第 18 回　岡シンポジウム
奈良女子大学

素数分布論

最近の進展への道程

本橋　洋一

0. 素数分布に関する「伝統的な難問」幾つかにつき, 最近の進展への道程を概観する. 正しくは, 平成 26 年春日本数学会企画特別講演「双子素数予想」(英文版を別添) を理解するに足る基礎, 沿革, 付帯知識の解説である. 従って, 素数分布論の俯瞰を試みるものではないが, 概ねそれに近い. 本講演では, 当然ながら, 詳細を割愛し論文等にては容易には伺い得ない綾を伝えることに専ら努める. 従って, ここにまとめるところは, 講演中の参照に供するものであり, その全てに言及する訳ではない. 参考文献は, 各節の必要に応じ中心的なものを掲示する. 関連の総合的な書籍は様々であり何れを採るべきか迷う. ここでは, 文献の簡明を旨とし, 次の自著を主に参照する:

[A] Sieve methods and prime number theory. Tata Lecture Notes, vol.72, 1983.
[B] Spectral theory of the Riemann zeta-function. Cambridge Tracts, vol.127, 1997.
[C] 解析的整数論 I. 朝倉書店, 2009.
[D] 解析的整数論 II. 朝倉書店, 2011.
[E] 整数論基礎講義. 朝倉書店, 2018.

これらの著述の通奏低音は, $\mathbb{Z}$ 内に差す様々な直交性の影がなすところである. 例えば,

$$\text{互いに素 (互除法)} \ \to \ \mathrm{SL}(2,\mathbb{Z}) \ \to \ \{ \text{保型形式} \}$$

なる図式から, 互いに素なる概念を出発点とする Euclid 整数論 ($\Sigma\tau o\iota\chi\epsilon\tilde{\iota}\alpha$ 巻 VII, VIII, IX) の上空に壮大な直交系があることが見て取れる (詳細は [D]). Gauss 整数論は群論に包まれ, それを受けた Dirichlet の整数論は (剰余群の) 指標の直交性に負うところ大. 更には, 本講演の核心をなす Linnik–Selberg 篩理論には他種の直交性が潜んでいる. 思うに, 篩は互いに素なる事象の解析である. 今日の解析的整数論は, 多様な直交性に起因するところを総動員し「整数の乗法的特性」に関する素朴な疑問に立ち向かう. ごく一部の描写にならざるを得ないが, 講演にてその機微が次第にほの見えて来ることであろう.

記号 p は添字も含め一般に素数を表すものとする. 記号 $s = \sigma + it$ ($\sigma, t \in \mathbb{R}$) は特に断りの無い限り複素変数である (Dirichlet–Riemann の記号). 数式中の $c > 0$ は常数. ただし, 出現箇所ごとに異なるもの, とする. さらに, $\varepsilon > 0$ は微小なる常数であるが, やはり出現箇所ごとに異なると理解すべきもの. ある ε_0 を定め, 各 ε は ε_0 の正整数倍とするも可. なお, Landau の 'O', 'o' 記号, Vinogradov の '$\ll$' 記号 (O 記号の代用) も用いるが, それらに含まれる陰伏常数 (implied constants) も場所により異なり, ε に関係する可能性もある. これら便法は解析的整数論の悪しき慣習. とは言え, 代わる術俄には見つけ難し.

ときおり, 計算可能性 effective computability に言及する. これは当該の常数などの「実際の数値」を明確に与えることができる, という状態を直観的 naïve に示唆するものである. 必ずしも, 多項式時間算法 (polynomial time algorithm: 演算 に要する universal logic gates の個数が, 具体的な常数 $a, b > 0$ をもって $a\big(\log \text{入力}\big)^b$ 以下) の存在を言明するものではない. 整数論は具体的議論の尊重を標榜するものの, 実態は, いわゆる初等整数論とも言えども, この計算可能性なる根本的な課題は置き去られ, ほぼ全てが存在論である. 典型例には, 与えられた整数の約数を求めることが含まれる. これの現行計算機上の多項式時間算法は未だ知られていない (理論的量子計算機上では知られている: Shor (1994), [E, §§48–51]).

[0.1] Euclid (ca 300 BCE): 彼の数論は巻 X (非通約性 incommensurability あるいは 無限連分数) も含め「乗法的」理論.
(1) Adelardus (1482). Opus elementorum Euclidis megarensis in geometriam artem in id quoque Campani perspicacissimi commentationes finiunt. E. Randolt, Venetiis.

(2) H. Billingsley (1570): The elements of geometrie of the most auncient philosopher Euclide of Megara. J. Daye, London.
(3) T.L. Heath (1956): The thirteen books of Euclid's Elements translated from the text of Heiberg. Second edition. Vols. I–III. Dover, New York: なお, 巻 VII, Prop.20 は, 根本定理

$$\text{最大公約数 } \langle a,b\rangle = 1,\ a|bc \quad \Rightarrow \quad a|c$$

であるが, その証明は (Heath 訳で読む限り) 不可解. D. Pengelley and F. Richman (2006): Did Euclid need the Euclidean algorithm to prove unique factorization? Amer. Math. Monthly, **113**, 196–205 を参照せよ. なお, (1)(2) の表題にある 'megarensis/of Megara' は周知の誤謬. 数学者 Euclid の生誕地年, 没地年は不明.
[0.2] C.F. Gauss (1801): Disquisitiones arithmeticae. Fleischer, Lipsiae. (Werke I, pp.1–478)
[0.3] P.G.L. Dirichlet (1863): Vorlesungen über Zahlentheorie. Herausgegeben von R. Dedekind. Friedrich Vieweg und Sohn, Braunschweig; Zweite Auflage. *Ibid.*, 1871; Dritte Auflage. *Ibid.*, 1879; Vierte Auflage. *Ibid.*, 1894.
[0.4] U.V. Linnik (1941): The large sieve. C.R. Acad. Sci. URSS (N.S.), **30**, 292–294.
[0.5] A. Selberg (1947): On an elementary method in the theory of primes. Norske Vid. Selsk. Forh., Trondhjem, **19**, 64–67. (Collected papers I, pp.363–366)
[0.6] P.W. Shor (1994): Algorithms for quantum computation: Discrete logarithms and factoring. Proc. 35th Ann. Symp. Found. Comp. Sci., IEEE Comp. Soc. Press, pp.124–134. なお, [8.4] を見よ.
[0.7] 上記 [C], [E] に関連し, 次の書籍を推奨する:
(1) K. Pracher (1957): Primzahlverteilung. Springer-Verlag, Berlin.
(2) W. Narkiewicz (2000): The development of prime number theory. Springer-Verlag, Berlin.
(3) R. Crandall and C. Pomerance (2005): Prime numbers. Second edition. Springer-Verlag, New York.

謝辞
伝統深き『岡シンポジウム』に招請頂き, 奈良女子大学岡数学研究所所長松澤淳一教授ならびに関係各位に深く感謝いたします.

1. 素数の個数 $\pi(x) = \sum_{p\le x} 1$ につき最初の言明は Euclid (IX, Prop.20) による $\lim_{x\to\infty} \pi(x) = +\infty$ であるが, 近代/現代における講究の端緒は Euler (1737, 1748 (Tomi primi, Caput XV)) の主張

$$\prod_p \left(1-\frac{1}{p}\right)^{-1} = +\infty. \tag{1.1}$$

些細な点ではあるが, Euclid も Euler も共に「素因数分解の一意性」を用いず. つまり, これらの事実の証明には, 素因数分解の「可能性」のみにて足りる. Euler は $\pi(x)$ 自体に関しては特段には何も残していない. 奇妙に感じられるところである. もっとも, 彼 (1737, Theorema 19) は, (1.1) に並び

$$\sum_{p\le x} \frac{1}{p} \sim \log\log x \quad (x\to\infty), \tag{1.2}$$

をやや不明瞭ながら主張してもいる. これは, n 番目の素数は $\sim n\log n$ であることを暗示するゆえ, 素数定理を予期させるとも言える. が, それは拡大解釈.

そのような区々を超え, Euler (1737, Theorema 8) の偉大な貢献は, 言うまでも無く,

$$\text{Euler 積}:\ \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1-\frac{1}{p^s}\right)^{-1} \neq 0, \quad \sigma > 1, \tag{1.3}$$

の発見である (ここでは $s\in\mathbb{C}$ とするが, そこまで彼が考察した形跡は無い). もっとも, 120 年以上もの後に $\zeta(s)$ が素数分布研究にて主たる座を占めることとなるとは, 彼には恐らくは思いもよらなかったことであろう.

ただし, (1.2) の把握は (1.1) の対数表示を経由するものであることから, $\pi(x)$ に直結する函数 $\log\zeta(s)$ を観察するに近い地点に Euler はいた, と言えぬこともない (Riemann はそれを踏襲). ただ, この函数の扱いは慎重を要する. 接続

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} - s\int_1^\infty \big(x - [x] - \tfrac{1}{2}\big)\frac{dx}{x^{s+1}}, \quad \sigma > 0, \tag{1.4}$$

を $\zeta(s)$ は持つが, $\log\zeta(s)$ の定義そのもの, およびその接続の扱い, は面倒. しかるに, 後に基本とされることとなる函数

$$-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^\infty \frac{\Lambda(n)}{n^s},\ \sigma > 1, \quad \text{von Mangold 函数}\,\Lambda(n) = \begin{cases} \log p & n = p^\nu,\ \nu \in \mathbb{N}, \\ 0 & \text{その他}, \end{cases} \tag{1.5}$$

には同様な困難は無い. 実際, (1.4) にて部分積分を繰り返すならば, $\zeta(s)$ は実は全平面にて有理型であると知れる. もっとも, より明確には後記の (4.3)–(4.4) に依るべきである. つまり, (1.5) の左辺は同様に全平面にて有理型. そこで, 函数 $\log\zeta(s)$ の明確な定義は, σ の値にかかわらず, 積分

$$\int_{+\infty}^{\sigma} \frac{\zeta'}{\zeta}(\alpha + it)d\alpha \quad (\text{積分路上に極を含まず}) \tag{1.6}$$

を経由するものである. これは, Cauchy–Riemann 関係式を経由し, 領域

$$\mathbb{C} - (-\infty, 1] - \bigcup_\rho (-\infty + i\gamma, \rho], \quad \zeta(\rho) = 0,\ \gamma = \operatorname{Im}\rho, \tag{1.7}$$

に含まれる $s = \sigma + it$ の正則函数と知れる. 除去された各半直線上の点については (1.6) の解析接続を用いる. つまり, 「枝」は $\log\zeta(+\infty) = 0$ を充たすべし. [C, pp.15–16] を見よ.

ここで, Stieltjes 積分表示を用い,

$$\pi(x) = \int_2^x \frac{d\psi(u)}{\log u} + O\big(\pi(x^{1/2})\big), \quad \psi(x) = \sum_{n\le x}\Lambda(n), \quad x > 2. \tag{1.8}$$

つまり, 函数 $\pi(x)$ の解析は函数 $\psi(x)$ のそれにて置き換え得るのであり, しかも展開 (1.5) 左辺の有理性ゆえに $\psi(x)$ の扱いは手段に恵まれていることであろう, と直観できよう. このため, 現今の解析的整数論では専ら $\psi(x)$ ないしは $\Lambda(n)$ とその様々な拡張を扱う. Euler 積は, 素数 p を直に数えず重み $\log p$ を付加すべし, と指示するのである.

[1.1] Euler (1737): Variae observationes circa series infinitas. Comm. Acad. Sci. Petropolitanae, **9** (1744), 160–188.
[1.2] Euler (1748): Introductio in analysin infinitorum. Tomus primus. M.M. Bousquet & Socios, Lausannæ; Tomus secundus. *Ibid.*
[1.3] 函数 $\log\zeta(s)$ の扱いにて不確かな議論を散見する.

2. 素数の量的な分布「素数定理」に相応しい言明を始めて公表したのは Legendre (1798) であり,

$$\text{予想}:\ \pi(x) \sim \frac{x}{\log x} \quad (x \to \infty). \tag{2.1}$$

たとえば Abel は甚く驚き, 郷里の恩師に伝えている (日付は Année $\sqrt[3]{6064321219} = 1823$ 年 8 月 4 日). これに先立ち, Legendre (1785) は, 任意の既約剰余類 $\ell \bmod q$ ($\langle q, \ell\rangle = 1$) につき, 次をも言明していた.

$$\text{予想}: \quad \pi(x; q, \ell) = \sum_{\substack{p\le x \\ p\equiv \ell \bmod q}} 1 \to +\infty \quad (x \to \infty). \tag{2.2}$$

‘平方剰余「相互律」の Legendre 証明’ にて必要とされ, Gauss ([0.2]) が執拗に (第 151, 296, 297 節などにて) 批判したことは周知である. その後の進展につき次節にて触れる. 一方, Gauss 自身は

$$\text{予想}:\ \pi(x) \sim \operatorname{li}(x) = \int_2^x \frac{du}{\log u} \quad (x \to \infty) \tag{2.3}$$

に想到していた, との由. しかし, 少年期のメモ (1791) や老齢期の手紙 (1849) に記されたものであり, まして公開は彼の没後 (前者は全集 X-1 (1917); 後者は II-1 (1863)) である. それをもって素数分布論黎明期における Gauss の寄与を云々するには無理がある. いずれにせよ, Legendre と Gauss 共に, 容易な数値統計以上の考察をなした痕跡は皆無と判じられる. なお, Legendre による素数分布観察には Gauss のそれを凌ぐ面がある. 次節末尾にて触れる.

[2.1] A.-M. Legendre (1785): Recherches d'analyse indéterminée. Histoire de l'Académie Royale des Sciences, 465–559.
[2.2] — (1798 (An VI)): Essai sur la théorie des nombres. Duprat, Paris; Seconde édition. Courcier, Paris 1808.
[2.3] 本節については [E, §11, §71] を見よ. Dirichlet も (2.3) に気がついていたことを示す興味深いエピソードがある ([E, p.28 のなかほど] を見よ).

3. このような未開の状況を超え初の数学上明確な結果をもたらしたのは, Dirichlet (1837) である.

$$\text{Dirichlet の素数定理}: \quad \text{Legendre 予想 (2.2) は正しい.} \tag{3.1}$$

彼の貢献は, 単に (2.2) の証明にある訳では無く, 当然ながらその論法にこそ重みがある. つまり, 指標 χ と L-函数の導入. Euler の (1.3) にならい,

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\prod_{p}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}, \quad \sigma>1. \tag{3.2}$$

ただし, Dirichlet は $s>1$ なる場合のみを考察した. これら概念には Dirichlet の名を冠するのが通例であるが, 以下ではそれを略す. 指標については, Gauss の円分理論にその始まりがある. 等式 (1.4) に対応し,

$$\chi\neq 1 \;\Rightarrow\; L(s,\chi)=s\int_{1-0}^{\infty}[x]_\chi\frac{dx}{x^{s+1}}, \quad [x]_\chi=\sum_{0<n\le x}\chi(n), \quad \sigma>0. \tag{3.3}$$

何故ならば, $[x]_\chi$ は有界. 部分積分を繰り返し, 整函数と知れる. 或は, より明確には後記の (6.3) に依るがよい.

Dirichlet の論法の核心は, 喧伝されているところではあるが,

$$\chi\neq\text{単位指標} \;\Rightarrow\; L(1,\chi)\text{ は }0\text{ ならざる有限値.} \tag{3.4}$$

「複素」指標の場合, これの証明は容易である. しかし, 「実」指標の場合には, Dirichlet は特段の工夫を要した. 整数係数 2 元 2 次形式論からの (後代の) 用語を用いるが, 問題は Kronecker 記号の場合に帰着され, つまりは「Dirichlet の類数公式」の (構造の) 応用となる. ここで, 注目すべきは, Kronecker 記号は Dirichlet 指標である, という一見当然かとも思える事実である. しかし, さにあらず. 相互律在りてこそ. 即ち, (3.4) つまり (3.1) の Dirichlet の証明は相互律の上に立つ. 従って, とくに, (3.1) をもって相互律の 'Legendre 証明' が完結した, と言うは tautology. これは Kummer らの誤認であり, それを Kronecker が指摘したところでもある. この歴史上の事実に注目するのは, 実指標は「種の理論」に直結するものであり, とくに Principal Genus Theorem (適宜な邦語あらず) への「二筋の道」の存在に係る故である. 代数的整数論の端緒に触れるところ. 一方は Gauss の代数的な手法, 他方は Legendre, Arndt, Dirichlet (Dedekind) 等が開いた解析的な手法. 後者にて Legendre の (2.2) は取り分け重要. 少なくともそれが故に, (3.1) を相互律とは独立に証明することには意義がある.

実は, Ingham (1930) が既にこの要請を成している. Ramanujan (1916) に雛形を持つ等式 ($\chi \bmod q$ は任意とし)

$$\sum_{n=1}^{\infty}\frac{1}{n^s}\Big|\textstyle\sum_{d|n}\chi(d)\Big|^2=\dfrac{\zeta(s)^2L(s,\chi)L(s,\overline{\chi})}{\zeta(2s)\prod_{p|q}(1+p^{-s})}, \quad \sigma>1, \tag{3.5}$$

と正項二重級数の収束性の至って簡潔にして素敵な応用. これに Legendre に由来する他の考察を多少加え, Gauss の杞憂を排し,

$$\text{相互律の Legendre (1785) による証明は基本的には正しい} \tag{3.6}$$

と結論できる (完全修正は [E, §71, §§91–92]). ここで, 大家の何れかに僭越にも軍配を挙げるは, 元より笑止. そのような瑣末を捨て, Legendre がごく一端ながら始めて把握した

$$\text{算術級数中の素数分布の根本的な重要性} \tag{3.7}$$

にこそ視座を置くべし. 実際, 今日の素数分布論は,「双子素数予想」の攻略などまでもを含め, ほぼこの範疇に含まれる. そこで最も重視されるは, 後に明確に述べるところであるが,「法に関する一様性」である. そして, 理論の中心部分には, 広大に拡張された「篩法」がある. この機構の瞥見こそが本講演の主目的である.

加筆であるが, Legendre (1830, II, pp. 102–104) は,「整数係数 2 元 2 次形式は, その原始性の条件下に, 無限に多くの素数を表す」と予想. これは後に Dirichlet–Weber 素数定理として確認 (Dirichlet (1840), Weber (1882)). 実指標 (いわゆる genus characters) と Kronecker 記号との連携の応用, あるいはまた, 有限 Abel 群に関する双対原理のごく初期の適用と言える. さらに, 保型形式論から観るならば, (3.5) は Rankin–Selberg L-函数の一例.

[3.1] P.G.L. Dirichlet (1837): Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. Abh. Königl. Preuss Akad. Wissens., 45–81. (Werke I, pp.313–342)
[3.2] A.E. Ingham (1930): Note on Riemann's ζ-function and Dirichlet's L-functions. J. London Math. Soc., **5**, 107–112.
[3.3] S. Ramanujan (1916): Some formulae in the analytic theory of numbers. Mess. Math., **45**, 81–84.
[3.4] A.-M. Legendre (1830): Théorie des nombres. Tome I et Tome II. Firmin Didot Frères, Paris.
[3.5] P.G.L. Dirichlet (1840): Auszug aus einer der Akademie der Wissenschaften zu Berlin am 5^{ten} März 1840 vorgelesenen Abhandlung. J. reine angew. Math., **21**, 98–100.
[3.6] H. Weber (1882): Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist. Math. Ann., **20**, 301–329.
[3.7] 2 次形式の古典論については類数公式の証明, Dirichlet–Weber 素数定理の証明も含め [E, 第 4 章] を見よ. また, Dirichlet 指標の由来など詳細は [E, 第 3 章]. さらに, Rankin–Selberg 理論への入門は [D, §5.1].
[3.8] 指標 $\chi \bmod q$ の定義にて, $\chi(a) = 0$, $\langle a, q\rangle \neq 1$, が課されるが, これの必要性を明確としたのは H. Kinkelin (1862): Allgemeine Theorie der harmonischen Reihen mit Angwendung auf die Zahlentheorie. Schweighauserische Buchdruckerei, Basel. 詳しくは, [E, §57] を見よ.

4. 定性的な (2.2) に対する Dirichlet による達成 (3.1) の後, 量的な予想 (2.1) につき初の成果を挙げたのは, Chebyshev (1851) である.

$$\text{Chebyshev の発見}: \quad \lim_{x\to\infty} \pi(x)/(x/\log x) = 1. \quad \text{但し, 極限が存在するならば.} \tag{4.1}$$

仮定上の結果ながら, 意味するところは重い. Chebyshev は, (1.5) の $s \to 1+0$ なる際の振る舞いの解析を経由し, (4.1) に到達しているのである. つまり, $\pi(x)$ の定量的な解析と $\zeta(s)$ とが緊密に関係する, という枠組みが彼により固められた.

この解析にあたり, Chebyshev は積分表示

$$\zeta(s) = \frac{1}{\Gamma(s)} \sum_{n=1}^{\infty} \int_0^{\infty} x^{s-1} e^{-nx} dx = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} dx, \quad \sigma > 1, \tag{4.2}$$

を使用 (彼は, $s > 1$ の場合のみを考察). Dirichlet (1837) が導入した表示に変数変換 $x = \log(1/u)$, $0 < u < 1$, を施したものに過ぎないのであるが, その効果は絶大: Riemann (1860) による積分表示

$$\zeta(s) = \frac{-1}{\Gamma(s)(e^{\pi i s} - e^{-\pi i s})} \int_C \frac{(-x)^{s-1}}{e^x - 1} dx, \quad s \in \mathbb{C}, \tag{4.3}$$

の誘因となる. 積分路 C は彼方 $+\infty$ より現れ, 実軸上を $\frac{1}{1859}$ まで下り, 原点を中心とする小円に沿い正の向きに一回転の後, 彼方 $+\infty$ へ去る. この間, $\arg(-x)$ は $-\pi$ から π まで連続的に変動する (Hankel 路: [D, 第 1 章] を見よ. ちなみに, Hankel は Riemann の学生であった). 積分は, 全ての $s \in \mathbb{C}$ につき収束し整函数. つまり, (4.3) は $\zeta(s)$ の全複素平面への解析接続を一挙に与える. そこで, 臨時に $\sigma < 0$ と制限し, C の小円部分を無限に膨張させるならば, 留数計算を経由し解析接続をもって函数等式

$$\begin{gathered} \zeta(1-s) = 2(2\pi)^{-s} \cos\big(\tfrac{1}{2}s\pi\big)\Gamma(s)\zeta(s), \\ \xi(1-s) = \xi(s), \quad \xi(s) = \tfrac{1}{2}s(s-1)\pi^{-s/2}\Gamma\big(\tfrac{1}{2}s\big)\zeta(s), \end{gathered} \quad \forall s \in \mathbb{C}, \tag{4.4}$$

に達する. ただし, 下辺は上辺への倍角公式 $\Gamma\big(\frac{1}{2}s\big)\Gamma\big(\frac{1}{2}(s+1)\big) = \pi^{1/2}2^{1-2}\Gamma(s)$ の応用結果.

多少の考察の後に, 函数 $\xi(s)$ は整函数 (genus $= 1$) であり,

$$\xi(\rho) = 0,\ \rho = \beta + i\gamma \ \Leftrightarrow\ \zeta(\rho) = 0,\ 0 \le \beta \le 1 \quad (\rho \text{ を非自明零点と呼ぶ}). \tag{4.5}$$

ここで, 函数 $(1 - 2^{1-s})\zeta(s)$ を実数区間 $(0, 1)$ にて観察することにより, $\gamma \neq 0$ と容易に知れる. かくして, Riemann は次の 4 項を言明 (恐らくは研究経過報告の心積もり故, 証明を付せず): 「今日の解釈」のもと,

(R_1)
$$N(T) = \big|\{\rho = \beta + i\gamma,\ 0 < \gamma < T\}\big| = \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T), \quad T \ge 2. \tag{4.6}$$

(R_2) 全ての非自明零点につき
$$\beta = \frac{1}{2} \quad \big(\textit{sehr wahrscheinlich}\big). \tag{4.7}$$

(R_3) 整函数 $\xi(s)$ の Hadamard 積表示に相当. 省略.

(R_4) 任意の $x = [x] + \frac{1}{2} > 1$, $T \ge 2$ をもって,
$$\psi(x) = x - \sum_{\rho,\,|\gamma|<T} \frac{x^\rho}{\rho} - \log(2\pi) - \frac{1}{2}\log\big(1 - x^{-2}\big) + O\left(\frac{x}{T}(\log xT)^2\right). \tag{4.8}$$

「Riemann 予想」(RH) と一般に呼ばれる (R_2) 以外は比較的容易に証明できることは周知 (次節の注意 [5.6] など). また, (R_4) から,
$$\mathrm{RH} \quad \Leftrightarrow \quad \begin{array}{l} \psi(x) = x + O\big(x^{1/2}(\log x)^2\big), \\ \pi(x) = \mathrm{li}(x) + O\big(x^{1/2}\log x\big). \end{array} \tag{4.9}$$

Riemann が如何にして RH に導かれたのか, もちろん真相は知れず. しかしながら, Siegel (1932) が明らかにしたところでは, Riemann は一遺稿にて驚くべき計算を (4.3) の小変形

$$\zeta(s) = \sum_{n \le N} \frac{1}{n^s} + \frac{-1}{\Gamma(s)(e^{\pi i s} - e^{-\pi i s})} \int_C \frac{(-x)^{s-1}e^{-Nx}}{e^x - 1}dx, \quad s \in \mathbb{C},\ N \in \mathbb{N}, \tag{4.10}$$

をもとに展開し, 非自明零点の幾つかを近似計算. それらが全て「臨界線」$\sigma = \frac{1}{2}$ 上にあることを確認. この計算は, 空前絶後の鞍点法活用 ($t/N > 0$ が大ならば, 鞍点は $(t/N)i$ の近傍; 最適には, $N = [(t/2\pi)^{1/2}]$). つまりは, Riemann は Chebyshev から深い霊感を得ていた, と推察するに充分. 何か壮大な機構の中で RH が捉えられた, とするは fantasy. 彼の足は地についていた.

