RIMS Kôkyûroku Bessatsu
B53 (2015), 251–278

Goldbach 問題　— 3 つの素数の和について *
(Goldbach's problem — on sums of three primes)

By

川田 浩一 (Koichi KAWADA)**

Abstract

The ternary Goldbach problem has recently resolved completely by Helfgott, thereby it is now known that every odd integer exceeding 5 can be written as the sum of three primes. This article overviews the history of research of this area, from Hardy-Littlewood, Vinogradov, to Helfgott.

§1. 序 — Goldbach 予想.

Goldbach が Euler に送った，1742 年 6 月 7 日付の手紙を発端とする次の予想が，**Goldbach 予想**と呼ばれるものである：

- 4 以上の偶数は全て，2 つの素数の和として表されるだろう.
- 7 以上の奇数は全て，3 つの素数の和として表されるだろう.

前者は binary Goldbach conjecture，後者は ternary Goldbach conjecture と呼ばれる．N が 7 以上の奇数なら $N-3$ は 4 以上の偶数だから，もし binary の方の予想が正しければ $N-3=p+q$ となる素数 p, q があり，$N=3+p+q$ ということで，ternary Goldbach 予想も正しい．つまり binary の方の予想は ternary の方の予想を含むわけで，そのため狭義には Goldbach 予想と言うと binary Goldbach 予想を指す．また，binary と ternary の代わりに，strong と weak という形容詞がそれぞれ使われることもある．

因みに，上記の Goldbach の手紙では，Goldbach は 1 も “素数” に含めた上で，

「N が 2 つの “素数” の和であれば，$2 \le k \le N$ なる任意の整数 k に対し，
N を k 個の “素数” の和として表すことができるだろう」

Received April 14, 2014. Revised September 9, 2014.
2010 Mathematics Subject Classification(s): 11P32, 11P55.
Key Words: *Goldbach's problem, primes.*

*口頭発表のタイトルは “The ternary Goldbach Problem — from Hardy-Littlewood, Vinogradov to Helfgott” であった.

**Faculty of Education, Iwate University, Morioka 020-8550, Japan.
e-mail: `kawada@iwate-u.ac.jp`

© 2015 Research Institute for Mathematical Sciences, Kyoto University. All rights reserved.

という意味の予想を記し（例えば 5 は $2+3$ というように 2 つの素数の和で表すことができるが，$5=1+1+3=1+1+1+2=1+1+1+1+1$ のように 3 つ，4 つ，5 つの“素数”の和にもなる，といった例も挙げられている)，さらに欄外に

「2 より大きい整数は 3 つの“素数”の和であろう」

と記している．この後者の予想は上述の Goldbach 予想に近いが，1 も“素数”に含めている分，厳密に言えば現在 Goldbach 予想と呼ばれているものより弱いことになる．その手紙に対する Euler から Goldbach への 1742 年 6 月 30 日付の返信に，上記の binary Goldbach 予想が記されているそうである [1]．

Goldbach 予想の述べ方としては,「素数」を「奇数の素数」に限定するバージョンもあり，その場合の予想は次の通りとなるが，大差はない．

- 6 以上の偶数は全て，2 つの奇素数の和として表されるだろう．
- 9 以上の奇数は全て，3 つの奇素数の和として表されるだろう．

言うまでもなく，2 つの素数の和が偶数なら，それらの素数は両方とも奇素数か，両方とも 2 か，どっちかだから，6 以上の偶数が 2 つの素数の和なら，それらの素数は両方とも奇素数である．つまり binary の場合は,「素数」を「奇素数」にすると $4=2+2$ が排除される，というだけのことである．一方の ternary の場合はそこまで自明ではないから，§3.3 の終わりにもう少し詳しく述べるつもりだが，やっぱり実質的に大した違いはなく，結局 $7=2+2+3$ を含めるかどうかだけの話となる．

いずれにしろ，この Goldbach 予想の解決をはじめ，素数の和として自然数を表すことに関わる問題を総称して，Goldbach 問題と言っている．現在でも binary Goldbach 予想は未解決であるが，ternary Goldbach 予想は，既に 1937 年に本質的に解決している．その年に「ある定数 V 以上の奇数は全て 3 つの素数の和になる」という所謂 Vinogradov の三素数定理が Vinogradov [19] により証明され，あとは「その V を計算し，V 以下の正の奇数 1 つずつについて 3 つの素数の和になるかどうかを確認する，という有限の時間で終わる単純作業によって ternary Goldbach 予想の真偽が分かる」という状況となった．本質的に，あるいは論理的には解決した，とはそういう意味だが，これを本当に解決したと言うためには，その定数 V 以下の全ての奇数に対するチェックが現存するコンピューターでそれなりの時間内 (例えば 1 年以内とか) に終わるくらい，V の値を小さくしなければならない．Vinogradov の仕事以降，このための努力が何人かの人たちによって為されたが，2013 年 5 月にとうとう Helfgott [6] が $V=10^{30}$ を得，これを実現した．

定理 1 (Helfgott [6])**.** 10^{30} 以上の奇数は全て 3 つの奇素数の和である．

一方，コンピューターを使って次のことが確認できるそうである．

定理 2 (Helfgott and Platt [9])**.** 次の範囲に含まれる奇数 N は全て 3 つの奇素数の和である； $9 \le N \le 8,875,694,145,621,773,516,800,000,000,000.$

[1] この段落の情報は，英語版の Wikipedia の Goldbach's conjecture の項による．

この最後の大きい数[2]は 31 ケタで，$8 \cdot 10^{30}$ を超えている．よって，これら 2 つの定理から次が従う．

定理 3. 7 以上の奇数は全て 3 つの素数の和であり，9 以上の奇数は全て 3 つの奇素数の和である．即ち，ternary Goldbach 予想は正しい．

ここで 1 つお断り申し上げたい．Helfgott のプレプリント [6] は何度か改変されていて，今回の研究集会の初日 (2013 年 12 月 9 日) に筆者が話をさせていただいた際に基にしたのは，2013 年 5 月 13 日に公開されたその初版であった．その集会が終わった後，そのプレプリントは 2013 年 12 月 30 日付で大きく改変され，[6] と [8] の 2 つに分割されたようである．その結果，[6] は下の §3.2 で触れるような指数和の major arcs 上での挙動に関わる計算に特化され，そこで得た結果を基に [8] の方で定理 1 のような結果を示す，という形式に変わっている．しかし，基本的には本稿は集会でさせていただいた発表の報告だと考え，本稿で [6] とあるのは，発表時点で筆者が基にした [6] の初版を意味するものとさせていただく．この段落は 2014 年 5 月に書き足したものだが，その時点で [6] は第 4 版，[8] は第 2 版となっており，その [8] では 10^{27} 以上の奇数は全て 3 つの奇素数の和となることが示されている．つまり定理 1 の 10^{30} は，これを書き加えている時点では 10^{27} に改良されている．

本稿の目的は，この分野にあまり馴染みのない方々に Helfgott の定理 1 の証明の概要を紹介することである．Helfgott の証明は circle method に基づいていて，その基本的な議論に様々な工夫を加えたものであるが，その骨組みとなる circle method の概要を §3 で紹介し，Helfgott がそれに加えた工夫等について §4 で述べる．

定理 2 のようなある限界までの奇数のチェックについては，そのアルゴリズムなどコンピューターに関することについて述べる能力を筆者は持たないが，その表面上の方針について §2.4 で少々触れてみた．なお，Helfgott-Platt [9] は，定理 2 にある範囲の奇数 N に 7 も加えて，それらが全て 3 つの素数の和になる，と書いていて，「奇素数」にこだわった書き方をしていないが，その議論をみれば「奇素数」にこだわった定理 2 の主張が実際には確認されていることは明らかである．

§ 2. Ternary Goldbach 問題解決までの歴史の概要.

数学的な議論の紹介に進む前に，ternary Goldbach 問題が最終的に解決するまでの歴史について，ざっと記してみたい．

§ 2.1. Hardy-Littlewood と Vinogradov.

1742 年の Goldbach と Euler の書簡から 170 年以上の長きにわたり，Goldbach 問題に関する研究の進展は全くなかった．1912 年には Landau [10, p. 105] が「Goldbach 問

[2]参考までに日本語で読むと，887 穰 (じょう) 5694 じょ 1456 垓 (がい) 2177 京 (けい) 3516 兆 8 千億．その「じょ」は，のぎへんに予をつくりとする漢字で，その代わりに，のぎへんに「弟」の下半分のようなつくりの漢字を使い「し」と読むのが正しい，とする説もあるようだが，いずれにしろ筆者はそれらの漢字を TeX で出力できなかった．

題は現状では攻撃不可能 (unangreifbar)」と言っているが，それから 10 年ほどで状況は一変した．もしかしたら，Landau がそう書いたことで注目が集まり，こういう問題の研究が活性化するきっかけとなった面もあるのかもしれない．

Goldbach 問題に関する歴史上初めての成果は，1919 年に Brun によってもたらされた．これは binary Goldbach 問題に関わるもので，篩の方法による成果だが，本稿の主題からは外れるので当面飛ばし，§2.5 において簡潔に述べることとする．

その Brun の仕事と同時期に，Hardy-Ramanujan の分割数の研究において circle method が開発され，Hardy-Littlewood はそれを様々な加法的問題に応用して，一連の目覚ましい成果を得た．とくに Goldbach 問題を中心とする素数に関わる加法的問題への応用についてまとめたものが 1923 年の論文 [5] であり，これが今回の Helfgott の仕事に至る出発点である．

以下，本稿を通して文字 p は添え字の有無にかかわらず常に素数を表すとする．また，$N = p_1 + p_2 + p_3$ となる素数 p_1, p_2, p_3 の組の個数を $R(N)$ で表す．つまり，3 つの素数の和として N を表す方法 (素数の順番も考慮する) が $R(N)$ 通り，ということである．

Hardy-Littlewood [5] は，circle method(あるいは Hardy-Littlewood method) を用いて，次のことを証明した：$\theta < \frac{3}{4}$ をみたすある定数 θ に対し，全ての Dirichlet L 函数の零点の実部が θ 以下であると仮定すると，漸近式

$$(1) \qquad R(N) = \big(\mathfrak{S}(N) + o(1)\big)\frac{N^2}{2(\log N)^3} \qquad (N \to \infty)$$

が成立する，ただし $\mathfrak{S}(N)$ は singular series と呼ばれるもので，

$$(2) \qquad \mathfrak{S}(N) = \prod_p \Big(1 + \frac{1}{(p-1)^3}\Big) \prod_{p|N} \Big(\frac{(p-1)(p-2)}{p^2 - 3p + 3}\Big).$$

この定義から，$2|N$ なら $\mathfrak{S}(N) = 0$，$2 \nmid N$ なら $1 \ll \mathfrak{S}(N) \ll 1$ であることが分かる [3]．実際，N が奇数なら $1.32 < \mathfrak{S}(N) < 2.301$ であることを確認できる．いずれにしろ漸近式 (1) は，N が充分大きい奇数なら $R(N) > 0$，即ち N は 3 つの素数の和となることを意味する．

Hardy-Littlewood のこの結果で，Dirichlet の L 函数の零点について仮定されている命題は，所謂 Dirichlet の L 函数に対する一般 Riemann 予想よりは弱いものの，現在でも全く証明できないような命題ではある．しかし，ternary Goldbach 問題の解決へ向かう 1 つの道筋 — Dirichlet の L 函数の零点に関する恐らくは正しいと思われる命題から，ternary Goldbach 予想の本質的解決に続く道筋 — を初めて示したことは，ternary Goldbach 問題の研究における最初の偉業と言えよう．

