素数と概素数の 3 乗の和について.

Joint work with Lilu Zhao (Shandong University).

Koichi Kawada （川田 浩一）
Faculty of Education, Iwate University
(岩手大学 教育学部)

1. 序 〜 Waring-Goldbach 問題の 3 乗の場合.

Waring-Goldbach 問題とは，自然数を素数のべき乗の和で表すことに関わる様々な問題の総称だが，その基本的な問題意識の 1 つは，例えば「10 個の素数の 3 乗の和」などと形を指定したとき，“その形” で表せない自然数はこれこれですべて，それら以外は全部 “その形” で表せる，ということを決定したい，という欲求である．3 乗数の Waring-Goldbach 問題の場合，その方向に寄与する歴史上初めての結果は次の定理である．

定理 1 十分大きい奇数はすべて 9 個の素数の 3 乗の和で表せる．

筆者は，Hua[4] がこの定理を証明した，という記述をどっかで見た気がして，自分自身も論文や過去の数理研講究録等でもそう書いたことがあったが，Brüdern さんに指摘されて確認したら，[4] にはその定理は記されていなかった．すいません *．

ただ，十分大きい奇数が 3 つの素数の和で表せることを証明した I. M. Vinogradov の有名な仕事 (1937 年) と，Waring 問題における基本的な道具の 1 つである Hua の補題 (1938 年) があれば，circle method によって定理 1 が証明できることは自明と言ってよい．そのため 1938 年の論文 [4](タイトルもいかにもそれらしい) で Hua が定理 1 を証明してるんだろう，といった誤解も生じたんだろうし，筆者が探してもその定理 1 を証明した論文を見つけられなかったのは 1938 年より後にはそれをわざわざ論文として書く意義がなかったからなのだろうと思う．その証明が記された初めての文献は，筆者が調べたところ，Hua がロシア語で書いて 1947 年に

*謝って済む問題ではないかもしれませんが….

当時のソビエト連邦で出版された本だったようだ．筆者はその本自体を実際に見たことはないが，1965 年にアメリカ数学会から出版されたその本の英語版 [5] には定理 1 の証明が書かれている†．

さて，定理 1 により，ある自然数 C 以上の奇数は 9 個の素数の 3 乗の和となる．すると自然数 n が $(C+27)$ 以上なら，$n-2^3$ も $n-3^3$ も C 以上でどっちかは奇数だから，どっちかは $=p_1^3+\cdots+p_9^3$ と 9 個の素数の 3 乗の和として表せるので (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)，

$$n=2^3+p_1^3+\cdots+p_9^3 \quad \text{または} \quad n=3^3+p_1^3+\cdots+p_9^3$$

ということになって，つまり $(C+27)$ 以上の自然数はすべて 10 個の素数の 3 乗の和となることがわかる．あとはその C の値を計算して (原理的にはできる…実際にやんのはすんごく大変だろうが)，$(C+26)$ 以下の有限個の自然数について調べれば (これも原理的にできるのは自明，もちろん現実的には別問題だが)，10 個の素数の 3 乗の和で表せない自然数を完全に特定でき,「10 個の素数の 3 乗の和」については上記の "欲求" が満たされることになる．10 個でできれば，11 個，あるいはそれより多い個数の素数の 3 乗の和についても同様のことができることは言うまでもない．

ということで，定理 1 が本質的に得られた 1938 年以降，9 個の素数の 3 乗の和で表せない自然数を特定することが，3 乗数の Waring-Goldbach 問題に関する次の大きな目標の 1 つとなった．もちろん定理 1 により奇数の方は本質的に解決してるから，偶数の方を考えるわけだが，偶数 n が 9 個の素数の 3 乗の和となるとすると，その 9 個の素数が全部奇数というわけにはいかないから，9 個のうちの少なくとも 1 つの素数は偶数でなければならない．が，偶数の素数は 2 しかないから，結局 $n-2^3$ という偶数が 8 個の素数の 3 乗の和になるかどうかを考えることになる．そして，次の予想を証明することが，実質的に 1938 年以後，大きな目標の 1 つとなっている；

