が等しくなるときが（定数倍を除き）最良の評価を与えます. これは

$$1=PM_k^{-k}$$

となるときなので

$$M_k=P^{\frac{1}{k}}\quad \text{つまり}\quad \phi_k=\frac{1}{k}$$

が $\phi_1,\dots,\phi_{k-1}$ の如何に関わらず ϕ_k の最適な値ということになります. （注意ですがこの最適値は条件 $\phi_k\in(0,\frac{1}{k}]$ を満たしています.）この最適値の下, (67) より

$$\begin{aligned}S_s(P,Q_{k-1},R;\Psi_{k-1};\mathscr{U}_{k-1})&\ll P^{2\varepsilon}R^{2s}U_{k-1}^2PQ_{k-1}^{\lambda_s}M_k^{2s-\lambda_s}\\&=P^{2\varepsilon}R^{2s}U_{k-1}^2P^{1+(2s-\lambda_s)\phi_k}Q_{k-1}^{\lambda_s}\end{aligned} \tag{68}$$

を得ます.

さて, $j=k-1,\dots,1$ に対して, 評価 (68) において $k-1$ を一斉に変数 j に置き換え, ϕ_k を ϕ_{j+1} に置き換えることで得られる同じような評価

$$S_s(P,Q_j,R;\Psi_j;\mathscr{U}_j)\ll P^{(k-j+1)\varepsilon}R^{2s(k-j)}U_j^2P^{1+(2s-\lambda_s)\phi_{j+1}}Q_j^{\lambda_s} \tag{69}$$

が成立する仮定して帰納的に考察しましょう. （注意ですが, P^{ε} と R^{2s} の部分は今後の蓄積を考えて多少書き換えました. また, もし $\lambda_s<2s$ ならば $\phi_{k+1}=\frac{1}{2s-\lambda_s}$ とおくことで (69) は $j=k$ のときも (66) と辻褄が合うようにできます.）仮定 (69) の下, これから評価するのは $S_s(P,Q_{j-1},R;\Psi_{j-1};\mathscr{U}_{j-1})$ です. 上記 $j=k-1$ のときと同様に, まず Theorem 12.2 より

$$\begin{aligned}&S_s(P,Q_{j-1},R;\Psi_{j-1};\mathscr{U}_{j-1})\\&\ll P^{\varepsilon}U_{j-1}(M_jR)^{2s-1}T_s(P,Q_{j-1},R,M_j;\Psi_{j-1},\mathscr{U}_{j-1})\end{aligned}$$

とします. 続いて (65) の通り Lemma 12.3 から

$$\begin{aligned}&S_s(P,Q_{j-1},R;\Psi_{j-1};\mathscr{U}_{j-1})\\&\ll P^{\varepsilon}U_{j-1}(M_jR)^{2s-1}\\&\quad\times(PU_{j-1}M_jRS_s(Q_j,R)+(S_s(Q_j,R)S_s(P,Q_j,R;\Psi_j,\mathscr{U}_j))^{\frac{1}{2}})\end{aligned}$$

として $S_s(Q_j,R)$ と $S_s(P,Q_j,R;\Psi_j,\mathscr{U}_j)$ の評価に帰着させます. そこで $S_s(Q_j,R)$ には (62) を用い, $S_s(P,Q_j,R;\Psi_j,\mathscr{U}_j)$ には (69) を用いることで

$$\begin{aligned}
&S_s(P,Q_{j-1},R;\Psi_{j-1};\mathscr{U}_{j-1})\\
&\ll P^{\varepsilon}U_{j-1}(M_jR)^{2s-1}\\
&\quad\times(P^{\varepsilon}PU_{j-1}M_jRQ_j^{\lambda_s}+(P^{\varepsilon}Q_j^{\lambda_s}\cdot P^{(k-j+1)\varepsilon}R^{2s(k-j)}U_j^2P^{1+(2s-\lambda_s)\phi_{j+1}}Q_j^{\lambda_s})^{\frac12})\\
&\ll P^{\varepsilon}U_{j-1}(M_jR)^{2s-1}\\
&\quad\times(P^{\varepsilon}PU_{j-1}M_jRQ_j^{\lambda_s}+(P^{(k-j+2)\varepsilon}R^{2s(k-j)}U_j^2P^{1+(2s-\lambda_s)\phi_{j+1}}Q_j^{2\lambda_s})^{\frac12})\\
&\ll P^{\varepsilon}U_{j-1}(M_jR)^{2s-1}\\
&\quad\times(P^{\varepsilon}PU_{j-1}M_jRQ_j^{\lambda_s}+P^{\frac12(k-j+2)\varepsilon}R^{s(k-j)}U_jP^{\frac12+(\frac{2s-\lambda_s}{2})\phi_{j+1}}Q_j^{\lambda_s})\\
&\ll P^{\varepsilon+\frac12(k-j+2)\varepsilon}R^{2s-1+s(k-j)}U_{j-1}M_j^{2s-1}\\
&\quad\times(PU_{j-1}M_jQ_j^{\lambda_s}+U_jP^{\frac12+(\frac{2s-\lambda_s}{2})\phi_{j+1}}Q_j^{\lambda_s})\\
&\ll P^{(k-j+2)\varepsilon}R^{2s(k-j+1)-1}U_{j-1}M_j^{2s-1}Q_j^{\lambda_s}(PU_{j-1}M_j+U_jP^{\frac12+(\frac{2s-\lambda_s}{2})\phi_{j+1}})
\end{aligned}$$

を得ます. ここで

$$U_j=\prod_{i=1}^{j}H_iM_iR=H_jM_jR\prod_{i=1}^{j-1}H_iM_iR=U_{j-1}H_jM_jR$$

を思い出すと

$$\begin{aligned}
&S_s(P,Q_{j-1},R;\Psi_{j-1};\mathscr{U}_{j-1})\\
&\ll P^{(k-j+2)\varepsilon}R^{2s(k-j+1)-1}U_{j-1}M_j^{2s-1}Q_j^{\lambda_s}\\
&\quad\times(PU_{j-1}M_j+U_{j-1}H_jM_jRP^{\frac12+(\frac{2s-\lambda_s}{2})\phi_{j+1}})\\
&\ll P^{(k-j+2)\varepsilon}R^{2s(k-j+1)}U_{j-1}^2M_j^{2s}Q_j^{\lambda_s}(P+H_jP^{\frac12+(\frac{2s-\lambda_s}{2})\phi_{j+1}})
\end{aligned}$$

ですが, さらに

$$H_j=PM_j^{-k},\quad Q_j=Q_{j-1}M_j^{-1}$$

も思い出すと

$$\begin{aligned}
&S_s(P,Q_{j-1},R;\Psi_{j-1};\mathscr{U}_{j-1})\\
&\ll P^{(k-j+2)\varepsilon}R^{2s(k-j+1)}U_{j-1}^2Q_{j-1}^{\lambda_s}M_j^{2s-\lambda_s}(P+PM_j^{-k}P^{\frac12+(\frac{2s-\lambda_s}{2})\phi_{j+1}})\\
&=P^{(k-j+2)\varepsilon}R^{2s(k-j+1)}PU_{j-1}^2Q_{j-1}^{\lambda_s}M_j^{2s-\lambda_s}(1+P^{\frac12+(\frac{2s-\lambda_s}{2})\phi_{j+1}}M_j^{-k})
\end{aligned}\tag{70}$$

を得ます. 先程の $j=k-1$ のときと同様にこの右辺のうち ϕ_j が関与するのは

$$M_j^{2s-\lambda_s}(1+P^{\frac12+(\frac{2s-\lambda_s}{2})\phi_{j+1}}M_j^{-k})$$

の部分のみでこの値を最小化する ϕ_j は

$$1=P^{\frac12+(\frac{2s-\lambda_s}{2})\phi_{j+1}}M_j^{-k}\iff k\phi_j=\frac12+\left(\frac{2s-\lambda_s}{2}\right)\phi_{j+1}$$

つまり

$$\phi_j=\frac{1}{2k}+\left(\frac{2s-\lambda_s}{2k}\right)\phi_{j+1}\tag{71}$$

で与えられます. （注意ですが, (63) より $2s-\lambda_s \le k$ なので $\phi_{j+1} \in (0, \frac{1}{k}]$ ならこの最適値は条件 $\phi_j \in (0, \frac{1}{k}]$ を満たします.）この最適な ϕ_j の下, (70) より

$$\begin{aligned}
&S_s(P, Q_{j-1}, R; \Psi_{j-1}; \mathscr{U}_{j-1}) \\
&\ll P^{(k-j+2)\varepsilon} R^{2s(k-j+1)} P U_{j-1}^2 Q_{j-1}^{\lambda_s} M_j^{2s-\lambda_s} \\
&= P^{(k-j+2)\varepsilon} R^{2s(k-j+1)} U_{j-1}^2 P^{1+(2s-\lambda_s)\phi_j} Q_{j-1}^{\lambda_s}
\end{aligned}$$