例え 2 であれ素数 1 個を検出するには, 無限に多くの非自明零点を要する: Landau (1911)

$$\sum_{0<\gamma<T} x^\rho = \begin{cases} -\dfrac{T}{2\pi}\log p + O(\log T) & \text{for } x = p^m, \\ O(\log T) & \text{for } x \neq p^m. \end{cases} \tag{4.11}$$

ただし, 陰伏常数は x に関係する. 言うなれば,

$$\text{各素数は非自明零点の統計結果.} \tag{4.12}$$

函数 $\zeta(s)$ そのものが自然数全体と複素数全体の上に存在する訳であり, その統計的な性格は至極当然とも言える. 第 9 節以降に述べるが, この観点は重要な帰結を素数分布論にもたらす.

[4.1] P.L. Chebyshev (1851): Sur la fonction qui détemine la totalité des nombres premiers inférieur à une limite donnée. Mémoire présentés à la Acad. Impériale de St. Pétersbourg par divers savants, **VI**, 141–157. Also: J. math. pures et appliq., **XVII**, 1852, 341–365. (Œuvres I, pp.29–48)

[4.2] B. Riemann (1860): Über die Anzahl der Primzahlen under einer gegebenen Gösse. Monatsber. Königl. Preuss. Akad. Wiss. Berlin, J. 1859, 671–680. この革命的論文は 1859 年 10 月 19 日に提出され, Kummer により同年 11 月 3 日に紹介された. なお, 言語は異なるものの表題は Chebyshev 論文のそれと同じであることに注意せよ.

[4.3] C.L. Siegel (1932): Über Riemanns Nachlass zur analytischen Zahlentheorie. Quellen und Studien zur Geschichte der Math. Astr. und Physik, Abt. B: Studien, **2**, 45–80.
[4.4] 本節については, [C, 第 1 章] を見よ. なお, 鞍点法 (saddle point/ steepest descent/ stationary phase method) の源は Riemann のこの遺稿. 解析的整数論における最近の必須的活用例としては, 例えば [B, Chapter 5] や後出の Jutila–Motohashi ([11.8]) がある.
[4.5] E. Landau (1911): Über die Nullstellen der Zetafunktion. Math. Ann., **71**, 548–564.

5. かくして, Riemann Paradigm にのっとり, Hadamard (1896) と de la Vallée Poussin (1896) は独立に

$$\text{Legendre 予想 (2.1) は正しい} \tag{5.1}$$

と証明. さらに後者 (1899/1900) は「残余項付き」素数定理

$$\begin{aligned} \psi(x) &= x + O\big(x\exp\big(-c(\log x)^{1/2}\big)\big), \\ \pi(x) &= \mathrm{li}(x) + O\big(x\exp(-c(\log x)^{1/2})\big), \end{aligned} \tag{5.2}$$

をも得た. しかし, 彼らの採った整函数論に発する手法の解説は割愛. より直接的かつ効力抜群の手法が Landau (1924) により後に得られているが故である.

これは, 模式的には,

$$\text{Landau の方法} \subset \big\{\text{Mertens 不等式, Jensen 公式, Borel–Carathéodory 定理}\big\}. \tag{5.3}$$

Mertens (1898) の不等式とは, 任意の $\sigma > 1$, $t \in \mathbb{R}$ につき,

$$-3\frac{\zeta'}{\zeta}(\sigma) - 4\mathrm{Re}\,\frac{\zeta'}{\zeta}(\sigma+it) - \mathrm{Re}\,\frac{\zeta'}{\zeta}(\sigma+2it) = 2\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^{\sigma}}(1+\cos(t\log n))^2 \geq 0, \tag{5.4}$$

あるいは, 同じことであるが,

$$\zeta^3(\sigma)|\zeta^4(\sigma+it)\zeta(\sigma+2it)| \geq 1. \tag{5.5}$$

Landau が (5.3) をもって明確としたところは,

$$\text{問題の本質は, 垂直線 } \sigma = 1 \text{ の近傍における } |\zeta(s)| \text{ の評価.} \tag{5.6}$$

粗い説明を加える: 表示式 (1.5) を出発点とし, 「臨界帯」$0 \leq \sigma \leq 1$ に進入せねばならない. つまり, $\sigma = 1$ の近傍における対数微分 $(\zeta'/\zeta)(s)$ の考察を要する. もちろん, この近傍に零点が含まれるべきではない ($\zeta(s)$ の「非消滅域」). このために, $f(s) = \zeta(s)/\prod_{\rho}(s-\rho)$ を観察する. ただし, $\{\rho\}$ は問題となる領域を充分に含む範囲にある全ての非自明零点の集合. 個数 $|\{\rho\}|$ を評価せねばならぬが, Jensen 公式による. 問題の対数微分は Cauchy 積分をもって表示する他無く, 積分円上の $\log f(s)$ の評価を要する. これを直接に行うのは困難. そこで Borel–Carathéodry 定理を援用する. つまり, 大略, 正則函数の大きさは, その点を中心とする円周上における「実部の上界」により統制される. よって, $\mathrm{Re}\,\log f(s) = \log|f(s)|$ に注意し, (5.6) に達する.

例えば, (1.4) から得られる $\zeta(s) = O(|s|)$ (ただし, $|s-1| \geq 1$, $\sigma \geq \frac{1}{2}$) なる「ごく平易な評価」のみをもって

$$\left|\frac{\zeta'}{\zeta}(s) + \frac{1}{s-1}\right| \ll \log(t+2), \quad \sigma \geq 1 - \frac{c}{\log(t+2)}, \quad t \geq 0, \tag{5.7}$$

を導くことができる. つまり, de la Vallée-Poussin の「非消滅域」

$$\zeta(s) \neq 0, \quad \sigma \geq 1 - \frac{c}{\log t}, \quad t \geq 2. \tag{5.8}$$

評価 (5.7) と素数定理 (5.2) は指呼の間. 平易な Perron の反転公式:

$$\frac{1}{2\pi i}\int_{a-iT}^{a+iT} y^s\frac{ds}{s} = \begin{cases} 1 + O\Big(y^a/(T\log y)\Big), & y > 1, \\ O\Big(y^a/(T|\log y|\Big), & 0 < y < 1, \end{cases} \qquad a > 0,\ T \geq 2, \tag{5.9}$$

を応用し, $a>1, T\geq 2, x=[x]+\frac{1}{2}$ につき一様に,

$$\psi(x)=-\frac{1}{2\pi i}\int_{a-iT}^{a+iT}\frac{\zeta'}{\zeta}(s)x^s\frac{ds}{s}+O\left(\frac{x^a}{T}\left|\frac{\zeta'}{\zeta}(a)\right|+\frac{x}{T}(\log x)^2\right). \tag{5.10}$$

積分路を左方向に適宜移動し (5.2) を得る. この移動に (5.7)–(5.8) を参照する訳である (その後, $a=1+1/\log x$, $T=\exp\big((\log x)^{1/2}\big)$ と採る). 言うなれば, 素数定理 (5.2) は (1.4) のごく近傍にある. ここに, Chebyshev の認識 (4.1) の背景が蘇る.

とりわけ, 深い Vinogradov 評価 (1958)

$$\zeta(s)\ll t^{c(1-\sigma)^{3/2}}(\log t)^{2/3},\quad \sigma\leq 1,\ t\geq 2, \tag{5.11}$$

を用いるならば, (5.7) は

$$\left|\frac{\zeta'}{\zeta}(s)\right|\ll(\log t)^{2/3}(\log\log t)^{1/3},\quad \sigma\geq 1-\frac{c}{(\log t)^{2/3}(\log\log t)^{1/3}},\quad t\geq 3, \tag{5.12}$$

と改良され, (5.10) を経由し現今最良の素数定理

$$\pi(x)=\mathrm{li}(x)+O\Big(x\exp\Big(-c(\log x)^{3/5}(\log\log x)^{-1/5}\Big)\Big),\quad x\geq 3, \tag{5.13}$$

に到達する. Vinogradov の手法については, 第 11 節の末尾にて触れる. 注意であるが, (5.11) そのものを Vinogradov が示した訳ではない. 彼の方法が (5.11) をもたらすのである. 評価 (5.12) の改良の可能性については, [5.11] を見よ.

なお, (5.4)–(5.5) を '算術的' と観ることもできる. すなわち,

$$\sum_{n=1}^{\infty}\frac{1}{n^s}\Big|\sum_{d|n}d^{i\eta}\Big|^4=\zeta^6(s)\zeta^4(s+i\eta)\zeta^4(s-i\eta)\zeta(s+2i\eta)\zeta(s-2i\eta)H(s). \tag{5.14}$$

ただし, $H(s)$ は $\sigma>\frac{1}{2}$ にて正則かつ有界. 保型形式論 (symmetric power L-函数) の介在が暗示されている.

加筆であるが, Landau (1903) はほぼ (5.4) のみを手段とし

$$\pi(x)=\mathrm{li}(x)+O\big(x\exp\big(-c(\log x)^{1/10}\big)\big) \tag{5.15}$$

を証明の上, 同じ方法をもって一般の代数体に関し「素イデアル定理」を得ている. この事実は, 代数的整数論の歴史上重要な意味を持つ. つまり, Landau は Dedekind zeta-函数の函数等式を必要としなかった (整函数論を用いるには, 半平面 $\sigma\leq 0$ における情報つまり函数等式あるいはそれに準ずるものを要する). 函数等式は後に Hecke (1917) により証明された.

素数定理 $\pi(x)\sim x/\log x$ は存外浅いところにある. 素イデアル定理も然り. (5.16)

[5.1] J. Hadamard (1896): Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. Bull. Soc. Math. France, **24**, 199–220.

[5.2] C.-J. de la Vallée–Poussin (1896): Recherches analytiques sur la théorie des nombres premiers. Premier Parte. La fonction $\zeta(s)$ de Riemann et les nombres premiers en général. Ann. Soc. Sci. Bruxelles, **20**, 183–256.

[5.3] — (1899/1900): Sur la fonction $\zeta(s)$ de Riemann et le nombres des nombres premiers inférieurs à une limite donnée. Mém. Courronnés et Autres Mém. Publ. Acad. Roy. Sci., des Letteres Beaux-Arts Belgique, **59**, Nr.1.

[5.4] F. Mertens (1898): Über eine Eigenschaft der Riemannschen ζ-Function. Sitz. Kaiser. Akad. Wiss. Wien, math.-natur. Classe, **107**, 1429–1434.

[5.5] E. Landau (1924): Über die Wurzeln der Zetafunktion. Math. Zeit., **20**, 98–104.

[5.6] 明示式 (4.8) も (5.3), (5.10) をもって証明できる.

[5.7] I.M. Vinogradov (1958): A new estimate for $\zeta(1+it)$. Izv. Akad. Nauk SSSR, Ser. Mat., **22**, 161—164. (Russian)

[5.8] 本節については, [C, 第 1 章, 第 2 章] を見よ. なお, 本講演の趣旨に沿う symmetric power L-函数理論の応用例としては, Motohashi (2015): On sums of Hecke–Maass eigenvalues squared over primes in short intervals. J. London Math. Soc., **91**, 367–382.

[5.9] E. Landau (1903): Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes. Math. Ann., **56**, 645–670.
[5.10] E. Hecke (1917): Über die Zetafunktion beliebiger algebraischer Zahlkörper. Nachr. Gesell. Wiss. Göttingen, Math.–Phy. Klasse, J. 1917, 77–89.
[5.11] Y. Motohashi (2001): An observation on the zero-free region of the Riemann zeta-function. Periodica Math. Hungarica, **42**, 117–122.

6. 算術級数中の素数分布の基礎を第 3 節に続き述べる. 函数 $\pi(x;q,\ell)$ に代え

$$\psi(x;q,\ell)=\sum_{\substack{p\le x\\ p\equiv\ell \bmod q}}\Lambda(n),\qquad \langle q,\ell\rangle=1,\ q\ge 3, \tag{6.1}$$

を専ら考察する. 関係式

$$\psi(x;q,\ell)=\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\overline{\chi}(\ell)\psi(x,\chi),\quad \psi(x,\chi)=\sum_{n\le x}\chi(n)\Lambda(n),\quad \varphi(q)=q\prod_{p\mid q}\big(1-1/p\big) \tag{6.2}$$

をもって (4.8) に対応する明示式を得る. 法 q に関し出来る限り一様な結論を得ることが目的 ((3.7)) である故, $L(s,\chi)$ の零点に関する知見にも同じ一様性を要する. しかしながら, 現今のところこの要請を充たすことは至難と認識されている. 以下にて問題の核心を明確とする.

指標 $\chi \bmod q$ が原始指標 $\chi^* \bmod q^*$ によって誘導されるならば, $L(s,\chi)=L(s,\chi^*)\prod_{p\mid q}\big(1-\chi^*(p)/p^s\big)$. つまり, 零点の考察においては, $L(s,\chi^*)$ を扱うも殆ど同じ. そこで, 臨時に, $\chi \bmod q$ は原始的 ($\chi\ne 1$) とする. 函数等式 (4.4) の拡張として,

$$\begin{aligned}\xi(1-s,\overline{\chi})&=\frac{i^{\delta_\chi}q^{1/2}}{G_\chi}\xi(s,\chi),\\ \xi(s,\chi)&=(q/\pi)^{s/2}\Gamma\big(\tfrac12(s+\delta_\chi)\big)L(s,\chi),\end{aligned}\qquad \forall s\in\mathbb{C}. \tag{6.3}$$

ただし, $\delta_\chi=\frac12\big(1-\chi(-1)\big)$, かつ G_χ は χ に付随する Gauss 和 $\sum_{a \bmod q}\chi(a)\exp(2\pi ia/q)$. 函数 $\xi(s,\chi)$ は整函数であり, その零点は全て臨界帯 $0\le\sigma\le 1$ にあり, それらは全て $L(s,\chi)$ の零点でもある. 逆に, $L(s,\chi)$ の零点の内, $s=0$ を除く臨界帯に属するものは, 全て $\xi(s,\chi)$ の零点である. これらを「$L(s,\chi)$ の非自明零点」と呼び, $\zeta(s)$ の場合と同じ記号 $\rho=\beta+i\gamma$ をもって表す. 記号の混乱は無かろう. ここで特に注意すべきは $\gamma=0$ なる状態を排除できないことである. つまり, 後に示すごとく, $L(s,\chi)$ は (望まれぬところの) 実根を持つ可能性がある. 念のために付け加えるが, $L(0,\chi)=0$ は $\chi(-1)=1$ である場合にのみ成立し, (3.4) により単根. しかし, 非自明零点には算入しない.

上記を念頭に置き, 一般の指標 $\chi \bmod q$ ($q\ge 3$, $\chi\ne 1$) に戻る (しばし, 原始指標なる仮定を要しない). 函数 $\zeta(s)$ の場合と同様に, 垂直線 $\sigma=1$ の近傍における $|L(s,\chi)|$ の大きさを必要とするが, (3.3) から容易に得られる

$$L(s,\chi)\ll q(|t|+1),\quad \frac12\le\sigma,\ t\in\mathbb{R}, \tag{6.4}$$

を基本とする. 虚部 t は正負あるいは零の何れでもありうる. Vinogradov の (5.11) に較べ得るものを「法 q と s の両者につき」一様に達成することは極めて困難 (ただし, [6.3] を見よ). Mertens の不等式 (5.4) を χ をもって twist し,

$$-3\frac{L'}{L}(\sigma,\jmath_q)-4\mathrm{Re}\,\frac{L'}{L}(\sigma+it,\chi)-\mathrm{Re}\,\frac{L'}{L}(\sigma+2it,\chi^2)\ge 0,\quad \sigma>1,\ t\in\mathbb{R}. \tag{6.5}$$

左辺は $2\sum_n \jmath_q(n)\Lambda(n)(1+\cos(\theta_n-t\log n))^2n^{-\sigma}$ に等しい. ただし, $\jmath_q$ は単位指標 $\bmod q$. および, $\chi(n)=\exp(i\theta_n)$.

まず, χ が複素指標であるならば, $L(\sigma+2it,\chi^2)$ は '$\sigma+2it$' に関し整函数であり, つまりは (6.5) は (5.4) と実質的に変わらない. Landau の手法 (5.3) を用い, (5.7) の類似

$$\chi\text{: 複素指標}\ \Rightarrow\ \frac{L'}{L}(s,\chi)\ll\log(q(|t|+1)),\quad \sigma>1-\frac{c}{\log(q(|t|+1))},\ t\in\mathbb{R}, \tag{6.6}$$

を得る. 一方, 実指標の場合には議論は多少込み入る. なぜならば, $L(s,\chi^2)=L(s,\jmath_q)$ は極 $s=1$ を持つ. しかし, $|t|$ が「極端に小ならざる」場合には, 手法 (5.3) は依然として有効であり,

$$\chi\text{: 実指標} \ \Rightarrow\ \frac{L'}{L}(s,\chi)\ll \log(q(|t|+1)),\quad \sigma>1-\frac{c}{\log(q(|t|+1))},\ |t|\ge\frac{c}{\log q}. \tag{6.7}$$

残る $|t|\le c/\log q$ なる場合であるが, $\beta+i\gamma$, $\gamma\neq 0$, と共に $\beta-i\gamma$ も根であることに注意する. これら近接した 2 根の存在は (5.3), (6.5) により否定される. つまり, 根が存在するとしても「実根」に限る. さらに, 同様にして, 区間 $1-c/\log q<\sigma<1$ に 2 個の実根が入ることもあり得ない, と知れる. 結論として,

$$\begin{gathered}\text{函数 } \textstyle\prod_{\chi \bmod q} L(s,\chi) \text{ は, 計算可能な絶対常数 } \kappa>0 \text{ をもって,}\\ \text{領域 } \sigma>1-\kappa/\log(q(|t|+1)),\ t\in\mathbb{R}, \text{ 内に高々1 個の零点を持つ.}\end{gathered} \tag{6.8}$$

$$\begin{gathered}\text{その様な零点 } \rho(q) \text{ が存在する可能性は, 法 } q \text{ につき唯一の}\\ \text{実指標 } \chi\not\equiv 1 \text{ であり } \rho(q) \text{ は実単根, かつ } 1-\frac{\kappa}{\log q}<\rho(q)<1.\end{gathered} \tag{6.9}$$

この唯一性を示すには, 「相異なる」実指標 χ,χ' をもって (6.5) に代え

$$-\frac{\zeta'}{\zeta}(\sigma)-\frac{L'}{L}(\sigma,\chi)-\frac{L'}{L}(\sigma,\chi')-\frac{L'}{L}(\sigma,\chi\chi')=\sum_n \Lambda(n)(1+\chi(n))(1+\chi'(n))\ge 0, \tag{6.10}$$

を用いる. かくして, 全ての指標 $\bmod q$ ($\chi\not\equiv 1$) につき,

$$\text{領域 (6.8) にて}\quad \frac{L'}{L}(s,\chi)-\frac{\eta_\chi}{s-\rho(q)}\ll\log(q(|t|+1)),\quad \eta_\chi=\begin{cases}1 & L(\rho(q),\chi)=0,\\ 0 & \text{その他.}\end{cases} \tag{6.11}$$

この陰伏常数は計算可能. とくに,

$$\eta_\chi=1 \text{ なるとき, } \chi \text{ を } q\text{-例外指標, } \rho(q) \text{ を } q\text{-例外零点と呼ぶ.} \tag{6.12}$$

しかしながら, 例外指標が存在するのか否かは, 未知 ([7.3] も見よ). ただし, Siegel (1935) により次が示されている:

$$\text{任意に定めた小 } \varepsilon>0 \text{ につき, 常数 } \tau_\epsilon>0 \text{ が存在し } \rho(q)<1-\frac{\tau_\varepsilon}{q^\varepsilon}. \tag{6.13}$$

とは言え,

$$\begin{gathered}\tau_\varepsilon \text{ は effective にあらず. つまり, 現今のところ}\\ \tau_\varepsilon \text{ を } \varepsilon \text{ をもって明示的に定める手段は未知.}\end{gathered} \tag{6.14}$$

かくして, (5.10) の $\psi(x,\chi)$ への自明な拡張を経由し, Siegel–Walfisz 素数定理:

$$\text{任意の } A\ge 1 \text{ につき常数 } c_A>0 \text{ が存在し, } 1\le q\le \log^A x \text{ なる法 } q \text{ に関し一様に} \tag{6.15}$$

$$\begin{aligned}\psi(x;q,\ell) &= \frac{x}{\varphi(q)}+O\Big(x\exp\big(-c_A(\log x)^{1/2}\big)\Big),\\ \pi(x;q,\ell) &= \frac{1}{\varphi(q)}\mathrm{li}(x)+O\Big(x\exp\big(-c_A(\log x)^{1/2}\big)\Big).\end{aligned} \tag{6.16}$$

$$\text{ただし, 現今のところ, } c_A \text{ および陰伏常数を } A \text{ をもって明示的に定める手段は未知.} \tag{6.17}$$

なお, より「例外性」を強調し

$$Q\text{-例外}:\quad \begin{gathered}\text{全ての原始指標 } \chi \bmod q,\ q\le Q, \text{ の内, 高々唯一の実指標 } \chi_1 \bmod q_1 \text{ のみにつき,}\\ \text{例外零点 } L\big(\chi_1,\rho(q_1)\big)=0,\ 1-\frac{\kappa}{\log Q}<\rho(q_1)<1.\end{gathered} \tag{6.18}$$

これは不等式 (6.10) から導かれる.

[6.1] C.L. Siegel (1935): Über die Klassenzahl quadratischer Zahlkörper. Acta Arith., **1**, 83–86.

[6.2] 本節については, [C, 第 4 章] を見よ.
[6.3] 素数 p を「固定」し, 法 $q = p^r$, $r \to \infty$, を考察するならば, 計算可能な $c > 0$, $0 < \vartheta < 1$ をもって, $L(s,\chi) \neq 0$, $\sigma > 1 - c\big(\log(q(|t|+1))\big)^{-\vartheta}$, であることが知られている. A.G. Postnikov (1955): On the sum of characters with respect to a modulus equal to a power of a prime number. Izv. Akad. Nauk SSSR Ser. Mat., **19**, 11–16. (ロシア語)

7. 確かに, 素数定理 (6.16) は法に関し一定の一様性を持つ. しかし, ineffective. 故に, (6.16) をもって, 例えば, $\pi(x;q,\ell) > 0$ となる最初の x (最小素数 $\equiv \ell \bmod q$) を「常識的な範囲内 (q の小冪以下)」に定めることすらできない.

そこで, 次が提出されている:

$$\text{例外指標非存在予想}: \quad \begin{array}{c} \text{計算可能な常数 } c > 0 \text{ が存在し,} \\ \text{任意の指標 } \chi \bmod q,\ q \geq 3 \text{ につき,} \\ L(s,\chi) \neq 0,\ 1 - c/\log q < s < 1. \end{array} \tag{7.1}$$

これは, 現今の解析的整数論において, その解決が最も望まれる問題の一つである.

関連し, 積分

$$\frac{1}{2\pi i}\int_{(2)} \zeta(s)L(s,\chi)((2X)^s - X^s)\Gamma(s)ds, \quad (\text{積分曲線は垂直線 } \sigma = 2), \tag{7.2}$$

を考察することにより, 計算可能な $c > 0$ が存在し

$$L(1,\chi) \geq \frac{c}{q^{1/2}}, \quad q \geq 3, \tag{7.3}$$

と容易に知れる. 従って ([C, pp.102–103]),

$$1 - \frac{\kappa}{\log q} < \rho(q) < 1 - \frac{c}{q^{1/2}(\log q)^2}, \quad q \geq 3. \tag{7.4}$$

ここで注目すべきは, Goldfeld (1976) の着想により, (7.3) を多少改良可能. 懸案であった「Gauss の類数問題」の解決をもたらした重要な発展である. しかしながら, 基本課題である素数定理 (6.16) の改良には, 残念ながら全くに無力である. 如何にしてこのような「極めて浅い」一様性を超えるのかがあくまでも課題となる. それは, 個々の法については目下は困難.

ところが,

$$\text{法に関する統計} \tag{7.5}$$

を念頭に置くならば, 進展を納めることが可能である. しかも, 幸いなことに,

$$\text{Rényi (1948) の視座:} \quad \text{古典的な難問, 例えば双子素数予想, などについては (7.5) をもって攻略可能.} \tag{7.6}$$

つまりは, 後に述べるところの「篩法と解析的手法の結合」であり,

$$\text{哲学:} \quad \text{より多くの直交構造を手段とすべし.} \tag{7.7}$$

ただし, 予め注意するが,

$$\begin{array}{c} \text{「双子素数予想等そのものの解決」に資するか否かは甚だ疑問である.} \\ \text{つまり, 解決への相当な接近をもって佳しとするならば, 紛れも無く可能.} \end{array} \tag{7.8}$$

されば解析的整数論は不等式の学問, 不完全なり, と誹るなかれ. 今日の数学において, 他に如何なる手法をもって素数に直接に触れ得るのか. 誰か知らむ.