予想 1.　十分大きい偶数は 8 個の素数の 3 乗の和として表せるだろう．

十分大きい奇数だって恐らく 8 個の素数の 3 乗の和だろうが，前段落の考察と同様に，奇数 n が 8 個の素数の 3 乗の和であることは $n-2^3$ が

---

†[5], Chapter VIII, §5, Corollary 3 が本稿の定理 1．その本 [5] の original form がロシア語で書かれ 1947 年に出版されたことは FORWARD にあり，さらに PREFACE ORIGINALLY INTENDED FOR THE RUSSIAN EDITION の脚注には，1941 年に原稿は編集部に送られていたが戦争の影響で出版が遅れた，との記述もある．

7 個の素数の 3 乗の和であることと同値で，明らかに一段難しい問題となるので，とりあえずは偶数の方だけ考えましょう，ということである．

「C 以上の偶数はすべて 8 個の素数の 3 乗の和」となるような C が理論的に計算可能，という形で予想 1 が解決されれば，9 個の素数の 3 乗の和で表せない有限個の自然数を原理的には決定できることになるわけだが，この原稿を打っている 2020 年 5 月の時点でも，その予想は証明されていない．しかし，その解決に向けた努力は続けられてきていて，それらの結果はそれなりの数の論文となっている．そういう研究は大きく 2 つの方向に分けられ，その一方は「8 個の素数の 3 乗の和とならない偶数は非常に少ない」ことを示そうとする研究である．本稿ではこの方向には深入りしないが，この方向の仕事については，Wooley[12]，Zhao[13] 等を参照されたい．とくに，その方向で現在最も良い結果は，「X 以下の偶数のうち，8 個の素数の 3 乗の和にならないものの個数は高々$O(X^{1/6+\varepsilon})$」という Zhao[13] の結果である (本稿を通し ε は任意に固定した正数を表す)．その個数は本当は $O(1)$ だ，というのが予想 1 に他ならない．

本稿で報告する結果が属す，もう一方の方向の研究は，「8 個の素数の 3 乗の和」は無理でも，できるだけそれに近い形の和で十分大きい偶数が表せることを示すことで予想 1 の主張に近づこうとするもので，1951 年に Roth[9] が証明した次の結果が端緒となる ;「十分大きい自然数 n は，

$$n = p_1^3 + \cdots + p_7^3 + x^3 \tag{1}$$

と，7 個の素数と 1 つの自然数 x の 3 乗の和で表せる.」8 個全部を素数にして予想 1 の解決，とまではいかないが，8 個中 7 個までは素数に限定できる，というわけである．1995 年には Brüdern[2] がこの問題に篩の方法を適用して，n が十分大きい偶数なら，自然数 x を P_4 に限定しても (1) の表示が可能であることを示した．こんなものをお読みくださる方はご存じでしょうが，P_r とは，高々 r 個の素数の積を意味する．

Brüdern[2] は weighted sieve を使ったが，その代わりに reversal role とか switching principle と称される篩の技術を使って，自然数 x を P_3 に限定しても十分大きい偶数 n に対して (1) の表示が可能であることを筆者[6] が指摘した．名古屋大学に移られる松本耕二さんの後任として筆者が岩手大学教育学部に採っていただいて，盛岡に住んで初めて書いた論文がこの [6] であった．[6] の原稿を名古屋の松本さんにお送りしたら，参考文献中のタイプミスを「Rothって F. K. じゃなくて K. F. じゃない?」と指摘してくださったことをよく覚えている．そのころも電子メールはあったが，それに拠らないやり取りもまだよく行われていた時代で，松本さ