を得て, (71) のもと, (69) が $(j-1)$ 番目も成立します. これにより帰納的に評価を続けることができて最終的に $j=0$ の場合の評価

$$\begin{aligned}
S_{s+1}(P, R) &= S_s(P, P, R; \Psi_0; \mathscr{U}_0) \\
&= S_s(P, Q_0, R; \Psi_0; \mathscr{U}_0) \\
&\ll P^{(k+1)\varepsilon} R^{2sk} U_0^2 P^{1+(2s-\lambda_s)\phi_1} Q_0^{\lambda_s} \\
&= P^{(k+1)\varepsilon} R^{2sk} P^{1+(2s-\lambda_s)\phi_1+\lambda_s}
\end{aligned}$$

を得ます. ここで ε を $\frac{1}{2(k+1)}\varepsilon$ に置き換え, η を $\frac{1}{4sk}\varepsilon$ よりも小さくしておけば

$$S_{s+1}(P, R) \ll P^{1+(2s-\lambda_s)\phi_1+\lambda_s+\varepsilon}$$

を得ます. さらに, $\lambda_s = 2s-k+\delta_s$ と書けば $2s-\lambda_s = k-\delta_s$ なので,

$$\begin{aligned}
\lambda_{s+1} &= 1 + (2s-\lambda_s)\phi_1 + \lambda_s \\
&= 1 + (k-\delta_s)\phi_1 + 2s - k + \delta_s \\
&= 2(s+1) - k + \delta_s + (k-\delta_s)\phi_1 - 1 \\
&= 2(s+1) - k + \delta_s(1-\phi_1) + k\phi_1 - 1
\end{aligned} \tag{72}$$

という指数 λ_{s+1} をとることができます.

さて, (72) を適用する際には, ϕ_1 の値が必要なので線形漸化式 (71) を初期値 $\phi_k = \frac{1}{k}$ の下で解きましょう. まず $j = 1, \dots, k-2$ と仮定して (71) と (71) の j に $j+1$ を代入したものの差を取って

$$\phi_{j+1} - \phi_j = \left(\frac{2s-\lambda_s}{2k}\right)(\phi_{j+2} - \phi_{j+1})$$

を得ます. また $2s-\lambda_s = k-\delta_s$ を思い出すと

$$\phi_{j+1} - \phi_j = \left(\frac{k-\delta_s}{2k}\right)(\phi_{j+2} - \phi_{j+1})$$

とも書けます. よって

$$\phi_{j+1} - \phi_j = \left(\frac{k-\delta_s}{2k}\right)(\phi_{j+2} - \phi_{j+1}) = \cdots = \left(\frac{k-\delta_s}{2k}\right)^{k-(j+1)}(\phi_k - \phi_{k-1}) \tag{73}$$

を得ます. 漸化式 (71) に $j = k-1$ を代入して

$$\phi_k - \phi_{k-1} = -\frac{1}{2k} + \frac{k+\delta_s}{2k}\phi_k = -\frac{1}{2k} + \frac{k+\delta_s}{2k^2} = \frac{\delta_s}{2k^2}$$

を得るので, (73) より

$$\phi_{j+1} = \phi_j + \frac{\delta_s}{2k^2}\left(\frac{k-\delta_s}{2k}\right)^{k-(j+1)}$$

を得ます. これを再度 (71) に代入して,

$$\phi_j = \frac{1}{2k} + \left(\frac{k-\delta_s}{2k}\right)\phi_j + \frac{\delta_s}{2k^2}\left(\frac{k-\delta_s}{2k}\right)^{k-j}$$

を得ますが, これは

$$\begin{aligned}
&\iff \left(\frac{k+\delta_s}{2k}\right)\phi_j = \frac{1}{2k} + \frac{\delta_s}{2k^2}\left(\frac{k-\delta_s}{2k}\right)^{k-j} \\
&\iff \phi_j = \frac{1}{k+\delta_s} + \frac{\delta_s}{k(k+\delta_s)}\left(\frac{k-\delta_s}{2k}\right)^{k-j} \\
&\iff \phi_j = \frac{1}{k+\delta_s} + \left(\frac{1}{k} - \frac{1}{k+\delta_s}\right)\left(\frac{k-\delta_s}{2k}\right)^{k-j}
\end{aligned}$$

となり, テキストの (12.31) が最適な選び方であることがわかり, また

$$\phi_1 = \frac{1}{k+\delta_s} + \left(\frac{1}{k} - \frac{1}{k+\delta_s}\right)\left(\frac{k-\delta_s}{2k}\right)^{k-1}$$

と知れます. 以上の議論より Lemma 12.4 が従います.

Note 31 (p.190, Theorem 12.4)**.** 方程式

$$\sigma + \log\sigma = 1 - \frac{2s}{k}$$

の出現は唐突ですが, これは以下のようにして現れます. まず, (12.34) を見れば

$$\delta_s = k\sigma_s$$

と（おおよそ）書いています. これは Lemma 12.4 で与えられた δ_s の漸化式

$$\begin{aligned}
\delta_{s+1} &= \delta_s(1-\theta) + k\theta - 1 = \delta_s - 1 + (k-\delta_s)\theta \\
&= \delta_s - \frac{2\delta_s}{k+\delta_s} + \frac{2\delta_s}{k+\delta_s}\left(\frac{k-\delta_s}{2k}\right)^k
\end{aligned}$$

を

$$\sigma_{s+1} = \sigma_s - \frac{2\sigma_s}{k(1+\sigma_s)} + \frac{2\sigma_s}{k(1+\sigma_s)}\left(\frac{1-\sigma_s}{2}\right)^k$$

と正規化したいというのが理由でしょう. この方程式において項

$$\frac{2\sigma_s}{k(1+\sigma_s)}\left(\frac{1-\sigma_s}{2}\right)^k \le \frac{2^{1-k}\sigma_s}{k(1+\sigma_s)}$$

は k が大きいときは非常に小さいので無視することにして

$$\sigma_{s+1} = \sigma_s - \frac{2\sigma_s}{k(1+\sigma_s)}$$

ないしは

$$\sigma_{s+1} - \sigma_s = -\frac{2\sigma_s}{k(1+\sigma_s)}$$

を考えてみると, この差分方程式に対応する微分方程式は

$$\sigma'(s) = -\frac{2\sigma(s)}{k(1+\sigma(s))}$$

という変数分離形の微分方程式であり, これは

$$\frac{\sigma'}{\sigma}(s)+\sigma'(s)=-\frac{2}{k}$$

として積分してあげれば

$$\log\sigma(s)+\sigma(s)=-\frac{2s}{k}+C$$

と解くことができます. ここで $\sigma(0)=\sigma_0=1$ と思えば（これは $S_0(P,R)=1$ という評価から $\lambda_0=0$, $\delta_s=k$ となることに対応しています）,

$$\log\sigma(s)+\sigma(s)=1-\frac{2s}{k}$$

という方程式を得ます. （Theorem 12.4 の証明で行っているのは上記差分方程式と微分方程式の近似が実際にうまくいくことの確認であり, p.191 で定義されている μ とは近似

$$\log\sigma_{s+1}-\log\sigma_s=\log\frac{\sigma_{s+1}}{\sigma_s}=\log\left(1-\frac{\sigma_s-\sigma_{s+1}}{\sigma_s}\right)=-\frac{\sigma_s-\sigma_{s+1}}{\sigma_s}-\cdots$$

における最後の Taylor 展開に現れる量 $\frac{\sigma_s-\sigma_{s+1}}{\sigma_s}$ に対応しています.）

Note 32 (p.190, 式 (12.36))**.** 注意ですが, σ_s の定義

$$\sigma_s+\log\sigma_s=1-\frac{2s}{k},\quad \sigma_s\in(0,1]$$

より

$$\log\sigma_s<\sigma_s+\log\sigma_s=1-\frac{2s}{k}$$

なので

$$\sigma_s<\exp\left(1-\frac{2s}{k}\right)$$

です. これを (12.34) に代入して (12.36) を得ます.