[7.1] D. Goldfeld (1976): The class number of quadratic fields and the conjecture of Birch and Swinnerton-Dyer. Ann. Scuola Norm. Sup. Pisa Cl. Sci., (4) **3**, 624–663.
[7.2] A. Rényi (1948): On the representation of an even number as the sum of a prime and an almost prime. Izv. Akad. Nauk SSSR Ser. Mat., **12**, 57–78. (Russian)

[7.3] 仮定「ABC 予想不等式が最も望ましい一様性をもって成立」のもとに, $\chi(-1)=-1$ ($\chi \bmod q$ は実指標) なる場合 (つまり, 虚二次体 $\mathbb{Q}(i\sqrt{q})$), 例外零点の存在を否定できる, と知られている. そこで,「望月理論」において主張されている ABC 予想肯定が例外零点に関しいかなる帰結をもたらすのか. この重要な観点につき, V. Dimitrov (workshop slides: October 30, 2016) の報告によるならば, 望月教授との議論の結果, 例外零点の存在を未だ否定できず, 計算可能な $c>0$ をもって, $L(s,\chi)\neq 0$, $s>1-c(q^{1/6}\log q)^{-1}$. よって, 素数分布論に関する限りではあるが,「目下」のところは望月理論を等閑に付すも可. なお, $\chi(-1)=1$ なる場合 (つまり, 実二次体 $\mathbb{Q}(\sqrt{q})$) に関しては (6.13) の他は (実質的には) 何も知られていない.

8. ここで, 拡張された Riemann 予想 the extended Riemann hypothesis について述べておく:

$$\text{ERH}: \quad \begin{array}{c} \text{全ての原始指標 } \chi \text{ につき,} \\ L(s,\chi) \text{ の非自明零点は直線 } \sigma=\frac{1}{2} \text{ 上にある.} \end{array} \tag{8.1}$$

言うまでも無く, ERH $\Rightarrow$ RH. また, (7.1) は ERH よりも遥かに弱い予想である. つまり, ERH と現状との間の落差は巨大.

RH の場合 (4.9) と同様に, 任意の既約剰余類 $\ell \bmod q$ につき,

$$\text{ERH} \quad \Leftrightarrow \quad \begin{array}{l} \psi(x;q,\ell)=\dfrac{x}{\varphi(q)}+O\big(x^{1/2}(\log qx)^2\big), \\ \pi(x;q,\ell)=\dfrac{1}{\varphi(q)}\mathrm{li}(x)+O\big(x^{1/2}\log qx\big). \end{array} \tag{8.2}$$

陰伏常数は x,q,ℓ に関し一様な絶対常数であり, かつ, 計算可能. 素数分布については, これら以上の結論を ERH から導くことの可能性は知られていないが, 極めて困難な課題であると映る. 念のための注意: (8.2) から

$$\text{ERH} \ \Rightarrow \ \text{最小素数} \equiv \ell \bmod q \ \text{は} \ O\big(q^2(\log q)^3\big). \tag{8.3}$$

なお, ERH の興味深い帰結として次がある:

$$\begin{array}{c} \text{任意の法 } q\geq 3 \text{ につき, 既約剰余類群 } (\mathbb{Z}/q\mathbb{Z})^* \text{ は} \\ \ell \leq c(\log q)^2 \text{ なる既約類 } \ell \bmod q \text{ をもって生成される.} \end{array} \tag{8.4}$$

つまり, $(\mathbb{Z}/q\mathbb{Z})^*$ の任意の「非自明」部分群の「外部」には $\ell \leq c(\log q)^2$ なる既約類 $\ell \bmod q$ が必ず存在する. 例えば, 各 $k\geq 2$ につき,

$$\text{最小 } k\text{-次非剰余 } \bmod q \ \text{は} \ O\big((\log q)^2\big). \tag{8.5}$$

何故ならば, k-次剰余 $\bmod q$ は $(\mathbb{Z}/q\mathbb{Z})^*$ の真部分群. Ankeny (1952) によるところであるが, その後 Bach (1990) は $c=2$ とできると示している. これは, 極めて簡便かつ迅速な「確率的」素数判定法を与える. 帰結 (8.4) の余りの強力さ故に, 逆に, ERH が如何に困難な課題であるかが知れる. 証明は, Abel 群の双対定理を用い, 指標の問題に転化するならば, 関係式

$$\text{ERH} \ \Rightarrow \ \sum_{n=1}^{\infty}\chi(n)\Lambda(n)k(n)=-\frac{1}{2\pi i}\int_{(2)}\frac{L'}{L}(s,\chi)\widetilde{k}(s)ds \ll N^{1/2}\log q \tag{8.6}$$

を考察し容易に得られる. ここに, $\chi\neq 1$ かつ $k(x)$ は区間 $[N/2,3N/2]$ に台を持つ任意の test 函数であり, $\widetilde{k}(s)$ はその Mellin 変換である. 不等式は, 積分路を $\mathrm{Re}\, s=\frac{1}{4}$ に移した結果.

[8.1] N.C. Ankeny (1952): The least quadratic non residue. Annals of Math., **55**, 65–72.

[8.2] E. Bach (1990): Explicit bounds for primality testing and related problems. Math. Comp., **55**, 355–380.

[8.3] 確率的素数判定法については, [E, §48] を見よ.

[8.4] 古典 (現行汎用) 計算機上の「決定論的 deterministic」多項式時間「素数判定法」は既に達成されている: M. Agrawal, N. Kayal, and N. Saxena (2004): PRIMES is in P. Annals of Math., **160**, 781–793. 因数分解の困難と比較し意外であろう. しかし, 素数判定の有効性は限られている. 何故ならば, 素数判定の結論を確かめるためには, 判定計算を再度行う他無いからである. これに較べ, 因数分解を確かめることは自明ながら至極容易. つまり, 確率的な手法であれ因数の特定がなされるならば, それは決定的な結論である. ここに Shor 理論 ([0.7]) の重大性がある.

[8.5] ERH の証明が成されたとして, それにより例えば双子素数予想の完全解決がもたらされるのか否か. 今日の知見をもってしては, 応答甚だ困難.

9. 実は, 着想 (7.5) の源流は Bohr–Landau (1914) による次の結果にある.

$$\text{RH は統計的には正しい.} \tag{9.1}$$

もちろん, この「統計的」なる用語の解説が必要となる. そこで

$$N(\alpha, T) = \big|\{\rho = \beta + i\gamma : \alpha \le \beta,\, |\gamma| \le T\}\big| \tag{9.2}$$

と定義する. 当該の矩形内の $\zeta(s)$ の非自明零点の個数である. このとき, (9.1) は, より明確には,

$$\text{任意の } \alpha > \tfrac{1}{2} \text{ につき } \lim_{T\to\infty} N(\alpha, T)/T = 0. \tag{9.3}$$

証明済みである (4.6) と組み合わせ,

$$\text{非自明零点は「殆ど全て」臨界線の近傍 } \big|\sigma - \tfrac{1}{2}\big| < \varepsilon \text{ にある.} \tag{9.4}$$

証明への着想は単純明解. まず, $K = K_\sigma$ を充分大と採るならば, Euler 積表示 (1.3) により $P_K(s) = \prod_{p\le K}(1 - p^{-s})$ をもって, 函数

$$\zeta(s)P_K(s) - 1 \tag{9.5}$$

は半平面 $\sigma > 1$ において小. そこで, naïve な観察

$$\text{半平面 } \sigma > \tfrac{1}{2} \text{ にて (9.5) が常に小 } \Rightarrow \text{ RH は正しい.} \tag{9.6}$$

この左辺を示すことは, もちろん希望の極. 対するに,

$$\text{Bohr–Landau は, (9.6) にて「常に」を外す可能性を考察.} \tag{9.7}$$

彼らの論旨に多少の解釈を加えるが, 「外す手段」として積分

$$\iint_S \Big|\zeta(s)P_K(s) - 1\Big|^2 d\sigma dt, \quad S = \{s : \alpha \le \sigma \le 2,\, 1 \le t \le T\},\ \alpha > \tfrac{1}{2} \tag{9.8}$$

の評価を採用. 充分大なる K を採り, これは $o(T)$ と知れるのである. 積分域 S の面積は $\approx T$ である故, (9.5) は S の「殆ど至る所」で小. この事実をもって (9.3) なる結論を導くには多少の議論を加えねばならないが, 詳細を示す必要は無かろう. 何れにせよ, 感得すべき核心は,

$$\begin{gathered}\text{zeta-函数の「適宜な平滑化」の効果測定が}\\ \text{「非自明零点の分布」と密接に関係する.}\end{gathered} \tag{9.9}$$

平滑化とは, $\zeta(s)$ の変動を出来る限り平坦とすべく努めることである. この目的のために $\zeta(s)$ に乗ずべき因子を mollifyer と呼ぶ. 上記は, mollifyer として $P_K(s)$ を選択可能と言うことに等しい. そこで問題は, 「目的夫々に応じ」効果優良な mollifyer の選択である. 注意すべきは $P_K(s)$ の採用は, 後に解説する Eratosthenes–Legendre 篩の応用と言え, それの「非効率性」が (9.8) の評価の弱さ (つまり $o(T)$ に留まる) の原因と判じられることである (K の大きさが強く制限される; 下記の (14.11) に続く注意を見よ).

ここでやや飛躍するが, 認識 (9.9) のもたらす視界には, 驚く勿れ,

$$\text{短区間素数定理 : } \begin{gathered}0 < \theta < 1 \text{ なる絶対常数 } \theta \text{ をもって,}\\ \pi(x + x^\theta) - \pi(x) = \big(1 + o(1)\big)\frac{x^\theta}{\log x}\end{gathered} \tag{9.10}$$

が含まれるのである:

$$\text{Hoheisel (1930) の大発見}: \quad N(\alpha,T) \ll T^{\lambda(1-\alpha)}(\log T)^c \ \Rightarrow\ 1-1/\lambda < \theta. \tag{9.11}$$

証明は容易である: (4.8) にて $T = x^{1-\omega}\log^3 x$, $\omega = 1-1/\lambda+\varepsilon$ とおくならば, 任意の $0<y<x$ について,

$$\psi(x+y)-\psi(x) = y - \int_x^{x+y}\Bigg(\sum_{\rho,\,|\gamma|<T} u^{\rho-1}\Bigg)du + o(x^\omega). \tag{9.12}$$

部分積分法を用い,

$$\Bigg|\sum_{\rho,\,|\gamma|<T} u^{\rho-1}\Bigg| \le -\int_0^1 u^{\alpha-1}dN(\alpha,T) = (\log u)\int_{\frac12}^1 N(\alpha,T)u^{\alpha-1}d\alpha + O\big(u^{-1/2}T\log T\big). \tag{9.13}$$

誤差項は (4.6) による. Vinogradov の (5.12) から, 例えば $\gamma = (\log T)^{-3/4}$ をもって,

$$\int_{\frac12}^1 N(\alpha,T)u^{\alpha-1}d\alpha \ll (\log x)^c\int_{\frac12}^{1-\gamma}\big(x^{-1}T^\lambda\big)^{1-\alpha}d\alpha \ll (\log x)^c x^{(\lambda(1-\omega)-1)\gamma}. \tag{9.14}$$

証明を終わる. ただし, 以上は後の知見 (5.12) をもって Hoheisel の論旨を強化したものである (彼自身が与えた θ の下限は $1-\frac{1}{33000}$). なお, 評価

$$N(\alpha,T) \ll T^{4\alpha(1-\alpha)}(\log T)^6 \tag{9.15}$$

をも彼は得ている. 従って, とくに,

$$(9.8)\text{ にて, } \theta > \tfrac34, \tag{9.16}$$

および,

$$\big|\sigma-\tfrac12\big| \ll \Big(\frac{\log\log|t|}{\log|t|}\Big)^{1/2} \quad (|t|\ge 3) \tag{9.17}$$

なる $\sigma=\frac12$ の極めて狭い近傍に殆どの非自明零点が集中している, と知れる. Bohr–Landau の (9.4) の改良である.

RH 完全証明への闘いから観るならば, (9.7) は敵前逃亡と揶揄されかねない. しかし, Riemann ([4.2]) の目的が何であったか, を思うならば見解は変わり得る. 彼は, 「素数分布を念頭に置き」$\zeta(s)$ の解析に思い至ったのである. 彼の論文表題からそれは明確. その立場からは, (9.10) なる素数定理は,

$$\text{quasi-RH}: \quad \zeta(s)\neq 0,\ \sigma > \theta-\varepsilon \tag{9.18}$$

からの帰結と同一 . ただし, 逆は不明. 多少踏み込むならば, (9.18) からは, (9.10) より深い結果を導き得ない, と思われる. 更に言うならば,

$$\text{短区間における素数分布に関しては, quasi-RH を必ずしも必要とはしない.} \tag{9.19}$$

以下, $N(\alpha,T)$ を「$\zeta(s)$ の零点密度」, また, Hoheisel の論法を「零点密度法」と呼ぶ. もっとも, $N(\alpha,T)$, $\alpha>\frac12$, は「存在せぬことが願われる集合の大きさ」である故, 零点密度法に違和感を覚えることは, ごく自然である. そこで, $N(\alpha,T)$ を経由せず, その様な評価をもたらす手段から直接に (9.10) に達することもなされている. しかし, 要は変わらず.

[9.1] H. Bohr et E. Landau (1914): Sur les zèros de la fonction $\zeta(s)$ de Riemann. Comptes rendus, **158**, 106–110.
[9.2] G. Hoheisel (1930): Primzahlprobleme in der Analysis. Sitz. Preuss. Akad. Wiss., **33**, 3–11.
[9.3] 本節については, [C, 第 3 章] を見よ.
[9.4] 素数定理 (9.10) は, $x<\exists p<x+x^\theta$ $(x\uparrow\infty)$ を意味する. しかし, 素数間の差の大きさの評価「のみ」を望むならば, 「漸近式」(9.10) を何らかの常数 $0<\vartheta<1$ をもって 不等式 $\pi(x+x^\vartheta)-\pi(x)>0$ に置き換えるも可. 篩法と零点密度法を結合することにより, $\vartheta\le 0.525$ が達成されている. 証明は至極複雑である. R.C. Baker, G. Harman, and J.

Pintz (2001): The difference between consecutive primes. II. Proc. London Math. Soc., **83**, 532–562. 当該の篩法の解説は割愛.
[9.5] 整数 $n>0$ につき $n^2<p<(n+1)^2$ なる素数 p が必ず存在するであろう. この予想は未だに未解決. RH の下にても.

10. 評価 (9.15) の証明に当たり, Hoheisel は Carlson (1921) の着想に従い, (9.5) に代え

$$\zeta(s)M_X(s)-1,\quad M_X(s)=\sum_{m\le X}\frac{\mu(m)}{m^s},\quad \mu:\text{ Möbius 函数},\tag{10.1}$$

を考察したのであるが, この mollifyer $M_X(s)$ の採用が今日では基本となっている. もちろん, $M_X(s)$ は $1/\zeta(s)$ への有限 Dirichlet 級数近似と捉え得る. かくして, Ingham (1940) は (10.1) をもって

$$N(\alpha,T)\ll\begin{cases}T^{2(1+2\eta)(1-\alpha)}(\log T)^c,\\ T^{3(1-\alpha)/(2-\alpha)}(\log T)^c,\end{cases}\quad T\ge 2,\tag{10.2}$$

を得た (1960 年代の末まで永く最良評価の座を占めた: [10.8] を見よ). ただし,

$$\zeta\big(\tfrac12+it\big)\ll t^{\eta}(\log t)^c,\quad t\ge 2.\tag{10.3}$$

この重要な常数 η 関し,

$$\text{Lindelöf 予想}:\quad \eta=\varepsilon\quad\Rightarrow\quad \pi(x+x^{\theta})-\pi(x)=\big(1+o(1)\big)\frac{x^{\theta}}{\log x},\ \theta>\frac12.\tag{10.4}$$

すなわち, RH からもたらされる短区間素数定理 (4.9) と実質的に同一 (注意: RH $\Rightarrow$ Lindelöf 予想). Phragmén–Lindelöf 定理 (垂直帯領域の場合) の直接的な帰結として,

$$\text{凸性評価:}\quad \eta\le\tfrac14\tag{10.5}$$

があるが, 当然に, これを凌ぐ非凸性 sub-convexity 評価を得ることにこそ意義がある.

Ingham は $(10.2)_{\text{上辺}}$ の証明に当たり,

$$\text{凸性}:\quad |\zeta(\alpha+it)|\ll|t|^{2\eta(1-\alpha)}(\log|t|)^c,\quad |t|\ge 2,\ \frac12\le\alpha\le 1\tag{10.6}$$

と共に, 今日の定式化をもって表現するならば, L^2-不等式

$$\int_{-T}^{T}\Big|\sum_{n=1}^{\infty}a_n n^{it}\Big|^2dt\ll\sum_{n=1}^{\infty}(n+T)|a_n|^2\quad\text{(仮定: 右辺は有限)}\tag{10.7}$$

を用いた. 一方, $(10.2)_{\text{下辺}}$ の証明には, 彼自身 (1926) による $\zeta(s)$ の「4 乗平均」

$$I_2(T)=\frac{1}{2\pi^2}T(\log T)^4+O\big(T(\log T)^3\big).\tag{10.8}$$

を応用した. ただし,

$$I_k(T)=\int_0^T\big|\zeta\big(\tfrac12+it\big)\big|^{2k}dt.\tag{10.9}$$

後の Gallagher (1970) の手法によるならば, L^2-不等式 (10.7) の証明は次の通り: より詳しく

$$\int_{-T}^{T}\left|\sum_{n=1}^{\infty}a_n n^{it}\right|^2dt\ll T^2\int_0^{\infty}\left|\sum_{x\le n\le x\exp(\pi/T)}a_n\right|^2\frac{dx}{x}.\tag{10.10}$$

このために, 函数 $F(x)=\sum_\omega c_\omega e^{i\omega x}$ の 2 乗平均を考察する．任意の $\tau>0$ につき, $v(x)=\tau^{-1}$ $(|x|\le\frac12\tau)$, $v(x)=0$ $(|x|>\frac12\tau)$ とおく．Parseval 公式により,

$$\int_{-\infty}^{\infty}|F(x)\hat v(x)|^2dx=2\pi\int_{-\infty}^{\infty}\left|\sum_\omega c_\omega v(x-\omega)\right|^2dx. \tag{10.11}$$

ここに，$\hat v(x)=(2/\tau x)\sin(\frac12\tau x)$．区間 $[-\pi/\tau,\,\pi/\tau]$ では $\hat v(x)\ge 2/\pi$ である故,

$$\int_{-\pi/\tau}^{\pi/\tau}|F(x)|^2dx\ll\tau^{-2}\int_{-\infty}^{\infty}\left|\sum_{|\omega-x|\le\frac12\tau}c_\omega\right|^2dx. \tag{10.12}$$

そこで $\tau=\pi/T$, $c_\omega=a_n$, $\omega=\log n$ と採り (10.10) を得る.

一方, (10.7) の証明には, Hardy–Littlewood(1925) による「$\zeta^2(s)$ の近似函数等式」が応用されている: $t\ge2$ につき,

$$\zeta^2\big(\tfrac12+it\big)=\sum_{n\le t/2\pi}d(n)n^{-\frac12-it}+i\Big(\frac{t}{2\pi e}\Big)^{-2ti}\sum_{n\le t/2\pi}d(n)n^{-\frac12+it}+O(\log t). \tag{10.13}$$

ただし, $d(n)$ は約数函数. これの証明は極めて入り組む. しかし, 零点密度評価に限るならば, (10.8) に代わり不等式

$$\int_0^T\left|\zeta\left(\tfrac12+it\right)\right|^4dt\ll T(\log T)^c \tag{10.14}$$

をもって足りる. これの証明は, 後の Ramachandra (1974) の着想によるならば, 函数等式 (4.4) と L^2 不等式 (10.7) の応用をもって容易. [C, §3.2] も見よ.

それ故,

非凸性評価 (10.3) と冪乗平均 $I_k(T)$ (10.15)

に関心が集中することになった. しかし, これは一種の「遡及」であり, 実際は素数分布を念頭に置かずに既に議論されていたのである. 一方は「絶対的」評価, 他方は「平均的」評価である. これらを統合するならば, 素数分布にて目覚ましい成果が得られる. 解析的整数論における中心的な paradigm の出現であった.

なお, $(10.2)_{下辺}$ は, 領域

$$\left|\sigma-\tfrac12\right|\ll\frac{\log\log|t|}{\log|t|}\quad(|t|\ge3) \tag{10.16}$$

への非自明零点の雲集を意味する. これは (9.17) の著しい改良. 4 乗平均 (10.8) (もしくは (10.14)) によりもたらされたことに注目すべし.

[10.1] F. Carlson (1921): Über die Nullstellen der Dirichletschen Reihen und der Riemannschen ζ-Funktion. Arkiv for Mat. Ast. och Fysik., **15**, No. 20.

[10.2] A.E. Ingham (1926): Mean-value theorems in the theory of the Riemann zeta-function. Proc. London Math. Soc., **27**, 273–300.

[10.3] — (1940): On the estimation of $N(\sigma,T)$. Quart. J. Math. Oxford, **11**, 291–292.

[10.4] 冪乗平均 $I_k(T)$ の総合報告は, A. Ivić (1991): Mean values of the Riemann zeta-function. Tata lecture note, vol.82.

[10.5] Gallagher (1970): A large sieve density estimate near $\sigma=1$. Invent. math., **11**, 329–339.

[10.6] G.H. Hardy and J.E. Littlewood (1929): The approximate functional equation for $\zeta(s)$ and $\zeta^2(s)$. Proc. London Math. Soc., **29**, 81–97. 誤差項 $O(\log t)$ は漸近展開可能であり, それにより実は $O\big(t^{-1/6}\big)$ と知れる. Y. Motohashi (1997): An asymptotic expansion of the square of the Riemann zeta-function. In: Sieve Methods, Exponential Sums, and their Applications in Number Theory: C. Hooley Festschrift, Cambridge Univ. Press, pp. 293–307.

[10.7] K. Ramachandra (1974): A simple proof of the mean fourth power estimate for $\zeta(\frac12+it)$ and $L(\frac12+it,\chi)$. Ann. Scuola Norm. Sup. Pisa, (4) **1**, 81–97.

[10.8] 評価 (10.2) の改良をもたらした現代的な零点密度評価の議論は, Montgomery (1969): Invent. math., **8**, 334–354 に始まる. 彼の手法は, 'large values method' とも呼ばれる. 本講演では逡巡の末, 割愛. [C, §7.3] も参照せよ.
[10.9] 短区間素数定理 (9.10) の文脈 (漸近式) にて現今最良の結果は $\theta \geq \frac{7}{12}$. Huxley (1972): On the difference between consecutive primes. Invent. math., 15, 164–170; Heat-Brown (1988): The number of primes in a short interval. J. reine angew. Math., **389**, 22–63. 後者にては, 上記第 9 節本文の終段の意味合いをもって, 零点密度理論の応用が避けられている.

11. 課題 (10.3) につき初の目覚ましい着想をもたらしたのは, Weyl (1916). 充分に滑らかな実数値函数 f をもって和

$$\sum_{N\leq n<2N} e(f(n)), \quad e(x)=\exp(2\pi i x), \tag{11.1}$$

の評価を考察する. 仮に点集合 $\{e(f(n))\}$ が単位円周上に平均的に分布するならば, (11.1) は自明な評価 ($\leq N$) よりも相当に小となろう. しかし, この集合が不規則に散乱するものであるならば, 「良好」な評価, つまり, ある常数 $\kappa<1$ をもって $\ll N^{\kappa}$ であろうとは期待し難い. 課題 (10.3) は $f(x)=(t/2\pi)\log x$ なる場合であり, とくに $t>0$ が大なるとき, 分布状態は均一からは程遠い. Weyl は, このような不均一分布の場合であっても, 点集合 $\{e(f(n))\}$ 内の「打ち消し合い」 cancellation を「検出可能でありえる」と示したのである. 論旨は簡単明瞭. まず, 区間 $[N,\,2N)$ を短区間に分割し, (11.1) に代え,

$$\sum_{0\leq u<U} e\big(f(u+M)\big), \quad M\approx N. \tag{11.2}$$

を考察する. ただし, $U=N^{\xi}$, $\xi<1$. 目下の仮定のもと, $f(u+M)$ は多項式 $g(u)\in\mathbb{R}[u]$ をもって充分に近似可能. よって, (11.2) に代え,

$$\text{Weyl 和}: \quad G(U)=\sum_{1\leq u\leq U} e\big(g(u)\big) \tag{11.3}$$

を考察する. さらに, 自明な省略をもって,

$$\text{Weyl shift}: \quad |G(U)|^2=\sum_{r}\sum_{u} e\big(g(u+r)-g(u)\big) \tag{11.4}$$

に注意する. ここで, 「u の多項式」$g(u+r)-g(u)$ の次数は g のそれよりも低い. 操作を繰り返し,

$$\begin{gathered} S=\sum_{a\leq u<b} e\left(\alpha u+\beta\right), \quad \alpha,\,\beta\in\mathbb{R}, \\ |S|\leq \min\left\{b-a,\,\frac{1}{|\sin\pi\alpha|}\right\}, \end{gathered} \tag{11.5}$$

に達する. かくして, (11.1) の非自明な評価を達成し得る訳である.

一方, van der Corput (1921) は Weyl shift を取り入れ, Cauchy 不等式を用い,

$$\begin{aligned} (11.1) &\approx \frac{1}{U}\sum_{N<n\leq 2N}\sum_{0<u\leq U} e(f(n+u)) \\ &\ll \frac{N}{U}+\frac{N^{1/2}}{U}\left(\sum_{0\leq u<v<U}\left|\sum_{N\leq n<2N} e\big(f(n+u)-f(n+v)\big)\right|\right)^{1/2}. \end{aligned} \tag{11.6}$$

さらに, 下辺の内部和に Poisson 和公式を応用. 得られる積分各々に「鞍点法」を応用. Weyl の手法と比較し, 「むだ」が少ない.