Hardy-Littlewood [5] の議論を見ると，実部が $\frac{3}{4}$ 以上の Dirichlet L 函数の零点が 1 つでもあったら全く成立しない，というものではないことが分かる．実部が $\frac{3}{4}$ 以上の零

[3] この記号 $\ll$ は Vinogradov の記号と呼ばれ，$f \ll g$ や $g \gg f$ は，いずれも Landau の記号による $f = O(g)$ という表記と同じ，つまり $|f| < Cg$ なる正定数 C が存在することを意味する．従ってここにおける $1 \ll \mathfrak{S}(N) \ll 1$ は，$C_1 < \mathfrak{S}(N) < C_2$ なる正定数 C_1, C_2 の存在を意味している．

点がちょっとくらいあっても，そんなに多くなければ良いわけで，このことは零点密度評価の研究の動機の 1 つにもなったのだろうと思われる．1935 年には所謂 Siegel zero に関する Siegel の定理が示され，当時の研究者は ternary Goldbach 予想の本質的解決まであともうほんのちょっとのところまで来ている，という感触をもったことだろう．その最後の「ちょっと」とは，具体的には §3.3 の補題 1 の評価であった．そして 1937 年，ついに Vinogradov [19] がその最後の困難を克服し，unconditional に，つまりその時点で証明されていなかったような仮説に一切依存せずに，漸近式 (1) を得た．その (1) は上述のように「V 以上の奇数は全て 3 つの素数の和となる」ような定数 V の存在を意味するから (こういう定数 V を Vinogradov 定数と呼ぶ人もいる)，これをもって ternary Goldbach 予想は本質的に解決された，と言われるわけである．因みに Vinogradov 自身は [19] において，“This is the complete resolution of Goldbach's problem for odd numbers.” として，「完全な解決」と書いている．

§ 2.2. Vinogradov 以後.

ただ，細かいことを言えば，[19] により ternary Goldbach 予想が本質的に解決した，と言うには注意が必要な点はある．論文 [19] では，major arcs の計算 (§3.2 参照) に Siegel の定理が使われているのだが，Siegel の定理で存在が保証される定数は非実効的 (ineffective) — 具体的にその値を計算する方法は不明 — であることが知られている．従って，さっきのような定数 V が存在することは [19] から直接言えるが，その V の値を具体的に計算してみろ，と言われると，[19] に示されている方法だけではできない，ということになる．よって，「3 つの素数の和とならない正の奇数は高々有限個」と言う分には問題ないが，V 以下の正の奇数 1 つずつについて 3 つの素数の和になるかどうか全て調べることは，V の値が具体的に分からなければ有限の時間で終わる作業とは言えないから，ternary Goldbach 予想の真偽が理論的には決定可能，と言うには，その点はちょっと引っかかるわけである．

が，上に書いた通り，[19] の本質は §3.3 の補題 1 の証明にあるのであって，そのため Vinogradov としてはそれ以外の記述は極力簡潔に済ませたかったのだろう．実際 [19] では，major arcs の計算については Siegel の定理 (直接には，Siegel-Walfisz の定理と呼ばれる，等差数列中の素数分布に関する定理) があるから簡単でしょ，って感じで，ほんの数行書いてあるだけである．さっきの V の値を計算可能にするためには，Siegel の定理を回避して major arcs の計算をすればいいわけで，それはかなり手間はかかるにしろ，まあ，やろうと思えばいろいろとやりようはあること，ではある．Vinogradov は [19] に，“The estimations of the present note can be replaced by much more exact estimations.” と書いているのみで，Siegel の定理の非実効的定数をどう回避するかについて，具体的な記述はしていないが，まあここまで出来てれば，あとはやれば出来ることだから，という意味で，Vinogradov の仕事 [19] によって ternary Goldbach 予想は本質的に解決された，といった言い方がされているのだろうと思う．

実際，[19] が発表されてからすぐに，その V の値は具体的に計算されたようである．そういうことが可能と分かれば，どのくらいの大きさの数になるのか実際に計算してみたく

なるのが人情であろう．Čudakov の 1947 年の論文には，Borozdkin が 1939 年に $V = 3^{3^{15}}$ を得ていたと書かれている．Borozdkin はその当時，Vinogradov の学生だったか助手をしていたか，そういう人だったと聞いた覚えがある．ただし，探しても見つからないので，その証明は論文として発表されていないようである．解析的整数論の論文は Landau の記号 O や Vinogradov の記号 $\ll$ を使って定数を省略して書かれるのが普通だが，そういう V の値を具体的に求めるには当然 O や $\ll$ を使うことは許されず，全ての定数を明確に計算しなければならない．他の論文の結果を引用する必要があれば，その論文の計算も O や $\ll$ を使わずに全て明確にやり直すことになる．1 度でも O や $\ll$ を使って論文を書かれたことのある方なら容易に想像できると思うが，それは大変な労力を要する仕事であるし，ページ数も結構要することになる．書き上げたとしてもそういう論文はどうしても単純計算が延々と続くという印象になりがちだろうし，掲載してくれる雑誌もなかなかなかったかもしれない．$V = 3^{3^{15}}$ とできるという Borozdkin の証明が発表されていないのは，そういう事情もあったのかもしれないと思う．

1956 年に Borozdkin [1] が $V = 3^{3^{15}}$ とできることを証明した，という記述も複数の文献で見られた．その [1] を見たいと思っていたがなかなか見つけられず，今回の研究集会に参加させていただいている期間中，京都大学数理解析研究所の図書室のスタッフの方にお願いして，探していただいた [4] が，それでも結局見つけることができなかったから，とりあえずはあきらめた．ただ，どうやら [1] は 1 ページの論文のようだから，$V = 3^{3^{15}}$ という結果を得たという報告と，高々その証明の方針を簡潔に書いてあるくらいのものであろうと想像する．その証明をちゃんと書いたものが 1 ページで済むことはあり得ない．

今回の研究集会でこういう話をさせていただくにあたり，そういう歴史についても調べようと努めたのだが，容易に見つけられない文献もあったし，また，発表されている論文でも Introduction 中の歴史に関する記述の信憑性に疑問を感じるものもあった．例えば，Vinogradov [19] が $V = 3^{3^{15}}$ を証明した，と書いてある文献も複数あったが，これなどははっきり誤りである．筆者は [19] は読んだが，そこにはそういう具体的な計算はない．そういうこともあって，V の値の計算の歴史については個人的にはまだよくわかっていない部分もある．

筆者が実際に見ることができた範囲では，V の具体的な値の計算をちゃんと書いた最初の文献は 1989 年の Chen-Wang [2] で，そこでは $V = e^{e^{11.503}}$ が得られている．その頃から 5，6 年ほどの間に V の計算をした論文が数編発表され，後から発表された結果が先に発表されたものより劣る，といった事例も見られたりしている．Helfgott の定理 1 の前の一番良い結果は，2002 年の Liu-Wang [12] によるもので，$V = e^{3100}$ であった．このへんに現れた V の値の大きさの比較のため，底を 10 にそろえ指数の小数第 1 位以下を切り捨てた近似値を書いてみると，

$$3^{3^{15}} \fallingdotseq 10^{6846168}, \qquad e^{e^{11.503}} \fallingdotseq 10^{43000}, \qquad e^{3100} \fallingdotseq 10^{1346}.$$

そして，定理 1 にあるように Helfgott が V を 10^{30} まで小さくしたのである．

[4]京都大学数理解析研究所図書室のスタッフの皆様のご協力に対して，この場で謝意を表させていただきます．

§ 2.3. 一般 Riemann 予想の下での結果.

さて，以上の V の値は unconditional に得られたものだが，それらとは別に conditional な結果もいくつかあった．そのうち特に次の結果を定理として挙げておく．

定理 4 (Zinoviev [20]). Dirichlet の L 函数に対する一般 Riemann 予想 (以下，単に **GRH** と略す) が正しければ，10^{20} 以上の全ての奇数は 3 つの奇素数の和である．

GRH の下での計算は，Hardy-Littlewood [5] の仕事の直後に Lucke [13] が初めて行い，$V = 10^{32}$ を得ている．Lucke は Landau の学生さんだったそうで，この [13] は学位論文である．筆者は [4] の Introduction を読んで存在を知っただけで，[13] を読んではいないが，時期から言って Hardy-Littlewood [5] の議論に沿うものだったのだろう．

GRH の下で $V = 10^{20}$ とできるというこの定理 4 は 1997 年の結果だが，その頃のコンピューターは既に 10^{20} くらいまでの奇数のチェックをするだけの能力があった．これがわざわざ Zinoviev [20] の結果をここに定理として記した理由の 1 つである．

実際，その結果を受けて，Deshouillers-Effinger-te Riele-Zinoviev [4] は，Riemann 予想 (Riemann の zeta 函数だけに対する元々のやつ) を仮定した上で，7 以上 10^{20} 以下の奇数は全て 3 つの素数の和になることを確認した．それと独立に，Saouter [16] は unconditional に同じ結果を確認した．論文が出たのは [4] が 1997 年，[16] が 1998 年だったが，論文の投稿は [16] の方が早かった．これらを読んでみると，Saouter は Zinoviev [20] の結果を知らないで [16] を書いたようで，これは考えてみるとちょっと不思議な気がする．定理 4 を知らなかったのなら，[16] でチェックしたのがちょうど 10^{20} までだった，というのは偶然の一致ということになる．逆に Zinoviev 達もその当時は Saouter の仕事 [16] を知らなかったようである．

いずれにしろ，1997 年には，GRH の下で ternary Goldbach 予想が解決された，という出来事があった．それから 15 年程して，Helfgott はその GRH の仮定を外し，ternary Goldbach 予想を unconditional に解決したのである．

§ 2.4. ある限界までの奇数に関する確認.