んからもブルーブラックのインクの万年筆で手書きされたお手紙でそのご指摘をいただいたものである．

いずれにしろ篩を使って(1)のxをP_3にはできたので，次はP_2を目指したいわけだが，xを篩ってP_2だけにするのは難しく，今でもできていない．ところで，Brüdern[2]にしろ筆者[6]にしろ，(1)のnを偶数に限定しているのは，(1)の右辺の各項が全部奇数の場合を考えるからで，右辺のどこかに2という素因子をくっつければ，証明を実質的に変えることなく大きい奇数nの表示が得られることは容易にわかる．具体的には，例えば筆者[6]の方法で，十分大きい奇数nが$n = p_1^3 + \cdots + p_6^3 + (2p_7)^3 + x^3$（ただし$x$は$P_3$）と表せることが証明できる．つまり，十分大きい自然数は，偶奇によらず,「6個の素数と，P_2とP_3が1個ずつ」の計8個の数の3乗の和で表せるから，従ってとくに，

$$\text{十分大きい自然数は，8 個の } P_3 \text{ の 3 乗の和となる．} \tag{2}$$

この(2)の主張の形でなら，P_3をP_2に替えることはできないか? この問いについてBrüdernさんと議論した．それほどの困難なくできるだろう，という見込みで始めたが，ちょっとした思い込みに嵌っていたことが原因で，思いのほか時間がかかった．結局できてみれば[6]と同じくらいの手間で済むことだったが，Brüdern–Kawada[3]は，十分大きい偶数nは

$$n = p_1^3 + \cdots + p_6^3 + x^3 + y^3 \quad (p_j \text{ は素数，} x \text{ と } y \text{ はどちらも } P_2)$$

と表せることを示した．例えば右辺のp_6を$2p_6$に置き換えることにより，十分大きい奇数nも表せることが示せるので，これで偶奇によらず十分大きい自然数は「5個の素数と3個のP_2」の3乗の和で表されることがわかり，(2)においてP_3をP_2に置き換えた主張が示されたことになる‡．

さて，本稿で報告する結果はこういう流れの中にあり，Kawada[6]やBrüdern–Kawada[3]の改良と言えるものだが，予想1の解決ではない．とすると，結果としては(1)のxをP_2にするしかないが，上でも書いた通り，それは今でも篩ってできることではない．証明の概要は後回しにするが，Zhao[13]の方法により篩を使わない別のアプローチが可能になり，(1)のxをある特殊なタイプの2つの素数の積に限定して，その表示が十分大きい偶数nに対して可能であることを，Zhaoさんと共同で証明することができた．

‡7個の3乗数の和についても同様の研究があり，筆者[7]は十分大きい自然数は7個のP_4の3乗の和で表せることを示した．

定理 2 (Kawada–Zhao[8]) 十分大きい偶数 n は,

$$n = p_1^3 + \cdots + p_7^3 + (p_8 p_9)^3$$

のように,7 個の素数の 3 乗と,2 つの素数の積の 3 乗の和で表せる.

もちろん,定理中の p_7 を $2p_7$ に置き換えて,十分大きい奇数 n も同様に表せる.

2. 序の続き 〜 4 個の 3 乗数の和について.

まだ「序」を続けたいが,既に長くなったので節を新たにする.前節では主に 8 個の 3 乗数の和に関する結果について記したが,そういった結果が,4 個の 3 乗数の和で表せない自然数がほとんどない,というタイプの結果と密接に関係することは,circle method が開発された初期のころから知られていたと思われる.

例えば Roth[9] は,前節 (1) 周辺に書いた結果と同時に,ほとんどすべての自然数は $p_1^3 +_2^3 +p_3^3 + x^3$ の形 (「3 つの素数と 1 つの自然数」の 3 乗の和) で表せることを示した.正確に言えば,任意に固定した (いくらでも大きい) 正定数 A に対し,「3 つの素数と 1 つの自然数」の 3 乗の和で表せない,X 以下の自然数の個数は $O(X(\log X)^{-A})$ であることを示している.Brüdern[2] はその x を P_4 に限定,Kawada[6] は x を P_3 に限定,Brüdern–Kawada[3] は $p_1^3 + p_2^3 + x^3 + y^3$ (p_j は素数,x と y は P_2) という形の 4 つの 3 乗数の和について,それぞれ同様の結果を示している.