何れにせよ

$$(10.3)\text{ において }\eta\leq\tfrac{1}{6} \tag{11.7}$$

が達成される. よって, (9.11) および $(10.2)_{\text{上辺}}$ により,

$$(9.10)\text{ において }\theta\leq\tfrac{5}{8}. \tag{11.8}$$

なお, Vinogradov の評価 (5.11) は, (11.6) における Cauchy 不等式に代え, 極めて高い冪をもって Hölder 不等式を用いる. Weyl shift を「多変数」に関し考察することとなるが, そのために, 重要な手段として, 多変数の連立方程式

$$\begin{gathered} x_1^l + x_2^l + \cdots + x_q^l = x_{q+1}^l + x_{q+2}^l + \cdots + x_{2q}^l, \\ 1 \le x_j \le U,\ 1 \le j \le 2q, \end{gathered} \quad 1 \le l \le k. \tag{11.9}$$

の整数解の個数の評価が核心をなす. それを「Vinogradov の平均値定理」と呼ぶこともある. 何故ならば, この個数は積分

$$\int_{[0,1]^k} \left| \sum_{u=1}^{U} e\big(\theta_1 u + \theta_2 u^2 + \cdots + \theta_k u^k\big) \right|^{2q} d\theta_1 d\theta_2 \cdots d\theta_k \tag{11.10}$$

に一致する. 理論の詳細は複雑であるが, 結論 (5.12)–(5.13) は目覚ましい. なお, Karatsuba (1975) による簡易化があり, その手法が現在では主. 彼の最終結果は,

$$\sum_{n \le N} n^{it} \ll N^{1-(\log N/\log t)^2}, \quad 2 \le N \le t. \tag{11.11}$$

これは, $N \gg \exp\big((\log t)^{2/3}\big)$ なる場合, 左辺にて cancellation が発生することを示す訳であり, 至極強力.

[11.1] H. Weyl (1916): Über die Gleichverteilung von Zahlen mod. Eins. Math. Ann., **77**, 313–352.
[11.2] J.G. van der Corput (1921): Zhalentheoretische Abschätzungen. Math. Ann., **84**, 53–79.
[11.3] I.M. Vinogradov (1958): A new estimate for $\zeta(1+it)$. Izv. Akad. Nauk SSSR, Ser. Mat., **22**, 161–164. (Russian)
[11.4] A.A. Karatsuba (1975): Elements of analytic number theory. Nauka, Moscow; Second edition. Fizmatlit, Moscow 1983. (Russian)

[11.5] 本節については, [C, 第 2 章] を見よ. なお, (11.8) は obsolete. [10.9] を見よ. 一方, 現在最良の評価 $\eta \le \frac{13}{84}$: J. Bourgain (2016): Decoupling, exponential sums and the Riemann zeta function. arXiv:1408.5794v2 [math.NT] は確かに (11.8) を凌ぐ結果 $\theta \le \frac{34}{55}$ を与えるが, これは [10.9] (ましてや [9.4]) よりも弱い. [9.4] を $(10.2)_{\text{上辺}}$ をもって達成するためには, $\eta \le \frac{1}{38}$ を必要とする. これは, 今日の zeta-函数論の力量にとり絶望的な要求である. [9.4] は漸近式を意味せぬとは言え, 篩法の助勢が如何に強力であるか知れよう.
[11.6] 評価 (11.11) を $N^{1-(\log N/\log t)^\tau}$, $\tau < 2$, へ改良することは極めて困難.
[11.7] 近時, Vinogradov の平均値定理に関し, 重要な発展がもたらされた. J. Bourgain, C. Demeter, and L. Guth (2016): Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher then three. arXiv:1512.01565v3 [math.NT]. しかし, (11.11) の改良は依然として得られていない.
[11.8] Sub-convexity exponent $\frac{1}{6}$ ((11.7)) は一種の普遍常数 universal constant と映る: 群 $\mathrm{SL}(2,\mathbb{Z})$ に関する保型 L-函数は, その函数等式の形態から $\zeta^2(s)$ に強く類似. これら L-函数は全て (11.7) に対応するところにて $\frac{1}{3}$ なる (sub-convexity) 指数を持つ. M. Jutila and Y. Motohashi (2005): Uniform bounds for Hecke L-functions. Acta Math., **195**, 61–115.

12. 課題 (10.9) の解説に進む. 先ず, 2 乗平均 $I_1(T)$ について述べる. Hardy, Littlewood, Ingham が先行したが, 彼らを遥かに超える Atkinson (1949) の結果に注目する. 大略

$$\text{Atkinson 公式}: \quad \begin{gathered} I_1(T) = T\log T + \big(2c_E - 1 - \log(2\pi)\big)T + E_1(T), \\ \text{残余項 } E_1(T) \text{ は漸近展開される.} \end{gathered} \tag{12.1}$$

ただし, $c_E = 0.577\ldots$ は Euler 常数. これより,

$$E_1(T) \ll T^{1/3}(\log T)^2, \quad E_1(T) = \Omega_\pm\big(T^{1/4}\big), \quad \int_0^V E_1(T)^2 dT \ll V^{3/2} \tag{12.2}$$

などが従う. ただし, $f(x) = \Omega_\pm(h(x))$, $h(x) > 0$, は何らかの常数 $c_\pm$ があり, $f(x_+) > c_+ h(x_+)$, $f(x_-) < -c_- h(x_-)$ なる無限列 $\{x_\pm\}$ が存在することを意味する.

しかし, 応用上は, (12.1) の「局所版」とも言われる次の結果がより有効と知られている: 充分大なる $A > 0$ をもって,

$$\begin{gathered} \text{函数 } g(z) \text{ は } \mathbb{R} \text{ 上実数値,} \\ \text{水平帯領域 } |\mathrm{Im}\ z| \le A \text{ にて正則, かつ } O\big((|z|+1)^{-A}\big). \end{gathered} \tag{12.3}$$

この仮定のもとに,

$$\int_{-\infty}^{\infty}\left|\zeta\big(\tfrac12+it\big)\right|^2 g(t)dt=\int_{-\infty}^{\infty}\left[\mathrm{Re}\left\{\frac{\Gamma'}{\Gamma}\big(\tfrac12+it\big)\right\}+2c_E-\log(2\pi)\right]g(t)dt+2\pi\mathrm{Re}\big\{g\big(\tfrac12 i\big)\big\}$$
$$+4\sum_{n=1}^{\infty}d(n)\int_0^{\infty}(y(y+1))^{-1/2}g_c\big(\log(1+1/y)\big)\cos(2\pi ny)dy. \tag{12.4}$$

ただし, $d(n)$ は約数函数であり,

$$g_c(Y)=\int_{-\infty}^{\infty}g(z)\cos(Yz)dz. \tag{12.5}$$

Atkinson の (12.1) から Heath-Brown (1978) により既に導かれていた事実であるが, (12.4) は「相当に深い」平均値

$$I_6(T)\ll T^2(\log T)^{21} \tag{12.6}$$

を与える. また, 更に (11.7) の少々大掛かりながら解析的にはより満足感のある別証明も得られる. すなわち, (12.4) あるいは (12.6) は $\zeta\big(\frac12+it\big)$ の個別評価をも含む訳である. これがために, Balasubramanian–Ramachandra (1989) の興味深い補題を示しておく.

$$\begin{gathered}\text{円盤 } |z|\le r \text{ にて函数 } f(z) \text{ は正則かつ } |f(z)|\le M,\ M>1, \text{ とするとき,}\\ \text{任意の } A>1 \text{ をもって, } f(0)\ll (A/r)\log M\int_{-r}^{r}|f(iy)|dy+M^{-A}.\end{gathered} \tag{12.7}$$

ここに, 陰伏常数は絶対的. 自明な帰結ながら:

$$\text{充分に離散的な数列 } \{z_j\}\subset i\mathbb{R} \text{ につき } \textstyle\sum_j|f(z_j)| \text{ は積分 } \int|f(iy)|dy \text{ をもって評価可能.} \tag{12.8}$$

[12.1] F.V. Atkinson (1949): The mean value of the Riemann zeta-function. Acta Math., **81**, 353–376.
[12.2] D.R. Heath-Brown (1978): The twelfth power moment of the Riemann zeta-function. Quart. J. Math. Oxford, **29**, 443–462.
[12.3] R. Balasubramanian and K. Ramachandra (1989): A lemma in complex function theory I. Hardy–Ramanujan J., **12**, 1–5.
[12.4] 展開 (12.4) の証明他については [B, §4.1], [C, §3.2] を見よ.

13. Atkinson 公式 (12.1) およびその局所版 (12.4) は, 実は, Weyl shift (11.4) の「完遂形」とも言える. かなり一般化し, この間の機微を述べておく.

解析的整数論の目的の多くは, 「数え上げ」手法の獲得である. つまり, 何らかの具体的な函数 F をもって, 和

$$\sum_n F(n) \tag{13.1}$$

を問題とすることしばしば. このために, Poisson 和公式や Dirichlet 級数が多用される. それゆえ, 和 (11.1) を扱うこととなる. その中で, Weyl shift (van der Corput 版 (11.6)) は「一次元」和を「二次元」和に引き上げる (lift する) 手法である. これにより, 自由度が上がるが, その効果は $(11.6)_{\text{下辺}}$ の 2 重和の評価をもって得られる.

この 2 重和を, 「非対角」(off-diagonal) 成分に関する和, と捉える. そこで, より一般に「二次元和の分解」

$$\sum_{m,n}F(m,n)=\left\{\sum_{m=n}+\sum_{m<n}+\sum_{m>n}\right\}F(m,n) \tag{13.2}$$

に想到する. 実は, Atkinson の着想は (明確には言及されていないが) この自明な等式の見事な応用結果. それ故, 当然に, 分解 (13.2) は最良なものであるのか否かが課題となる. つまり, 「対角」の意味が問われる. 一つの「算術的」提案として, 分解

$$\sum_{m,n}F(m,n)=\left\{\sum_{km=ln}+\sum_{km<ln}+\sum_{km>ln}\right\}F(m,n) \tag{13.3}$$

に気づく. ただし, $k,\, l \neq 0$ は整数. つまり, 新たに $y = (k/l)x$ を対角線あるいは対称軸と見る訳である. そして, これは「4 次元」和の一部. かくして, 分解

$$\sum_{k,l,m,n} F(k,l,m,n) = \left\{ \sum_{kn=lm} + \sum_{kn<lm} + \sum_{kn>lm} \right\} F(k,l,m,n) \tag{13.4}$$

に至り整数行列 $K = \left(\begin{smallmatrix} k & m \\ l & n \end{smallmatrix}\right)$ が現れる. すなわち, (13.4) は次と同一.

$$\sum_{K} F(K) = \left\{ \sum_{|K|=0} + \sum_{|K|<0} + \sum_{|K|>0} \right\} F(K). \tag{13.5}$$

そこで, Hecke の同値類 $\bmod \mathrm{SL}(2,\mathbb{Z})$ にもとづき,

$$\sum_{|K|>0} F(K) = \sum_{n=1}^{\infty} \sum_{|K|=n} F(K) = \sum_{n=1}^{\infty} \sum_{ad=n} \sum_{b=1}^{d} \sum_{L\in \mathrm{SL}(2,\mathbb{Z})} F\left(L \begin{pmatrix} a & b \\ & d \end{pmatrix} \right). \tag{13.6}$$

和 (13.4) の調和解析 (つまりは, Casimiri 作用素に関するスペクトル分解) と共に Hecke 作用素の介在が察知される. 序文にて示唆したところである.

とくに (13.6) を $I_2(T)$ あるいは $(12.4)_{左辺}$ の「4 乗平均版」に用い, 仮定 (12.3) のもとに,

$$\int_{-\infty}^{\infty} \left|\zeta\left(\tfrac{1}{2}+it\right)\right|^4 g(t)dt = \left\{ {}^{r}\mathcal{Z}_2 + {}^{0}\mathcal{Z}_2 + {}^{e}\mathcal{Z}_2 \right\}(g). \tag{13.7}$$

但し, 絶対常数 $\varpi_{k,l}^{a,b}$ をもって

$$\begin{aligned} {}^{r}\mathcal{Z}_2(g) &= \int_{-\infty}^{\infty} \sum_{\substack{a,b,k,l\geq 0 \\ ak+bl\leq 4}} \varpi_{k,l}^{a,b} \,\mathrm{Re}\left[\left(\frac{\Gamma^{(a)}}{\Gamma}\right)^k \left(\frac{\Gamma^{(b)}}{\Gamma}\right)^l \left(\tfrac{1}{2}+it\right) \right] g(t)dt \\ &\quad - 2\pi \mathrm{Re}\left\{ \left(c_E - \log(2\pi)\right) g\left(\tfrac{1}{2}i\right) + \tfrac{1}{2} i g'\left(\tfrac{1}{2}i\right) \right\}, \end{aligned} \tag{13.8}$$

$${}^{0}\mathcal{Z}_2(g) = \sum_{V} |\varrho_V(1)|^2 H_V^3\left(\tfrac{1}{2}\right) \Lambda(\nu_V, \epsilon_V; g), \tag{13.9}$$

$${}^{e}\mathcal{Z}_2(g) = \frac{1}{4\pi} \int_{-\infty}^{\infty} \frac{|\zeta\left(\frac{1}{2}+iu\right)|^6}{|\zeta(1+2iu)|^2} \Lambda(iu, 1; g) du. \tag{13.10}$$

ここに,

$$\begin{aligned} \Lambda(\nu,\kappa;g) \;&= 4\int_0^{\infty} (y(1+y))^{-1/2} g_c\big(\log(1+1/y)\big) \\ &\quad \times \mathrm{Re}\left[y^{-1/2-\nu} \Big(\kappa - \frac{1}{\sin(\pi\nu)} \Big) \frac{\Gamma^2\left(\frac{1}{2}+\nu\right)}{\Gamma(1+2\nu)} {}_2F_1\left(\tfrac{1}{2}+\nu, \tfrac{1}{2}+\nu; 1+2\nu; -1/y\right) \right] dy. \end{aligned} \tag{13.11}$$

記号は大略以下の通り: 群 $\mathrm{G} = \mathrm{PSL}(2,\mathbb{R})$, $\mathit{\Gamma} = \mathrm{PSL}(2,\mathbb{Z})$. Iwasawa 分解 $\mathrm{G} = \mathrm{NAK}$, $\mathrm{N} = \{\mathrm{n}[x] : x \in \mathbb{R}\}$, $\mathrm{A} = \{\mathrm{a}[y] : y > 0\}$, $\mathrm{K} = \{\mathrm{k}[\theta] : \theta \in \mathbb{R}/\pi\mathbb{Z}\}$ をもって不変測度 $d\mathrm{g} = dxdyd\theta/\pi y$. ただし,

$$\begin{gathered} \mathrm{G} \ni \mathrm{g} = \mathrm{n}[x]\mathrm{a}[y]\mathrm{k}[\theta]; \quad \mathrm{n}[x] = \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}, \quad \mathrm{a}[y] = \begin{bmatrix} \sqrt{y} & \\ & 1/\sqrt{y} \end{bmatrix}, \quad \mathrm{k}[\theta] = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}, \\ L^2(\mathit{\Gamma}\backslash\mathrm{G}) = \mathbb{C}\cdot 1 \bigoplus {}^{0}L^2(\mathit{\Gamma}\backslash\mathrm{G}) \bigoplus {}^{e}L^2(\mathit{\Gamma}\backslash\mathrm{G}). \end{gathered} \tag{13.12}$$

部分空間 ${}^{0}L^2(\mathit{\Gamma}\backslash\mathrm{G})$ は cusp forms により, 部分空間 ${}^{e}L^2(\mathit{\Gamma}\backslash\mathrm{G})$ は Eisenstein 級数の積分により張られ,

$${}^{0}L^2(\mathit{\Gamma}\backslash\mathrm{G}) = \oplus V, \quad \mathrm{Casimir}|_V = \left(\tfrac{1}{4} - \nu_V^2\right) \cdot 1 \tag{13.13}$$

更に, 各不変部分空間 V は Hecke 不変; $\rho_V(n)$ を V を生成する cup form の (通常の正規化のもとに) Fourier 系数とし, $\varrho_V(-n) = \epsilon_V \varrho_V(n)$. ただし, $\epsilon_V = \pm 1$ (主系列), $\epsilon_V = 0$ (離散系列). さらに, $H_V(s)$ は V に付随する Hecke L-函数.

スペクトル分解 (13.7) から導かれる結論には目覚ましいものがある. 例えば, ある 4 次多項式 P_4 が存在し,

$$I_2(T) = TP_4(\log T) + E_2(T), \quad E_2(T) \ll T^{2/3}(\log T)^8, \quad E_2(T) = \Omega_\pm(T^{1/2}). \tag{13.14}$$

かつ,

$$\int_0^V E_2(T)^2 dT \ll V^2(\log V)^{22}. \tag{13.15}$$

もちろん, これらは (12.2) の拡張であり, (10.8) の非常な深化. 評価 (12.6) をも含む.

なお, (13.7) は次のごとき結論ももたらす: Mellin 変換

$$\int_1^\infty \left|\zeta\left(\tfrac{1}{2} + iu\right)\right|^4 u^{-s} du, \quad \operatorname{Re} s > 1, \tag{13.16}$$

は全 s-平面にて有理型函数であり, とくに $\operatorname{Re} s = \frac{1}{2}$ 上に 1 位の極 $\frac{1}{2} \pm \nu_V$ が並ぶ. ただし, V は主系列に含まれる ($\nu_V \in i\mathbb{R}$). この事実は, $\mathrm{SL}(2,\mathbb{Z})$ に付随する Selberg zeta-函数と (13.16) との密接な関係を示唆している. さらに, これら極の留数は $H_V^3\left(\frac{1}{2}\right)$ を明示的に含む故, zeta-函数は保型形式 (とくに, Maass 形式) の一種の母函数であろう, との仄かな暗示ももたらす. 実際, (13.16) に代わる Mellin 変換

$$\int_1^\infty \left\{\zeta\left(\tfrac{1}{2}(w+\tfrac{1}{2}) + iu\right)\zeta\left(\tfrac{1}{2}(w+\tfrac{1}{2}) - iu\right)\right\}^2 u^{-s} du, \quad \frac{1}{2} \le \operatorname{Re} w < 1, \tag{13.17}$$

は $s = 1 - w \pm i\nu_V$ なる 1 位の極を持ち, その留数は $H_V^2\left(\frac{1}{2}\right) H_V(w)$ を明示的に含む. つまり, やや強引な推論ながら, 保型 L-函数 H_V の値を ζ-函数の値から導き得る: 模式的には,

$$\zeta \longleftrightarrow \left\{H_V : V\right\}. \tag{13.18}$$

ちなみに, 等式 (13.5) をかなり特殊化するならば,

$$\text{the binary additive divisor problem :} \quad \sum_{n \le N} d(n)d(n+h) \tag{13.19}$$

に導かれる. この和は $h = 0$ の場合と $h \neq 0$ の場合とでは全く異なる性格を持つ. 前者は乗法的函数 $d^2(n)$ の和 (Ramanujan ([3.3])). 後者はこれに加法的な twist を加えたものであり (shifted Rankin–Selberg convolution), 乗法と加法の間に位置する. 僅かな加法的揺動が「無限に多くの」保型形式を呼び起こす. よって, 和 $(13.19)_{h\neq 0}$ の扱いは容易とは言えない. Motohashi (1994) を見よ. 同様の乗法と加法の干渉は「素数分布論の 2 大問題」に顕在:

$$\text{双子素数予想 :} \sum_{n \le N} \Lambda(n)\Lambda(n+2), \quad \text{Goldbach 予想 :} \sum_{n \le 2N} \Lambda(n)\Lambda(2N-n). \tag{13.20}$$

[13.1] 恐らくは, $E_1 = O(T^{1/4+\varepsilon})$, $E_2 = O(T^{1/2+\varepsilon})$ であり, これらは「最良評価」. 例えば, 6 乗平均については, 類似の事実は未知である. [B, §5.4] を見よ. なお, RH のもとに $I_k(T)$ を考察する議論があるが, それは本末転倒と映る.

[13.2] $E_2(T) = \Omega_\pm(T^{1/2})$ なる結論は, 或る種の困惑を与えるものでもある. [B, pp.218–219] を見よ.

[13.3] 本節は [B], [D] の核心部分. Motohashi (1993): An explicit formual for the fourth power mean of the Riemann zeta-function. Acta Math., **170**, 181–220 も見よ. 直接の先行研究は Iwaniec (1979/80) であるが, 基礎は, Kuznetsov (1977), Selberg (1965), Linnik (1962), Atkinson (1941) と遡る.

[13.4] H. Iwaniec (1979/80): Fourier coefficients of cusp forms and the Riemann zeta-function. Exp. No.18, Sém. Th. Nombres, Univ. Bordeaux.

[13.5] N.V. Kuznetsov (1977): Petersson hypothesis for forms of weight zero and Linnik hypothesis. Preprint: Khabarovsk Complex Res. Inst., East Siberian Branch Acad. Sci. USSR, Khabarovsk. (Russian)

[13.6] A. Selberg (1965): On the estimation of Fourier coefficients of modular forms. Proc. Symp. Pure Math., AMS, **8**, 1–15. (Collected papers I, pp.506–520). この論文の主な目的 (p.9/p.514) は Kloosterman 和

$$S(q;a,b)=\sum_{\substack{\ell \bmod q\\ \langle \ell,q\rangle=1}} e\big((a\ell+b\bar{\ell})/q\big),\quad \ell\bar{\ell}\equiv 1 \bmod q$$

の集団 (法 q が変動する) において「打ち消し合い」があるのか否か, という Linnik (1962) の課題の究明. 解析的整数論にては, 単独の $S(q;a,b)$ の評価よりも, 法 q に関する統計的評価がより本質的. Kuznetsov (1977) の解答は

$$\sum_{q\le Q} S(q;a,b)/q \ll Q^{1/6}(\log Q)^{1/3}$$

であり, Weil 評価 $S(q;a,b)\ll q^{1/2}$ から得られるところを遥かに超える (陰伏常数は a,b に関係する). 言わば, 「有限体上の RH」の壁を打ち破ることが可能. この機構が (13.7) の背後にある. なお, Linnik (*ibid.*) は $Q^{1/6}$ に代え Q^{ε} を予想.

[13.7] Yu.V. Linnik (1962). Additive problems and eigenvalues of the modular operators. Proc. Internat. Congress Math., Stockholm, pp.270–284.

[13.8] F.V. Atkinson (1942): The mean value of the zeta-function on the critical line. Proc. London Math. Soc., **47**, 174–200. この論文にて zeta-函数の 4 乗平均 (但し, $|\zeta\big(\frac{1}{2}+it\big)|^4$ の Laplace 変換) と Kloosterman 和との関係が始めて指摘されたのである. もっとも, (13.19) から観るならば, その様な関係の初出は, T. Estermann (1931): Über die Darstellung einer Zahl als Differenz von zwei Produkten. J. reine angew. Math., **164**, pp.173–182.

[13.9] Y. Motohashi (1994): The binary additive divisor problem. Ann. Sci. École Norm. Sup., 4$^{\rm e}$ ser., **27**, 529–572.

14. 以上から, 確かに見える:

$$\mathbb{Z} \text{ に密着し膨大な直交構造がある.} \tag{14.1}$$

解析的整数論の神髄は, 「良き」直交構造を探し求めそれらを使い尽くすことにある. 既に前書きや (7.7) にて強調したところである. 実は Bohr–Landau の着想の延長上にもその様な構造がある. Selberg の発見によるところである (ただし, in retrospect). 今日, それを Λ^2-sieve と呼ぶ. 解説の前に, 篩の一般論を簡略に記しておくべきであろう.

まず, 恒等値函数 $\imath\equiv 1$ および Möbius 函数 μ をもって, 篩法の根本:

$$(\mu*\imath)\big(\langle a,b\rangle\big)=\sum_{d|a,d|b}\mu(d)=\begin{cases}1 & a,b \text{ 互いに素,}\\ 0 & \text{他.}\end{cases} \tag{14.2}$$

ただし, $*$ は Dirichlet 積: $(f*g)(n)=\sum_{d|n} f(d)g(n/d)$. より一般に, 任意の算術的函数 f につき,

$$f(\langle a,b\rangle)=\sum_{d|a,d|b}(\mu*f)(d). \tag{14.3}$$

篩問題の素朴な定式化: 各素数 p につき, $\Omega(p)$ は何らかの剰余類 $\bmod p$ の集合とし, $n\in\Omega(p)$ は $n \bmod p\in\Omega(p)$ を意味するものとする. このとき, 与えられた整数の有限集合 $\mathcal{A}$ につき,

$$\mathcal{S}(\mathcal{A},z)=\{n\in\mathcal{A}: n\notin\Omega(p),\forall p<z\}, \tag{14.4}$$

と書き,

$$\text{篩問題とは, } |\mathcal{S}(\mathcal{A},z)| \text{ の評価.} \tag{14.5}$$

なお, 一般性を失うこと無く, $0<|\Omega(p)|<p$, $\forall p$, と仮定できる ($|\Omega(p_1)|=0$ ならば, p_1 は, 当該の篩に参加せず, また $|\Omega(p_2)|=p_2$ ならば, $p_2<z$ にて篩問題そのものが意味を失う). 「評価」とは上下どちらか, 或は両者. もちろん,

$$\begin{aligned}\mathcal{S}(\mathcal{A},z)&=\mathcal{A}-\bigcup_{p<z}\mathcal{A}_p,\quad \mathcal{A}_p=\{n\in\mathcal{A}: n\in\Omega(p)\},\\ |\mathcal{S}(\mathcal{A},z)|&=\sum_{d|P(z)}\mu(d)|\mathcal{A}_d|,\quad \mathcal{A}_d=\{n\in\mathcal{A}: n\in\Omega(d)\},\ P(z)=\prod_{p<z}p.\end{aligned} \tag{14.6}$$

ただし, $\Omega(d)=\bigcap_{p|d}\Omega(p)$. 下辺は, 周知の 'exclusion–inclusion principle' と同一. また, (14.2) の直接の応用結果でもある. これを Erathosthenes (あるいは, Eratosthenes–Legendre) 篩と呼ぶが, 実際的な応用には耐え得ない, と知られている.