Deshouillers 達 [4] は 10^{20} 以下の奇数のチェックのために Riemann 予想を仮定した，と聞くと不思議に感じられる方もあると思うので，ここで，定理 2 のような，ある限界以下の正の奇数に対するチェックに関して少しだけ述べてみる．そのためには，次の 2 つの形の命題をそれぞれ確認するのが基本的な方針である (この方針自体は Riemann 予想を仮定するかどうかとは無関係である)：

(I) $6 \leq n \leq C_0$ なる偶数 n は全て 2 つの奇素数の和となる．

(II) $3 < x \leq C$ なる任意の実数 x に対し，$x - C_0 + 4 \leq p < x$ なる奇素数 p がある．

これら 2 つの命題が正しければ，$9 \leq N \leq C$ なる任意の奇数 N に対して，(II) から $N - C_0 \leq p < N - 4$ なる奇素数 p があり，すると $N - p$ は偶数で $4 < N - p \leq C_0$ だか

ら (I) により $N-p=p_1+p_2$ なる奇素数 p_1, p_2 があることになり，N は 3 つの奇素数の和となることが分かる．

(I) に関しては binary Goldbach 予想との関係から，できるだけ大きい C_0 に対してそれを確認する努力が続けられている．一方 (II) は，要するに C 以下の素数を小さい順に並べたとき隣り合う素数の差が全て C_0-4 より小さい，という主張だが，素数定理によればその隣り合う素数の差の平均値は $\log C$ くらいのはずだから，(II) における C は大雑把に言って e^{C_0-4} に近いくらい大きくても良いと期待される．もちろん現実にはそこまで大きくはできないが，それでも 2 つの素数の和に対してチェックした限界 C_0 よりもずうーっと大きい C まで 3 つの素数の和に対するチェックができていることになる，というのがミソである．

さて，その 2 つの命題を両方ともコンピューターで確認すればいいわけだが，(II) は純粋に素数分布の問題だから Riemann zeta 函数の零点と直結する．Deshouillers 達は，GRH の下での結果である Zinoviev の定理 4 を受けて，conditional に ternary Goldbach 予想を解決する目的で 10^{20} 以下の奇数のチェックに乗り出したわけだから，そのチェックに普通の Riemann 予想を使ったって構わなかったし，Riemann 予想の下でそういう隣り合う素数の差を評価するのは，そのための下地となる研究もあるお陰で，コンピューターを使うより Riemann 予想を仮定して手で計算する方がむしろ楽，という状況もあって，(II) を示すのに Riemann 予想を使うという選択をしたのだろう [5]．

一方，(II) に当たることをコンピューターで確認することも当然できるわけだが，その際には特殊な形をした素数を探すのが効率的のようである．Saouter [16] も同様の方針を採用しているが，Helfgott-Platt [9] は，次の平易な定理に基づいて素数を探している：$k<2^n$ をみたす自然数 k, n に対して，$N=k\cdot 2^n+1$ としたとき，もし

$$\left(\frac{a}{N}\right)=-1 \qquad \text{かつ} \qquad a^{(N-1)/2}\equiv -1 \pmod N$$

をみたす整数 a があれば，N は素数である．これを Proth の定理といい，その N の形の数を Proth 数と呼ぶそうである．

(I) に関する最新の結果は，$C_0=4\cdot 10^{18}$ としてよい，というもので，Oliveira e Silva-Herzog-Pardi [14] による．よって，それより狭い間隔で素数が順次見つかって，10^{30} を超える素数まで到達できれば良いことになる．そこで Helfgott-Platt [9] は，まず上記の Proth の定理に基づいて素数を探し，素数をたくさん見つけてみて，間隔が $4\cdot 10^{18}$ より広いところについては，別途都合の良い大きさの素数を探して見つけた，とのことである．このようにして定理 2 は得られている．

§ 2.5. Circle method とは異なるアプローチ.

さて，§2.1 から §2.3 にかけては ternary Goldbach 予想解決に至る歴史の流れを記した．その流れには乗せ難かった，circle method 以外の方法による，Goldbach 問題に関わ

[5] Riemann 予想を仮定すると，C 以下の素数については隣りとの差は $C^{1/2}$ 強で抑えられるから，C は C_0^2 よりちょっと小さいくらいにはできる，ということになる．因みに，[4] では Riemann 予想の下で，$C=10^{20}$ に対して C_0 は 10^{12} くらいの大きさとなっている．

る 2 つの成果について，ここで少々補足する．

1919 年，Brun は篩の方法に画期的なアイディアを導入し，充分大きい偶数は 2 つの P_9 の和として表せることを証明した．P_9 とは，高々9 個の素数の積となる自然数を指す (より一般に，高々r 個の素数の積となる自然数は P_r と呼ばれる [6])．この Brun による binary Goldbach 予想に対する “近似” が，Goldbach 問題に関する史上初めての理論的な成果である．

数学の世界で「篩」という言葉が使われたのは，もちろん Eratosthenes の篩が最初で，紀元前の大昔からあった概念だから，そういう意味では，篩の方法は歴史も古い … わけだが，現在の篩の理論は Brun に始まった，と言うこともできよう．この Brun の重要な仕事以降，篩に関わる理論は 20 世紀中に大きく発展し，Goldbach 問題に関して言えば，充分大きい偶数は素数と P_2 の和で表せる，という Chen の定理にまで到達することになる．

また，Hardy-Littlewood [5] と Vinogradov [19] の間に，Schnirel'man の興味深い仕事があった．1930 年，Schnirel'man は「2 以上の全ての自然数が高々k 個の素数の和となる」ような有限な k の存在を証明した．Hardy-Littlewood [5] は，(1) の直前にある L 函数の零点に関する仮定の下にそういう k の存在を証明していたことになるが，これを unconditional に証明したのは Schnirel'man が最初である．Schnirel'man の証明は，Schnirel'man 密度と呼ばれる概念に基づくもので，Brun の篩の方法によって得られる結果も用いるが，全体として極めて素朴で初等的であり，そのような議論からこんな結果が導かれるというのは大変面白いと思う．Schnirel'man の仕事は，additive combinatorics などと呼ばれる分野において重要な位置にある．

「2 以上の全ての自然数が高々k 個の素数の和となる」ような最小の k を Schnirel'man 定数と言う．例えば 27 など，高々2 個の素数の和とならない奇数はいくらでもあり，Schnirel'man 定数の値はたぶん 3 だろうと思われるが，これは binary Goldbach 予想から従う．Schnirel'man 定数について，Schnirel'man 自身は存在を示したのみで具体的な数値による評価は与えていないが，それ以後，具体的な評価を与えた論文は 8 編ほどある．ただし，良い数値評価を導くには，Schnirel'man の方法ではなく，circle method が用いられる．さて，7 以上の奇数は定理 3 により 3 つの素数の和であり，すると N が 10 以上の偶数なら，$N-3$ は 7 以上の奇数だから $N-3$ は 3 つの素数の和であり，よって N は 4 つの素数の和である．もちろん 10 未満の自然数については言うまでもないから，Helfgott の今回の仕事により，Schnirel'man 定数は 4 以下，というか，4 か 3 かどっちかであることが示されたわけである．

§ 3.　Circle method による議論の概要．

Helfgott の定理 1 の証明は circle method に基づくもので，証明の骨組みは Vinogradov [19] のそれと同じと言える．Vinogradov [19] の証明に，最終的に得られる Vinogradov 定

[6] 例えば $12(=2^2\cdot 3)$ は P_3 であり，ということは P_4 でもあるし P_{10} でもあるが，P_2 ではない，というようなことである．

数 V の値が小さくなるような様々な工夫を加えたものが Helfgott の仕事 [6] である．そこでまずこの節では，Vinogradov [19] に沿って circle method の議論の概要を紹介する．既に circle method についてご存知の方は，この §3 を飛ばして §4 に進まれてよいと思う．以下の概要より詳しい，厳密な議論をご覧になりたい方には，例えば Vaughan [18] の 3 章，あるいは Davenport [3] をお勧めしたい．[18] は現在最も良い circle method の教科書だと思う．素数分布論自体のことは [18] では扱ってないが，[3] の方にはその方面の丁寧な解説があり，Vinogradov の三素数定理まで必要なことがひと通り書いてある．

では，N を 2 以上の自然数とし (とりあえず N の偶奇は問わない)，

$$S(\alpha) = \sum_{p \le N} e(p\alpha), \qquad \text{ただし} \quad e(\alpha) = e^{2\pi i\alpha}, \tag{3}$$

とおく．§2.1 の最初から 4 番目の段落に書いたが，本稿では文字 p は添え字の有無にかかわらず常に素数を表すと約束してあること，ついでに $R(N)$ は N を 3 つの素数の和として表す方法の数であったことも，ここで思い出していただく．さて，m が整数なら，

$$\int_0^1 e(m\alpha)\,d\alpha = \begin{cases} 1 & (m=0) \\ 0 & (m \ne 0) \end{cases} \tag{4}$$

となることは簡単に分かる．このことに注意すると，

$$\begin{aligned} \int_0^1 S(\alpha)^3 e(-N\alpha)\,d\alpha &= \sum_{p_1 \le N} \sum_{p_2 \le N} \sum_{p_3 \le N} \int_0^1 e((p_1+p_2+p_3-N)\alpha)\,d\alpha \\ &= \sum_{p_1 \le N} \sum_{p_2 \le N} \sum_{\substack{p_3 \le N \\ p_1+p_2+p_3=N}} 1 \;=\; R(N) \end{aligned} \tag{5}$$

である．これが circle method の始点となる式だが，これ自身は自明なことで，問題はこの (5) の左端の積分をどう計算するか，である．そのため $S(\alpha)$ の挙動を調べる必要がある．

§ 3.1. 指数和 $S(\alpha)$ と Dirichlet L 函数の零点.

実数 α がある有理数 a/q に近い状況を想定して (q と a は互いに素な自然数とする)，

$$\alpha = \frac{a}{q} + \beta \ \ \text{とおくと，} \quad S(\alpha) = S\Big(\frac{a}{q}+\beta\Big) = \sum_{p \le N} e\Big(p\frac{a}{q}\Big) e(p\beta)$$

となるが，$p \equiv b \pmod q$ なら $e(pa/q) = e(ba/q)$ であることに注意して，右辺の和を p が属す法 q の剰余類によって分ける．その際，法 q の既約剰余類に属さない素数 p は q の素因数以外にはないからその分を自明に評価して，

$$S\Big(\frac{a}{q}+\beta\Big) = \sum_{\substack{b=1 \\ (b,q)=1}}^{q} e\Big(b\frac{a}{q}\Big) \sum_{\substack{p \le N \\ p \equiv b \ (\mathrm{mod}\ q)}} e(p\beta) \;+\; O(\log q).$$

この右辺の 2 重和の内側の和は公差 q の等差数列中の素数にわたる和であるが，そのような素数の分布については explicit formula と言うのがあって，法 q の Dirichlet 指標に対する L 函数の零点によって表現することができる．その explicit formula を使って partial summation と言われる手続きをすると，次のような表現に至る：

$$(6)\quad S\Big(\frac{a}{q}+\beta\Big)=\frac{\mu(q)}{\varphi(q)}\int_2^N\frac{e(t\beta)}{\log t}\,dt \\ -\frac{1}{\varphi(q)}\sum_{\chi\ (\mathrm{mod}\ q)}\sum_{\substack{b=1\\(b,q)=1}}^{q}\frac{1}{\chi(b)}e\Big(\frac{ab}{q}\Big)\sum_{\substack{\rho\\|\mathrm{Im}\rho|\le T}}\int_2^N\frac{t^{\rho-1}e(t\beta)}{\log t}\,dt \\ +O\bigg(\Big(\frac{N}{T}+N^{1/2}\Big)\big(\log(qNT)\big)^2q^{1/2}(1+N|\beta|)\bigg).$$

ここで $\varphi(q)$ は Euler totient 函数，$\mu(q)$ は Möbius 函数 [7]，$\sum$ の下に $\chi\ (\mathrm{mod}\ q)$ とあるのは，法 q の全ての Dirichlet 指標 χ にわたる和を表し，その和の内側にある ρ は L 函数 $L(s,\chi)$ の自明でない零点，言い換えると実部が 0 と 1 の間にあるような $L(s,\chi)$ の零点を表す．その自明でない零点 ρ のうち虚部の絶対値が T 以下のものについて足す，というのが内側にある ρ についての和の意味だが，T はパラメーターで ($T\ge 2$ とする)，それが誤差項に影響する．

と，記号の説明が長くなったが，こんな (6) のような式を書いて何が言いたいかと言うと，T を大きくとれば，つまり L 函数の零点をたくさん使えば，最後の誤差項は充分小さくできるので (誤差項にある $N^{1/2}$ は必要ならもっと精密に書けるもので，実質的に気にしなくて大丈夫)，

$S(\alpha)$ という指数和は，Dirichlet L 函数の零点を用いて非常に精密に記述できる

ということである．

(6) の ρ についての和の内側にある $t^{\rho-1}$ というのを見ていただくと，現状では unconditional には ρ の実部は 1 に非常に近いかもしれないから $|t^{\rho-1}|$ は 1 に近いかもしれないわけだが，GRH を仮定すれば $|t^{\rho-1}|=t^{-1/2}$ であり，ρ に関わる部分に対して簡単に強い評価を与えることができる．例えば定理 4 などで，GRH を仮定することによっていい結果が得られる理由は，こういうことである．

§3.2. Major arcs の寄与.