ということは,定理 2 を証明した Kawada–Zhao[8] が 4 個の 3 乗数の和についてどういうことを示したかは,かなり明らかであろう.ただ,上では 4 個の 3 乗数の和に関する [2],[6],[3] の結果について雑に書いたが,これらの主張を正確に書くには,合同式に関する初等的な考察から生じる制約に触れなければならない.

2 でも 3 でも 7 でもない素数 p について,簡単にわかることだが,

$$p^3 \equiv 1 \pmod 2, \qquad p^3 \equiv \pm 1 \pmod 9, \qquad p^3 \equiv \pm 1 \pmod 7$$

なので,そういう素数の 3 乗を 4 つ足した和は偶数で,かつ,9 および 7 を法として $0,\ \pm 2,\ \pm 4$ のどれかに合同でなければならない.そこで,これらの制約を満たす自然数の集合を $\mathcal{N}$ としよう;

$$\begin{aligned}\mathcal{N} &= \{n \in \mathbb{N} :\ \forall q \in \{2,\ 7,\ 9\},\ n \equiv 0,\ \pm 2,\ \pm 4 \pmod q\} \\ &= \{n \in \mathbb{N} :\ n \equiv 0 \pmod 2,\ n \not\equiv \pm 1, \pm 3 \ (\mathrm{mod}\ 9),\ n \not\equiv \pm 1\ (\mathrm{mod}\ 7)\}.\end{aligned}$$

この $\mathcal{N}$ に属さない自然数が 4 つの素数の 3 乗の和になったとすると，その 4 つの素数のうちの少なくとも 1 つは 2 か 3 か 7 のどれか，ということである．こういう事情で，4 つの素数の 3 乗の和による表現を考えるときは，$\mathcal{N}$ に属す自然数だけを対象とするのが普通である．

今の話で素数を概素数に置き換えると，どれか 1 つの概素数が特定されるとまではいかないが，$\mathcal{N}$ に属さない自然数が 4 つの概素数の 3 乗の和なら，そのうち少なくとも 1 つの概素数が特定の素因数 (2 か 3 か 7) をもつという制約は受けるので，4 つの概素数の 3 乗の和による表現を考える場合でもやはり $\mathcal{N}$ に属す数に限定するのが自然なのである．こういうわけで，Brüdern[2]，Kawada[6]，Brüdern–Kawada[3] は，$\mathcal{N}$ に属す数に限って，上記のそれぞれの型の 4 つの概素数の 3 乗の和で表せないものは少ない，という評価を与えている．これに関して今回報告する結果は，ここまでお読みくださった方は既にお見通しであろうが，次の通りである．

定理 3 (Kawada–Zhao[8]) 任意の正定数 A に対し，$\mathcal{N}$ に属す X 以下の自然数 n のうち，$n = p_1^3 + p_2^3 + p_3^3 + (p_4p_5)^3$ のように 3 個の素数の 3 乗と，2 つの素数の積の 3 乗の和で表せないものの個数は $O(X(\log X)^{-A})$．

少し脇道にそれるが，集合 $\mathcal{N}$ について補足させていただく．自然数 s に対し,「全ての自然数 q に対して，合同式

$$n \equiv x_1^3 + x_2^3 + \cdots + x_s^3 \pmod q$$

が，どの x_j も q と互いに素であるような整数解 $x_1, x_2, \ldots, x_s$ をもつ」という条件を満たす自然数 n 全体の集合を $\mathcal{N}_s$ と表せば，先に定義した集合 $\mathcal{N}$ は $\mathcal{N}_4$ に他ならない．

上述の話において 4 個を s 個にすれば，$\mathcal{N}_s$ に属さない自然数 n に対しては，ある素べき q を法として上の合同式が $(x_1x_2\ldots x_s, q) = 1$ なる解をもたないわけだから，その n が s 個の素数の 3 乗の和なら，s 個の素数のうちの少なくとも 1 つがその q の素因数だと特定される．つまり $\mathcal{N}_s$ に属さない自然数が s 個の素数の 3 乗の和で表せるかどうかを論じることは，実質的には高々$(s-1)$ 個の素数の 3 乗の和を扱うことになる．このため，s 個の素数の 3 乗の和による表現を考えるときは，$\mathcal{N}_s$ に属す数に限定するのが自然というわけである．そして，次のように予想される．