Buchstab (1938) は, (14.6) の上辺を

$$\mathcal{S}(\mathcal{A},z)=\mathcal{A}-\bigsqcup_{p<z}\mathcal{S}(\mathcal{A}_p,p)\ \Rightarrow\ |\mathcal{S}(\mathcal{A},z)|=|\mathcal{A}|-\sum_{p<z}|\mathcal{S}(\mathcal{A}_p,p)| \tag{14.7}$$

と書き換え, $|\mathcal{S}(\mathcal{A},z)|$ の「下から」の評価を $|\mathcal{S}(\mathcal{A}_p,p)|$ の「上から」の評価に転化可能と観察し, 先行した Brun (1919) と共に近代的な篩法に先鞭を付けた. 更に, Rosser (ca 1955: 未発表) は Buchstab の等式を

$$|\mathcal{S}(\mathcal{A},z)|=|\mathcal{A}|-\sum_{p<z}\kappa(p)|\mathcal{S}(\mathcal{A}_p,p)|-\sum_{p<z}(1-\kappa(p))|\mathcal{S}(\mathcal{A}_p,p)| \tag{14.8}$$

と変形. ただし, κ は $\kappa(1)=1$ の他は任意. これを繰り返し,

$$|\mathcal{S}(\mathcal{A},z)|=\sum_{d|P(z)}\mu(d)\rho(d)|\mathcal{A}_d|+\sum_{d|P(z)}\mu(d)\sigma(d)|\mathcal{S}(\mathcal{A}_d,p(d))|. \tag{14.9}$$

ただし, $p(d)$ は d の最小素因数, ρ は $\rho(1)=1$ の他は任意, $\sigma(d)=\rho(d/p(d))-\rho(d)$. 等式 $(14.6)_{\text{下辺}}$ の精密化である.

重み ρ を「工夫をもって」選定するならば, ほぼ自明な (14.9) から思いもよらぬ結果が得られる. しかも, 極めて「初等的」に, である. それらの意味深い選定について詳細を述べることは割愛せざるを得ないが, 最初の実例である Brun's pure sieve (1919) については特に述べておく: 任意に $L\in\mathbb{N}$ を採り,

$$\rho(d)=\begin{cases}1 & \nu(d)\le 2L-1,\\ 0 & \nu(d)\ge 2L,\end{cases}\quad\text{または}\quad \rho(d)=\begin{cases}1 & \nu(d)\le 2L,\\ 0 & \nu(d)\ge 2L+1,\end{cases}\qquad d|P(z), \tag{14.10}$$

と設定する. ただし, $\nu(d)$ は d の相異なる素因数の個数. このとき, 前者ならば, $\nu(d)=2L$ のときのみ $\sigma(d)=1$, 他では $\sigma(d)=0$. 偶奇を入れ替え, 後者も同様. よって, (14.9) から

$$\sum_{\substack{d|P(z)\\ \nu(d)\le 2L-1}}\mu(d)|\mathcal{A}_d|\le|\mathcal{S}(\mathcal{A},z)|\le\sum_{\substack{d|P(z)\\ \nu(d)\le 2L}}\mu(d)|\mathcal{A}_d|. \tag{14.11}$$

ここで重要な点は $d\le z^{2L}$. すなわち, z^{2L} があまり大ならざれば, これらの和は「扱い可能」である. 同様な可能性は (14.6) には無く, これがために, Eratosthenes–Legendre 篩は (14.4) に対しほぼ無力. 数列 $\mathcal{A}=\{n(n+2):n\le N\}$ に (14.11) を応用し, 記念碑

$$\sum\frac{1}{\text{双子素数}}<\infty. \tag{14.12}$$

を得る. 実際, これこそが現代の篩理論の端緒である ((16.20) にて別証明を与える). 不等式 (14.11) の効果大なることと共に, その余りの初等性に驚く次第. なお, $\rho(d)=1,0$ ($P(z)$ の約数の特殊な選択) なる場合, (14.9) を「組み合わせ論的篩」combinatorial sieve と呼ぶ.

Brun の着想の根本は, 篩における等式 (14.6) を諦めたことにある.
これは, (9.7) と同類, と言えよう. つまり, Bohr–Landau の論旨には篩が潜む. (14.13)

次節以降にて, 詳らかとする. 言うなれば,

等式はしばしば雑音を含む (Matti Jutila). (14.14)

あるいは, 完全均衡の古典世界から, 不安定均衡の近代へ.

[14.1] H.J.S. Smith (1876): On the value of a certain arithmetical determinant. Proc. London Math. Soc., **7**, 208–212.
任意の $K\ge 1$ につき,

$$\det\Big(f\big(\langle m,n\rangle\big)\Big)=\prod_{k=1}^{K}(\mu*f)(k).$$

[E, p. 52] を見よ.
[14.2] 'Eratosthenes–Legendre' の篩: 「Eratosthenes の篩」という通常の呼称は, Nicomachus (ca 100 CE) に始まる. しかし, (14.2) の正確な応用は Legendre ([2.1], Théorème II) に源がある (ただし, Möbius 函数の使用は後代). 従って, 両者の名を冠することがよかろう. 実は, 原始根 $\bmod p$ の存在がその個数も含め始めて明確に証明されたのは Legende のこの定理においてである. 通例言われるところの Gauss [0.2] にあらず. [E, §41] を見よ.
[14.3] A. Buchstab (1938): New improvements in the method of the sieve of Eratosthenes. Mat. Sbornik (N.S.), (2) **46**, 375–387. (Russian with German résumé)
[14.4] Rosser の篩については, Selberg (Collected papers I, p.568) の言及がある. Iwaniec (1980): Rosser's sieve. Acta Arith., **36**, 171–202 は原論文とは独立の復元である.
[14.5] V. Brun (1919): La série $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ oú les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie. Bull. Sci. Math., (2)**43**, 100–104, 124–128.
[14.6] 篩の現代的理論については, [A], [C] を見よ. 概観は, Y. Motohashi (2008): An overview of the sieve method and its history. Sugaku Expositions, **21**, 1–32. (arXiv:math/0505521v2)
[14.7] 至言 (14.14) は篩法のみを念頭に置いてなされた訳では無い. 解析的整数論全般における「不等式」の意味を語ったものである.

15. 前節の始めに戻り, 更に (10.1) を観察する. Selberg (1942, §7; 1946, §3) は, 係数としては Möbius 函数は最良の選択ではないことを見抜き,

$$\liminf_{\substack{\lambda\in\mathbb{R}\\ \lambda_1=1}} \int_{-T}^{T} \left|\zeta(s)\sum_{d\le z}\frac{\lambda_d}{d^s}-1\right|^2 dt \tag{15.1}$$

なる最適化を考察 (in retrospect). 主項を計算し, これは本質的には

$$\sum_{n\le N}\Big(\sum_{d\mid n, d\le z}\lambda_d\Big)^2 \tag{15.2}$$

を境界条件 $\lambda_1=1$ の元に扱うことと同じ. さらに, 2 次形式

$$\sum_{d_1,d_2\le z}\frac{\lambda_{d_1}\lambda_{d_2}}{[d_1,d_2]},\quad [d_1,d_2]\text{ は最小公倍数}, \tag{15.3}$$

の最小値を境界条件 $\lambda_1=1$ の元に定めることと「ほぼ」同一と見なし得る (つまり, 誤差項を無視するならば).

Selberg による「対角化」はすこぶる興味深い:

$$\begin{aligned}(15.3) &= \sum_{d_1,d_2\le z}\frac{\lambda_{d_1}\lambda_{d_2}}{d_1d_2}\langle d_1,d_2\rangle = \sum_{d_1,d_2\le z}\frac{\lambda_{d_1}\lambda_{d_2}}{d_1d_2}\sum_{f\mid d_1,f\mid d_2}\varphi(f)\\ &= \sum_{f\le z}\varphi(f)L_f^2,\quad L_f=\sum_{\substack{d\le z\\ f\mid d}}\frac{\lambda_d}{d}.\end{aligned} \tag{15.4}$$

ただし, $\varphi(f)$ は Euler 函数. 線形変換 $\lambda\mapsto L$ は反転可能であり,

$$\lambda_g = g\sum_{\substack{f\le z\\ g\mid f}}\mu(f/g)L_f\quad\text{(Möbius 反転と実質同じ)}. \tag{15.5}$$

とくに, 条件 $\lambda_1=1$ は

$$1=\sum_{f\le z}\mu(f)L_f. \tag{15.6}$$

それ故,

$$(15.3)=\sum_{f\le z}\varphi(f)\big(L_f-\mu(f)/(\varphi(f)K)\big)^2+K^{-1},\quad K=\sum_{f\le z}\frac{\mu^2(f)}{\varphi(f)}. \tag{15.7}$$

つまり,

$$(15.3)\text{ の最小値は, } L_f=\mu(f)/(\varphi(f)K)\text{ をもって, } K^{-1}. \tag{15.8}$$

さらに,

$$\begin{aligned} K &= \sum_{f\le z}\frac{\mu^2(f)}{f}\prod_{p\mid f}\Big(1-\frac{1}{p}\Big)^{-1} = \sum_{f\le z}\frac{\mu^2(f)}{f}\sum_{v\mid f^\infty}\frac{1}{v} \\ &\ge \sum_{n\le z}\frac{1}{n} \ge \int_1^z\frac{d\xi}{\xi} = \log z. \end{aligned} \tag{15.9}$$

以上をまとめ,

$$\sum_{n\le N}\Big(\sum_{d\mid n, d\le z}\lambda_d\Big)^2 \le \frac{N}{\log z}+z^2. \tag{15.10}$$

この「誤差項」z^2 は, (15.5) および (15.8) が $|\lambda_d|\le 1$ を意味することによる.

Selberg (1946, §7) は, かく演繹し,

$$N(\alpha,T)\ll T^{1-\frac{1}{4}(\alpha-\frac{1}{2})}\log T \quad \big(\tfrac{1}{2}\le\alpha\le 1\text{ にて一様}\big) \tag{15.11}$$

を示し, (9.12) の改良:

$$\text{任意の }\phi(x)\uparrow\infty\text{ をもって, }\big|\sigma-\tfrac{1}{2}\big|\ll\frac{\phi(|t|)}{\log|t|}\quad(|t|\to\infty) \tag{15.12}$$

なる極めて狭い領域に $\zeta(s)$ の殆ど全ての非自明零点が集中していることを証明した.

実は, 論文 (1942) の前半にて, $\beta=\frac{1}{2}$ なる非自明零点が実際に「positive %」存在することをも Selberg は証明しているが, その後の発展を含め, ここでは割愛する. 何故ならば, そのような結果が素数分布に何らかの帰結をもたらすとは (目下のところ) 映らないからである. とは言え, この割合が 40% 以上であることは RH への強い支持に相違ない. Conrey (1986) を見よ.

[15.1] A. Selberg (1942): On the zeros of Riemann's zeta-function. Skr. Norske Vid. Akad. Oslo, No. 10, 1–59. (Collected papers I, pp.85–141)
[15.2] — (1946): Contributions to the theory of the Riemann zeta-function. Arkiv for Math. og Naturv. B, **48**, No.5, 89–155. (Collected papers I, pp.214–280)
[15.3] 評価 (15.11) へ向かう Selberg の議論は, 'twisted' 2 乗平均

$$\int_0^T\big|\zeta(\sigma+it)\big|^2(a/b)^{it}dt,\quad \langle a,b\rangle=1,$$

の詳細な計算を基とする. 上記の Atkinson の方法を応用可能. Y. Motohashi (1986): A note on the mean value of the zeta and L-functions. V. Proc. Japan Acad., **62A**, 399–401 を見よ.
[15.4] 「positive %」の証明にて, Selberg は $1/\sqrt{\zeta(s)}$ への有限 Dirichlet 級数近似を用いている. 要するに, 上記 (10.1) の類似思考である. 従って, 論文 (1942) もまた篩理論の範疇に含まれる訳である.
[15.5] B. Conrey (1986): More than two fifths of the zeros of the Riemann zeta-function are on the critical line. J. reine angew. Math., **399**, 1–26.

16. 結論 (15.12) は, 目覚ましい. しかし, 遥かに重要な事実は (15.10) である. Selberg ([0.5]) は,

$$\Big(\sum_{d\mid n,\,d\le z}\lambda_d\Big)^2\begin{cases}=1 & p\mid n\ \Rightarrow\ p>z,\\ \ge 0 & \text{その他}\end{cases} \tag{16.1}$$

に着目し,

$$\pi(N)\le\frac{N}{\log z}+z^2+\pi(z)\quad\text{すなわち}\quad \pi(N)\le\big(2+o(1)\big)\frac{N}{\log N}. \tag{16.2}$$

これは素数定理よりも劣る. しかし, ここに用いられた手段は「驚くほどに」初等的である. かくして, 「Selberg の Λ^2-篩」が登場. 強調すべきは, Bohr–Landau の「RH の統計的証明」から Λ^2-篩が生まれたことである. つまり, (14.13) の確認. なお, (14.10)–(14.11) を (16.1) と比較するが良い.

もっとも, 解析的整数論の現在から Λ^2-篩を観察するならば, その始まりは先ず Linnik ([0.4]) によりもたらされ, 続いて Selberg によりなされた, と多少の牽強はあるものの言い得る. 彼らの考察は, zeta- 及び L-函数の理論と結合し素数定理を深化させたのである. Linnik の着想は, 篩としての効力はもとより, 援用された手段そのものに絶大な意味を含んでいた. 一般に, 篩法の応用は与えられた数列が「多くの」算術級数中に如何に分布しているか, との考察を迫る. 一種の「有限」Fourier 解析の状況とも言える. この根本的な課題に対し Linnik の着想は, 現在に続く解析的整数論全般の発展を牽引する「枠組み」を与えるのである. 他方, Selberg の着想は zeta-函数の零点分布を考察する中で生まれたが故に, zeta 及び L-函数あるいは更に保型 L-函数の如く Euler 積表示を有する函数全体の精妙な解析的性質を議論するにあたり良く親和し, 「乗法的」課題全般に統一的な手段を与える. 関連する諸々を総合し

$$\begin{gathered}\text{「}L^2\text{-篩」あるいは「Large sive」と称する.}\\ \text{「大なる値の稀なること」の希望される算術的あるいは解析的な事象を,}\\ \text{なにがしかの } L^2\text{-不等式 (つまり, 統計) の中に埋蔵し観測する論法.}\end{gathered} \tag{16.3}$$

その素朴な姿は (9.8) や (16.1)–(16.2) に現れている.

やや唐突ながら, (16.3) の基礎となる L^2-不等式は次の通り: 単位区間内に点列 $\{\theta_j : 1 \le j \le J\}$ をとり, 隣り合うもの同士の距離が $\bmod 1$ にて $\delta > 0$ 以上であるとする (かく設定する理由は (16.9) にて明らかとなる). このとき, 任意の複素数列 $\{a_n\}$, $\{b_j\}$ について,

$$\begin{aligned}&\sum_{j=1}^{J}\Big|\sum_{M\le n<M+N} a_n e(n\theta_j)\Big|^2 \le (N+2\delta^{-1})\sum_{M\le n<M+N}|a_n|^2,\\ &\sum_{M\le n<M+N}\Big|\sum_{j=1}^{J} b_j e(n\theta_j)\Big|^2 \le (N+2\delta^{-1})\sum_{j=1}^{J}|b_j|^2,\end{aligned}\qquad e(x)=\exp(2\pi i x). \tag{16.4}$$

後者の証明は容易である. 適宜に 'taper' $w(n)$ を付加し, 平方を開き, 和 $\sum_n w(n)e(n(\theta_j-\theta_{j'}))$ を考察すれば済む. 一方, 前者については, 有界線形作用素のノルムにつき, 周知の

$$\text{双対 (duality) 等式:}\quad \|D\| = \|D^*\|,\quad D^*\text{: adjoint,} \tag{16.5}$$

を用いるが良い. これら上界は最良なものでは無いが, 以下の応用には充分. 言うなれば,

$$\text{函数系 } \big\{e(x\theta_j)\big\} \text{ は適宜に分散する数列 } \big\{\theta_j\big\} \text{ のもとに「概ね」直交系.} \tag{16.6}$$

篩問題 (14.4) に対し,

$$\mathcal{S}(\mathcal{A},z) \le \sum_{M\le n<M+N}\Big(\sum_{n\in\Omega(d)\, d<z}\lambda_d\Big)^2,\quad \mathcal{A}\subseteq[M,M+N). \tag{16.7}$$

ここで, 有限 Fourier 解析 (加法的指標の直交性) を用い, 集合 $\{n\in\mathbb{Z} : n\in\Omega(d)\}$ の特性函数を

$$\frac{1}{d}\sum_{a \bmod d}\sum_{h\in\Omega(d)} e\Big(\frac{a}{d}(n-h)\Big) = \frac{1}{d}\sum_{q\mid d}\sum_{\substack{a \bmod q\\ \langle a,q\rangle=1}}\Big(\sum_{h\in\Omega(d)} e\Big(-\frac{a}{q}h\Big)\Big)\cdot e\Big(\frac{a}{q}n\Big) \tag{16.8}$$

と表す. これを (16.7) に挿入し,

$$|\mathcal{S}(\mathcal{A},z)| \le \sum_{M\le n<M+N}\Big|\sum_{q<z}\sum_{\substack{a \bmod q\\ \langle a,q\rangle=1}} b_{a/q}e\Big(\frac{a}{q}n\Big)\Big|^2. \tag{16.9}$$

但し,

$$b_{a/q} = \sum_{\substack{d<z \\ d\equiv 0 \bmod q}} \frac{\lambda(d)}{d} \sum_{h\in\Omega(d)} e\Big(-\frac{a}{q}h\Big). \tag{16.10}$$

L^2-不等式 $(16.4)_{下辺}$ を (16.9) の右辺に適用し,

$$|\mathcal{S}(\mathcal{A},z)| \le (N+2z^2)\sum_{q<z}\sum_{\substack{a \bmod q \\ \langle a,q\rangle=1}} \Big|b_{a/q}\Big|^2. \tag{16.11}$$

何故ならば, 相異なる既約分数 a/q, a'/q' につき, $|a/q - a'/q'| \ge (qq')^{-1}$. この二重和は

$$\begin{aligned}
&\sum_{d_1,d_2<z} \frac{\lambda(d_1)\lambda(d_2)}{d_1d_2} \sum_{h_1\in\Omega(d_1)}\sum_{h_2\in\Omega(d_2)} \sum_{q\mid(d_1,d_2)} \sum_{\substack{a \bmod q \\ (a,q)=1}} e\Big(\frac{a}{q}(h_1-h_2)\Big) \\
&= \sum_{d_1,d_2<z} \frac{\lambda(d_1)\lambda(d_2)}{d_1d_2} \prod_{p_1,p_2\mid \frac{[d_1,d_2]}{\langle d_1,d_2\rangle}} |\Omega(p_1)||\Omega(p_2)| \prod_{p\mid\langle d_1,d_2\rangle} p|\Omega(p)| \\
&= \sum_{d<z} \frac{\mu(d)^2}{|\Omega(d)|}\prod_{p\mid d}(p-|\Omega(p)|)\cdot\xi_d^2.
\end{aligned} \tag{16.12}$$

変換 $\lambda \mapsto \xi$ は可逆

$$\xi_d = \sum_{g<z,\, d\mid g} \frac{|\Omega(g)|}{g}\lambda_g, \quad \lambda_d = \frac{d}{|\Omega(d)|}\sum_{g\mid f}\mu(f/g)\xi(g). \tag{16.13}$$

ここで注意であるが, $|\Omega(d)| \ne 0$ として一般性を失わない ((14.5) の直後を見よ). 境界条件 $\lambda_1 = 1$ を念頭におき,

$$(16.11) = \frac{1}{K(z,\Omega)} + \sum_{d<z}\frac{\mu(d)^2}{|\Omega(d)|}\prod_{p\mid d}(p-|\Omega(p)|)\cdot\Big(\xi(d) - \frac{1}{K(z,\Omega)}\mu(d)H(d,\Omega)\Big)^2. \tag{16.14}$$

ただし,

$$H(g,\Omega) = \prod_{p\mid g}\frac{|\Omega(p)|}{p-|\Omega(p)|}, \quad K(z,\Omega) = \sum_{g<z}\mu(g)^2H(g,\Omega). \tag{16.15}$$

従って,

$$\lambda_d = \frac{\mu(d)}{K(z,\Omega)}\prod_{p\mid d}\frac{p}{p-|\Omega(p)|}\cdot\sum_{\substack{g<z/d \\ (d,g)=1}}\mu(g)^2H(g,\Omega) \tag{16.16}$$

と定めるとき, Selberg の篩は

$$|\mathcal{S}(\mathcal{A},z)| \le \frac{N+2z^2}{\displaystyle\sum_{g<z}\mu^2(g)\prod_{p\mid g}\frac{|\Omega(p)|}{p-|\Omega(p)|}} \tag{16.17}$$

を与える.

これは「極めて」強力な結果である. 写像 Ω は, 全くに任意である. 例えば, $\Omega(p)$ を非 2 次剰余 $\bmod p$ 全ての集合としてみるがよい. あるいは, より象徴的に, $\mathcal{A}$ は算術級数 $\ell \bmod q$, $\langle q,\ell\rangle = 1$, かつ

$$p\nmid q \Rightarrow \Omega(p) = \{0 \bmod p\}, \quad p\mid q \Rightarrow \Omega(p) = \emptyset \tag{16.18}$$

と採るならば,

$$\text{Brun–Titchmarsh 定理:}\quad q<x \text{ につき一様に } \pi(x;q,\ell) \le \frac{2x}{\varphi(q)\log(x/q)} \tag{16.19}$$

に導かれる (但し, [16.3] を見よ). あるいは, $\Omega(p)=\{0,-2 \bmod p\}$ と採るならば,

$$\sum_{\substack{p\le x\\ p+2:\text{素数}}} 1 \le (1+o(1))\frac{16x}{(\log x)^2}\prod_{p\ge 3}\Big(1-\frac{1}{(p-1)^2}\Big). \tag{16.20}$$

とくに, Brun の (14.12) はこれより容易に従う. Linnik 及び Selberg の斯くも初等的な方法がこの様な結果をもたらすとは真に驚くべきである. しかも,

同様の評価を解析的手段のみをもって導くことは未だ知られず. (16.21)

[16.1] Large sieve 理論全般については, Bombieri (1974/1987): Le grand crible dan la théorie analytique des nombres. Second édition. Astérisque **18**, Paris 1987; および, Montogomery (1978): The analytic principle of the large sieve. Bull. Amer. Math. Soc., **84**, 547–567 を見よ. 合わせて, [A], [C] を参照することを勧める.
[16.2] 篩不等式 (16.17) そのものを large sieve と呼ぶことがある. これは, $|\Omega(p)|$ が「大」となる場合にも有効であることを意味している. 上記の論法は [A, Chap. I] に含まれている. [C, 第 7 章] も見よ.
[16.3] 不等式 (16.19) は, Montgomery–Vaughan (1973): The large sieve. Mathematika, **20**, 119–134 による. 係数を 2 より小とできるならば, 予想 (7.2) が解決される ([A, §4.3] を見よ). 従って, (16.18) の改良が切実に望まれるゆえんである. 後出の (20.11) を見よ.
[16.4] 不等式 (16.4) の証明は容易であるが, 最良にはあらず. 因子 $N+2\delta^{-1}$ は $N+\delta^{-1}-1$ へ改良可能 (かつ最良). Selberg による (Montgomery [16.1, p.559]). ただし, 下記 (20.11) に続くところを参照せよ.

17. ここで, (14.1) の観点に立ち返る. Selberg Λ^2-篩 (16.7) は (16.16) なる「最適選択」を誘導する. この最適性は何らかの直交構造の反映ではなかろうか. かく推測されるところを以下にて確かめる.