我々は (5) の左端の積分を計算したいわけだが，(6) によって，分母が小さい有理数に近い α がその積分に大きい寄与をするであろうと期待される．そこで，ある程度大き

[7] 蛇足だが，ここに Möbius 函数が現れるのは，$\displaystyle\sum_{\substack{b=1\\(b,q)=1}}^{q}e\Big(\frac{ab}{q}\Big)=\mu(q)$ だから．

い正定数 A に対し (A は例えば 15 とかに決めてもいいんだが)，$Q=(\log N)^A$ とし，

$$\mathfrak{M}(q,a)=\Big\{\frac{a}{q}+\beta\,;\,|\beta|\le\frac{Q}{N}\Big\},\qquad \mathfrak{M}=\bigcup_{q\le Q}\bigcup_{\substack{a=1\\(a,q)=1}}^{q}\mathfrak{M}(q,a),\qquad \mathfrak{m}=\Big[\frac{Q}{N},1+\frac{Q}{N}\Big]\setminus\mathfrak{M},$$

とする．こういう分母の小さい有理数に近い実数の集合 $\mathfrak{M}$ を **major arcs**，そうでない実数の集合 $\mathfrak{m}$ を **minor arcs** と呼ぶ．$S(\alpha)$ は α の函数として 1 を周期とすることに注意して，(5) より

$$\begin{aligned}R(N)&=\int_0^1 S(\alpha)^3e(-N\alpha)\,d\alpha=\int_{Q/N}^{1+Q/N}S(\alpha)^3e(-N\alpha)\,d\alpha\\&=\int_{\mathfrak{M}}S(\alpha)^3e(-N\alpha)\,d\alpha+\int_{\mathfrak{m}}S(\alpha)^3e(-N\alpha)\,d\alpha.\end{aligned}\tag{7}$$

最後の右辺第 1 項の $\mathfrak{M}$ 上の積分を計算して，そこから $R(N)$ の main term を引き出し，第 2 項の $\mathfrak{m}$ 上の積分に対してはその絶対値を上から評価することによって，N が大きい奇数なら $R(N)>0$ であることを証明することになる．

そこで，ここからは N はある程度大きいと仮定する．とりあえず $N>2Q^3$ をみたすくらい N が大きいとすると，$1\le a_j\le q_j\le Q$, $(a_j,q_j)=1$ なる自然数 a_j, q_j $(j=1,\,2)$ に対して，

$$\frac{a_1}{q_1}\ne\frac{a_2}{q_2}\ \text{ であれば，}\quad \Big|\frac{a_1}{q_1}-\frac{a_2}{q_2}\Big|=\frac{|a_1q_2-a_2q_1|}{q_1q_2}\ge\frac{1}{q_1q_2}\ge\frac{1}{Q^2}>2\frac{Q}{N}$$

となるから，$\mathfrak{M}$ を構成している $\mathfrak{M}(q,a)$ 達はどの 2 つも共通部分をもたないことが分かり，$1\le a\le q\le Q$ かつ $(a,q)=1$ をみたす全ての q と a に対して $\mathfrak{M}(q,a)$ の寄与を足し合わせたものが，$\mathfrak{M}$ の寄与となる．

そこで，$\alpha\in\mathfrak{M}(q,a)$ に対し $\alpha=a/q+\beta$ とおけば，(6) の右辺の第 1 項以外の部分は，Siegel の定理とそれ以前から知られていた L 函数の zero free region によって簡単に評価できる．これは (6) より 5 行前の式の右辺に Siegel-Walfisz の定理と partial summation を適用する，と言う方がより直接的だが，いずれにしろ Q が $\log N$ の定数乗程度の大きさなら本質的には Siegel の定理によって平易に次の式を得る：

$$S(\alpha)=S\Big(\frac{a}{q}+\beta\Big)=\frac{\mu(q)}{\varphi(q)}v(\beta)+O(NQ^{-5}),\quad \text{ただし}\quad v(\beta)=\int_2^N\frac{e(t\beta)}{\log t}\,dt.$$

こうなればあとは単純で，

$$\begin{aligned}\int_{\mathfrak{M}}S(\alpha)^3e(-N\alpha)\,d\alpha&=\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{|\beta|\le\frac{Q}{N}}S\Big(\frac{a}{q}+\beta\Big)^3e\Big(-N\Big(\frac{a}{q}+\beta\Big)\Big)\,d\beta\\&=\sum_{q\le Q}\frac{\mu(q)}{\varphi(q)^3}c_q(-N)\int_{-\frac{Q}{N}}^{\frac{Q}{N}}v(\beta)^3e(-N\beta)\,d\beta+O(N^2Q^{-2}),\end{aligned}\tag{8}$$

ここで $c_q(-N)$ は Ramanujan 和である；

$$c_q(-N)=\sum_{\substack{a=1\\(a,q)=1}}^{q} e\Big(-\frac{a}{q}N\Big).$$

(8) の最後の β についての積分の扱い方はいろいろあるが，$\beta\neq 0$ に対して $v(\beta)\ll|\beta|^{-1}$ といった程度の評価が部分積分によって確認されるので，

$$I(N)=\int_{-\infty}^{\infty} v(\beta)^3 e(-N\beta)\,d\beta$$

とおくと，この積分 (singular integral と呼ばれる) は絶対収束し，

$$\int_{-\frac{Q}{N}}^{\frac{Q}{N}} v(\beta)^3 e(-N\beta)\,d\beta = I(N)+O(N^2Q^{-2}). \tag{9}$$

一方，Fourier の反転公式により，

$$I(N)=\iint\limits_{\substack{t_1\geq 2,\ t_2\geq 2\\ t_1+t_2\leq N-2}} \frac{dt_1\,dt_2}{\log t_1\log t_2\log(N-t_1-t_2)} \tag{10}$$

であり，この表示から容易に次の漸近式が従う；

$$I(N)=\Big(\frac{1}{2}+o(1)\Big)\frac{N^2}{(\log N)^3}\quad (N\to\infty). \tag{11}$$

また，Ramanujan 和に対する自明な評価 $|c_q(-N)|\leq\varphi(q)$ を使っても，

$$\sum_{q\leq Q}\frac{\mu(q)}{\varphi(q)^3}c_q(-N)=\sum_{q=1}^{\infty}\frac{\mu(q)}{\varphi(q)^3}c_q(-N)+O(Q^{-1}) \tag{12}$$

くらいの評価が得られ，この右辺の無限和を $\mathfrak{S}(N)$ とすると，$\mu(q)$, $\varphi(q)$, $c_q(-N)$ が全て q に関して乗法的なことから $\mathfrak{S}(N)$ は Euler 積で表示でき，その際 $p|N$ か否かに応じて $c_p(-N)$ は $(p-1)$ か (-1) であることに注意すれば，

$$\mathfrak{S}(N)=\prod_p\Big(1-\frac{c_p(-N)}{\varphi(p)^3}\Big)=\prod_{p\nmid N}\Big(1+\frac{1}{(p-1)^3}\Big)\prod_{p|N}\Big(1-\frac{1}{(p-1)^2}\Big)$$

となって，これからすぐ singular series $\mathfrak{S}(N)$ の表示 (2) が導かれる．

(9) と (12) を (8) に代入し，major arcs $\mathfrak{M}$ の寄与について次式を得る：

$$\int_{\mathfrak{M}} S(\alpha)^3 e(-N\alpha)\,d\alpha=\mathfrak{S}(N)I(N)+O(N^2Q^{-1}). \tag{13}$$

§3.3. Minor arcs の寄与.

(7), (13) および (11) より，あとは (7) における minor arcs $\mathfrak{m}$ の寄与が $o\big(N^2(\log N)^{-3}\big)$ であることが証明できれば，漸近式 (1) が得られる．そのために，まず $S(\alpha)$ の複素共役は $S(-\alpha)$ であることに注意して，あと (4) も思い出して，次の観察をする：

$$\begin{aligned}\int_0^1 |S(\alpha)|^2\,d\alpha &= \int_0^1 S(\alpha)S(-\alpha)\,d\alpha\\ &= \sum_{p_1\le N}\sum_{p_2\le N}\int_0^1 e((p_1-p_2)\alpha)\,d\alpha \;=\; \sum_{p_1\le N} 1 \;\ll \frac{N}{\log N}.\end{aligned} \tag{14}$$

ここまで来ると，あと欠けているのは次の結果だけとなる.

補題 1 (Vinogradov [19]). $\displaystyle\sup_{\alpha\in\mathfrak{m}} |S(\alpha)| \ll N(\log N)^{-\frac{A}{3}+2}.$

有名な三素数定理の論文 [19] で Vinogradov がやったことは実質この補題 1 の証明だけである．この証明以外の記述はあっさりしたもので，(13) の証明もほとんど書かれてない — その時点ではもうそんなことは常識だった，という雰囲気が感じられる.

言うまでもなく自明に $S(\alpha) \ll N(\log N)^{-1}$ だから，補題 1 の評価はその自明な評価より “ちょっと良いだけ” とも言えるが，そのような自明でない評価を unconditional に証明することが，ternary Goldbach 予想の本質的解決を阻む最後の壁であったのである.

補題 1 と (14) から，

$$\begin{aligned}\left|\int_{\mathfrak{m}} S(\alpha)^3 e(-N\alpha)\,d\alpha\right| &\le \int_{\mathfrak{m}} |S(\alpha)|^3\,d\alpha\\ &\le \sup_{\alpha\in\mathfrak{m}} |S(\alpha)| \int_0^1 |S(\alpha)|^2\,d\alpha \ll N^2(\log N)^{-\frac{A}{3}+1}.\end{aligned} \tag{15}$$

$A=15$ とでもすれば，これと (13) と (7) より，

$$R(N) = \mathfrak{S}(N)I(N) + O(N^2(\log N)^{-4}), \tag{16}$$

さらに (11) により漸近式 (1) が従う.