Note 33 (p.191, l.10–12)**.** 評価

$$\nu+\frac{1}{2}\left(\frac{\nu}{2}\right)^2+\frac{1}{3}\left(\frac{\nu}{2}\right)^3<\frac{2}{k} \tag{74}$$

（テキストの左辺第三項目の指数が 2 なのは恐らく誤植でしょう.）から

$$\nu<\frac{2-2^{1-k}}{k}=\frac{2}{k}(1-\varepsilon)\quad(\varepsilon:=2^{-k}) \tag{75}$$

を導く部分は単純計算ですが, 一応計算を残しておきます. 評価 (74) の左辺は $\nu>0$ に関して単調増加なのでこれに (75) の右辺を代入した

$$\frac{2}{k}(1-\varepsilon)+\frac{1}{2k^2}(1-\varepsilon)^2+\frac{1}{3k^3}(1-\varepsilon)^3$$

が $\frac{2}{k}$ より大きくなればよいです. これは

$$\begin{aligned}&\frac{2}{k}(1-\varepsilon)+\frac{1}{2k^2}(1-\varepsilon)^2+\frac{1}{3k^3}(1-\varepsilon)^3\geq\frac{2}{k}\\ \iff\ &\frac{1}{2k^2}(1-\varepsilon)^2+\frac{1}{3k^3}(1-\varepsilon)^3\geq\frac{2\varepsilon}{k}\\ \iff\ &\frac{3k}{2}(1-\varepsilon)^2+(1-\varepsilon)^3\geq 6k^2\varepsilon\end{aligned} \tag{76}$$

と言い換えられます. また $k \geq 4$ のときは（例えば帰納法でも用いて）

$$\varepsilon = 2^{-k} \leq k^{-2}$$

なので先の不等式 (76) は

$$\frac{3k}{2}(1-\varepsilon)^2 + (1-\varepsilon)^3 \geq 6$$

より従います. この左辺は $k \geq 4$ より

$$\begin{aligned}\frac{3k}{2}(1-\varepsilon)^2 + (1-\varepsilon)^3 &\geq 6(1-\varepsilon)^2 + (1-\varepsilon)^3 = (1-\varepsilon)^2(7-\varepsilon) \\ &= (1-2\varepsilon+\varepsilon^2)(7-\varepsilon) \geq (1-2\varepsilon)(7-\varepsilon) \\ &= 7 - 15\varepsilon + 2\varepsilon^2 \geq 7 - 15\varepsilon\end{aligned}$$

ですが, $\varepsilon = 2^{-k} \leq \frac{1}{16}$ なので

$$\frac{3k}{2}(1-\varepsilon)^2 + 2(1-\varepsilon)^3 \geq 6 + \frac{1}{16} > 6$$

を得ます. 以上で (75) がわかりました.

On Lemma 5.3 & Lemma 5.4

Note 34 (Lemma 5.3)**.** Lemma 5.3 は "multidimensional large sieve" ですが, 今回のセミナーでは 1 次元の場合しか使わないので, あまり効果はないかも知れませんが, わかりやすさと時間の節約のために次の Lemma 5.3 の 1 次元版を示してください.

Lemma 14. 実数 N, δ が $N \geq 1$ かつ $\delta > 0$ を満たすとし, 実数の有限集合 Γ が

$$\forall \gamma, \gamma' \in \Gamma,\ \gamma \neq \gamma' \implies \|\gamma - \gamma'\| > \delta$$

を満たすとする. すると, 任意の複素数列 $(a(n))_{1 \leq n \leq N}$ に対して

$$\sum_{\gamma \in \Gamma} \left| \sum_{1 \leq n \leq N} a(n) e(n\gamma) \right|^2 \ll \left(N + \frac{1}{\delta} \right) \sum_{1 \leq n \leq N} |a(n)|^2$$

が成立する. ただし implicit constant は絶対定数である.

Proof. まず, いわゆる「双対原理」により, 示したい主張と同じ N, δ, Γ に対して, 次の双対版の評価を示せば良いことを見ます：「任意の $(b(\gamma))_{\gamma \in \Gamma}$ に対して

$$\sum_{1 \leq n \leq N} \left| \sum_{\gamma \in \Gamma} b(\gamma) e(n\gamma) \right|^2 \ll \left(N + \frac{1}{\delta} \right) \sum_{\gamma \in \Gamma} |b(\gamma)|^2$$

が成立する. ただし implicit constant は絶対定数である.」実際, 次のように議論すればもともとの主張が従います. 双対版の評価が成り立つと仮定して, 与えられた複素数列 $(a(n))_{1 \leq n \leq N}$ に対して

$$b(\gamma) \coloneqq \overline{\sum_{1 \leq n \leq N} a(n) e(n\gamma)} \tag{77}$$

とおきます. すると,

$$\sum_{\gamma \in \Gamma} \left| \sum_{1 \leq n \leq N} a(n) e(n\gamma) \right|^2 = \sum_{\gamma \in \Gamma} b(\gamma) \sum_{1 \leq n \leq N} a(n) e(n\gamma)$$

$$= \sum_{1\le n\le N} a(n) \sum_{\gamma\in\Gamma} b(\gamma) e(n\gamma)$$

となりますが, ここで Cauchy–Schwarz 不等式より

$$\Bigg(\sum_{\gamma\in\Gamma} \Bigg| \sum_{1\le n\le N} a(n) e(n\gamma) \Bigg|^2 \Bigg)^2$$

$$\le \sum_{1\le n\le N} |a(n)|^2 \sum_{1\le n\le N} \Bigg| \sum_{\gamma\in\Gamma} b(\gamma) e(n\gamma) \Bigg|^2$$

です. さらに仮定している双対版の評価を使えば

$$\Bigg(\sum_{\gamma\in\Gamma} \Bigg| \sum_{1\le n\le N} a(n) e(n\gamma) \Bigg|^2 \Bigg)^2 \ll \left(N + \frac{1}{\delta} \right) \sum_{1\le n\le N} |a(n)|^2 \sum_{\gamma\in\Gamma} |b(\gamma)|^2 \tag{78}$$

を得ます. ここで (77) を思い出すと

$$\sum_{\gamma\in\Gamma} |b(\gamma)|^2 = \sum_{\gamma\in\Gamma} \Bigg| \sum_{1\le n\le N} a(n) e(n\gamma) \Bigg|^2$$

です. この値が 0 なら示すべきことはなく, 0 でないならばこの値で (78) の両辺を割れば示したかった元々の評価が従います.

さて, 双対版の評価を示しましょう. Cesàro weight

$$w(n) = w_N(n) \coloneqq \max\left(\left(1 - \frac{|n|}{2N} \right), 0 \right) \quad (n \in \mathbb{Z})$$

を用います. この Cesàro weight に対して

$$\begin{aligned}
\sum_{n\in\mathbb{Z}} w(n) e(n\gamma) &= \sum_{\substack{n \\ |n|<2N}} \left(1 - \frac{|n|}{2N} \right) e(n\gamma) \\
&= \frac{1}{2N} \sum_{\substack{n \\ |n|<2N}} (2N - |n|) e(n\gamma) \\
&= \frac{1}{2N} \sum_{\substack{n \\ |n|<2N}} \Bigg(\sum_{\substack{1\le m,m'\le 2N \\ m-m'=n}} 1 \Bigg) e(n\gamma) \\
&= \frac{1}{2N} \sum_{\substack{n \\ |n|<2N}} \Bigg(\sum_{\substack{1\le m,m'\le 2N \\ m-m'=n}} e((m-m')\gamma) \Bigg) \\
&= \frac{1}{2N} \sum_{1\le m,m'\le 2N} e((m-m')\gamma) = \frac{1}{2N} \left| \sum_{m=1}^{2N} e(m\gamma) \right|^2
\end{aligned}$$

より

$$\sum_{n\in\mathbb{Z}} w(n) e(n\gamma) \ll \frac{1}{N} \left(\min\left(N, \frac{1}{\|\gamma\|} \right) \right)^2 = \min\left(N, \frac{1}{N\|\gamma\|^2} \right) \tag{79}$$

であったことを思い出しておきましょう. さて,

$$1 \le n \le N \implies w(n) = 1 - \frac{|n|}{2N} \ge \frac{1}{2}$$

なので

$$\sum_{1\le n\le N}\left|\sum_{\gamma\in\Gamma}b(\gamma)e(n\gamma)\right|^2\ll\sum_{n\in\mathbb{Z}}w(n)\left|\sum_{\gamma\in\Gamma}b(\gamma)e(n\gamma)\right|^2$$