最適な λ_d をもって,

$$\sum_{n\in\Omega(d)}\lambda_d=\frac{1}{K(z,\Omega)}\sum_{r<z}\mu(r)^2H(r,\Omega)\Psi_r(n,\Omega),\quad \Psi_r(n,\Omega)=\prod_{\substack{p\mid r\\ n\in\Omega(p)}}\Big(\frac{-1}{H(p,\Omega)}\Big). \tag{17.1}$$

よって, (16.17) は

$$\sum_{M\le n<M+N}\Big(\sum_{r<z}\mu(r)^2H(r,\Omega)\Psi_r(n,\Omega)\Big)^2\le (N+2z^2)\sum_{r<z}\mu^2(r)H(r,\Omega) \tag{17.2}$$

とも現し得る. ここに, 作用素あるいは行列

$$\Big(\mu^2(r)H(r,\Omega)^{1/2}\,\Psi_r(n,\Omega)\Big),\quad M\le n<M+N,\ r<z, \tag{17.3}$$

の介在に気づく. 函数系 $\{\mu^2(r)H(r,\Omega)^{1/2}\,\Psi_r(n,\Omega)\}$ には一種の「直交性」が内在する, と (17.2) から見てとれよう ($\Psi_r(n,\Omega)$ は剰余系 $n \bmod r$ を変数として持つことに注意せよ). 即ち, 次の「算術的」L^2-不等式の成立が予想される. 任意の複素数列 $\{a_n\}$, $\{b_{v/u}(r)\}$ について,

$$\sum_{\substack{ru<Q\\ \langle r,u\rangle=1}}\mu^2(q)H(q,\Omega)\sum_{\substack{v=1\\ \langle u,v\rangle=1}}^{u}\Big|\sum_{M\le n<M+N}a_n\Psi_r(n,\Omega)e\Big(\frac{v}{u}n\Big)\Big|^2\le (N+2Q^2)\sum_{M\le n<M+N}|a_n|^2, \tag{17.4}$$

$$\sum_{M\le n<M+N}\Big|\sum_{\substack{ru<Q\\ \langle r,u\rangle=1}}\sum_{\substack{v=1\\ \langle u,v\rangle=1}}^{u}b_{v/u}(r)\mu^2(r)H(q,\Omega)^{1/2}\Psi_r(n,\Omega)e\Big(\frac{v}{u}n\Big)\Big|^2\le (N+2Q^2)\sum_{\substack{ru<Q\\ (r,u)=1}}\sum_{\substack{v=1\\ (v,u)=1}}^{u}|b_{v/u}(r)|^2. \tag{17.5}$$

実際, 等式 (Fourier 展開)

$$\Psi_r(n,\Omega)=\frac{\mu(r)}{|\Omega(r)|}\sum_{\substack{t=1\\ \langle t,r\rangle=1}}^{r}\Big(\sum_{h\in\Omega(r)}e\Big(-\frac{t}{r}h\Big)\Big)e\Big(\frac{t}{r}n\Big) \tag{17.6}$$

を用いるならば, (16.4) により証明は容易である.

[17.1] 本節については [A, §1.2], [C, §7.2] を見よ.
[17.2] 特に, $\Omega(p)=\{0 \bmod p\}$ の場合, $\Psi_r(n,\Omega)=\mu(\langle r,n\rangle)\varphi(\langle r,n\rangle)$ となるが, 函数系 $\big\{\mu(\langle r,n\rangle)\varphi(\langle r,n\rangle)\big\}$ の「概」直交性とも言うべき特性を見出したのは A. Selberg (1972): Remarks on sieves. Proc. 1972 Number Theory Conf., Boulder, pp. 205–216 (Collected papers I, pp.609–615) である. 但し, 彼は自身の Λ^2-篩とこの函数系との関連を指摘することは無かった. 指摘は Y. Motohashi (1977): On the Deuring–Heilbronn phenomenon. I. Proc. Japan Acad., **53**, 1–2 にて行われ, それ後に, 上記のごとき一般的議論が可能となったのである. [A, §1.2] も見よ.

18. 視点 (14.1) に再度立ち返り, 函数系 $\{H(r,\Omega)^{1/2}\,\Psi_r(n,\Omega)\}$ と $\{\chi \bmod q : \text{原始的}, q\le Q\}$ との間にある一種の '独立性' を指摘する: 任意の複素数列 $\{a_n\}$ について

$$\sum_{\substack{qr<Q\\ \langle q,r\rangle=1}}\mu^2(r)H(r,\Omega)\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\Big|\sum_{M\le n<M+N}a_n\Psi_r(n,\Omega)\chi(n)\Big|^2\le(N+2Q^2)\sum_{M\le n<M+N}|a_n|^2. \tag{18.1}$$

但し, $\sum^*$ は原始指標への和の制限を意味する. 証明は容易である: G_χ を原始指標 χ に付随する Gauss 和とし,

$$\sum_{M\le n<M+N}a_n\chi(n)=\frac{G_\chi}{q}\sum_{h \bmod q}\overline{\chi}(h)\sum_{M\le n<M+N}a_ne\Big(-\frac{h}{q}n\Big). \tag{18.2}$$

よって,

$$\begin{aligned}\sideset{}{^*}\sum_{\chi \bmod q}\Big|\sum_{M\le n<M+N}a_n\Psi_r(n)\chi(n)\Big|^2&\le\frac{1}{q}\sum_{\chi \bmod q}\Big|\sum_{h \bmod q}\overline{\chi}(h)\sum_{M\le n<M+N}a_n\Psi_r(n)e\Big(-\frac{h}{q}n\Big)\Big|^2\\&=\frac{\varphi(q)}{q}\sum_{\substack{h \bmod q\\ \langle h,q\rangle=1}}\Big|\sum_{M\le n<M+N}a_n\Psi_r(n)e\Big(-\frac{h}{q}n\Big)\Big|^2.\end{aligned} \tag{18.3}$$

これを (18.1) の左辺に挿入し, 残るは (17.4) の応用.

さらに, Mellin 変換 (付随する Parseval 直交) との独立性: 任意の $T\ge1$ につき

$$\sum_{\substack{qr<Q\\ \langle q,r\rangle=1}}\mu^2(r)H(r,\Omega)\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\int_{-T}^{T}\Big|\sum_{n=1}^{\infty}a_n\Psi_r(n,\Omega)\chi(n)n^{it}\Big|^2dt\ll\sum_{n=1}^{\infty}(n+Q^2T)|a_n|^2. \tag{18.4}$$

但し, 右辺は有界であると仮定する. もちろん, (10.10) と (18.1) の混成である.

[18.1] 本節については, [C, 第 7 章] を見よ.
[18.3] 任意の Ω をもって定式化 (18.4) を行うのは, やや過剰に一般と映り得る. しかし, 将来の応用の無きにしもあらず. ここでは, 篩法と在来の直交系 (2 種) との親和を示すことに専ら関心がある.

19. L^2-不等式 (18.4) は, 既にその最も単純な場合 $r=1$:

$$\sum_{q<Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}\int_{-T}^{T}\Big|\sum_{n=1}^{\infty}a_n\chi(n)n^{it}\Big|^2dt\ll\sum_{n=1}^{\infty}(n+Q^2T)|a_n|^2 \tag{19.1}$$

をもって華麗な帰結「Bombieri の平均素数定理」をもたらす: 任意の常数 $B \geq 1$ につき常数 $C = C(B)$ が存在し

$$\sum_{q \leq Q} \max_{\ell \bmod q} \left| \pi(x; q, \ell) - \frac{\mathrm{li}(x)}{\varphi(q)} \right| \ll \frac{x}{(\log x)^B}, \quad Q = \frac{x^{1/2}}{(\log x)^C}. \tag{19.2}$$

証明に当たっては, Siegel–Walfisz の素数定理 (6.16) を先ず応用し, $(\log x)^A \leq q$ なる場合に (6.2) を考察する. Hoheisel (第 9 節) にならい, 零点密度

$$\sum_{q \leq Q} \sideset{}{^*}\sum_{\chi \bmod q} N(\alpha, T, \chi) \tag{19.3}$$

の評価を行う. ただし, $N(\alpha, T, \chi)$ は $N(\alpha, T)$ の $L(s, \chi)$ に関する類似である. 例えば, Ingham の $(10.2)_{\text{下辺}}$ に向かう議論は (19.1) をもってごく容易に拡張可能であり,

$$(19.3) \ll (Q^2 T)^{3(1-\alpha)/(2-\alpha)} (\log QT)^c \tag{19.4}$$

を得る. 函数 $\prod_{q<Q} \prod^*_{\chi \bmod q} L(s, \chi)$ の非自明零点は「殆ど全て」臨界線 $\sigma = \frac{1}{2}$ の「ごく」狭い近傍に雲集しているのである. Bohr–Landau の発見 (9.1) の大幅な拡張:

$$\text{ERH は「統計的」には正しい.} \tag{19.5}$$

つまり, 至極不正確な表現ではあるが: 殆どの L-函数は Riemann 予想をほぼ充たす. よって算術級数に関する素数定理 (8.2) が殆どの法について成立する. それ故, (19.2) を得る. もちろん, 統計評価を厳格に行い, 実際に (19.2) を得る訳である.

あるいは, Vaughan (1980) の手法に多少の解釈を加え, 等式

$$-\frac{L'}{L}(s, \chi) = -\frac{L'}{L}(s)\big(1 - L(s, \chi) M_X(s, \chi)\big)^2 - 2L'(s, \chi) M_X(s, \chi) + L(s, \chi) L'(s, \chi) M_X(s, \chi)^2 \tag{19.6}$$

を用いる. ここに, $M_X(s, \chi) = \sum_{m \leq X} \mu(m) \chi(m) / m^s$. 両辺に $x^s/(2\pi i s)$ を乗じ Perron の反転公式 (5.9) を応用する. 積分路を左方向に適宜移動し (19.1) をもって議論の後, 迅速に (19.2) に達する. なお, $L(s, \chi) L'(s, \chi)$ の 2 乗平均を要するが, つまりは $L(s, \chi)$ の 4 乗平均であり, Ramachandra ([10.7]) の着想により容易に処理可能 (これは, (19.4) の証明にても同様).

注意であるが, Vinogradov, A.I. (1965) は Linnik (1961) の「分散法 Dispersion method」を用いて, Bombieri とは独立に

$$(19.1) \text{ ただし, } Q = x^{1/2-\varepsilon} \tag{19.5}$$

を得ている. 応用上は, (19.1) とほぼ同等である. Linnik による二つの着想がほぼ同時に平均素数定理をもたらしたという事実に刮目すべし.

平均素数定理 (19.1) は素数分布論における有史来の画期的な進展. その帰結は多々. 例えば, Goldbach 予想については Chen (1966/1973) による

$$2N = p + P_2. \tag{19.6}$$

ただし, $P_2 = p$ あるいは $p'p''$. この目覚ましい結果は, Rényi の視座 (7.6) のもたらしたところでもある. 実際, 平均素数定理への第 1 歩 ((19.2) にて $Q = x^\xi$, ξ はある絶対常数) を成したのは Rényi である. 双子素数予想への応用は, 本講演資料への別添を見よ.

なお, (19.1) と同様な統計的結論は乗法的函数の一群についても成立する. Motohashi (1976) を見よ. また, (19.2) の直前までの沿革は Barban (1966) に詳しい.

[19.1] E. Bombieri (1965): On the large sieve. Mathematika, **12**, 201–225.
[19.2] R.C. Vaughan (1980): An elementary method in prime number theory. Acta Arith., **37**, 111–115.
[19.3] A.I. Vinogradov (1965): The density hypothesis for Dirichlet L-series. Izv. Akad. Nauk SSSR Ser. Mat., **29**, 903–934; Corrigendum. *Ibid.*, **30** (1966), 719–720. (Russian)

[19.4] U.V. Linnik (1961): Dispersion Method in Binary Additive Problems. Leningrad Univ. Press, Leningrad. (Russian); 分散法の核心の解説は Y. Motohashi (1980): An asymptotic series for an additive divisor problem. Math. Z., **170**, 43–63 に含まれている.
[19.5] J.-R. Chen (1966): On the representation of a large even integer as a sum of a prime and a product of at most two primes, Kexue Tongbao, **17**, 385–386; a detailed version. Sci. Sinica, **16** (1973), 157–176. この「7 年間」の遅れの原因は「文化大革命」による破壊.
[19.6] Y. Motohashi (1976): An induction principle for the generalization of Bombieri's prime number theorem. Proc. Japan Acad., **52**, 273–275.
[19.7] M.B. Barban (1966): The large sieve method and its application to number theory. Uspehi Mat. Nauk, **21**, 51–102. (Russian)
[19.8] 本節については [C, 第 8 章] を参照せよ.

20. 平均素数定理 (19.2) は確かに刮目すべき結果である.

$$\text{しかし, その証明の何れも} \quad \begin{array}{l}\text{(1) 個々の } \pi(x;q,\ell) \text{ が正であるのか否か語らず;}\\ \text{(2) } Q = x^{\vartheta},\ \vartheta > \tfrac12, \text{ なる可能性につき語らず.}\end{array} \tag{20.1}$$

実は, 課題 (1) はやや部分的ながら「Linnik の最小素数定理」として, 既に (1944 年) 解決されているのである:

$$\text{絶対常数 } \mathcal{L} \text{ があり, } \pi\big(q^{\mathcal{L}};q,\ell\big) > 0. \tag{20.2}$$

Linnik の論旨は, 短区間素数定理に関する Hoheisel の議論を「比較的短い」算術級数に移し替える工夫. ただし, 法に関する一様性を保持するために特別の考察を要する. つまり, $L(s,\chi)$, $\chi \bmod q$ $(q \ge 3)$, は Vinogradov の非消滅域 (5.12) に類似する特性を (q につき一様なる条件下には) 欠き, なおかつ例外零点を持ち得る. 共に極めて重い障害 (obstacles). Linnik はこれらを克服するために, 次の 2 結果を証明し用いた:

$$\text{(無対数因子) 零点密度評価 :} \quad \begin{array}{c}\text{絶対常数 } \omega > 0 \text{ があり, } q, T \ge 2,\ \tfrac12 \le \alpha \le 1 \text{ につき一様に}\\ \displaystyle\sum_{\chi \bmod q} N(\alpha,T,\chi) \ll (qT)^{\omega(1-\alpha)};\end{array} \tag{20.3}$$

$$\text{Deuring–Heilbronn 現象 :} \quad \begin{array}{c}\text{任意の } \rho = \beta + i\gamma \ne \rho(q),\ \prod_{\chi \bmod q} L(\rho,\chi) = 0, \text{ につき}\\ \displaystyle\beta < 1 - \frac{\kappa}{\log q(|\gamma|+1)} \log\left(\frac{e\kappa}{(1-\rho(q))\log q(|\gamma|+1)}\right).\end{array} \tag{20.4}$$

ここに, ω は計算可能 effective であり, κ は (6.8)–(6.9) におけると同じ. Linnik が 'Deuring–Heilbronn 現象' なる名称を採用したことは, Gauss 類数問題への二者の貢献を念頭においてのもの. 'Linnik 現象' がより相応しい ([20.4] を見よ). 例外零点についての状況がいわば悪化するほどに (つまり, $\rho(q)$ が 1 に近い程に) $\prod_{\chi \bmod q} L(s,\chi)$ の他の零点は直線 $\mathrm{Re}\, s = 1$ の左方より深くに押しやられることとなる. 例えば, $\rho(q) > 1 - q^{-\xi}$, $\xi > 0$, であるならば, (20.4) は $\beta < 1 - \frac13\kappa\xi$ $(|\gamma| < q)$ となり, (準) ERH の成立に近い状況. 例外指標の「例外」たることを鮮明とする事実である.

Linnik (1944) の議論は入り組み読解は困難を極める. このために, Turán (1953) による「冪和法」Power sum method による比較的に簡易な証明が提出された ((20.3) については Turán 自身 (1961); (20.4) は Knapowski (1962)). しかし, 冪和法の応用は課題との乖離大 (語弊があろうが, 一種の暗箱の持ち込み). かくする内に, Selberg ([17.2]) により「篩法を直接に取り込み (20.3) を得る」手法が示唆された. 実は, Linnik, Turán の (20.3) の証明には Brun–Titchmarsh 定理が重要な役割を演じている ((16.19) より弱く $\pi(x;q,\ell) \ll x/(\varphi(q)\log x)$, $q \le x^{1/2}$, をもって充分; この $1/\log x$ が「無対数因子」をもたらす). その篩効果を, 関連する L^2-不等式の「内部」に取り込む訳である. 既に [17.2] にて暗示したが, この解釈の延長上にて (20.4) も同様に証明されるのである. 略解は以下の通り:

第 17 節の議論の主目的は函数系 $\{\Psi_r(n,\Omega)\}$ 出処を示すことであった. それは, 既に述べた通り, (16.7) の右辺の最適化の中にあり, 且つ, 銘記すべきはこの方法を適用できる数列の範囲は, 上記で専ら扱われた単純な点列よりも遥かに広い, という事実である. 例えば, 乗法的函数 $f(n) \ge 0$ をもって重みを付加し,

$$\sum_{M \le n < M+N} f(n) \left(\sum_{d \mid n} \lambda_d\right)^2 \tag{20.5}$$

なる 2 次形式を条件 $\lambda_1 = 1$ の下に考察することも可能である．最適な λ につき上記の $\Psi_r(n, \Omega)$ の類似を求め，対応する新たな算術的 L^2-不等式を得ることができる．しかし, そのためには多少の制限を f に課す必要がある:

$$\begin{aligned} &\text{函数 } f \text{ は非負, 乗法的, 且つ } f(n) \ll d_k(n), \\ &\text{全ての素数 } p \text{ につき } F_p = \sum_{l=0}^{\infty} f(p^l)p^{-l} \geq 1 + Cp^{-\alpha}, \\ &\sum_{n<N} \chi(n)f(n) = E_\chi \mathcal{F} F_q^{-1} N + O(Dq^\beta N^\gamma), \quad N \geq 1. \end{aligned} \tag{20.6}$$

但し, $d_k(n)$ は $\zeta^k(s)$ の展開係数; $C \geq 0$, $\alpha \geq 1$, $\mathcal{F} > 0$, $D \geq 0$, $0 \leq \beta, \gamma < 1$ は全て f により固定され, 指標 χ は法 q に属し, $F_q = \prod_{p|q} F_p$, 且つ E_χ は単位指標のとき 1 その他にて 0. この条件下に, (18.1) の類似が成立する: 任意の複素数列 $\{a_n\}$，$N \ll M$，につき,

$$\begin{aligned} &\sum_{\substack{q<Q;\, r<z \\ \langle q,r\rangle=1}} \mu^2(r)K(r)F_q \sideset{}{^*}\sum_{\chi \bmod q} \Big| \sum_{M \leq n < M+N} a_n \chi(n)\Phi_r(n)f(n) \Big|^2 \\ &\qquad \leq \big(\mathcal{F}N + O(Z_f(M; Q, z))\big) \sum_{M \leq n < M+N} |a_n|^2 f(n). \end{aligned} \tag{20.7}$$

但し,

$$\begin{aligned} \Phi_r(n) &= \frac{\mu(\langle n, r\rangle)}{K(\langle n, r\rangle)}, \quad K(r) = \prod_{p|r} \big(F_p - 1\big), \\ Z_f(M; Q, z) &= M^\gamma z^{1+\varepsilon}(\mathcal{F} + DQ^{2(1+\beta)+\varepsilon})(z^{\alpha-2\gamma} + z^{\alpha/2-\gamma}). \end{aligned} \tag{20.8}$$

また，任意の $T \geq 1$ につき,

$$\begin{aligned} &\sum_{\substack{q<Q;\, r<z \\ \langle q,r\rangle=1}} \mu^2(r)K(r)F_q \sideset{}{^*}\sum_{\chi \bmod q} \int_{-T}^{T} \Big| \sum_{n=1}^{\infty} a_n \chi(n)\Phi_r(n)f(n)n^{it} \Big|^2 dt \\ &\qquad \ll \sum_{n=1}^{\infty} \big(\mathcal{F}n + TZ_f(n; Q, z)\big) f(n)|a_n|^2. \end{aligned} \tag{20.9}$$

右辺は収束するものと仮定する.

現象 (20.4) の別証明は, (6.8)–(6.9) にて定義された例外指標 $\chi_1 \bmod q$, 例外零点 $\rho(q)$ をもって

$$f(n) = \sum_{d|n} \chi_1(d) d^{\rho(q)-1} \tag{20.10}$$

と (20.9) にて採ることにより成される. 他に補助的な議論を要するが, 当該の論文 (Motohashi (1978)) の根幹は以上の通り. なお, (20.9) は Q-例外 (6.18) への (20.4) の拡張も可能とする. もちろん, (20.3) も同様. [C, 第 9 章] を参照せよ.

一方, 課題 $(20.1)_{(2)}$ は別添にて議論されているところである. ここでは, その可能性を始めて示唆したと思われる発見を指摘するに留める: Motohashi ([20.8]) にて Brun–Titchmarsh 定理 (16.19) の改良

$$\pi(x; q, \ell) \leq (2 + o(1)) \frac{x}{\varphi(q) \log(x/\sqrt{q})}, \quad q \leq x^{6/17} \tag{20.11}$$

が得られているが, これは (16.17) から観るならば, 特殊な場合ではあるものの, 項 z^2 が $(z/q^{1/4})^2$ に引き下げられたことを意味する. つまり, (17.4) などにおける項 Q^2 は必ずしも (つまり, 数論上意味ある特殊な $\{a_n\}$ に対し) 最良なものではない. 実際, Motohashi ([20.9]) にはこの現象に関係する L^2-不等式が報告されている. さらに, Motohashi ([20.10]) には一般の Λ^2-篩の誤差項 ((16.17) の z^2 部分) を双一次形式をもって表現することも得られている. それにより, (20.11) の相当な改良も達成される. 恐らくは, L^2-不等式は何らかの「算術的 twists」の元に更に深きに達することであろう. 可

能性としては, 保型形式論との一層の混成である. それにより, 視界 (14.1) を意義深く深めることとなるに違いない. 示唆は, [13.6] に潜むと映る.

[20.1] U.V. Linnik (1944): On the least prime in an arithmetic progression. I. The basic theorem. Rec. Math. (Mat. Sbornik), **15**, 139–178; II. The Deuring–Heilbronn phenomenon. *Ibid.*, 347–368.
[20.2] P. Turán(1953): Eine Neue Method in der Analysis und deren Anwendungen. Akademiai Kiado, Budapest.
[20.3] —(1961): On a denisty theorem of Yu.V. Linnik. Magyár Tud. Akad. Mat. Kutató Intéz., (2) **6**, 165–179.
[20.4] S. Knapowski (1962): On Linnik's theorem concerning exceptional L-zeros. Publ. Math. Debrecen, **9**, 168–178.
[20.5] Y. Motohashi (1978): Primes in arithmetic progressions. Invent. math., **44**, 163–178.
[20.6] ちなみに, $\mathcal{L}$ の最新の評価は,

$$\mathcal{L} \leq 5, \quad q \geq q_0 \quad (q_0 \text{ は計算可能}).$$

ERH のもとに得られる (8.3) と比較するがよい. T. Xylouris (2011): Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression. Dissertation. Rheinischen Friedrich–Wilhelms–Universität Bonn.
[20.7] 現象 (20.4) は Dirichlet L-函数の集団に特異なものではなく，Euler 積表示を有する函数全てについて原理的には成立すべきもの, と映る．Y. Motohashi (2013): An extension of the Linnik phenomenon. Proc. Steklov Inst. Math., **280**, Supplement 2, 56–64. この観点の保型 L-函数への応用は Motohashi ([5.8]) にて行われている.
[20.8] Y. Motohashi (1974): On some improvements of the Brun–Titchmarsh theorem. J. Math. Soc. Japan, **26**, 306–323.
[20.9] — (1977): A note on the large sieve. Proc. Japan Acad., **53**, 17–19.
[20.10] — (1999): On the error term in the Selberg sieve. In: Number Theory in Progress, 2, Proc. Zakopane Conf., 1997, Walter de Gruyter, Berlin, pp.1053–1064.

THE TWIN PRIME CONJECTURE

By Yoichi Motohashi

The conjecture
'*there should be infinitely many pairs of primes* $\{p, p+2\}$'
has not been conquered yet.

However, a spectacular drama is now unfolding itself in the theory of the distribution of primes. The complete resolution of the conjecture is thus within the range of modern mathematics — *perhaps*. Luckily enough, I have been witnessing the series of recent great events as a contemporary specialist. The purpose of the present expository talk is to share my excitement with my audience. Any mathematical discovery is an eventual outcome of the rich and long history of our cherished discipline, and the recent amazing discovery by Y. Zhang is a typical instance. I shall describe the essence of the fundamental ideas initiated by GPY (D.A. Goldston, J. Pintz and C.Y. Yildirim) and others which had prepared the way for the discovery, while briefly reviewing the relevant history. You will find all basic ideas are so simple that you will certainly be persuaded that the proverb "*small things stir up great*" is indeed a truth.

Looking back almost half a century ago, I (then in my 20's) was eager to learn Yu.V. Linnik's and A. Selberg's works in analytic number theory, dreaming the way to the Never-Never Land of prime numbers. They taught me a lot, and I owe them tremendously. I am really happy that their mathematical spirit is still vividly felt in recent developments. Indeed, so many wonders in analytic number theory can be traced back to their ideas. By trekking further and steadily along the way they prepared, you will (I believe) be able to bring us more wonders on primes.