(2) の直後に書いたが，N が奇数なら $\mathfrak{S}(N) > 1.32$ であることが確認でき，singular integral $I(N)$ に対しては (10) の積分表示から，

$$I(N) \ge \frac{1}{(\log N)^3}\iint\limits_{\substack{t_1\ge 2,\ t_2\ge 2\\ t_1+t_2\le N-2}} dt_1dt_2 \;=\; \frac{(N-4)^2}{2(\log N)^3} \;=\; \frac{N^2}{2(\log N)^3} + O(N(\log N)^{-3})$$

であるから，これまでの全ての議論に現れた O や $\ll$ などの記号によって省略していた定数を全て計算して明確にすれば，(16) より，

$$R(N) > 0.66N^2(\log N)^{-3} + E, \qquad |E| < KN^2(\log N)^{-4}$$

となる定数 K が求まるはずで，すると $N \geq e^{K/0.66}$ なる奇数 N に対しては，

$$R(N) > 0.66\frac{N^2}{(\log N)^3} - K\frac{N^2}{(\log N)^4} = \Big(0.66 - \frac{K}{\log N}\Big)\frac{N^2}{(\log N)^3} \geq 0,$$

即ち N は 3 つの素数の和になることが分かる．これが所謂 Vinogradov 定数 V を求める方法の概要である．今の例では $V = e^{K/0.66}$ が得られたわけだが，あとはこの V の値を，従って K の値を，できるだけ小さくするためにどういう工夫をするか，という話になるわけである．

ところで，本稿の最初の方に，「3 つの素数の和」でも「3 つの奇素数の和」でも大差ない，と述べたが，ternary の場合については明確な根拠は示していなかったので，つまらないことで恐縮だが，そのことに触れて本小節を終えたい.「奇素数」にこだわりたければ要するに 2 を除けば良いので，例えば指数和 $S(\alpha)$ の定義 (3) において素数 p の条件を $2 < p \leq N$ に代えて 2 を排除すればいい．言い換えれば上の議論において $S(\alpha)$ を $S(\alpha) - e(2\alpha)$ で置き換えるということだが，それらの差は絶対値にして 1 だから，上の計算に実質的な影響はない．

または，こんな言い方もある．奇数 N が 3 つの素数の和で，その 3 つの素数のうちの少なくとも 1 つが 2 だったら，その 3 つの素数のうちのちょうど 2 つが 2 でなければならないから，$N-4$ が素数のときに限って奇数 N は $2+2+(N-4)$ のように 2 を含む 3 つの素数の和となるわけだが，項の順番を考えてその様な表現は 3 通りである．従って N が奇数で $R(N) > 3$ なら，N は 3 つの奇素数の和となる．さっきは $R(N) > 0$ となる N の条件を求めたが，$R(N) > 3$ となる条件でも実際ほとんど変わりないのはお分かりいただけるだろう．

コンピューターを使ってある限界以下の奇数をチェックすることについては §2.4 でちょっと述べたが，いずれにしろ,「奇素数」に限定することにこだわっても大した違いはないわけである．

§ 3.4. Vinogradov の補題 1 の証明について.

Ternary Goldbach 問題の本質的解決のための最後の難問となったのが，minor arcs 上での $|S(\alpha)|$ の最大値に対する自明でない評価を与えることで，それを初めて成し遂げたのが Vinogradov [19] であると書いたが，その大論文 [19] のページ数の少なさが示す通り，実はそれは，出来てみれば簡単なことだった．

(6) に書いたように，$S(\alpha)$ は Dirichlet L 函数の零点を用いて精密に記述できる．だから,「$|S(\alpha)|$ を抑えたい」となれば,「じゃあ L 函数の零点についてあんたは何が言えるんだ」となるのは自然な展開である．しかもいかにもそういう方針で出来そうだ — ということで，たぶんその当時は Vinogradov のような初等的な方法は盲点になっていたのではないか，という気はする．ずっとあとの時代の，それも私のような者が想像でものを言うのもなんだが．

実際，今ではそういう方針でも，つまり Dirichlet L 函数の零点と正々堂々と戦っても，補題 1 と同等の結果を証明できる．それを初めて実現して見せたのは Linnik [11] で，

Vinogradov [19] から 9 年後の 1946 年のことだった．

Vinogradov の補題 1 の証明のアイディアは，まず $S(\alpha)$ を次のような 2 つのタイプ [8] の 2 重和の組み合わせとして表し，そしてそれぞれの 2 重和を評価する，というものである；

$$\text{(Type I)} \quad \sum_{m\le M} a_m \sum_{n\le N/m} e(mn\alpha)\,; \qquad \text{(Type II)} \quad \sum_{M<m\le 2M} a_m \sum_{n\le N/m} b_n e(mn\alpha).$$

Type I の方は，Type II と比べると b_n が全て 1 である場合というようなことで，Type II の方は，内側の n に関する和にも b_n という何らかの重みが付いている代わりに，外側の m の大きさの制限がポイントである．ここにおいて，a_m とか b_n とかはとりあえず何でもいいと言えば何でもいいのだが，例えば $|a_m|\le 1$, $|b_n|\le 1$ といった大きさに関する情報だけを基に，それらの和を評価するのである．Type I の方は，内側の和は単なる等比数列の和だから簡単に評価できる．Type II の方についてはまず Cauchy の不等式を使って，

$$\left|\sum_{M<m\le 2M} a_m \sum_{n\le N/m} b_n e(mn\alpha)\right| \le \left(\sum_{M<m\le 2M} |a_m|^2\right)^{\frac12} \left(\sum_{M<m\le 2M}\left|\sum_{n\le N/m} b_n e(mn\alpha)\right|^2\right)^{\frac12}$$

とし，さらに最後の n についての和の絶対値の 2 乗を展開して，

$$\sum_{M<m\le 2M}\left|\sum_{n\le N/m} b_n e(mn\alpha)\right|^2 = \sum_{n_1\le N/M}\sum_{n_2\le N/M} b_{n_1}\overline{b_{n_2}} \sum_{M<m\le \min\{2M,\,N/n_1,\,N/n_2\}} e(m(n_1-n_2)\alpha)$$

とすると，最後の 3 重和の 1 番内側の m についての和が等比数列の和になっていて簡単に計算できるので，それを基に Type II の和の評価を得られる．このように Type I にしろ Type II にしろ，初等的に評価することができるが，補題 1 のためにはちょっと non-trivial な評価が得られれば良いので，それで充分なのである．

あとは $S(\alpha)$ を Type I，Type II の和の組み合わせで表現すればいいわけだが，それは篩えばいい．N 以下の自然数 n について足し合わせたものから，N 以下の素数でない n 達の寄与を引くと，N 以下の素数についての和が残るわけで，素数でないということは 1 か合成数だから，式で書くと，

$$\sum_{n\le N} e(n\alpha) \;-\; e(\alpha) \;-\; \sum_{\substack{n\le N\\ n\ \text{は合成数}}} e(n\alpha) \;=\; \sum_{p\le N} e(p\alpha) \;=S(\alpha).$$

この左辺の第 1 項の和は Type I の $M=1$, $a_1=1$ の場合だし，あとはごまかさせていただくが，合成数は 2 つの整数の積で書けるということで，合成数の n を mn と書き直

[8] これらを Type I, Type II と呼ぶのは，誰が言い始めたのか筆者は知らないのだが，この業界では広く使われる用語になっている．

して，m の大きさに応じて和をうまく分けることによって，左辺第 3 項の和も Type I と Type II の組み合わせで表現できる．このようにして $S(\alpha)$ を Type I と Type II の組み合わせで表すことができるが，これは正に篩である．そして，Type I と Type II の和をいずれも上記のように評価して，補題 1 を導く，というのが Vinogradov の方針である．

Dirichlet の L 函数の零点を直接相手にしていると，いかにも素数ならでは，という感じがするのだが，この Vinogradov の議論には，その「素数ならでは感」があんまりない気がする．素数だから L 函数の零点なのであって，素数列がなんか他の数列に代わったらその議論は全く通用しないが，Vinogradov の方法は素数列でなくても Type I と Type II の組み合わせで表現できるものなら何でも同じである．もちろん素数だから篩をかけて Type I と Type II の組み合わせになるわけだが，素数でなくてももっと広いクラスの数列に対して通用する方法である．その意味では優秀であるわけだが．いずれにしろ，このようなかなり初等的な方法によって Vinogradov [19] は重要な補題 1 を証明したのである．

§3.5. 重みを von Mangoldt 函数にする場合.

上で circle method による議論を紹介する際，指数和 $S(\alpha)$ の定義として (3) を採用した．これは Vinogradov [19] に倣ったのだが，実は Goldbach 問題に circle method を使う際に (3) の $S(\alpha)$ が使われることは極めて稀で，Hardy-Littlewood [5] をはじめほとんどの人は von Mangoldt 函数 [9] $\Lambda(N)$ を重みにした指数和

$$T(\alpha) = \sum_{n \le N} \Lambda(n) e(n\alpha),$$

あるいはそれにちょっとした手を加えたものを，$S(\alpha)$ の代わりに使っている．どっちでも本質的な差があるわけではないが，von Mangoldt 函数を使う方がより直接的に解析的な道具を使えるという利点がある．その理由は，Riemann zeta 函数 $\zeta(s)$ に対し，s の実部が 1 より大きいとき，

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)} \text{ だが，} \sum_{p} \frac{1}{p^s} \text{ を } \zeta(s) \text{ で表すとそう綺麗にはなんないから}$$

という程度のことである．もっと具体的に言うと，$S(\alpha)$ に対して (6) を導くとき，

$$\sum_{\substack{n \le N \\ n \equiv b \ (\mathrm{mod}\ q)}} \Lambda(n) \text{ に対する explicit formula を } \sum_{\substack{p \le N \\ p \equiv b \ (\mathrm{mod}\ q)}} 1 \text{ に対する explicit formula に翻訳}$$

して使ってるので，$S(\alpha)$ でなく von Mangoldt 函数を重みとする $T(\alpha)$ のような指数和にしておくと，その翻訳の手間が省け，より直接的に L 函数の零点と結び付けられる．また，(6) の右辺で積分されているものにはどれも分母に $\log t$ が現れているが，von Mangoldt

[9] 自然数 n を割り切る素数がただ 1 つ p だけのとき，つまり $n = p^a$ (a は自然数) のときに $\Lambda(n) = \log p$, それ以外のときは $\Lambda(n) = 0$ と定義される数論的関数 $\Lambda(n)$ が，von Mangoldt 函数である．

函数を重みにするとその分母が消えて見た目にもきれいになって書く手間も楽になるのである．

$S(\alpha)$ の代わりに $T(\alpha)$ を使って上と同じような議論をすれば，もちろん $R(N)$ に対する漸近式が直接得られるわけではなく，(16) の代わりに

$$\sum_{n_1+n_2+n_3=N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) \ = \ \frac{1}{2}\mathfrak{S}(N)N^2 + O(N^2(\log N)^{-1}) \tag{17}$$

のような漸近式が得られることになる．言うまでもなく n が素数じゃなくても $\Lambda(n)$ が正の値をとることはあるから，(17) の左辺の和が正だからといって即 N は 3 つの素数の和とは言えないけれど，$\{n_1, n_2, n_3\}$ が素数でないものを含むような組からの (17) の左辺の和への寄与は $O(N^{3/2}(\log N)^3)$ といった評価がすぐに得られるので，やっぱり (17) からも，充分大きい奇数 N は 3 つの素数の和になることが分かるのである．さらに，$R(N)$ に対する漸近式 (1) を (17) から導くことも，至極簡単な作業である．

言ってみれば，素数の 2 乗，3 乗，$\cdots$ というノイズをどこかで除去する必要があるが，それを (6) のような circle method の計算の途中でやるよりも，(17) まで到着してから最後の最後にやる方が，全体として楽なのだ．$S(\alpha)$ より $T(\alpha)$ の方が採用されることが多いのはそのためである．因みに，Helfgott [6] も von Mangoldt 函数を重みに採用している．