です. ここで 2 乗を開いて和を入れ替えると (79) より

$$\begin{aligned}\sum_{1\le n\le N}\left|\sum_{\gamma\in\Gamma}b(\gamma)e(n\gamma)\right|^2&\ll\sum_{\gamma,\gamma'\in\Gamma}b(\gamma)\overline{b(\gamma')}\sum_{n\in\mathbb{Z}}w(n)e(n(\gamma-\gamma'))\\&\ll\sum_{\gamma,\gamma'\in\Gamma}|b(\gamma)||b(\gamma')|\min\left(N,\frac{1}{N\|\gamma-\gamma'\|^2}\right)\end{aligned}$$

を得ます. ここで相加相乗平均の不等式ないしは

$$|b(\gamma)||b(\gamma')|\le(\max(|b(\gamma)|,|b(\gamma')|))^2\le|b(\gamma)|^2+|b(\gamma')|^2$$

を用いれば

$$\begin{aligned}&\sum_{1\le n\le N}\left|\sum_{\gamma\in\Gamma}b(\gamma)e(n\gamma)\right|^2\\&\ll\sum_{\gamma,\gamma'\in\Gamma}|b(\gamma)|^2\min\left(N,\frac{1}{N\|\gamma-\gamma'\|^2}\right)+\sum_{\gamma,\gamma'\in\Gamma}|b(\gamma')|^2\min\left(N,\frac{1}{N\|\gamma-\gamma'\|^2}\right)\end{aligned}$$

を得ます. さらに右辺 2 つめの和において γ と γ' の名前を付け替えて

$$\min\left(N,\frac{1}{N\|\gamma'-\gamma\|^2}\right)=\min\left(N,\frac{1}{N\|\gamma-\gamma'\|^2}\right)$$

を使えば

$$\sum_{1\le n\le N}\left|\sum_{\gamma\in\Gamma}b(\gamma)e(n\gamma)\right|^2\ll\sum_{\gamma\in\Gamma}|b(\gamma)|^2\sum_{\gamma'\in\Gamma}\min\left(N,\frac{1}{N\|\gamma-\gamma'\|^2}\right)$$

を得ます. あとは

$$\sum_{\gamma'\in\Gamma}\min\left(N,\frac{1}{N\|\gamma-\gamma'\|^2}\right)\ll N+\frac{1}{\delta}\tag{80}$$

を示せば十分です.

関数 $\|*\|$ は周期 1 を持ったことと, Lemma の仮定より Γ の異なる 2 元は (mod 1) で等しくないことを注意すれば, Γ の元を (mod 1) 分だけシフトすることで

$$\gamma_0\coloneqq\gamma,\quad\Gamma=\{\gamma_{-S}<\cdots<\gamma_{-1}<\gamma_0<\gamma_1<\cdots<\gamma_R\}\subset(\gamma_0-\tfrac{1}{2},\gamma_0+\tfrac{1}{2}]$$

となっていると仮定して (80) を示せばよいです. (ここで S,R は 0 以上の整数です.) 今 $\Gamma\subset(\gamma_0-\frac{1}{2},\gamma_0+\frac{1}{2}]$ なので $i\in\{0,\dots,R\}$ のとき, 仮定より

$$\begin{aligned}\|\gamma_i-\gamma_0\|=\gamma_i-\gamma_0&=(\gamma_i-\gamma_{i-1})+\cdots+(\gamma_1-\gamma_0)\\&=|\gamma_i-\gamma_{i-1}|+\cdots+|\gamma_1-\gamma_0|\\&=\|\gamma_i-\gamma_{i-1}\|+\cdots+\|\gamma_1-\gamma_0\|>\delta i\end{aligned}$$

を得ます. $i\in\{-S,\dots,0\}$ のときも同様に議論して, $i\in\{-S,\dots,R\}$ のとき

$$\|\gamma_i-\gamma_0\|\ge\delta|i|$$

であることがわかります. したがって,

$$\sum_{\gamma'\in\Gamma}\min\left(N,\frac{1}{N\|\gamma-\gamma'\|^2}\right)=\sum_{i=-S}^{R}\min\left(N,\frac{1}{N\|\gamma_i-\gamma_0\|^2}\right)$$
$$\leq\sum_{i=-S}^{R}\min\left(N,\frac{1}{N(\delta|i|)^2}\right)\ll\sum_{i=0}^{\infty}\min\left(N,\frac{1}{N(\delta i)^2}\right)$$

です. ここで和を $i\leq\frac{1}{N\delta}$ であるか否かで分けることで

$$\sum_{\gamma'\in\Gamma}\min\left(N,\frac{1}{N\|\gamma-\gamma'\|^2}\right)\leq\sum_{0\leq i\leq\frac{1}{N\delta}}N+\sum_{\frac{1}{N\delta}<i}\frac{1}{N(\delta i)^2}$$
$$\ll N\left(\frac{1}{N\delta}+1\right)+\frac{1}{N\delta^2}\sum_{\frac{1}{N\delta}<i}\frac{1}{i(i+1)}$$
$$\ll\left(N+\frac{1}{\delta}\right)+\frac{1}{N\delta^2}\left(\frac{1}{N\delta}\right)^{-1}\ll N+\frac{1}{\delta}$$

を得るので (80) が従い, Lemma の証明を終わります. □

Note 35 (Lemma 5.4 の主張)**.** ほぼ変わりませんが, セミナーの目的のためには以下の形で Lemma 5.4 を示す必要があります（証明は全く同じです. 主張における違いですが, 内側の和に絶対値をつけています. 他の一般化として絶対値を y に渡る和に付ける代わりに p に渡る和に係数 $a(p)$ を導入するという方法もあります）:

Lemma 15 (Lemma 5.4)**.** 実数 α および実数 $X,Y\geq1$ に対して, 有理近似

$$\alpha=\frac{a}{q}+\beta,\quad q,a\in\mathbb{Z},\quad 1\leq q\leq 2X^k,\quad (q,a)=1,\quad |\beta|\leq\frac{1}{2qX^k}$$

が成立したとする. さらにある実数 $C>1$ によって

$$X^k\leq CY$$

および

$$1\leq q\leq X\implies|\beta|>\frac{1}{CqX^{k-1}Y}$$

が成立したとする. このとき任意の複素数列 $(b(y))_{1\leq y\leq Y}$ と $\varepsilon>0$ に対して,

$$\sum_{X/2<p\leq X}\left|\sum_{1\leq y\leq Y}b(y)e(\alpha p^k y)\right|\ll\left(XY^{1+\varepsilon}\sum_{1\leq y\leq Y}|b(y)|^2\right)^{\frac{1}{2}}$$

が成立する. ただし implicit constant は ε,C に依存する.

Note 36 (Lemma 5.4 の証明, l.3–l.5)**.** ここで “When $(h,q)=1$, the number J ... satisfies $J\ll q^{\varepsilon}$” とりありますが, これは次のようにしてわかります：

まず, 夏の部でも用いた次の評価を示します.

Lemma 16. 自然数 $q\geq9$ に対して

$$\omega(q)\leq\frac{4\log q}{\log\log q}.$$

ただし $\omega(q)$ は q の互いに異なる素因数の個数.

Proof. 実数 $U > 1$ をとります.（あとで U の具体的な値を定めます.）そこで

$$\omega(q) = \omega_1(q) + \omega_2(q)$$

ただし

$$\omega_1(q) \coloneqq \sum_{\substack{p \mid q \\ p \le U}} 1 \quad \text{および} \quad \omega_2(q) \coloneqq \sum_{\substack{p \mid q \\ p > U}} 1$$

とおきましょう. すると, 明らかに

$$\omega_1(q) \le \sum_{p \le U} 1 \le U$$

です. また

$$U^{\omega_2(q)} < \prod_{\substack{p \mid q \\ p > U}} p \le q \quad \text{なので} \quad \omega_2(q) \le \frac{\log q}{\log U}$$

です. 以上を合わせて

$$\omega(q) \le U + \frac{\log q}{\log U}$$

を得ます. ここで例えば

$$U = \frac{2 \log q}{\log \log q}$$

とでもおけば（q が大のときこれは最良ではありませんけれど）,

$$U = \frac{\log q}{\log((\log q)^{\frac{1}{2}})} \ge (\log q)^{\frac{1}{2}} > \log 3 > 1$$

なので

$$\omega(q) \le \frac{2 \log q}{\log \log q} + \frac{\log q}{\log\left((\log q)^{\frac{1}{2}}\right)} \le \frac{4 \log q}{\log \log q}$$