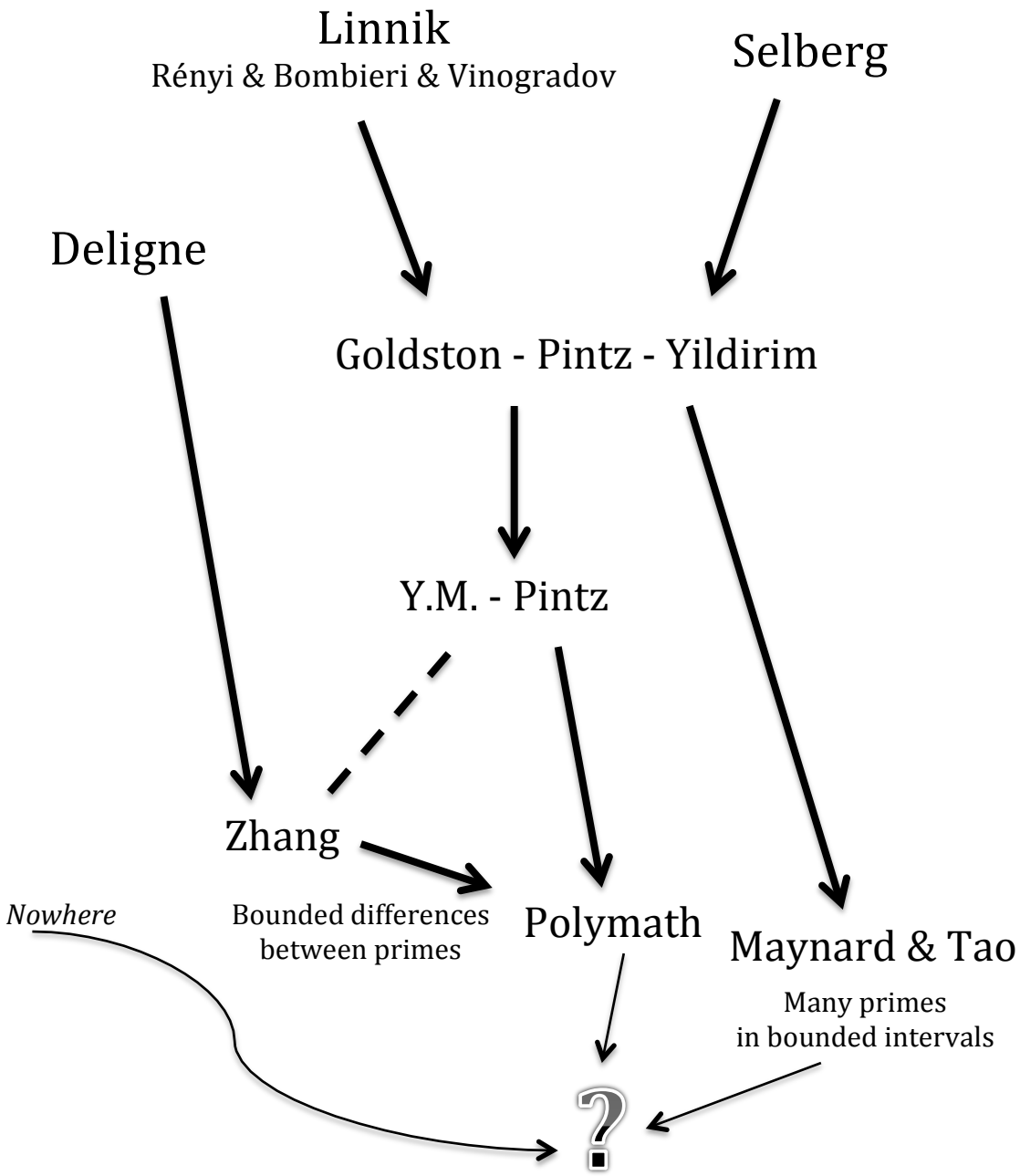
I shall have to be brief in some sections, in order to acquire time for more recent work done by T. Tao (2013) and J. Maynard (2013) independently, which has made Sections 10 and 11 somewhat less relevant to our main issue of finding infinitely often bounded differences between primes. Nevertheless, you will be better off knowing all the facts that I have put in this text, which I hope will encourage you to delve into the professional literature on primes.

Remark 1: The present text is a substantially improved and augmented version of the one in Japanese that I had prepared for my talk which I delivered at the annual meeting of the Mathematical Society of Japan (15 March 2014)†. The expressions that I shall use, whilst being adequate for my present (didactic) purpose, are not always perfectly precise/correct. All facts and details on sieve method and distribution of primes which are needed to understand recent developments are available in my books [10][12].

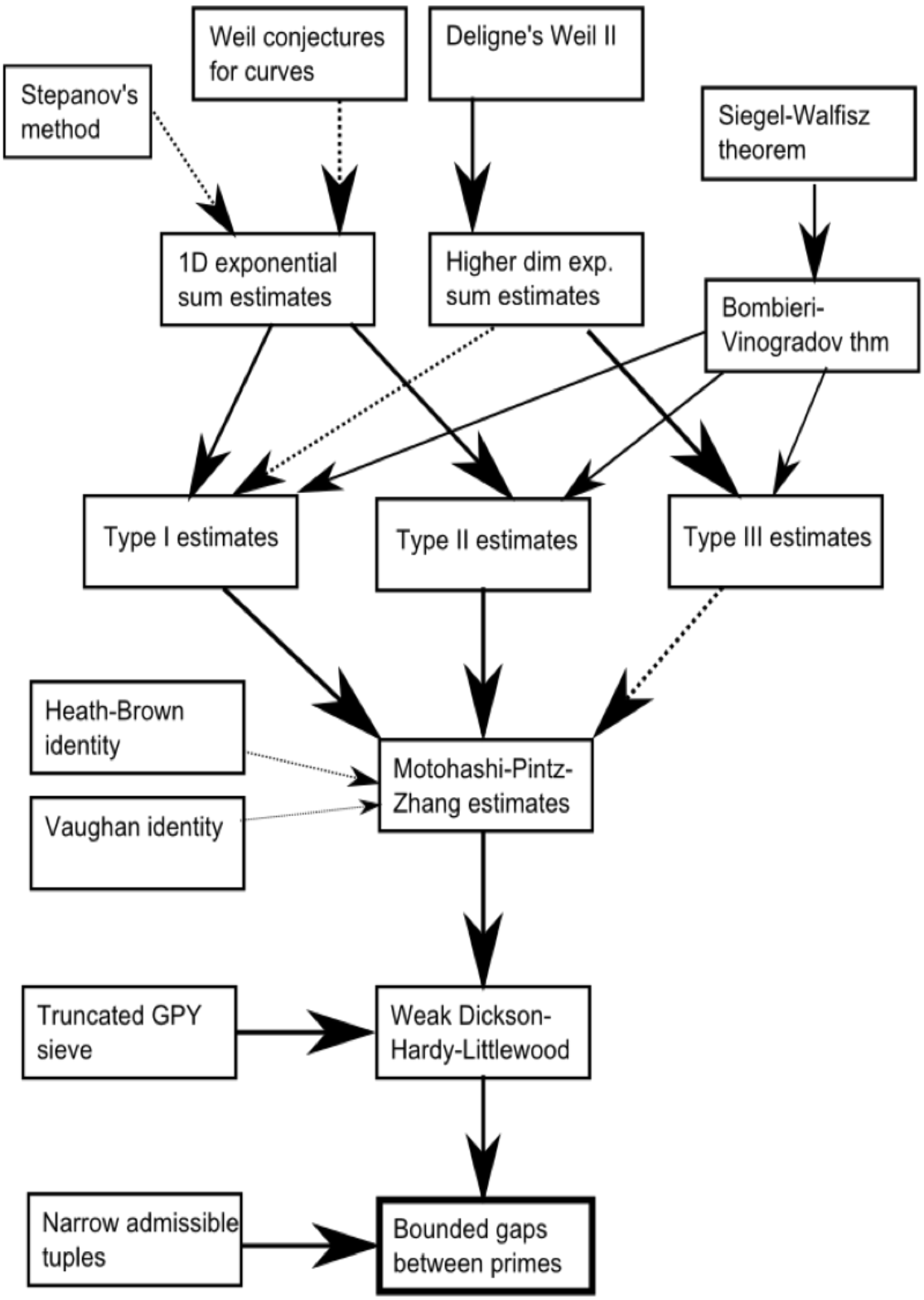
Remark 2: It is highly recommended to visit T. Tao's excellent blog:
http://terrytao.wordpress.com/2013/06/03/ the-prime-tuples-conjecture
-sieve-theory-and-the-work- of-goldston-pintz-yildirim-motohashi-pintz-and-zhang/
which has various links to more recent developments.

Acknowledgments. I am deeply grateful to A. Ivić, M. Jutila, J. Maynard, A. Perelli, T. Tao, N. Watt and H.M. for their kind comments on the draft of the present text; to D.A. Goldston, J. Pintz and C.Y. Yildirim for having been sharing their epoch-making manuscripts; and to D.H.J. Polymath for kindly putting their diagram on [15, p.10] at my disposal.

† While preparing my talk at the 18th Oka Sympositum (November 30, 2019), I did not alter any part of the original text save for the addition of the item [22] to the references. This insertion should make it clear that the highly crucial idea '*smoothing*' GPY sieve, mentioned in Section 10 below, occurred for the first time in [22, the formula (20)]; the main part of [22] was written in the middle of 2005. It should be mentioned also that a proof of the function field analogue of the Twin Prime and the Goldbach conjectures has been asserted by W. Sawin and M. Shusterman: arXiv:1808.04001v2, 7 Sep. 2019.



This is the structure of the present exposition. `&' menas that the relevant works were done independently. As to the work by Polymath see the diagram on the next page.



This is the logical structure of D.H.J. Polymath [15] , a clear and comprehensible account of those ideas flowing into Zhang's discovery and its improvements.

1. The conjecture.
Let

$$\varpi(n) = \begin{cases} 1 & n \text{ is a prime,} \\ 0 & n \text{ is not a prime,} \end{cases}$$

and put

$$\pi(x) = \sum_{n<x} \varpi(n), \qquad \pi_2(x) = \sum_{n<x} \varpi(n)\varpi(n+2).$$

Anyone who loves mathematics knows

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

Anyone who ardently loves analytic number theory is bitterly defied by the conjecture

$$\pi_2(x) \sim C_0 \frac{x}{(\log x)^2}, \quad C_0\text{: an absolute constant,} \tag{1.1}$$

and even by the far more modest statement

$$\textit{The twin prime conjecture}\text{:} \quad \lim_{x\to\infty} \pi_2(x) = \infty. \tag{1.2}$$

2. To detect twins.
There are two naive means to detect twin primes:

$$(A) \quad \varpi(n)\varpi(n+2) > 0,$$
$$(B) \quad \varpi(n) + \varpi(n+2) - 1 > 0.$$

These are of course equivalent to each other as far as one applies them to *individual* n's, but they are *statistically* different: always $\varpi(n)\varpi(n+2) \geq 0$ but almost always $\varpi(n) + \varpi(n+2) - 1 = -1$. It appears that opinions of sieve specialists are now converging upon

(A) is too strict,

(B) is more flexible.

But why? It is hard to explain the real situation to people who are not familiar with sieve method. Thus, let me put it bluntly: (A) is too exact as it gives the definition of $\pi_2(x)$. A sage (M.J.) in analytic number theory said that exact formulas contain often too much noise. There were a lot of attempts, probably since A.M. Legendre's time (the late 18th century), to clinch to (1.2) by means of (A); but all eventuated in failure. In fact, GY (Goldston and Yildirim) commenced their investigations in 1999 still brandishing the sharp sword (A). Only in 2004/5, after a few futile (but highly interesting) attempts with (A), did they turn instead to (B). This was a great turning point in their work. Note that GY actually considered *primes in tuples*: see Section 7. Here I employ an *over*-simplification in order to make the issue clearer. As far as I know, A. Selberg (1950) was the first who exploited (B), but in a configuration different to GY's.

3. Sieving out noise.
Imitating the definition of $\pi_2(x)$, one might consider

$$\sum_{n<x} \big(\varpi(n) + \varpi(n+2) - 1\big). \tag{3.1}$$

If the sum is positive and large, then the conjecture (1.2) will be resolved. But this argument is awfully absurd, since obviously (3.1) is essentially equal to $2\pi(x) - x$, and one can utter only the nonsense

$$(3.1) \sim \ -x\,. \tag{3.2}$$

Nevertheless! Things should look pretty different if (3.1) is replaced by

$$\sum_{n<x} \big(\varpi(n)+\varpi(n+2)-1\big)W(n). \tag{3.3}$$

Here $W(n)$'s are *non-negative* weights. If one succeeds finding a nice sequence $\{W(n)\}$ such that (3.3) tends to positive infinity, then the conjecture (1.2) will be resolved. This must be, however, an extremely difficult task, since such $\{W(n)\}$ should yield a considerable dumping of the terms '1' and simultaneously should not affect much the situation of n being a twin prime. That is, $\{W(n)\}$ is preferably to satisfy

$$W(n) \text{ is } \begin{cases} \geq 0 & \text{but very small on average,} \\ 1 & \text{when } n \text{ is a large twin prime.} \end{cases}$$

4. Lovely lambda's.

In his work mentioned above, Selberg employed the Λ^2-sieve, his great invention (1947). If translated into our present situation, it becomes:

$$\text{Consider the quadratic form } \sum_{n<x}\Big(\sum_{d\mid n(n+2)}\lambda(d)\Big)^2,$$
$$\text{under the side-condition } \lambda(1)=1 \text{ and } \lambda(d)=0 \text{ for } d\geq D,$$

where D is a parameter to be fixed optimally eventually, but initially satisfying only $D<x^{1/2-\varepsilon}$ with an arbitrary small $\varepsilon>0$. Expanding the squares out and exchanging the order of summation, we get the main term and the error term. Selberg diagonalised the main term in a highly original way (in fact an application of Möbius inversion) and found an explicit expression for optimal λ's that minimises the main term. It is expedient to know that these optimal λ's satisfy

$$\lambda(d)\sim\mu(d)\left(\frac{\log D/d}{\log D}\right)^2, \tag{4.1}$$

with μ being the Möbius function, and to note that

$$\nu(n)>2 \quad\Longrightarrow\quad \sum_{d\mid n}\mu(d)(\log d)^j=0,\ j\leq 2. \tag{4.2}$$

where $\nu(n)$ is the number of prime factors of n which are different to each other. Namely, the choice (4.1) is an *approximation* to (4.2), which explains the fact that Selberg's λ's yield necessary dumping.

We construct, with these *quasi-optimal* λ's,

$$W(n)=\left(\sum_{d\mid n(n+2)}\lambda(d)\right)^2 \tag{4.3}$$

to be used in (3.3). We have, with an appropriate D,

$$\sum_{n<x}W(n)\sim C_1\frac{x}{(\log x)^2}, \tag{4.4}$$

and

$$\sum_{n<x}\big(\varpi(n)+\varpi(n+2)\big)W(n)\sim C_2\frac{x}{(\log x)^2} \tag{4.5}$$

with certain constants C_1, $C_2>0$. Amazing! Compare these with the conjecture (1.1).

It should be noted that Selberg (ca. 1950) examined also the use of the weights

$$\left(\sum_{\substack{d_1\mid n,\ d_2\mid(n+2)\\ d_1d_2<D}}\lambda(d_1,d_2)\right)^2, \tag{4.6}$$

but in a configuration different to (4.4)–(4.5) that I briefly mentioned already in Section 2.

5. RH vs. statistics.
The assertion (4.5) is, in fact, a consequence of

The mean prime number theorem

For each $A > 0$ there exists a $\vartheta > 0$ (the *level*) such that

$$\sum_{q\le x^{\vartheta}} \max_{(a,q)=1} \left|\pi(x;a,q) - \frac{\mathrm{li}(x)}{\varphi(q)}\right| \ll x(\log x)^{-A}, \tag{5.1}$$

$$\pi(x;a,q) = \sum_{\substack{n<x\\ n\equiv a \bmod q}} \varpi(n),$$

where li is the logarithmic integral, φ the Euler totient function, and '$\ll$' means that the left side is less than a constant multiple of the right side. The reason why we need this is simple: With (4.3),

$$\sum_{n<x} \varpi(n)W(n) = \sum_{d_1,d_2<D} \lambda(d_1)\lambda(d_2) \sum_{\substack{a \bmod [d_1,d_2]\\ a(a+2)\equiv 0 \bmod [d_1,d_2]}} \pi(x;a,[d_1,d_2]),$$

where $[d_1,d_2]$ is the least common multiple of d_1, d_2. The replacement of each $\pi(x;a,[d_1,d_2])$ by $\mathrm{li}(x)/\varphi([d_1,d_2])$, providing $(a,d_1d_2)=1$, causes an error which can be estimated with (5.1) if $D < x^{\vartheta/2-\varepsilon}$.

The first result that gave an absolute constant $\vartheta > 0$ in (5.1) is due to A. Rényi (1948). He exploited the "large sieve" of Yu.V. Linnik (1941). This *statistical equi-distribution* property of primes among arithmetic progressions to relatively large moduli must remind you of the extended Riemann hypothesis ERH. Rényi's prime number theorem states that in some important applications the extended *quasi*-Riemann hypothesis could be avoided! Because of this, a lot of notable people poured their strenuous efforts into improving upon Rényi's prime number theorem, and E. Bombieri (1965) established that

$$\text{(5.1) holds for any } \vartheta < \tfrac{1}{2}, \tag{5.2}$$

which, *in practice*, is essentially at the same depth as ERH (actually he proved (5.1) with $x^{1/2}(\log x)^{-B(A)}$ in place of x^{ϑ}). I should stress that A.I. Vinogradov (1965) proved (5.2) independently; he exploited another fundamental innovation due to Linnik: the "dispersion method" (1958).

By the way, in January 1970 I left for Budapest aspiring to learn analytic number theory under Rényi and P. Turán, but Rényi passed away a day after my arrival (1 February).

6. Powerful modesty.
However, with the best effort one could achieve only $C_2 < C_1$ in (4.4)–(4.5). That is, the asymptotic value $(C_2 - C_1)x/(\log x)^2$ thus attained for (3.3) is negative and large, and so is of no more use to us than the nonsense (3.2). In fact, in order to truly appreciate (4.4)–(4.5) you ought to be well versed in the theory of the distribution of primes in arithmetic progressions as well as in sieve method. Here, be simply amazed that despite its inability to yield anything about the conjecture (1.2) the assertion comes close to the dreamy asymptotic formula (1.1) at least outwardly, and moreover, there we have $W(n) = 1$ whenever n is a large twin prime. That is, twin primes are probably counted in (4.5) but only in an ineffective way; they must be buried in rubbish. Then, how to make (3.3) more effective and salvage primes proximate to each other?

That is very difficult. The accumulation of past futile attempts suggests that we ought not to be so daring as to confront (1.2) directly. The strategy GY (2004/5) chose was this: We should be modest. Let us give up trying to directly touch the 'twin'. Let us consider instead

$$\sum_{n<x} \Big(\sum_{j=1}^{k} \varpi(n+h_j) - 1\Big) W(n), \tag{6.1}$$

with a new $\{W(n)\}$. Here $h_1 < h_2 < \cdots < h_k$ are even integers. They should not be trivial like $\{2,4,6\}$ because one of $n+2, n+4, n+6$ is always divisible by 3. A natural condition on the tuple $\{h_1, h_2, \dots, h_k\}$ is that

$$\text{the number of different } h_j \bmod p \text{ be less than } p \text{ for any prime } p, \tag{6.2}$$

which avoids the redundancy that a member among $\{n+h_j : j = 1, \dots, k\}$ is always divisible by a fixed prime. Obviously,

$$\sum_{j=1}^{k} \varpi(n+h_j) - 1 > 0$$
$$\Longrightarrow \{n+h_1, n+h_2, \dots, n+h_k\} \text{ contains at least two primes.}$$

If this holds with infinitely many n, then

$$\liminf_{t\to\infty} (p_{t+1} - p_t) \le h_k - h_1,$$

with p_t the t-th prime. Bounded differences between primes should occur infinitely often. The establishment of this will be a tremendous achievement, even though it is perhaps less impressive than the ultimate assertion (1.2).

7. Gem box principle.

We have to choose the weights $\{W(n)\}$ in (6.1). Here a truly decisive observation was made by GPY (2005): Let $P(n) = (n+h_1)(n+h_2)\cdots(n+h_k)$. Then,

$$\nu(P(n)) = k+\ell \text{ with } 0 \le \ell < k \quad \Longrightarrow \quad \begin{array}{c}\text{there are at least } k-\ell \text{ primes} \\ \text{among } n+h_1, \dots, n+h_k\,.\end{array} \tag{7.1}$$

This is an application of Dirichlet's pigeon box principle; but I very much prefer *gems* to pigeons. Here n's are actually to be restricted so that (7.1) is valid, which can be realised in a simple way that does not cause any loss of generality.

8. Magical tapering.

The new parameter $\ell \ge 0$ is to be incorporated. In practice, however, it is hard to utilise (7.1) without making any compromise; that would be a return to the stiffness we wished to depart from. I am not very sure if this is what really occurred to them, but GPY seem to have turned to Selberg's argument which I indicated in the first paragraph of Section 4. The relevant approach is to consider

$$\sum_{n<x} \Big(\sum_{d|P(n)} \lambda(d) \Big)^2, \quad \begin{cases} \lambda(1) = 1, \\ \lambda(d) = 0, \quad d > D. \end{cases}$$

The optimal λ satisfies

$$\lambda(d) \sim \mu(d) \left(\frac{\log D/d}{\log D} \right)^k.$$

Then, GPY practised real magic by introducing

$$\text{the further tapering factor } \left(\frac{\log D/d}{\log D} \right)^\ell,$$

and they constructed the weight

$$W(n) = \left(\sum_{d|P(n),\, d<D} \mu(d) \left(\frac{\log D/d}{\log D} \right)^{k+\ell} \right)^2. \tag{8.1}$$

As a matter of fact, this is an approximation to the filtering concerning (7.1), since

$$\nu(P(n)) > k+\ell \quad \Longrightarrow \quad \sum_{d|P(n)} \mu(d) (\log d)^j = 0, \ j \le k+\ell.$$

9. Divine multiplier.
With $W(n)$ as in (8.1), GPY computed asymptotically the sums

$$\begin{aligned} T^{(1)}(x;k,\ell;D) &= \sum_{n<x} W(n), \\ T^{(2)}(x;k,\ell;D) &= \sum_{n<x} \Big(\sum_{j=1}^{k} \varpi(n+h_j) \Big) W(n). \end{aligned} \tag{9.1}$$

They discovered that, with $D = x^{\vartheta/2}$ (ϑ as in (5.1)) and a positive $\Delta(x) \approx x(\log x)^{-k}$, one has:

$$\Big(T_P^{(2)} - T_P^{(1)}\Big)(x;k,\ell;D) \sim \Big(\vartheta \cdot \frac{k}{k+2\ell+1} \cdot \frac{2\ell+1}{\ell+1} - 1\Big)\Delta(x). \tag{9.2}$$

This multiplier of $\Delta(x)$ is probably *one of the greatest surprises* in the entire history of number theory. Setting $\ell = [\sqrt{k}]$ for instance, we find readily that

$$\begin{gathered} \text{if } \vartheta > \tfrac{1}{2} \text{ and } k \text{ large, then } \{n+h_1, n+h_2, \dots, n+h_k\} \\ \text{contains at least two primes. } \Longrightarrow \text{Bounded differences between primes!} \end{gathered} \tag{9.3}$$

If you had not the extra parameter ℓ; that is, if you put $\ell = 0$, then (9.2) would be nothing. Without $\vartheta > 1$, which is truly beyond any science fiction, nothing would come out from (9.2) with $\ell = 0$. In fact it is known that (5.1) does not hold for any $\vartheta > 1$.

10. Divide and conquer.
The assertion (9.3) is indeed wonderful, if only one can leap beyond the barrier $\vartheta = \frac{1}{2}$ in (5.1).

Let me be a little bit personal: I may count myself as one of the earliest people who tried seriously to make this leap, of course without any surmise of recent developments. I was aware at least that not the large sieve but the dispersion method of Linnik is the key. But I could publish only a short report (1976) which relied still on the large sieve; my work relevant to the dispersion method was utterly incomplete, which was inevitable because of my meagre experience with the theory of exponential sums à la A. Weil. Later BFI (Bombieri, J. B. Friedlander and H. Iwaniec (1986)) made a remarkable progress in this direction. Their main result is valid with any ϑ less than $\frac{4}{7}$, but under a restriction on the moduli of the arithmetic progressions which makes it inadequate for the computation of the second sum in (9.1).

Thus a genuinely new insight was needed into the problem (6.1) and the barrier problem. In this situation an idea occurred to MP (2005) (see [11][14] as well); actually we each independently had essentially the same idea, which involved the use of some corner-cutting in order to break the stalemate. On my side: soon after getting the first version of GPY (from G in early April 2005) I realised that a *smoothing* could be applied to the summation variable d in (8.1). That is, we need not sum over all $d < D$ but it suffices to restrict ourselves to those d which have relatively *small* prime divisors only; I mean that even after applying such a corner-cutting the multiplier of $\Delta(x)$ in (9.2) does not change essentially, although $\Delta(x)$ itself ought to be altered accordingly.

Actually, MP (2005/6) modified the argument of GGPY (GPY and S. Graham (2005)) in order to incorporate this smoothing. Let me nevertheless employ an asymptotic expression for the sake of temporary convenience. Then, what MP did is the same as to replace (8.1) by

$$W(n) = \left(\sum_{d \mid P(n),\, d<D}^{(\omega)} \mu(d) \left(\frac{\log D/d}{\log D} \right)^{k+\ell} \right)^2, \tag{10.1}$$

where $\sum^{(\omega)}$ indicates that all prime divisors of d are less than D^ω. Then the multiplier in (9.2), of course under the new setting, is found to be larger than

$$\vartheta_{\mathrm{MP}} \cdot \frac{k}{k+2\ell+1} \cdot \frac{2\ell+1}{\ell+1} - 1 - \exp(-3k\omega/8), \tag{10.2}$$

provided that one has, for any given $A > 0$,

$$\sum_{q \le x^{\vartheta_{\rm MP}}}^{(\omega)} \sum_{\substack{(a,q)=1 \\ P(a) \equiv 0 \bmod q}} \left| \pi(x;a,q) - \frac{\mathrm{li}(x)}{\varphi(q)} \right| \ll x(\log x)^{-A}, \tag{10.3}$$

where $\sum^{(\omega)}$ means that all prime factors of q are less than x^{ω}. Here I am not very precise, since MP tacitly assumed for the sake of convenience that $\ell \approx \sqrt{k}$, $\omega \approx 1/\sqrt{k}$ with k large; however, these assumptions are not of critical importance for the application in question, that is, to detect infinitely often bounded differences between primes. I remark also that the hypothetical mean prime number theorem which is required by MP is a consequence of (10.3); that is, MP assumed in fact somewhat less. Anyway we have:

$$\begin{array}{c} \vartheta_{\rm MP} > \frac{1}{2} \text{ in (10.3)} \\ \Longrightarrow \quad \text{bounded differences between primes occur infinitely often.} \end{array} \tag{10.4}$$

Why is this important? Because, with (10.3), instead of (5.1), the feasibility of a proof by the dispersion method of Linnik becomes much higher. More precisely, the smoothing yields a *quasi*-infinitely factorable structure in the moduli set $\{q\}$; namely, we now have instead

$$\{q_1 q_2 : q_1 \le Q_1, q_2 \le Q_2\},$$

essentially for any multiplicative decomposition $Q_1 Q_2 \le x^{\vartheta_{\rm MP}}$. In practice, we put the summation over q_1, say, outside and consider the *dispersion* of the inner sum over q_2, via the Cauchy inequality. We will be able to detect more cancellation than with the ordinary setting (5.1). Further, we may appeal to R.C. Vaughan's reduction argument (1980), or the like, in dealing with the sums over primes. This strategy is nothing other than "divide et impera".