では，Vinogradov [19] はなぜ $T(\alpha)$ ではなく，敢えて $S(\alpha)$ を選んだか，と言うと，繰り返しになるが，その論文における彼の主目的が補題 1 の証明にあったからであろう．そのために指数和を Type I や Type II の 2 重和の組み合わせに分解する必要があるが，$S(\alpha)$ ならその部分は篩で簡単にできる．だから彼は $T(\alpha)$ ではなく $S(\alpha)$ を選んだ．

$T(\alpha)$ を選んだら，そういう分解はどうするか? $T(\alpha)$ でも $S(\alpha)$ でも似たようなものだから，$T(\alpha)$ についても同様に分解できるのは当たり前と言えばそうだし，実際いろいろやり方はあるだろうが，非常にスマートな方法を Vaughan [17] が見つけた．

$$F(s) = \sum_{n\le U} \Lambda(n)n^{-s}, \qquad G(s) = \sum_{n\le U} \mu(n)n^{-s} \qquad \text{とおいて，}$$

$$\Big(-\frac{\zeta'(s)}{\zeta(s)} - F(s)\Big) = G(s)\big(-\zeta'(s)\big) - F(s)G(s)\zeta(s) - (\zeta(s)G(s)-1)\Big(-\frac{\zeta'(s)}{\zeta(s)} - F(s)\Big)$$

という恒等式の両辺を Dirichlet 級数で書いたときの係数を比較すると，$n > U$ なら

$$\Lambda(n) = \sum_{\substack{mk=n\\ m\le U}} \mu(m)\log k \ - \sum_{\substack{mkl=n\\ m\le U,\, k\le U}} \Lambda(m)\mu(k) \ - \sum_{\substack{mk=n\\ m>U,\, k>U}} \Big(\sum_{\substack{d|m\\ d\le U}} \mu(d)\Big)\Lambda(k).$$

Vaughan の恒等式と呼ばれるこの $\Lambda(n)$ の表示を $T(\alpha)$ の定義式に代入する ($n \le U$ のと

ころは何もしない) と，$T(\alpha) = T_0(\alpha) + T_1(\alpha) - T_2(\alpha) - T_3(\alpha)$ となる，ここで，

$$T_0(\alpha) = \sum_{n \le U} \Lambda(n) e(n\alpha), \qquad T_1(\alpha) = \sum_{m \le U} \mu(m) \sum_{k \le N/m} e(mk\alpha) \log k,$$
$$T_2(\alpha) = \sum_{r \le U^2} a_r \sum_{l \le N/r} e(rl\alpha), \qquad T_3(\alpha) = \sum_{U < m \le N/U} b_m \sum_{\substack{k \le N/m \\ k > U}} \Lambda(k) e(mk\alpha),$$

ただし，

$$a_r = \sum_{\substack{mk=r \\ m \le U,\, k \le U}} \Lambda(m)\mu(k), \qquad b_m = \sum_{\substack{d|m \\ d \le U}} \mu(d). \tag{18}$$

$U = N^{1/3}$ とでもすると，$T_0(\alpha)$ は自明に $O(N^{1/3})$ で，無視して良い．$T_1(\alpha)$ は内側の k についての和に $\log k$ があるがこれは 1 みたいなものだから (partial summation で外せる)，$T_1(\alpha)$ は実質的に Type I，$T_2(\alpha)$ は正に Type I，$T_3(\alpha)$ は m についての和を $M < m \le 2M$ という形に分けることで，$O(\log N)$ 個の Type II の和に分解できる．ま，$M < m \le 2M$ という形にこだわらなくてもいいんだが，いずれにしろ $\Lambda(n)$ を重みにした指数和は Vaughan の恒等式によって簡単に Type I，Type II の 2 重和に分解することができ，するとあとは Vinogradov がやったようにして，補題 1 と同等の評価を得ることができるのである．

§ 3.6. 明確な誤差項評価.

具体的な数値の大きさはともかく，circle method で定理 1 のような明確な結果を証明することは可能だが，そのためにはこの節で紹介した議論に沿って計算する際，全ての誤差項の評価を明確にしなければならない．その誤差項を大きく分けると，§3.2 に書いた major arcs の計算から生じるものと，§3.3 に書いた minor arcs の寄与の評価の，2 種類がある．後者は，補題 1 と (14) の組み合わせだが，§3.4 や §3.5 に書いた通り，補題 1 は L 函数の零点等とは無関係にかなり初等的に証明できるもので，その計算を全て明確に実行するのは，わりと簡単ではある．(14) の方は，普通 $\pi(N)$ で表される，N 以下の素数の個数を上から評価するだけでいいから，素数定理が証明されるより前の Chebyshev の初等的な方法でも充分で，自分の手で計算するとしてもそれほどの苦労なく結構良い評価が得られるものである．それに $\pi(N)$ なら詳しい研究もたくさんあって，自分でやんなくても誰かがやってくれた結果を引用してすませることもできる．よって，minor arcs の寄与に対する評価 (15) において $\ll$ で省略されていた定数を明確に計算することは，それほど大変ではない．

一方の major arcs の計算はどうだったか振り返ってみると，こっちも (8) まで来てしまえば，あとはそれほど大したことない作業なのだが，その (8) に至るまでには (6) にある L 函数の零点の相手をしなければならない．L 函数の zero free region とか零点密度評価とか Siegel zero に関することとか，いろんなことがあるが，解析的手法で得られるそういう結果を全部明確に計算し直さなければならないのである．$R(N)$ に対する漸近式

(16) における誤差項の評価を明確にするには，その部分が最大の障壁となる．ただ大変，計算しなくちゃいけないことが多くて面倒，というだけなら，頑張ってやればいいだけのことだが，そうやって頑張って得られた結果が — 自分でやったこともないくせに他人様の結果にこういうことを言うのもなんですが — まあ，やっぱりどうしても，そんなにいいってわけにはいかない…んでしょうかね．

結局，我々が L 函数の零点について分かってることはそれだけ少ない，ということであろう．Zinoviev [20] が示した定理 4 にあるように，GRH を仮定すれば $V = 10^{20}$ を得られるが，その 5 年後の Liu-Wang [12] の unconditional な結果は $V = e^{3100}(\fallingdotseq 10^{1346})$ であった．これら 2 つの数値の大きな隔たりは，現状で L 函数の零点を unconditional に扱うことがどれだけ大変かを如実に表していると言えよう．逆に，そういう V の値に当たるようなものを具体的に問うことさえしなければ，つまり「ある定数 V 以上のやつは OK」という言い方をしている限りにおいては，零点の分布をはじめ L 函数の解析的性質についてこういう加法的問題への応用に必要な程度のことは一応分かっている，と言うこともできる．

§ 4. Helfgott の仕事．

Helfgott [6] の定理 1 の証明は，§3 で紹介した Vinogradov の議論と基本的な構造は同じである．そこに加えられた Helfgott のアイディアや様々な工夫のうち，筆者が主要と思うものを本節で紹介する．

§2.3 で紹介した通り，GRH の下では ternary Goldbach 予想は完全に解決している．だから GRH を証明できれば，話は早い，けれど，それも難しい．ところで元々の Riemann 予想は“ある高さまで正しい”，あるいはもう少し具体的に，“Riemann 予想は 10^{11} の高さまで正しい”，とか，そういったことをお聞きになった方はいらっしゃるだろうか．例えば後者は，厳密に言えば，Riemann zeta 函数 $\zeta(s)$ の零点のうち，虚部が正で 10^{11} 以下のものの実部は全て $\frac{1}{2}$ である，というような主張である．そういうことはコンピューターを使った計算で確認できるのである．そもそも Riemann 自身が $\zeta(s)$ の非自明零点を虚部の絶対値が小さい方から 3 つほど手で計算していた，というのは有名な話であろう．それを計算で確認した Riemann は思わず，現代の日本語に訳せば「ちょーやべー，これぜんぶ 2 分の 1 なんじゃね?」というような主旨のことをドイツ語でおっしゃった，のではないかと思う [10]．それが後年 Riemann 予想と呼ばれるものの出自のようだが，いずれにせよ，$\zeta(s)$ でできるということは，1 つの L 函数に対しても同じことはできるだろうし，1 つでできるということは，2 個でも 3 個でも，100 個でも 1000 個でも，ある程度の個数ならできるはず，である．

Platt はこれを実行し，複素変数 s の虚部を t，Dirichlet 指標 χ の法を q で表すとき，

30 万以下の奇数の q に対しては，$|t| \le 10^8/q$,
40 万以下の偶数の q に対しては，$|t| \le \max\{10^8/q,\ 200 + 7.5 \cdot 10^7/q\}$,

[10] 根拠はないが．

という範囲で，全ての L 函数 $L(s,\chi)$ に対する一般 Riemann 予想は“正しい”こと，即ちそういう範囲の L 函数の所謂非自明零点の実部は全て $\frac{1}{2}$ であること，を確認した．この結果について書いた Platt の論文は Helfgott の preprint[6] の参考文献として挙がってないので，その時点ではまだ発表されてなかったのだろうが，Platt は学位論文 [15] では $q \leq 10^5$, $|t| \leq 10^8/q$ の範囲まで GRH が正しいことを確認しており，Helfgott の仕事 [6] との関係でそれを上記の範囲まで拡げた，と [6] の Introduction に書いてある．たぶん Helfgott が Platt に出来るだけ拡げるよう求めたのだろう．いずれにせよ，この結果を Helfgott [6] は使った．

定理 4 の通り，Zinoviev [20] は GRH が正しければ $V = 10^{20}$ とできることを示した．有限とは言え結構広い範囲で GRH が正しいことが確認できれば，10^{20} にそれなりに近い V の値を得ることができるはずである．

Deshouillers-Effinger-te Riele-Zinoviev [4] や Saouter [16] から 15 年程たち，コンピューターでのチェックが 10^{30} くらいまでは届くようになっていることを Helfgott は分かっていて，想像だが，恐らく彼はそのくらい以上の奇数が全て 3 つの素数の和になることを証明しようと思い，それを実現したのだろう．しかし ternary Goldbach 予想を完全に解決するだけなら，10^{30} 以上の奇数「全て」を相手にする必要はない．e^{3100} まででいいのだ．それを超えたところはもう Liu-Wang [12] が確認している．そして GRH が正しければ Zinoviev [20] の計算が 10^{20} 以上で通用する．とくに e^{3100} までの奇数に限るなら，Zinoviev [20] の計算に現れる L 函数の零点も有限個であり，完全な GRH は必要ない，有限であっても充分広い範囲で GRH が確認できればそれで事足りるのである．

尤も，有限な範囲で確認すれば充分，という言い方をするなら，元々有限な範囲の奇数をチェックするだけで充分だったわけで，それぞれのチェックがどれだけ大変なことか，どれだけの時間を要することなのか，という比較について論じなければ無意味だが，筆者にはそういう感覚 (能力) がないから，たぶん §2.4 の (II) の C を e^{3100} くらいまで大きくすることと比べて，上記の範囲における Platt の GRH の確認に必要な計算量は恐らく圧倒的に少なくて済む，ということなのだろう，と想像するのみである．もしかしたら，そういうこと — ある限界までの奇数が 3 つの素数の和になることを直接調べるより，GRH の確認をする方がずっと楽で効率が良いこと — に気付いたことが，今回の Helfgott の仕事の要点の 1 つであると言えるのかもしれない．いずれにせよ，Helfgott の定理 1 は，Liu-Wang [12] の e^{3100} を 10^{30} まで小さくしたわけだが，その著しい改良の一番の原動力となったのは，上記の範囲で GRH を確認した Platt の結果であると言えよう．