予想 2. 4 以上の各 s に対し，$\mathcal{N}_s$ に属す十分大きい数は s 個の素数の 3 乗の和で表せるだろう．

各 s に対して $\mathcal{N}_s$ を，前々頁最下行のように具体的に表示することは初等的な作業であり，とくに $s \ge 8$ なら，$\mathcal{N}_s$ は単に s と偶奇が一致するすべての自然数の集合となる．言うまでもなく定理 1 は予想 2 の $s = 9$ の場合を意味し，それにより $s \ge 10$ の場合は自明だから，予想 2 の $s \ge 9$ の部分は解決している．予想 2 の $s = 8$ の場合が予想 1 であり，定理 2 などが偶数に限って主張を述べるのは，$\mathcal{N}_8$ が偶数の集合だからである．

8 以下の s に対して予想 2 は未解決だが，$5 \le s \le 8$ なら，$\mathcal{N}_s$ に属す X 以下の数のうち s 個の素数の 3 乗の和にならないものの個数は $o(X)$ $(X \to \infty)$ であること — 雑に言えば，$\mathcal{N}_s$ に属すほとんどすべての数は s 個の素数の 3 乗の和になること — が示されている[§]．これにあたることすら $s = 4$ の場合には示すことができていないので，予想 2 よりずっと弱い主張だが，予想として記しておく．$\mathcal{N}_4 = \mathcal{N}$ に注意されたい．

予想 3. $\mathcal{N}$ に属す X 以下の自然数のうち，4 個の素数の 3 乗の和で表せないものの個数は $o(X)$ $(X \to \infty)$.

それが $o(X)$ どころか $O(1)$ だ，というのが予想 2 である．いずれにしろ，我々の定理 3 は，この予想 3 を意識したものである．

なお，X 以下の自然数 n が $\mathcal{N}$ に属さないのに 4 つの素数の 3 乗の和になれば，それら 4 個の素数は全部 $X^{1/3}$ 以下で，そのうち 1 個は 2 か 3 か 7 ということになるが，そういう 4 個の素数の組の個数は

$$O\Big(\big(X^{1/3}(\log X)^{-1}\big)^3\Big) = O\big(X(\log X)^{-3}\big).$$

これが，$\mathcal{N}$ に属さない X 以下の自然数のうち 4 つの素数の 3 乗の和になるものの個数の上界になるから，この意味で，$\mathcal{N}$ に属さないほとんどすべての自然数は 4 つの素数の 3 乗の和にならない．蛇足だが．

3. 補足 〜 8 個の 3 乗数の和と 4 個の 3 乗数の和の関係.

ここまでに紹介した結果達を見比べると，ある種の集合 $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$ に対し，次の 2 つの命題の間には密接な関係があることに気付かれよう．

命題 A. 十分大きい偶数は，$p_1^3+p_2^3+p_3^3+p_4^3+x_1^3+x_2^3+x_3^3+x_4^3$ $(x_j \in \mathcal{A}_j)$ の形で表せる．

命題 B. $\mathcal{N}$ に属す X 以下の自然数のうち，$x_1^3+x_2^3+x_3^3+x_4^3$ $(x_j \in \mathcal{A}_j)$ の形で表せないものの個数は $o(X)$ $(X \to \infty)$.