11. From nowhere.

As to the proof of (10.3) for a $\vartheta_{\rm MP} > \frac{1}{2}$, I was somehow inclined to be optimistic; and I thought I would have 'time'. Thus, in the mean time, I was playing with automorphic L-functions, enjoying some success, but for too long perhaps. Then, in early April last year I felt a jolt. The epicentre was an unknown mathematician named Y. Zhang; I mean that the man had not been known among specialists. Soon I got a copy of his paper (probably a draft). I felt as if I had seen it some 7 years ago, for its overall strategy was the same as that of MP(2005/6).

Of course I was truly impressed by the extremely important fact that Zhang cleared away the level barrier in the context of (10.3). The man who came from nowhere struck the target indeed. Therefore, mankind has now

$$\liminf_{t \to \infty} (p_{t+1} - p_t) < \infty. \tag{11.1}$$

To achieve (10.3), for some $\vartheta_{\rm MP} > \frac{1}{2}$, Zhang appealed to P. Deligne's famous work (1980) on the Weil conjecture; in this respect, he followed, to a large extent, the work by BFI mentioned above. Thus I am unable to confirm his reasoning on my own but have to rely on the affirmative opinion of experts. I have no courage to exploit any result which I do not fully understand; neither have I any other way than to trust, with considerable caution, competent authors whose claims depend on works which are far beyond my expertise. Nevertheless, here I may try to explain why such heavy machinery comes into play in dealing with (10.3). In essence, it is because of the factoring of various terms and summation intervals, which is described in the previous section. I mean that the strategy there reduces the problem into pieces, all of which are more or less equivalent to counting integers in various arithmetic progressions. To manage this entangled task, presently we have essentially only one means: the Poisson summation formula. Main terms are not troublesome, though often complicated. Real trouble comes naturally from the tail parts, which are expressed in terms of finite or infinite exponential sums. Arguments of the exponentiated terms involve rational numbers with varying numerators and denominators; then Deligne's work becomes relevant, as it gives strong and *uniform* bounds for such sums.

12. Phase transition.

Another sensation came more recently from a postdoc: J. Maynard (November 2013), claiming

$$\liminf_{t\to\infty}(p_{t+1}-p_t)\le 600. \tag{12.1}$$

What is really sensational is in his statement that his argument *does not incorporate any of the technology used by Zhang; the proof is essentially elementary, relying only on the Bombieri–Vinogradov theorem*, i.e., (5.2). This is a true phase transition, and a great gift to all who feel uneasiness when they have to chew works that depend on the highly demanding work of Deligne and A. Weil (1949), even though the efforts of S.A. Stepanov (since 1969) have yielded accessible elementary proofs of some of the consequences of their work.

And more. According to Maynard, Tao (October 2013) got essentially the same idea; and they independently established, only on Rényi's (5.1),

$$\begin{gathered}\text{For each } m\ge 2 \text{ there exists a } k \text{ such that}\\ \text{with any } \{h_j\} \text{ satisfying (6.2)}\\ \text{the tuple } \{n+h_1, n+h_2,\dots,n+h_k\}\\ \text{contains at least } m \text{ primes for infinitely many } n.\end{gathered} \tag{12.2}$$

They even got an estimate for k in terms of m. Fantastic!

Their argument is, to some extent, a realisation as well as an extension of Selberg's approach (4.6). Hence, in a sense, (12.1) would have been possible to attain in 1965 when (5.2) was established; and (12.2) in 1950! By this I mean that for more than half a century, indeed until a few months ago, no sieve experts had ever tried to seriously look into the ending remark (on p.245) in Selberg's 'Lectures on sieves'. I should of course add that the phase transition brought about by Maynard and Tao was an outcome of the sieve movement commenced by Goldston and Yildirim in 1999, without which I suspect that not only Maynard–Tao's discovery but also the recent wonders concerning bounded differences between primes would have remained under sand, and perhaps would have lain undiscovered for decades to come. Better ideas always survive; what I described in the last two sections may appear obsolete, at least for now.

The key points of Maynard's argument are as follows: Basically we are dealing with the quadratic form

$$\sum_{n<x}\left(\sum_{d_j\mid(n+h_j),\ \forall j\le k}\lambda(d_1,d_2,\dots,d_k)\right)^2,\quad d_1d_2\cdots d_k\le D. \tag{12.3}$$

We need to be cautious in dealing with the prime factors of d_j; but let us ignore this presently: a correct procedure is indicated in Appendix below. Then, in a fashion familiar to those who are experienced in dealing with sums of arithmetical functions in sieve method, an application of Selberg's change of variables (in fact, an instance of the Möbius inversion) allows one to express λ's in terms of any given $F(\xi_1,\xi_2,\dots,\xi_k)$ as far as F is supported on $\{\xi_1+\xi_2+\cdots+\xi_k\le 1\,:\,\xi_j\ge 0,\forall j\le k\}$. This is in fact an extension of the argument due to GGPY (2005); their choice corresponds to the specialisation $F\big(\underline{\xi}\big)=f(\xi_1+\xi_2+\cdots+\xi_k)$. We let $W(n)$ stand for the squares in (12.3) with such λ's, and engage in the evaluation of

$$\sum_{n<x}\Big(\sum_{j=1}^{k}\varpi(n+h_j)-\rho\Big)W(n), \tag{12.4}$$

which is an obvious analogue of (6.1); the parameter ρ is to be fixed later. Actually we need to apply *pre-sifting* to n's as indicated in $(A.3)$ below, which is not of absolute necessity but for the sake of technical comfort in dealing with d's coming from (12.3). In this way, with ϑ as in (5.1), we find that the appropriate analogue of the multiplier of $\Delta(x)$ in (9.2) is:

$$\frac{\vartheta}{2}\sum_{j=1}^{k}J_k^{(j)}(F)-\rho I_k(F), \tag{12.5}$$

where

$$\begin{aligned}I_k(F)&=\int_0^1\cdots\int_0^1 F(\xi_1,\xi_2,\dots,\xi_k)^2d\xi_1\cdots d\xi_k,\\ J_k^{(j)}(F)&=\int_0^1\cdots\int_0^1\left(\int_0^1 F(\xi_1,\xi_2,\dots,\xi_k)d\xi_j\right)^2 d\xi_1\cdots d\xi_{j-1}d\xi_{j+1}\cdots d\xi_k.\end{aligned}$$

If we put $\rho = 1$ and $F\big(\underline{\xi}\big) = (1 - \xi_1 - \cdots - \xi_k)^\ell$, then we recover (9.2) due to GPY (2005).

We are naturally interested in the variation problem

$$M_k = \sup_F \frac{\sum_{j=1}^k J_k^{(j)}(F)}{I_k(F)},$$

where the supremum is over functions F that are piece-wise differentiable in the domain indicated above and such that $I_k(F) \neq 0$, $J_k^{(j)}(F) \neq 0$ for each $j \leq k$. Let

$$\rho = m - 1, \quad m = \inf\{r \in \mathbb{N} : r \geq \vartheta M_k/2\}.$$

Then one finds that there are at least m primes in $\{n + h_1, n + h_2, \dots, n + h_k\}$ for infinitely many n's. With a delicate optimisation, Maynard has found

$$M_{105} > 4.002,$$

which together with (5.2) implies (12.1) as there exists $\{h_1, h_2, \dots, h_{105}\}$ such that $h_{105} - h_1 = 600$. More strikingly, he has shown via a simple choice of F that for sufficiently large k

$$M_k > \log k - 2\log\log k - 2.$$

This implies (12.2).

I repeat: Rényi established his prime number theorem (5.1) in 1948 and the argument of Manynard and Tao has its root in Selberg's work of 1950. Thus, more than 60 years ago when I entered elementary school, the notion that bounded differences between primes occur infinitely often could easily have already belonged to common knowledge.

Appendix. As an induction for students who intend to study Maynard's work, I shall provide details of his *arithmetic* manipulations in the case $k = 2$, which is enough typical so that one may readily infer that the general case is to be settled as is shown in (12.5). As to Tao's argument, the difference is only in the way of computing asymptotically the main terms which arise after sieving. He employed Fourier analysis in place of the usual method of summing arithmetic functions which Maynard used; see Tao's polymath8 blog, the address of which is given in the references below.

We assume that N tends to infinity, and we put

$$Y = \log\log N, \quad Z = \prod_{p \leq Y} p. \tag{A.1}$$

The rôle of Y or rather that of Z is important, as it makes the co-primality requirement in various sums easy to attain and also yields crucial truncations after the change of variables in the mode of Selberg; for the latter, see (A.10), for instance. The prime number theorem implies $Z \ll (\log N)^2$, which can be regarded to be negligibly small in our discussion. We choose c_0 mod Z to satisfy $(Z, (c_0 + h_1)(c_0 + h_2)) = 1$, which is possible whenever $\{h_1, h_2\}$ satisfies the case $k = 2$ of (6.2). We shall work on the assumption:

$$\begin{gathered}\lambda(u, v) = 0 \text{ if any of the following holds} \\ uv > D,\ |\mu(uv)| = 0,\ (uv,\ Z) > 1.\end{gathered} \tag{A.2}$$

With this, we shall consider

$$\sum_{\substack{N \leq n < 2N \\ n \equiv c_0 \bmod Z}} \left(\sum_{d_1 | (n+h_1), d_2 | (n+h_2)} \lambda(d_1, d_2) \right)^2. \tag{A.3}$$

Because of the choice of c_0 and since N is large, we have always $(n + h_1, n + h_2) = 1$ and thus $(d_1, d_2) = 1$ in (A.3), conforming with (A.2). We shall exploit this fact in the sequel without mention.

Expanding the squares and changing the order of summation, we see that the sum equals

$$(N/Z)S_0 + O\big(\lambda_{\max}^2 (D\log D)^2\big), \tag{A.4}$$

where $\lambda_{\max} = \sup|\lambda(u,v)|$ and

$$S_0 = \sum_{\substack{d_1,f_1,d_2,f_2 \\ (d_1f_1,d_2f_2)=1}} \frac{\lambda(d_1,d_2)\lambda(f_1,f_2)}{[d_1,f_1][d_2,f_2]}. \tag{A.5}$$

Because of (A.2), the condition $(d_1f_1, d_2f_2) = 1$ is equivalent to $(d_1, f_2)(d_2, f_1) = 1$. Then we have

$$\begin{aligned}
S_0 &= \sum_{\substack{d_1,f_1,d_2,f_2 \\ (d_1,f_2)(d_2,f_1)=1}} \frac{\lambda(d_1,d_2)\lambda(f_1,f_2)}{d_1d_2f_1f_2} \sum_{u_1|(d_1,f_1),\, u_2|(d_2,f_2)} \varphi(u_1)\varphi(u_2) \\
&= \sum_{u_1,u_2} \varphi(u_1)\varphi(u_2) \sum_{\substack{d_1,f_1,d_2,f_2 \\ (d_1,f_2)(d_2,f_1)=1 \\ u_1|(d_1,f_1),u_2|(d_2,f_2)}} \frac{\lambda(d_1,d_2)\lambda(f_1,f_2)}{d_1d_2f_1f_2} \\
&= \sum_{u_1,u_2} \varphi(u_1)\varphi(u_2) \sum_{\substack{d_1,f_1,d_2,f_2 \\ u_1|(d_1,f_1),u_2|(d_2,f_2)}} \frac{\lambda(d_1,d_2)\lambda(f_1,f_2)}{d_1d_2f_1f_2} \sum_{v_1|(d_1,f_2),\, v_2|(d_2,f_1)} \mu(v_1)\mu(v_2) \\
&= \sum_{u_1,u_2,v_1,v_2} \varphi(u_1)\varphi(u_2)\mu(v_1)\mu(v_2) \sum_{\substack{d_1,f_1,d_2,f_2 \\ u_1|(d_1,f_1),u_2|(d_2,f_2) \\ v_1|(d_1,f_2),\, v_2|(d_2,f_1)}} \frac{\lambda(d_1,d_2)\lambda(f_1,f_2)}{d_1d_2f_1f_2} \\
&= \sum_{u_1,u_2,v_1,v_2} \varphi(u_1)\varphi(u_2)\mu(v_1)\mu(v_2) \sum_{\substack{u_1v_1|d_1 \\ u_2v_2|d_2}} \frac{\lambda(d_1,d_2)}{d_1d_2} \sum_{\substack{u_1v_2|f_1 \\ u_2v_1|f_2}} \frac{\lambda(f_1,f_2)}{f_1f_2}.
\end{aligned} \tag{A.6}$$

Hence, we put

$$\eta(w_1,w_2) = \mu(w_1)\mu(w_2)\varphi(w_1)\varphi(w_2) \sum_{\substack{d_1,d_2 \\ w_1|d_1,\, w_2|d_2}} \frac{\lambda(d_1,d_2)}{d_1d_2}, \tag{A.7}$$

and have

$$S_0 = \sum_{\substack{u_1,u_2,v_1,v_2 \\ (u_1u_2v_1v_2,Z)=1}} \mu^2(u_1u_2v_1v_2) \frac{\eta(u_1v_1,u_2v_2)\eta(u_1v_2,u_2v_1)}{\varphi(u_1)\varphi(u_2)} \cdot \frac{\mu(v_1)\mu(v_2)}{(\varphi(v_1)\varphi(v_2))^2}. \tag{A.8}$$

Applying the Möbius inversion formula to (A.7), we have

$$\lambda(d_1,d_2) = \mu(d_1)\mu(d_2)d_1d_2 \sum_{\substack{w_1,w_2 \\ (w_1w_2,Z)=1 \\ d_1|w_1,d_2|w_2}} \mu^2(w_1w_2) \frac{\eta(w_1,w_2)}{\varphi(w_1)\varphi(w_2)}. \tag{A.9}$$

The condition (A.2) is readily seen to be well satisfied with any *any* $\eta(u,v)$ as far as it vanishes for $uv > D$. Namely, under this specification of η one may regard (A.9) as the definition of λ's, as we shall do in the sequel. Then, (A.8) implies that

$$S_0 = \sum_{\substack{u_1,u_2 \\ (u_1u_2,Z)=1}} \mu^2(u_1u_2) \frac{\eta^2(u_1,u_2)}{\varphi(u_1)\varphi(u_2)} + O\big(\eta_{\max}^2 (\log D)^2/Y\big), \tag{A.10}$$

since we have

$$\sum_{u\le D} \frac{1}{\varphi(u)} \ll \log D, \qquad \sum_{v>1,\,(v,Z)=1} \frac{1}{\varphi(v)^2} \ll Y^{-1}. \tag{A.11}$$

Next, we shall consider

$$\sum_{\substack{N\le n<2N\\ n\equiv c_0 \bmod Z}} \varpi(n+h_1)\left(\sum_{d_1\mid(n+h_1),d_2\mid(n+h_2)} \lambda(d_1,d_2)\right)^2. \tag{A.12}$$

It makes no difference if the condition $d_1 \mid (n+h_1)$ is replaced by the apparently stronger condition $d_1 = 1$, and so we see that (A.12) equals

$$\frac{1}{\varphi(Z)}(\mathrm{li}(2N)-\mathrm{li}(N))S_1 + O\big(\lambda_{\max}^2 E_3(2N, D^2Z)\big), \tag{A.13}$$

where

$$S_1 = \sum_{d,f} \frac{\lambda(1,d)\lambda(1,f)}{\varphi([d,f])} \tag{A.14}$$

and

$$E_l(x,Q) = \sum_{q\le Q} \tau_l(q) \max_{(a,q)=1}\left|\pi(x;a,q) - \frac{\mathrm{li}(x)}{\varphi(q)}\right|. \tag{A.15}$$

Here $\tau_l(q)$ is the number of ways expressing q as a product of l factors; in fact, the number of representations of q as the least common multiple of two integers is bounded by $\tau_3(q)$. Using the relation

$$\frac{\varphi(d)\varphi(f)}{\varphi([d,f])} = \sum_{u\mid(d,f)} \gamma(u), \quad \gamma(u) = \prod_{p\mid u}(p-2) \tag{A.16}$$

we have

$$S_1 = \sum_u \gamma(u)\left(\sum_{u\mid d} \frac{\lambda(1,d)}{\varphi(d)}\right)^2. \tag{A.17}$$

Imitating (A.7), we put

$$\eta_1(u) = \mu(u)\gamma(u)\sum_{u\mid d} \frac{\lambda(1,d)}{\varphi(d)}, \tag{A.18}$$

so that

$$S_1 = \sum_u \frac{\eta_1^2(u)}{\gamma(u)}. \tag{A.19}$$

Inserting (A.9) into (A.18), we have, after an arrangement,

$$\begin{aligned}\eta_1(u) &= u\gamma(u)\mu(u) \sum_{\substack{(w_1w_2,Z)=1\\ u\mid w_2}} \mu^2(w_1w_2)\frac{\eta(w_1,w_2)\mu(w_2)}{\varphi(w_1)\varphi^2(w_2)}\\ &= \frac{u\gamma(u)}{\varphi^2(u)} \sum_{(w_1u,Z)=1} \mu^2(w_1u)\frac{\eta(w_1,u)}{\varphi(w_1)} + O\big(\eta_{\max}(\log D)/Y\big).\end{aligned} \tag{A.20}$$

This error term is due to the fact that if $w_2 \ne u$, then $w_2/u > Y$. Further, we have

$$\eta_1(u) = \sum_{(w_1u,Z)=1} \mu^2(w_1u)\frac{\eta(w_1,u)}{\varphi(w_1)} + O\big(\eta_{\max}(\log D)/Y\big), \tag{A.21}$$

since

$$\frac{u\gamma(u)}{\varphi^2(u)} = \prod_{p\mid u}\left(1-\frac{1}{(p-1)^2}\right) = 1 + O(1/Y), \quad u > 1. \tag{A.22}$$

With this, we put

$$\eta(d_1,d_2) = F\left(\frac{\log d_1}{\log D}, \frac{\log d_2}{\log D}\right), \tag{A.23}$$

where F is as in the last section but with $k=2$. Collecting $(A.10)$, $(A.19)$ and $(A.21)$, we find that we need to evaluate asymptotically the sums

$$\begin{gathered}\sum_{\substack{u_1,u_2\\(u_1u_2,Z)=1}}\frac{\mu^2(u_1u_2)}{\varphi(u_1)\varphi(u_2)}F\left(\frac{\log u_1}{\log D},\frac{\log u_2}{\log D}\right)^2,\\ \sum_{\substack{u\\(u,Z)=1}}\frac{1}{\gamma(u)}\left(\sum_{\substack{w_1\\(w_1,Z)=1}}\frac{\mu^2(w_1u)}{\varphi(w_1)}F\left(\frac{\log w_1}{\log D},\frac{\log u}{\log D}\right)\right)^2.\end{gathered}\tag{$A.24$}$$

Here one may replace $\mu^2(u_1u_2)$ by $\mu^2(u_1)\mu^2(u_2)$ and do the same with the factor $\mu^2(w_1u)$, since $\mu(u_1u_2)=0$, for instance, implies that u_1 and u_2 are divisible by a $u>Y$ and such terms can be discarded in much the same way as is done in $(A.10)$. Thus, the computation can be performed in a fashion quite familiar in the theory of sums of arithmetic functions weighted with smooth functions; in essence it is an application of summation/integration by parts. We may skip the details and show only the end result: The last two sums are asymptotically equal to

$$\begin{gathered}(\log D)^2\left(\frac{\varphi(Z)}{Z}\right)^2\int_0^1\int_0^1F^2(\xi_1,\xi_2)d\xi_1d\xi_2,\\ (\log D)^3\left(\frac{\varphi(Z)}{Z}\right)^3\int_0^1\left(\int_0^1F(\xi_1,\xi_2)d\xi_1\right)^2d\xi_2,\end{gathered}\tag{$A.25$}$$

respectively, as D tends to infinity.

Now, we choose $D=N^{\vartheta/2-\varepsilon}$, with ϑ as in (5.1). Then, the assertions $(A.4)$ and $(A.13)$ yield the multiplier

$$\begin{gathered}\frac{\vartheta}{2}\left[\int_0^1\left(\int_0^1F^2(\xi_1,\xi_2)d\xi_1\right)^2d\xi_2+\int_0^1\left(\int_0^1F(\xi_1,\xi_2)d\xi_2\right)^2d\xi_1\right]\\ -\rho\int_0^1\int_0^1F^2(\xi_1,\xi_2)d\xi_1d\xi_2\end{gathered}\tag{$A.26$}$$

for the sum

$$\sum_{\substack{N\le n<2N\\ n\equiv c_0 \bmod Z}}\big(\varpi(n+h_1)+\varpi(n+h_2)-\rho\big)W(n),\tag{$A.27$}$$

where $W(n)$'s stand for the squares in $(A.3)$ with λ's as in $(A.9)$ along with $(A.23)$. We may skip the estimation of the error terms coming from $(A.10)$ and $(A.21)$ as they should not cause any difficulty. As to the error term in $(A.13)$, we need to eliminate the factor $\tau_3(q)$ in $(A.15)$. This can be achieved via an application of the Cauchy inequalty; that is,

$$E_l^2(x,Q)\ll x(\log Q)^{l^2}E_1(x,Q).\tag{$A.28$}$$

References

[1] E. Bombieri: *Le Grand Crible dan la Théorie Analytique des Nombres* (second éd.). Astérisque **18**, Paris 1987.

[2] E. Bombieri, J.B. Friedlander and H. Iwaniec: Primes in arithmetic progressions to large moduli. I. Acta Math., **156**(1986), 203–251.

[3] D.A. Goldston, S. Graham, J. Pintz and C.Y. Yildirim: Small gaps between primes or almost primes. Trans. AMS., **361** (2009), 5285–5330. See also arXiv: math/0506067 v1. June 2005.

[4] D.A. Goldston, J. Pintz and C.Y. Yildirim: Primes in tuples. I. Ann. Math., (2), **170** (2009), 819–862. See also arXiv: math/0508185 v1. August 2005.

[5] D.A. Goldston and C.Y. Yildirim: Small gaps between primes I. arXiv: math/0504336 v1. April 2005.

[6] Yu.V. Linnik: The large sieve. C.R. Acad. Sci. URSS (N.S.), **30** (1941), 292–294.

[7] —: *Dispersion Method in Binary Additive Problems*. Leningrad Univ. Press, Leningrad 1961. (Russian)
[8] J. Maynard: Small gaps between primes. arXiv: 1311.4600 v2. November 2013.
[9] Y. Motohashi: An induction principle for the generalization of Bombieri's prime number theorem. Proc. Japan Acad., **52** (1976), 273–275.
[10] —: *Sieve Methods and Prime Number Theory*. Tata IFR Lect. Math. Phy., **72**, Tata IFR–Springer 1983.
[11] —: Talk at the AIM workshop '*Gaps between primes*'. November/December 2005. http://aimath.org /pastworkshops/primegapsrep.pdf
[12] —: *Analytic Number Theory* I. Asakura, 2009. (Japanese; English edition is under preparation)
[13] Y. Motohashi and J. Pintz: A smoothed GPY sieve. Bull. London Math. Soc., **40** (2008), 298–310. See also arXiv: math/0602599 v1. February 2006; v2. July 2013.
[14] J. Pintz: Polignac numbers, conjectures of Erdös on gaps between primes, arithmetic progressions in primes, and the bounded gap conjecture. arXiv: 1305.6289. May 2013.
[15] D.H.J. Polymath: New equidistribution estimates of Zhang type, and bounded gaps between primes. arXiv: 1402.0811 v1. February 2014.
[16] A. Rényi: On the representation of an even number as the sum of a prime and an almost prime. Izv. Akad. Nauk SSSR Ser. Mat., **12** (1948), 57–78. (Russian)
[17] A. Selberg: Lectures on sieves. In *Collected Papers*. II. Springer, Berlin 1991, pp. 65–247.
[18] T. Tao: http://terrytao.wordpress.com/2013/11/19/ polymath8b-bounded -intervals-with-many-primes-after-maynard/
[19] R.C. Vaughan: An elementary method in prime number theory. Acta Arith., **37** (1980), 111–115.
[20] A.I. Vinogradov: The density hypothesis for Dirichlet L-series. Izv. Akad. Nauk SSSR Ser. Mat., **29** (1965), 903–934; Corrigendum. ibid., **30** (1966), 719–720. (Russian)
[21] Y. Zhang: Bounded gaps between primes. Preprint, April 2013.
[22] Y. Motohashi: Smoothed GPY sieve. Kokyuroku RIMS Kyoto Univ., **1512** (2006), 89–94.