話が脇道にそれるが，個人的には Platt の検査で，実部が $\frac{1}{2}$ じゃない L 函数の非自明零点が見つかったら面白かったのに，という不謹慎な感情もちょっとある．もしそんなことがあったら，否定的に GRH は解決するわけで，ternary Goldbach 予想解決どころじゃない大騒ぎになったことだろう．因みに，もし本当にそうだったら Helfgott の仕事 [6] はおじゃんだったかと言うと，そういうことではない．まあ，実部が $\frac{1}{2}$ から外れた非自明零点が 100 個も 1000 個もあったら大変だったろうが，2 個とか 5 個くらいなら，手間は掛かるが，それらの零点の影響を精密に記述すれば定理 1 の結果にはあんまり大き

な影響はなかっただろうと思う．今回の Helfgott の仕事のためには，L 函数の零点の位置が充分広い範囲で正確に分かればいいわけである．しかし，それにしてもそれだけ多くの L 函数に対してそれだけ広い範囲を調べて，GRH に反する零点が 1 つもないというのは，なんか不思議，という感じすら覚える．GRH は正しいから，と言えばそれまでだが，証明できない現状では，ただ感嘆するのみである．

話を戻そう．Helfgott の証明において，その影響が一番大きいとは言え，しかしその Platt の結果が全てではない．それ以外にも，様々な工夫が Helfgott の仕事には含まれている．まず，上の Platt の結果だけで §3.2 に書いたような major arcs の計算を済ませるために必要となる工夫について述べるが，そのために，§3.2 における $Q=(\log N)^A$ という設定を反故にして，任意のパラメーター $Q\,(\geq 1)$ に対して §3.2 の冒頭のように major arcs $\mathfrak{M}$ と minor arcs $\mathfrak{m}$ を定義し，それらの Q への依存を強調してここではそれぞれ $\mathfrak{M}(Q)$, $\mathfrak{m}(Q)$ と書くことにしよう．とくに，距離が Q/N 以下の範囲に分母が Q 以下の分数がないような $\alpha\in(0,1]$ の集合が $\mathfrak{m}(Q)$ である．

§3.2 に書いたような方法で普通に $\mathfrak{M}(Q)$ の寄与を計算しようとすると，法が Q 以下の Dirichlet 指標に対する L 函数達の零点が関与するから，そこを Platt による GRH の検証結果だけで済ませようとすると，Q は精々30 万程度の大きさに抑えなければならない．ところが，Q が有限だと，§3.3 のような方法で minor arcs の寄与に対する充分な評価が得られないのだ．

このことを認識するには，補題 1 において $\mathfrak{m}=\mathfrak{m}(Q)$ が Q に依存していることに注意する必要がある．Vinogradov [19] はこうは書いていないが，その議論を直接たどると，

$$\sup_{\alpha\in\mathfrak{m}(Q)}|S(\alpha)|\ll NQ^{-1/3}(\log N)^2+N(\log N)^{-A}$$

という評価が得られる [11]．ここで $Q=(\log N)^A$ とすれば正に補題 1 だが，Q を例えば 30 万などと有限値にすればこれは自明な評価 $S(\alpha)\ll N(\log N)^{-1}$ より悪い．これは Vinogradov の結果自体が弱い，というようなことではない．実は，$|S(\alpha)|\gg N(\log N)^{-1}Q^{-1}$ となるような $\alpha\in\mathfrak{m}(Q)$ がある．このことは，(6) において，右辺第 1 項が $S(a/q+\beta)$ の主項となる状況を想定すれば納得されよう．従って $Q\ll 1$ だと，$\mathfrak{m}(Q)$ 上で $|S(\alpha)|$ は本当に $N(\log N)^{-1}$ のオーダーまで大きくなることがある．(14) の方はほとんど等式だから，(15) のようにして $\mathfrak{m}(Q)$ 上の積分に対する充分な評価を得るためには，$\mathfrak{m}(Q)$ 上で $|S(\alpha)|<cN(\log N)^{-2}$ となる小さい正定数 c が存在するような状況でなければならず，よって Q が有限値だとまずい．この点では，N と共に大きくなるように Q を設定しなければならないのである．

そのため Helfgott [6] は，雑に言って [12]，Q を $N^{0.275}$ 程度の大きさとしたときに対応

[11] Vinogradov としてはそれ以上の必要はなかったが，もっと気を使えば $Q^{-1/3}$ を $Q^{-1/2}$ にするとか，右辺第 2 項の $N(\log N)^{-A}$ をもっと小さくするといった改良ができる．

[12] 本稿の major arcs, minor arcs の定義は Vinogradov [19] に倣ったもので，それで良ければその方がちょっと楽だったりするのだが，普通は $\mathfrak{M}(q,a)$ の定義に現れている条件 $|\beta|\leq Q/N$ を，$|\beta|\leq Q/(qN)$ という形にする．Helfgott [6] も後者のようないわば普通の形を採用しているため，このあたりの本稿の記述は，そういう意味では厳密ではない．

する minor arcs $\mathfrak{m}(Q)$ に対して，(15) のような評価をしている．一方の major arcs $\mathfrak{M}(Q)$ の方では Q を 30 万程度に抑えたいわけだから，そこにギャップが生じる．

そういう状況は，実は circle method の応用の際に間々生じるもので，そのギャップの部分を評価する作業は major arcs の pruning と呼ばれる．Helfgott [6] は large sieve を用いて pruning に当たる手続きを行っているが，Goldbach 問題への応用で pruning をしたのはこの論文 [6] が初めてのはずである．

次に，補題 1 に当たる評価について，方針は §3.4 や §3.5 に記した通りだが，ここでも Helfgott は大変な労力を払って数値的に良い評価を導いている．このために [6] とは独立した論文 [7] が 1 編丸々費やされている．これに関わる Helfgott の工夫のうち，最も目立つものを 1 つ挙げる．(18) で定義される b_m に対し，その重みを含む指数和 $T_3(\alpha)$ がその (18) の 2 行上で定義されているが，その $T_3(\alpha)$ を評価する際，§3.4 に記した Type II の和の評価の方法を適用して，

$$|T_3(\alpha)| \le \left(\sum_{U<m\le N/U} |b_m|^2\right)^{\frac{1}{2}} \left(\sum_{U<m\le N/U} \left|\sum_{U<k\le N/m} \Lambda(k)e(mk\alpha)\right|^2\right)^{\frac{1}{2}}$$

とし，さらにこの右辺の第 2 因子の方について，k についての和の 2 乗を展開して m についての和を内側に入れることによって評価を得るのであった．このとき，右辺の第 1 因子の方にある $|b_m|^2$ の和に対しては，Möbius 函数を自明に $|\mu(d)| \le 1$ と潰して，

$$\sum_{U<m\le N/U} |b_m|^2 \le \sum_{U<m\le N/U} \left|\sum_{d|m} 1\right|^2 \ll NU^{-1}(\log N)^3$$

などと評価するのが普通である．ここを Helfgott [7] は，b_m の定義 (18) をそのまま残し，

$$\sum_{U<m\le N/U} |b_m|^2 = \sum_{U<d_1\le N/U,\, U<d_2\le N/U} \mu(d_1)\mu(d_2) \sum_{\substack{U<m\le N/U \\ m\equiv 0 \pmod{d_1} \\ m\equiv 0 \pmod{d_2}}} 1$$

と変形して計算を進め，Möbius 函数の振動による打ち消し合いの効果を引き出している．このような様々な計算上の努力を重ね，補題 1 のような，minor arcs 上での指数和の絶対値に対する良い評価を得ているのである．

Helfgott [6] の工夫を，あともう 1 つ紹介したい．それは，(3) のような指数和を定義する際，最終的な数値の結果が良くなるように注意深く選んだ重みを付ける，ということである．実際，(3) の代わりに Helfgott [6] が使う指数和は，

$$S_f(\alpha) = \sum_{n=1}^{\infty} \Lambda(n)e(n\alpha)f(n)$$

という形で，ここで函数 f はとりあえず常に 0 以上の値をとり，その無限和の収束を保証するもの，としておく．この重みの函数 f をうまく選ぼうというわけである．

例えば，$n \le N$ のとき $f(n)=1$, $n>N$ なら $f(n)=0$ とすれば，$S_f(\alpha)$ は我々が §3.5 で $T(\alpha)$ と書いたものに他ならない．このように N のとこでバチッと不連続に切るのではなく，n が N くらいを超えたら滑らかに，しかしそれなりに素早く 0 に近づくような函数 f を使う方が，誤差項の評価が良くなる，といったようなことは解析的整数論ではよくみられることで，こういうアイディア自体は昔からあった．Goldbach 問題に関する論文で言えば，Linnik [11] や Zinoviev [20] が $f(n)=e^{-n/N}$ に対する指数和 $S_f(\alpha)$ を使っている．

Helfgott [6] は，非常に雑に言うと $f(n)=e^{-(n/N)^2}$ のような選択をするのだが，これは n が N を超えてから 0 に近づくスピードが Linnik [11] らの $f(n)=e^{-n/N}$ よりも明らかに早い．Helfgott はそれに複雑に手を加えたような 2 つの函数 f_1, f_2 を用意し，(5) の左端の積分の代わりに，

$$\int_0^1 S_{f_1}(\alpha)S_{f_2}(\alpha)^2 e(-N\alpha)\,d\alpha$$

を考察する．そしてこの積分を circle method で計算し，$\Lambda(n)$ が含むノイズを消去し，

$$\sum_{p_1+p_2+p_3=N}(\log p_1)(\log p_2)(\log p_3)f_1(p_1)f_2(p_2)f_2(p_3)$$

という形の和が，10^{30} 以上の奇数 N に対しては正であると証明することにより，定理 1 を導く．その際 minor arcs の寄与を，(15) のように，

$$\left|\int_{\mathfrak{m}} S_{f_1}(\alpha)S_{f_2}(\alpha)^2 e(-N\alpha)\,d\alpha\right| \le \sup_{\alpha\in\mathfrak{m}}|S_{f_1}(\alpha)|\int_0^1 |S_{f_2}(\alpha)|^2\,d\alpha \tag{19}$$

と評価する．つまり，f_1 は，minor arcs 上での $|S_{f_1}(\alpha)|$ の評価に都合がいいように，f_2 は (14) のような $|S_{f_2}(\alpha)|$ の 2 乗平均に対する評価に都合がいいように — もちろん f_1 と f_2 は major arcs の寄与にも影響するから，そっちとの兼ね合いを考慮して — うまく選ぶ，というわけである．実際に選ばれた f_1 と f_2 を見ると，奇数 N に対する $N=p_1+p_2+p_3$ という 3 つの素数の和による表示のうち，p_1 は大体 $N/100$ あたりの小ささで，p_2 と p_3 は $N/2$ よりちょっと小さいくらい，といったような表示を効率的にカウントするような重みになっている．Helfgott は minor arcs の寄与を (19) のように評価することと major arcs の寄与との兼ね合いから，そのような N の表示を重視するのが得であると看破し，その思想の下で恐らくはある程度の試行錯誤をした末に，f_1 と f_2 を決めたのであろう．

Helfgott の f_1 と f_2 の定義は複雑なので，これ以上のことをここに書く意味は無いとは思ったが，何も書かないと気になさる方もあるだろうし，[6] を読んでも簡単にはそれらの定義が見えないので，ご参考までに書くだけ書いておく：

$$f_1(n)=4\int_0^\infty y^2e^{-y^2/2}\cdot\max\Bigl\{\log 2-\Bigl|\log(49(2+1/(36\sqrt{2\pi}))n/(Ny))\Bigr|,\,0\Bigr\}\,dy,$$

$$f_2(n)=e^{-\frac12\left((2+1/(36\sqrt{2\pi}))n/N\right)^2}\int_0^{2N/\left((2+1/(36\sqrt{2\pi}))n\right)} h\bigl((2+1/(36\sqrt{2\pi}))ny/N\bigr)\frac{\sin(200\log y)}{\pi y\log y}\,dy,$$

ただし，$h(t) = t^3(2-t)^3e^{t-1/2}$.