[§] この方向の最新の結果は Zhao[13] を参照されたい．

これら2つのタイプの結果をcircle methodで証明しようとすると，本質的に必要となるminor arc上の積分の評価は同じもの，というのが現在の常識的な感覚で，一方が証明できれば他方も同時に証明できるだろうと思われている．実際，[2], [6], [3], [8]のそれぞれにおいては，命題Aのタイプの結果と命題Bのタイプの結果が同時に示されているし，Roth[9]の結果だけは概素数に限定しない自然数の3乗を1つ含むため合同式条件が関係しないが，同様である．予想1と予想3も同じこと，と現状では思われるのである．

今書いたのは，circle methodで証明しようとする立場から見ると命題Aと命題Bは同じに見える，という話だが，その2つの命題は論理的にも直接関係している．この関係を見るため，自然数nに対して，

$$\{n - p_1^3 - p_2^3 - p_3^3 - p_4^3 \;:\; p_j \text{ は素数}\} \cap \mathcal{N}$$

という集合に含まれる自然数の個数を$T(n)$とする．関係する合同式条件を処理するのは簡単なことなので，$T(n)$の値を調べることは，n未満の数のうち4つの素数の3乗の和で表せる自然数の個数を数えることと実質的に同じであり，Huaの補題(後出の(8)参照)を基に，この分野で古典的に知られている方法により，十分大きい偶数nに対して，$T(n) \gg n(\log n)^{-A_0}$となるような絶対定数$A_0$の存在が示される．例えば定理3の主張中の定数$A$はこの$A_0$より大きくとれるから，引き出し論法により命題B型の定理3から命題A型の定理2が導かれる．さらに現在では，十分大きい偶数nに対して$T(n) \gg n$であることが示せる¶ので，一般に命題Bから命題Aが導かれる．逆に命題Aから命題Bを論理的に直接証明することは，たぶんできないであろう．

4. 本質的な評価.

前節に書いたように，定理2は定理3から得られるが，circle methodで証明する場合はどちらもある積分評価から同時に得られる．その積分評価がKawada–Zhao[8]の本質的な結果であり，それを定理4として記すが，まず，そのために必要な記号の定義から始める．

十分大きい実数Pに対し，

$$Q = P^{3/4}, \qquad L = \log P$$

¶この証明を書いた文献を筆者は知らないが，本質的にはBrüdern[2]によると言っていいと思う．

とおく．とくに，以下においては $\underline{\log P \text{ を } L \text{ と略記}}$ することは強調しておきたい．さらに，$e(\alpha) = e^{2\pi i\alpha}$ とし，実数 X に対し，

$$f_X(\alpha) = \sum_{X<p\le 2X} e(p^3\alpha)$$

とする‖．実際には X が P か Q のどちらかの場合しか使わない．また，区間 $(Q, 2Q]$ に含まれる自然数のある部分集合 $\mathcal{A}$ に対し，次のようにおく；

$$g(\alpha) = g(\alpha; \mathcal{A}) = \sum_{x\in\mathcal{A}} e(x^3\alpha), \qquad I_0 = \int_0^1 |f_Q(\alpha)^2 g(\alpha)^4| d\alpha.$$

次に，B を適当に大きく固定した正定数とし，

$$\mathfrak{N} = \bigcup_{1\le q\le L^B} \bigcup_{\substack{1\le a\le q\\(a,q)=1}} \left[\frac{a}{q} - \frac{L^B}{P^3},\ \frac{a}{q} + \frac{L^B}{P^3}\right], \qquad \mathfrak{n} = \left[\frac{L^B}{P^3}, 1 + \frac{L^B}{P^3}\right) \setminus \mathfrak{N}$$

と定義する．こういう $\mathfrak{N}$, $\mathfrak{n}$ はそれぞれ major arc, minor arc と呼ばれ，major arc 上の積分は大抵それほどの困難なく計算できるので，minor arc 上の積分に対する十分な評価を得られるかどうかが要点となる．そして，次の評価が Kawada–Zhao[8] の本質的な結果である．

定理 4 今定義した記号の下，次の不等式が成立する；

$$\int_{\mathfrak{n}} |f_P(\alpha)^2 f_Q(\alpha)^2 g(\alpha)^4| d\alpha \ll P^{1+\varepsilon} I_0 + Q^{145/48+\varepsilon} I_0^{1/2} + Q^6 P^{-1} L^{-B/5}.$$

まず，この定理の意味について記したい．$\mathfrak{B} \subset [0, 1)$ に対し，

$$I(\mathfrak{B}) = \int_{\mathfrak{B}} |f_P(\alpha)^2 f_Q(\alpha)^2 g(\alpha)^4| d\alpha \tag{3}$$