を得ます. □

評価 $J \ll q^{\varepsilon}$ の証明に戻ります. 一般性を失わず $0 < \varepsilon < 1$ と仮定できます. さて

$$J(q) = J(q, h) \coloneqq \#\{x \pmod q \mid x^k \equiv h \pmod q,\ (x, q) = 1\}$$

とおくと, 中国式剰余定理より

$$J(q, h) = \prod_{p^v \| q} J(p^v, h)$$

です. ここでテキストの p.22 の l.17–19 より

$$J(p^v, h) \le p^{\gamma - \tau - 1}(k, \phi(p^{\tau+1})) \le 2k$$

なので（ここで γ はテキストの式 (2.25) で定義されました. よって $p \neq 2$ ならば $\gamma = \tau + 1$ であり, $p = 2$ のときでも $\gamma \le \tau + 2$ です.）,

$$J(q, h) \le \prod_{p \mid q} (2k) = (2k)^{\omega(q)}$$

を得ます. よって Lemma 16 を用いれば $q \ge \exp((2k)^{\frac{2}{\varepsilon}}) \ge 9$ のとき,

$$J(q, h) \le \exp\left(\log 2k \cdot \frac{2 \log q}{\log \log(\exp((2k)^{\frac{2}{\varepsilon}}))}\right) = q^{\varepsilon}$$

となるので, $q \le \exp((2k)^{\frac{2}{\varepsilon}})$ のときは自明に $\omega(q) \le q \le \exp((2k)^{\frac{2}{\varepsilon}})$ と評価すれば

$$J = J(q,h) \le \exp((2k)^{\frac{2}{\varepsilon}}) q^{\varepsilon}$$

がすべての自然数 q に対して成立します.

Note 37 (Lemma 5.4 の証明, l.5–l.8)**.** ここで行われている分割

$$\mathscr{P} \coloneqq \{X/2 < p \le X\} = \bigsqcup_{1 \le j \le L} \mathscr{P}_j, \quad L \ll q^{\varepsilon}$$

であって条件

$$\forall j \in \{1, \dots, L\},\ \forall p_1, p_2 \in \mathscr{P}_j,\ p_1^k \equiv p_2^k \pmod q \implies p_1 \equiv p_2 \pmod q$$

を満たすものは次のようにして与えられます. まず,

$$\mathscr{P} = \mathscr{P}^{\sharp} \sqcup \mathscr{P}^{\flat}$$

ただし

$$\mathscr{P}^{\sharp} \coloneqq \{p \in \mathscr{P} \mid (p,q) = 1\} \quad \text{および} \quad \mathscr{P}^{\flat} \coloneqq \{p \in \mathscr{P} \mid (p,q) > 1\}$$

と分割します. まず $\mathscr{P}^{\flat}$ について考えます. 観察

$$2^{\omega(q)} \le \prod_{p \mid q} p \le q$$

を用いれば

$$J^{\flat} \coloneqq \#\mathscr{P}^{\flat} \le \omega(q) \le \frac{\log q}{\log 2} = \frac{\log q^{\varepsilon}}{\varepsilon \log 2} \le \frac{1}{\varepsilon \log 2} q^{\varepsilon}$$

です. つまり $\mathscr{P}^{\flat}$ については単に singleton たちにバラバラにしてしまえば十分です. 次に $\mathscr{P}^{\sharp}$ について考えます. まず

$$\mathscr{A}_k(q) \coloneqq \{h \pmod q \mid (h,q) = 1,\ \exists x \pmod q,\ x^k \equiv h \pmod q\}$$
$$\mathscr{B}_k(q,h) \coloneqq \{x \pmod q \mid (x,q) = 1,\ x^k \equiv h \pmod q\}$$

とおきましょう. 明らかに（ただの $(\mathrm{mod}\ q)$ の乗法群での coset 分解）

$$(\mathbb{Z}/q\mathbb{Z})^{\times} = \bigsqcup_{h \in \mathscr{A}_k(q)} \mathscr{B}_k(q,h)$$

と分割されます. するとテキストの p.22 の l.17–19 より任意の $h \in \mathscr{A}_k(q)$ に対して

$$J(q,h) \coloneqq \#\mathscr{B}_k(q,h) = J(q)$$

となる h によらない定数 $J = J(q)$ が存在します. したがって,

$$\mathscr{B}_k(q,h) = \{b_1(h) \pmod q, \dots, b_J(h) \pmod q\}$$

と互いに異なる剰余たち $b_1(h) \pmod q, \dots, b_J(h) \pmod q$ を用いて $\mathscr{B}_k(q,h)$ を表示することができます. このとき j, h で添字付けられた

$$b_j(h) \pmod q \quad (1 \le j \le J,\ h \in \mathscr{A}_k(q)) \quad \text{は互いに異なる}$$

ことに注意します. この記号の下,

$$\mathscr{P}_j^{\sharp} \coloneqq \bigsqcup_{h \in \mathscr{A}_k(q)} \{p \in \mathscr{P} \mid p \equiv b_j(h) \pmod q\} \quad (1 \le j \le J)$$

とおきましょう. すると目的の分割は

$$\mathscr{P} = \bigsqcup_{j=1}^{J} \mathscr{P}_j^\sharp \sqcup \bigsqcup_{p \in \mathscr{P}^\flat} \{p\}$$

という形で与えられます. 対応する L は

$$L = J + J^\flat \ll q^\varepsilon$$

となり, また任意の $1 \le j \le J$ と $p_1, p_2 \in \mathscr{P}_j^\sharp$ に対して,

$$h \coloneqq p_1^k \equiv p_2^k \pmod q$$

ならば $\mathscr{P}_j^\sharp$ の定義より

$$p_1 \equiv b_j(h) \equiv p_2 \pmod q$$

となります.

Note 38 (Lemma 5.4 の証明, 式 (5.45))**.** Large sieve を用いるとまずは

$$\sum_{\substack{X/2 < p \le X \\ p \in \mathscr{P}_j}} \left| \sum_{y \le Y} b_y e(\alpha p^k y) \right| \ll (Y+q) \sum_{y \le Y} |b_y|^2$$

を得ますが, ここで仮定されている

$$q \le 2X^k \quad \text{および} \quad X^k \ll Y$$

を用いれば $q \ll Y$ となるので式 (5.45) を得ます.

Note 39 (Lemma 5.4 の証明, p.73, l.14–15)**.** ここでの "$\gg$" における評価ですが, $p_1, p_2 > X/2$ なので仮定

$$|\beta| \gg \frac{1}{qX^{k-1}Y}, \quad p_1 \equiv p_2 \pmod q \quad \text{および} \quad p_1 \ne p_2$$

より $|p_1 - p_2| \ge q$ となることに気をつけて

$$\begin{aligned} |\beta||p_1^k - p_2^k| &\gg \frac{1}{qX^{k-1}Y} |p_1 - p_2| (p_1^{k-1} + \cdots + p_2^{k-1}) \\ &\gg \frac{1}{X^{k-1}Y} X^{k-1} = \frac{1}{Y} \end{aligned}$$

となることで従います.

12.5 Wooley's upper bound for $G(k)$

Note 40 (Proof of Lemma 12.5, l.6)**.** Lemma 5.4 ないしは上記 Lemma 15 の適用方法ですが, まず, c_m の定義より

$$m > uX^k \implies c_m = 0$$

なので Lemma 15 における Y を $Y = uX^k$ と選べば（Lemma 15 における内側の和の長さを表す Y と現在の Lemma における smoothness を controll する Y は違うものです）, Lemma 15 の仮定が満たされているので,

$$h(\alpha)^{2u} \ll X^{2u-2} \cdot X(uX^k)^{1+\varepsilon} \sum_m |c_m|^2$$

$$\ll u^2 X^{2u-1+k+\varepsilon} \sum_m |c_m|^2$$

を得ます. (最後の u^2 の部分はあまり重要ではなく implicit constant に含めても良いです.)