この節では，§3 に記した基本的な circle method の証明に Helfgott [6] が加えた工夫について，全てではないが，筆者が主要と思うものを列挙した．整理すると，次の 4 点である：

1. 有限な (しかし広い) 範囲で“ GRH の成立 ”を確認した Platt の結果を利用する．
2. Large sieve に基づく pruning を実行する．
3. Vaughan の恒等式の応用の際，従来より手の込んだ扱いをすることにより，minor arcs 上での指数和の評価に関して強い結果を導く．(Helfgott [7])
4. Circle method の議論を注意深く観察して重みを選び，それを指数和の定義に導入する．

§ 5. 終わりに.

Helfgott の仕事 [6] について筆者が紹介するとすれば，以上のようなことになる．

18 世紀の中頃に発生した ternary Goldbach 予想は，1937 年に本質的に解決し ([19])，20 世紀末には GRH の下で条件付きの解決 ([20], [4], [16])，そしてとうとう本当に完全に解決した ([6])．私事だが，筆者の父・邦雄は，[19] が出版された 1937 年の 10 月 14 日に生まれ，プレプリント [6] が流布する少し前，2013 年 4 月 1 日 [13] に他界した．Ternary Goldbach 予想の本質的解決から完全解決まで，ちょうど 1 人の人間の一生分の時間が掛かったわけである．

この研究集会のプログラム委員をされていた富山大学の木村巌先生や，研究代表者をされた大阪大学の落合理先生から，「Helfgott さんの今回のブレークスルーについて説明をお願いしたい」という主旨のご連絡を電子メールでいただき，話をさせていただくことになったのだが，なんとなくそういう文面から自分の感覚との温度差が感じられて，お引き受けして良いか，実はちょっと躊躇した．そういうブレークスルーを期待されているのなら，自分が話をするとがっかりさせることになるんじゃないか，という不安を感じたのである．

何をもって「ブレークスルー」と言うかは，人によって多少違い得るだろうが，ternary Goldbach 予想の完全な解決までの歴史を振り返って，その言葉が最も相応しいのは Hardy-Littlewood の仕事 [5] であろう．それまで全く攻撃手段がなかったところに，circle method という方法を与えたのであって，ternary Goldbach 問題は発生から 180 年経って，その

[13]「あなたのお父さんが亡くなりました」とエイプリルフールに聞いても，なかなかすぐには信じられないものである．選べるものじゃないんだろうが，自分の命日は違う日にしたい．父は文系の人間で，和文英訳の仕事などをしていて，もちろん数学は素人だったが，筆者が幼い頃，父が数理パズルの類の問題を多く提供してくれたのがとても楽しかったことを良く覚えている．父自身は筆者に，数学ではなくもっと直接世の中と関係する実学の道に進んでほしかったようだったが，今こうして数学を生業にしているのは父との幼なかった頃の交流の影響は大きいと思う．ここに記し，謝意を表させていただく．

論文 [5] からやっと研究が始まったのである [14]．Vinogradov [19] の仕事は，コロンブスの卵という言葉が正にぴったりだと思うが，コロンブスの卵というのもブレークスルーの一種と言えよう．

今回の Helfgott の仕事は，コンピューターによる GRH の検証結果を中心に，数多くの工夫を積み重ねた大仕事であって，その結果 ternary Goldbach 予想をついに完全な解決に導いた歴史的な偉業である．しかし，ブレークスルーという言葉は似合わないと筆者は思う．

さて，Vinogradov 定数という言葉があって，今回本文中には使わないようにしようと思っていたのだが，使った方が分かりやすい場面もあるような気もして迷った末，結局途中で中途半端に使ってしまった．使わないようにしようと思ったのは，その「定義」を表現するのが難しいと思ったからである．数学用語じゃなく厳密な定義があるわけではない，と開き直る手もあるが，例えばちょっと前までは

(20) 「V 以上の奇数が全て 3 つの素数の和で表せる」

という命題が真となるような V の値，あるいはそういう V の最小 (整数) 値，といったあたりが Vinogradov 定数の定義と認識されていたんじゃないかと思う．それで問題なかったわけだが，じゃあ ternary Goldbach 予想が解決した現在は，$V = 7$ を Vinogradov 定数と言うか，というと，別にそう言っても悪いわけじゃないが，心情的にはそうは言わないように思う．

Vinogradov 定数とは，まだ ternary Goldbach 予想が完全に解決する前は，circle method で命題 (20) を証明できるような V の値であって，そこまでコンピューターでチェックできれば ternary Goldbach 予想が完全に解決する，という目標となる数値だった．例えば Liu-Wang [12] は Vinogradov 定数として e^{3100} を得た，といった言い方がされていた．そういう意味では，ternary Goldbach 予想が完全に解決した後は，もはや Vinogradov 定数という用語は無意味になった，と思うが，今敢えて Vinogradov 定数はいくつかと言えば，定理 1 より 10^{30} がそれ，ということになるだろうか．しかし筆者はこれにも同意し難い．

これまでの Vinogradov 定数と言えば，気分的には命題 (20) が成立することを，自分で計算して確かめたと思えるような，そういう V の値であったのだ．とは言っても，実はこれまでの仕事でも結構コンピューターは使われていた．例えばへんてこな積分に対する出来るだけ正確な上界を得たいのでコンピューターを使って近似値を計算，というようなことは間々あった．しかし，うまく言えないのだが，それでもなんとなく自分で計算して (20) を確認出来るような気がしていたのである．それが，Helfgott の定理 1 は最早自分で確認するのは無理，と思う．Platt による GRH の確認の結果を使うからである．

もし「コンピューターとプログラムが進歩したんで，7 から e^{3100} までの奇数を全部チェックできまして，ternary Goldbach 予想が正しいことが確認されましたよ」と言われたら，自分では確認できないし,「ああ，そうですか」と納得するだけだったし，その予想

[14] §2.5 に書いたが，binary Golbdach 問題に関しては Brun の仕事があり，それは [5] より少し早い．

解決に関する解説を筆者がすることにはならなかったように思う．今回の Helfgott のプレプリントを見て感じたのは，それと似たような感覚である．筆者には自力だけで完全に確認することができないものだ，ということである．

これまでは，(20) の証明は人間がするもの，V 以下の奇数に対するチェックはコンピューターに確認してもらうもの，と別れている意識があったが，Helfgott の今回の仕事は，その境界にあるような感じと言えよう．

定理 1 の証明のためには，[6]，[7]，それと Platt の GRH のチェックの論文が必要だが，プレプリント [6] は 133 ページ [15]，[7] は 79 ページと，大変な量である．Goldbach 問題は ternary の方は解決し，binary の方が依然大問題として残っているが，解決した ternary の方についても，証明の簡略化に向けた努力があって良いと思う．

最後に，こういう機会を下さいましたこの研究集会の世話人の皆様に，厚く御礼申し上げます．また，世話人の方々，並びに査読をしてくださった方から，この拙文の原稿に対して有益なご意見をいただきましたので，ここに記し，感謝申し上げます．

References

[1] Borozdkin, K. G., On I. M. Vinogradov's constant, (in Russian) in: *Proc. 3rd All-Union Math. Conf., Izdat. Akad. Nauk SSSR, Moscow*, **1** (1956), 3.

[2] Chen, J.-R. and Wang, T.-Z., On odd Goldbach problem, *Acta Math. Sinica*, **32** (1989), 702–718.

[3] Davenport, H., *Multiplicative Number Theory*, 2nd ed., Springer-Verlag, New York, 1980.

[4] Deshouillers, J.-M., Effinger, G., te Riele, H. and Zinoviev, D., A complete Vinogradov 3-primes theorem under the Riemann hypothesis, *Electr. Res. Ann. Amer. Math. Soc.*, **3** (1997), 99–104.

[5] Hardy, G. H. and Littlewood, J. E., Some problems of 'partitio numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.*, **44** (1923), 1–70.

[6] Helfgott, H. A., Major arcs for Goldbach's problem, preprint; arXiv:1305.2897.

[7] Helfgott, H. A., Minor arcs for Goldbach's problem, preprint; arXiv:1205.5252.

[8] Helfgott, H. A., The ternary Goldbach conjecture is true, preprint; arXiv:1312.7748.

[9] Helfgott, H. A. and Platt, D, Numerical verification of ternary Goldbach, preprint; arXiv:1305.3062.

[10] Landau, E., Gelöste und ungelöste Probleme aus Theorie der Primzahlverteilung und der Riemannschen Zetafunktion, *Proceedings of the fifth International Congress of Mathematicians*, Cambridge, **1** (1912), 93–108.

[11] Linnik, Ju. V., A new proof of the Vinogradov–Goldbach theorem, *Mat. Sbornik.*, **19** (1946), 3–8.

[12] Liu, M.-C. and Wang, T.-Z., On the Vinogradov bound in the three primes Goldbach conjecture, *Acta Arith.*, **105** (2002), 133–175.

[13] Lucke, B., Zur Hardy-Littlewoodschen Behandlung des Goldbachschen Problems, *Doctoral Dissertation*, Göttingen, 1926.

[15] §1 で定理 3 の後に記した通り，これは [6] の初版のページ数である．その初版は [6] と [8] の 2 つに分割されたようで，2014 年 5 月の時点では [6] も [8] も 79 ページである．[6], [7], [8] がどれも 79 ページとなったのは偶然か，それとも Helfgott 氏のこだわりだろうか．79 は素数である．

[14] Oliveira e Silva, T., Herzog, S. and Pardi, S., Empirical verification of the even Goldbach conjecture, and computation of prime gaps, up to $4 \cdot 10^{18}$, *Math. Comp.*, **83** (2014), 2033–2060.

[15] Platt, D., Computing degree 1 L-functions rigorously, *PhD thesis*, Bristol Univ., 2011.

[16] Saouter, Y., Checking the odd Goldbach conjecture up to 10^{20}, *Math. Comp.*, **67** (1998), 863–866.

[17] Vaughan, R. C., An elementary method in prime number theory, in: *Recent progress in analytic number theory*, edited by Halberstam, H., and Hooley, C., Academic Press, 1981, 341–348.

[18] Vaughan, R. C., *The Hardy-Littlewood Method*, 2nd ed., Cambridge University Press, 1997.

[19] Vinogradov, I. M., Representation of an odd number as a sum of three primes, *C. R. Acad. Sci. URSS*, **15** (1937), 6–7.

[20] Zinoviev, D., On Vinogradov's constant in Goldbach's ternary problem, *J. Number Theory*, **65** (1997), 334–358.