Note 41 (Proof of Lemma 12.5, l.7)**.** Lemma 12.5 の証明の最後の部分ですが, ここでは

$$\begin{aligned}\sum_m |c_m|^2 &= \sum_m \#\{\boldsymbol{x} \in \mathscr{A}(X,Y)^u \mid p(\boldsymbol{x}) = m\} \times \#\{\boldsymbol{y} \in \mathscr{A}(X,Y)^u \mid p(\boldsymbol{y}) = m\} \\ &= \sum_m \#\{(\boldsymbol{x},\boldsymbol{y}) \in \mathscr{A}(X,Y)^u \times \mathscr{A}(X,Y)^u \mid p(\boldsymbol{x}) = p(\boldsymbol{y}) = m\} \\ &= \#\{(\boldsymbol{x},\boldsymbol{y}) \in \mathscr{A}(X,Y)^u \times \mathscr{A}(X,Y)^u \mid p(\boldsymbol{x}) = p(\boldsymbol{y})\} = S_u(X,Y)\end{aligned}$$

であることに注目して Theorem 12.4 を用いると,

$$h(\alpha)^{2u} \ll u^2 X^{2u-1+k+\varepsilon} S_u(X,Y) \ll u^2 X^{4u-1+k\exp(1-\frac{2u}{k})+\varepsilon}$$

となるので, $u^{\frac{1}{u}} \ll 1$ を用いて

$$h(\alpha) \ll X^{2-(\frac{1}{2u}-\frac{k}{2u}\exp(1-\frac{2u}{k}))+\varepsilon} = X^{2(1-(\frac{1}{4u}-\frac{k}{4u}\exp(1-\frac{2u}{k})))+\varepsilon}$$

となります. さらに u を最適化すれば Lemma12.5 の最初の主張

$$h(\alpha) \ll X^{2(1-\sigma)+\varepsilon}, \quad \sigma \coloneqq \max_{u\in\mathbb{N}} \left(\frac{1}{4u} - \frac{k}{4u}\exp\left(1-\frac{2u}{k}\right)\right)$$

が得られます.

次に上記 max の漸近評価である (12.39) と (12.41) を導出しましょう. 評価 (12.39) と (12.41) は漸近評価なので k は十分大きいとして良いです. まず上で得られた max の中身を

$$\phi(u) \coloneqq \frac{1}{4u} - \frac{k}{4u}\exp\left(1-\frac{2u}{k}\right)$$

とおきます. しばらくの間これを $u \in (0,+\infty)$ 上の関数とみます. 微分を通して ϕ の増減を見ます. 関数 ϕ 自身の微分を計算すると

$$\phi'(u) = -\frac{1}{4u^2} + \frac{k}{4u^2}\exp\left(1-\frac{2u}{k}\right) + \frac{1}{2u}\exp\left(1-\frac{2u}{k}\right)$$

です. そこで

$$\psi(u) \coloneqq \phi'(u)\cdot 4u^2 e^{\frac{2u}{k}} = -e^{\frac{2u}{k}} + (k+2u)e$$

とおきましょう. すると $\phi'(u)$ と $\psi(u)$ の符号は等しくなります. 再度微分して

$$\psi'(u) = -\frac{2}{k}e^{\frac{2u}{k}} + 2e \tag{81}$$

を得ます. よって $\psi'(u)$ は

$$\psi'(0) = 2e - \frac{2}{k} > 0, \quad \psi'(u_2) = 0, \quad \psi'(u) \begin{cases} > 0 & (\text{for } 0 < u < u_2), \\ < 0 & (\text{for } u > u_2) \end{cases}$$

をある u_2 に対して満たします. (実際には $u_0 = \frac{k}{2}(\log k + 1)$.) 従ってまた $\psi(u)$ は

$$\psi(0) = ke - 1 > 0, \quad \psi(u_1) = 0, \quad \psi(u) \begin{cases} > 0 & (\text{for } 0 < u < u_1), \\ < 0 & (\text{for } u > u_1) \end{cases}$$

をある τ に対して満たします. さらに $\phi'(u)$ も同様の符号変化を持ち, 従って $\phi(u)$ は $\psi(u_1)=0$ なる u_1 に対して,

$$\begin{cases} u\in(0,u_1) \text{ にて } \phi(u) \text{ は単調増加}, \\ u\in(u_1,+\infty) \text{ にて } \phi(u) \text{ は単調減少}, \end{cases}$$

を満たします. この u_1 は

$$\psi(u_1)=0 \iff e^{\frac{2u_1}{k}}=ke\left(1+\frac{2u_1}{k}\right)$$

で決まるので,

$$e^{\tau}=ke(1+\tau) \tag{82}$$

なる τ を取っておけば,

$$u_1=\frac{k}{2}\tau$$

で与えられます. 従って u が正の実数値を動くとき $\phi(u)$ の最大値は (82) より

$$\phi(u_1)=\frac{1}{2k\tau}-\frac{1}{2\tau}e^{1-\tau}=\frac{1}{2k\tau}-\frac{1}{2k\tau(1+\tau)}=\frac{1}{2k(1+\tau)} \tag{83}$$

となります. しかし実際には u の値は自然数で与えなければいけないので

$$u_0=[u_1] \quad \text{または} \quad u_0=[u_1]+1$$

が σ の値を

$$\sigma=\phi(u_0)$$

と定めます. どちらにせよ $|u_0-u_1|\leq 1$ です. 注意ですが,

$$e^{\tau}=ke(1+\tau)\geq e$$

なので $\tau\geq 1$ であり, $u_1\geq\frac{k}{2}\geq 1$ を得て, 上記 2 つの u_0 の値, 特に $[u_1]$ は正の整数になります. これから σ 自身が $\phi(u_1)$ とどれだけ近いか評価しますが, まずその前に τ ないしは u_1 に対して評価を行います.

上記 τ の定義 (82) より

$$e^{\tau}=ke(1+\tau)\geq ke$$

なので

$$\tau\geq\log k+1$$

です. 再び τ の定義 (82) に戻り

$$e^{\tau}=ke(1+\tau)\geq k(\log k)e$$

なので

$$\tau\geq\log k+\log\log k+1$$

を得ます. よって k が十分大きいとき, また τ の定義 (82) の対数を取り

$$\tau=\log k+1+\log(1+\tau)\leq\log k+\frac{\tau}{2} \tag{84}$$

となるので

$$\tau\leq 2\log k$$

です. これを再度 (84) に代入して

$$\tau \leq \log k + \log\log k + O(1)$$

を得ます. 以上を合わせて

$$\tau = \log k + \log\log k + O(1) \tag{85}$$

を得ます.

さて, σ の考察に戻ります. 微積分学における平均値の定理と (83) より

$$\sigma = \phi(u_0) = \phi(u_1) + \phi'(\xi)(u_0 - u_1) = \frac{1}{2k(1+\tau)} + \phi'(\xi)(u_0 - u_1) \tag{86}$$

を得ます. ただし ξ は u_0 と u_1 の間の実数です. 次に $\phi'(\xi)$ を抑えます. まず,

$$\phi'(\xi) = \frac{1}{4\xi^2 e^{\frac{2\xi}{k}}}\psi(\xi) \tag{87}$$

を思い出します. 再び平均値の定理と u_1 の定義より

$$\psi(\xi) = \psi(u_1) + \psi'(\eta)(\xi - u_1) = \psi'(\eta)(\xi - u_1) \tag{88}$$

を得ます. ただし η は ξ と u_1 の間の実数, よって u_0 と u_1 の間の実数となります. 従って少なくとも $\eta \leq u_1 + 1$ であり, (81) と (85) より

$$|\psi'(\eta)| \leq \frac{2}{k}e^{2\eta}k + 2e \ll \frac{1}{k}e^{\tau} + 1 \ll \log k$$

を得ます. 明らかに $|\xi - u_1| \leq |u_0 - u_1| \leq 1$ なので, ここから (88) より

$$\psi(\xi) \ll \log k$$

を得ます. この評価と (82), (85) を用いつつ (87) を経由して

$$\phi'(\xi) \ll \frac{1}{(k\tau)^2 e^{\tau}}\log k \ll \frac{1}{k^3(1+\tau)\log k}$$

を得ます. この評価を (86) に代入し $|u_0 - u_1| \leq 1$ に気をつけることで

$$\sigma = \frac{1}{2k(1+\tau)}\left(1 + O\left(\frac{1}{k^2\log k}\right)\right)$$

つまり (12.39) を得ます. すると (12.41) はこの評価と (85) を組み合わせれば直ちに従います. なお, 注意ですが, 十分大の u に対して $\phi(u) > 0$ であることと, 自然数 u に対して $\phi(u) < 1/4u \leq 1/4$ なので

$$\sigma \in (0, \tfrac{1}{4}) \tag{89}$$

です.

Note 42 (Theorem 12.5 の証明)**.** まず, 夏までに示したことを復習しておきます. 自然数をいくつかの k 乗数の和で書き表すわけですが, この和で書き表したい自然数を n とおき,

$$N = [n^{\frac{1}{k}}], \quad P = \frac{N}{2k}, \quad \mathscr{U} := \left[\frac{P}{n}, 1 + \frac{P}{n}\right], \quad \mathfrak{M}(q,a) := \left[\frac{a}{q} - \frac{P}{qn}, \frac{a}{q} + \frac{P}{qn}\right]$$

とおきます. すると, 夏に行った議論と同様にして

$$\mathfrak{M} \coloneqq \bigsqcup_{q\le P} \bigsqcup_{\substack{1\le a\le q\\(a,q)=1}} \mathfrak{M}(q,a) \subset \mathscr{U}$$

を得ることが出来ます（§4.4 の冒頭参照）. 夏の部の後半では major arc 上での積分

$$R_{\mathfrak{M}}(m) \coloneqq \int_{\mathfrak{M}} f(\alpha)^s e(-\alpha m)d\alpha, \quad f(\alpha) \coloneqq \sum_{1\le x^k\le n} e(\alpha x^k)$$

が非常に広い範囲の s で計算可能であることを示しました（Theorem 4.4 および夏の部の際の Memo の Note 6 を参照）:

Theorem 3. 自然数 k と $s > \max(8,k)$ に対して, ある正の実数 δ が存在して, 任意の自然数 $m \in [1,n]$ に対して

$$R_{\mathfrak{M}}(m) = \Gamma\left(1+\frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} \mathfrak{S}(m) m^{\frac{s}{k}-1} + O(n^{\frac{s}{k}-1-\delta})$$

が成立する.

ここで $R_{\mathfrak{M}}(m)$ を考えるのでは k 乗数の和で書き表したいのは n よりむしろ m であるように見えます. しかし, これはこの後行う細工のため, 少し一般の m を考えているというだけです. また singular series $\mathfrak{S}(m)$ に対しては夏の考察をまとめると次が得られていました（Lemma 2.15, Theorem 4.5, 4.6 および夏の部の際のプログラムに付随した分担の詳細の 20 を参照）:

Theorem 4. 自然数 $k \ge 2$ と $s \ge 4k$ に対して, $\mathfrak{S}(m) \gg 1$.

以上の Theorem 3 と Theorem 4 を組み合わせて次を得ます：

Theorem 5. 自然数 $n \ge 1$, $k \ge 2$, $s \ge 4k$ および $m \in [n/2, n]$ に対して,

$$R_{\mathfrak{M}}(m) \gg_{s,k} n^{\frac{s}{k}-1}$$

が十分大の $n \ge n_0(s,k)$ に対して成立する.

さて, 冬の部でのアイデアは minor arc の評価をうまくコントロールするために k 乗数の動く範囲を都合よく操作できる構造を持つ自然数に制限するというものでした. Chapter 2 での minor arc の評価では Hua の補題 (Lemma 2.5) で与えられる平均値定理と Weyl の不等式（Lemma 2.4）で与えられる minor arc 上の各点評価が要でした. 冬の部で示した Hua の補題（Lemma 2.5）に対応する平均値定理は

$$S_b(Q,R) = \int_0^1 |g(\alpha)|^{2b} d\alpha \ll Q^{\lambda_b+\varepsilon}$$

というように Theorem 12.4 で与えられました. ただしここで

$$g(\alpha) \coloneqq \sum_{y\in\mathscr{A}(Q,R)} e(\alpha y^k), \quad \lambda_b \le 2b - k + k\exp\left(1-\frac{2b}{k}\right)$$

および R は b,k,ε に依存した定数 $\eta > 0$ によって $R = Q^\eta$ と与えられます. 一方, Weyl の不等式（Lemma 2.4）に対応する minor arc 上の各点評価は有理近似

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{2qX^k}, \quad q \le 2X^k \tag{90}$$

と条件

$$q \le X \implies \left|\alpha - \frac{a}{q}\right| > \frac{1}{qX^{2k-1}}$$

が成立している α に対して

$$h(\alpha) \ll X^{2(1-\sigma)+\varepsilon}$$

と Lemma 12.5 で与えられました. ただしここで

$$h(\alpha) \coloneqq \sum_{X/2<p\le X} \sum_{z\in\mathscr{A}(X,Y)} e(\alpha p^k z^k), \quad \sigma \sim \frac{1}{2k\log k} \quad (k\to\infty)$$

および Y は k,ε に依存した定数 $\zeta>0$ によって $Y = X^{\zeta}$ と与えられます. 上記 b,ε,η,ζ ですが, k のみに依存して b と ε が選ばれて, そののちに η,ζ が選ばれるので結局 η,ζ も k のみに依存します. 上記 2 つの評価を同時に使うためには

$$\int_0^1 g(\alpha)^{2b} h(\alpha)^c e(-\alpha n) d\alpha$$

というような積分を考えることになります. しかし, このように k 乗数の動く範囲を制限してしまうと major arc のコントロールが難しくなるように見えます. そこで,Theorem 5 が適用可能な分まで普通の k 乗数を無理やり付加し

$$\begin{aligned} r(n) &= \int_0^1 f(\alpha)^{4k} g(\alpha)^{2b} h(\alpha)^c e(-\alpha n) d\alpha \\ &= \#\left\{ \begin{array}{c} \boldsymbol{x}\in([1,N]\cap\mathbb{N})^{4k} \\ \boldsymbol{y}\in\mathscr{A}(Q,R)^{2b} \\ X/2<p_1,\dots,p_c\le X \\ z_1,\dots,z_c\in\mathscr{A}(X,Y)^c \end{array} \middle| \ n = p(\boldsymbol{x}) + p(\boldsymbol{y}) + \sum_{i=1}^{c} (p_i z_i)^k \right\} \le R_{k,s}(n) \end{aligned} \tag{91}$$

(記号 $p(\boldsymbol{x})$ についてはこのノートの p.10 の l.4 を参照のこと.) ただし

$$s = 4k + 2b + c$$

という積分を考えてしまうことで major arc 上の積分もきちんと下から評価できるようにします. 実際 $r(n)$ に対応する major arc 上の積分は

$$r_{\mathfrak{M}}(n) \coloneqq \int_{\mathfrak{M}} f(\alpha)^{4k} g(\alpha)^{2b} h(\alpha)^c e(-\alpha n) d\alpha$$

となりますが, $g(\alpha)$ と $h(\alpha)$ の定義を開いて

$$\begin{aligned} r_{\mathfrak{M}}(n) = &\sum_{y_1,\dots,y_{2b}\in\mathscr{A}(Q,R)} \sum_{X/2<p_1,\dots,p_c\le X} \sum_{z_1,\dots,z_c\in\mathscr{A}(X,Y)} \\ &\times \int_{\mathfrak{M}} f(\alpha)^{4k} e(-\alpha(n - (y_1^k + \cdots + y_{2b}^k + (p_1z_1)^k + \cdots + (p_cz_c)^k))) d\alpha \end{aligned}$$

を得ます. よって

$$y_1^k + \cdots + y_{2b}^k + (p_1z_1)^k + \cdots + (p_cz_c)^k \le \frac{n}{2}$$

となるように, 例えば

$$Q = \left(\frac{n}{2s}\right)^{\frac{1}{k}}, \quad X = Q^{\frac{1}{2}}$$

とおけば実際に

$$y_1^k + \cdots + y_{2b}^k + (p_1z_1)^k + \cdots + (p_cz_c)^k$$

$$\leq 2bQ^k + cX^{2k} = (2b+c)Q^k \leq sQ^k \leq \frac{n}{2}$$

となるので, Lemma 12.1-(ii) と Theorem 5 および R と Y の選び方より

$$\begin{aligned} r_{\mathfrak{M}}(n) &\gg n^{\frac{4k}{k}-1} \sum_{y_1,\dots,y_{2b}\in\mathscr{A}(Q,R)} \sum_{X/2<p_1,\dots,p_c\leq X} \sum_{z_1,\dots,z_c\in\mathscr{A}(X,Y)} 1 \\ &\gg n^3 A(Q,R)^{2b}(\pi(X)-\pi(X/2))^c A(X,Y)^c \qquad (92) \\ &\gg n^3 Q^{2b}\left(\frac{X}{\log X}\right)^c X^c = n^3 Q^{2b} X^{2c} (\log X)^{-c} \end{aligned}$$

と下からの評価を得ます. 注意ですが, (91) でも暗に見たように $r(n)$ は

$$n = x_1^k + \cdots + x_{4k}^k + y_1^k + \cdots + y_{2b}^k + (p_1 z_c)^k + \cdots + (p_c z_c)^k$$

ただし

$$\begin{aligned} &1 \leq x_1^k, \dots, x_{4k}^k \leq n, \quad y_1, \dots, y_{2b} \in \mathscr{A}(Q,R), \\ &X/2 < p_1, \dots, p_c \leq X, \quad z_1, \dots, z_c \in \mathscr{A}(X,Y) \end{aligned}$$

という k 乗数の和による表示の個数を数えるので $r(n) \leq R_{k,s}(n)$ を得ます. 従って, もし十分大きいすべての自然数 n に対して $r(n) > 0$ であることが示せれば, そこから $G(k) \leq 4k + 2b + c$ が得られます.

残るは冬の部で得たことを組み合わせて minor arc 上の積分

$$r_{\mathfrak{m}}(n) \coloneqq \int_{\mathfrak{m}} f(\alpha)^{4k} g(\alpha)^{2b} h(\alpha)^c e(-\alpha n) d\alpha$$

を評価して major arc の寄与の下からの評価 (92) より order が小さいことを示すことです. まず, $f(\alpha)$ に関しては取り扱うのを諦めて自明に評価し, 残りの部分は作戦通り

$$\begin{aligned} r_{\mathfrak{m}}(n) &\ll n^{\frac{4k}{k}} \int_{\mathfrak{m}} |g(\alpha)|^{2b} |h(\alpha)|^c d\alpha \\ &\ll n^4 \left(\sup_{\alpha\in\mathfrak{m}} |h(\alpha)|\right)^c \int_0^1 |g(\alpha)|^{2b} d\alpha \\ &= n^4 \left(\sup_{\alpha\in\mathfrak{m}} |h(\alpha)|\right)^c S_b(Q,R) \end{aligned}$$

とします. この後 Lemma 12.5 を用いるために Lemma 12.5 での α の条件が $\alpha \in \mathfrak{m}$ ならば（n が十分大のとき）成立することを確認します. Dirichlet の有理近似定理によって与えられる有理近似 (90) において $q \leq X$ とすると,

$$q \leq X = Q^{\frac{1}{2}} \leq n^{\frac{1}{2k}} \leq \frac{[n^{\frac{1}{k}}]}{2k} = P$$

となるので, $\alpha \in \mathfrak{m}$ だから $\alpha \notin \mathfrak{M}(q,a)$ なので

$$\left|\alpha - \frac{a}{q}\right| > \frac{P}{qn} = \frac{[n^{\frac{1}{k}}]}{2kqn} \geq \frac{\left(\frac{n}{2s}\right)^{\frac{1}{2k}}}{q\left(\frac{n}{2s}\right)} = \frac{1}{qX^{2k-1}}$$

を得て α は Lemma 12.5 の条件を満たすことがわかります. ここで Theorem 12.4 と Lemma 12.5 を用いて

$$r_{\mathfrak{m}}(n) \ll n^4 X^{2c(1-\sigma)+c\varepsilon} Q^{2b-k+k\exp(1-\frac{2b}{k})+\varepsilon}$$

$$\ll n^3Q^{2b}X^{2c}\cdot nQ^{-k}\cdot X^{-2c\sigma+c\varepsilon}Q^{k\exp(1-\frac{2b}{k})+\varepsilon}.$$

ここで

$$Q=\left(\frac{n}{2s}\right)^{\frac{1}{k}},\quad X=Q^{\frac{1}{2}}$$

を思い出すと

$$r_{\mathfrak{m}}(n)\ll n^3Q^{2b}X^{2c}\cdot Q^{-c\sigma+k\exp(1-\frac{2b}{k})+c\varepsilon} \tag{93}$$

を得ます.

これから (93) が (92) より小さくなるようにしつつも, $G(k)$ の上界 $4k+2b+c$ がなるべく小さくなるように b,c を選んでいきます. まず, major arc の寄与 (92) と minor arc の寄与の評価 (93) を比べると $n^3Q^{2b}X^{2c}$ の部分は同じなので少なくとも残りの Q の指数の主たる部分

$$-c\sigma+k\exp\left(1-\frac{2b}{k}\right)$$

は負でないといけません. また $G(k)$ の上界 $4k+2b+c$ は c が小さいほど小さくなりますので, 与えられた b に対し, 最適な c はおおよそ上の指数が 0 となる

$$c\approx\frac{k}{\sigma}\exp\left(1-\frac{2b}{k}\right)$$

周辺であるとわかります. 実際には Q^{ε} や $(\log X)^c$ 等の小さな因子を打ち消さないといけない上に c は自然数でないといけないので

$$c=\left[\frac{k}{\sigma}\exp\left(1-\frac{2b}{k}\right)\right]+2>\frac{k}{\sigma}\exp\left(1-\frac{2b}{k}\right)+1$$

ととりましょう. (c の値を $O(1)$ 程度動かしても最終的な $G(k)$ の上界も $O(1)$ 程度しか動きません.) すると最終的な $G(k)$ の上界は

$$4k+2b+c=4k+2b+\left[\frac{k}{\sigma}\exp\left(1-\frac{2b}{k}\right)\right]+2$$

となりますので, 次の課題はおおよそ

$$\phi(b)\coloneqq 2b+\frac{k}{\sigma}\exp\left(1-\frac{2b}{k}\right),\quad b\in\mathbb{N}$$

の最小化です. 微分を取れば

$$\phi'(b)=2-\frac{2}{\sigma}\exp\left(1-\frac{2b}{k}\right)$$

となるので, ((89) を思い出して $\phi'(0)<0$ を確認すれば) 最適な b は $\phi'(b)=0$ となる

$$b\approx\frac{k}{2}\log\frac{e}{\sigma}>0$$

におおよそなる事がわかります. この値より $O(1)$ だけ大きい b を取る分には上記 $\phi(b)$ の第 2 項は小さくなるだけで第 1 項は $O(1)$ しか増加しないので整数値を取るように

$$b=\left[\frac{k}{2}\log\frac{e}{\sigma}\right]+1>\frac{k}{2}\log\frac{e}{\sigma}$$

ととりましょう.（テキストとは選び方が少しだけ違います.）すると

$$\frac{k}{\sigma}\exp\left(1-\frac{2b}{k}\right)\le\frac{k}{\sigma}\exp\left(1-\log\frac{e}{\sigma}\right)=k$$

なので

$$4k+2b+c=k\log\frac{e}{\sigma}+O(k)=k\log\frac{1}{\sigma}+O(k) \tag{94}$$

を得ます. 上記 b,c の選び方の下,

$$c=\left[\frac{k}{\sigma}\exp\left(1-\frac{2b}{k}\right)\right]+2\le k+2$$

です. そこで最初に ε を

$$\varepsilon=\frac{\sigma}{2(k+2)}$$

とでも選び（これは k のみに依存します）, 対応して η,ζ を選べば,

$$-c\sigma+k\exp\left(1-\frac{2b}{k}\right)<-\sigma$$

なので (93) より

$$\begin{aligned}r_{\mathfrak{m}}(n)&\ll n^3Q^{2b}X^{2c}\cdot Q^{-c\sigma+k\exp(1-\frac{2b}{k})+(k+2)\varepsilon}\\&\ll n^3Q^{2b}X^{2c}\cdot Q^{-\frac{\sigma}{2}}=n^3Q^{2b}X^{2c}\cdot X^{-\sigma}\end{aligned}$$

を得ます. そこで (92) と合わせて,

$$\begin{aligned}R_{k,s}(n)&\ge r(n)=r_{\mathfrak{M}}(n)+r_{\mathfrak{m}}(n)\\&\ge c_1(k)n^3Q^{2b}X^{2c}(\log X)^{-c}-c_2(k)n^3Q^{2b}X^{2c}\cdot X^{-\sigma}\end{aligned}$$

がなんらかの正の定数 $c_1(k),c_2(k)$ に対して成立します. よってあとは n を十分大（従って X を十分大）にすることで $R_{k,s}(n)>0$ が知れて (94) より

$$G(k)\le 4k+2b+c=k\log\frac{1}{\sigma}+O(k)$$

がわかります. また (12.41) を用いれば

$$G(k)\le k\log k+k\log\log k+O(k)$$

となることも直ちにわかります.

References

1. H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory: I. Classical Theory*, Cambridge studies in advanced mathematics, vol. 97, Cambridge University Press, 2006.
2. R. C. Vaughan, *The Hardy–Littlewood Method*, 2nd ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, 1997.