とおけば，定理 4 は $I(\mathfrak{n})$ の評価を与えている．指数和が 1 を周期とすることから $I(\mathfrak{N}) + I(\mathfrak{n}) = I([0, 1))$ だが，一方，$|f_X(\alpha)|^2 = f_X(\alpha) f_X(-\alpha)$，$|g(\alpha)|^4 = g(\alpha)^2 g(-\alpha)^2$ ということと，整数 m に対し，

$$m \ne 0 \text{ なら } \int_0^1 e(m\alpha) d\alpha = 0 \text{ で，} \quad m = 0 \text{ ならこの積分の値は } 1, \tag{4}$$

‖[8] では $\log p$ の重みを付けた指数和を $f_X(\alpha)$ としたが，本稿では話し易さを優先して外した．後の $I([0, 1))$ を (5) の「解の個数」と端的に言える，という程度のことで，本質的な差はない．

ということから，$I([0,1))$ は，次の不定方程式の解の個数に等しい；

$$\left.\begin{array}{c} p_1^3+p_2^3+x_1^3+x_2^3=p_3^3+p_4^3+x_3^3+x_4^3, \\ P<p_1,p_3\leq 2P, \quad Q<p_2,p_4\leq 2Q, \quad x_j\in\mathcal{A}\,(1\leq j\leq 4), \end{array}\right\} \tag{5}$$

その等式の両辺は P^3 の定数倍程度の大きさだから，8 個の変数 p_j, x_j をそれぞれが指定された条件の下で勝手に選んだとき，その等式が成り立つ確率は $\asymp P^{-3}$ と予想される ($X\asymp Y$ は，$X\ll Y$ かつ $X\gg Y$ を意味する) ので，集合 $\mathcal{A}$ に含まれる数の個数を $\sharp\mathcal{A}$ と表せば，

$$I([0,1)) \;\asymp\; (P/L)^2(Q/L)^2\big(\sharp\mathcal{A}\big)^4\cdot P^{-3} \;\;\asymp\; P^{-1}Q^2\big(\sharp\mathcal{A}\big)^4L^{-4}$$

と期待される．例えば予想 1 に挑戦することを考えると，$\mathcal{A}$ を区間 $(Q,2Q]$ 内の素数全体の集合としてうまくいったらいいなと思うわけだが，そういった場合は $\sharp\mathcal{A}\asymp Q/L$ だから，$I([0,1))$ の大きさは Q^6P^{-1} に L の負の何乗かが掛かった程度の大きさであろうと予想される．そして実際，$\mathfrak{N}$ の寄与 $I(\mathfrak{N})$ は正確に計算出来て，その期待される大きさと一致する．

従って，$\mathcal{A}$ が $(Q,2Q]$ 内の素数の集合とか，そうでなくてもそれと似たようなものであるときに，定理 4 の不等式の右辺が最後の項 $Q^6P^{-1}L^{-B/5}$ だけで抑えられるくらい I_0 が小さければ，我々は $I([0,1))$ を，即ち不定方程式 (5) の解の個数を，（主項）＋（誤差項）の形に表示できるという意味で正確に計算できる — これが定理 4 の直接の意味である．

さて，I_0 も (5) と似たような 6 変数の不定方程式の解の個数と理解される．そう考えれば明らかなように I_0 が一番大きいのは $\mathcal{A}=(Q,2Q]\cap\mathbb{N}$ のときだが，そのときでも真実としては $I_0\ll Q^3$ であろうと予想される．そこで，I_0 の評価を，

$$I_0=\int_0^1|f_Q(\alpha)^2g(\alpha)^4|d\alpha\;\ll Q^{3+\delta} \tag{6}$$

という形で書いてみて，ちょっと計算してみると，定理 4 によれば，

$$I(\mathfrak{n})\;\ll Q^6P^{-1}L^{-B/5}\quad\Longleftrightarrow\quad\delta<\frac{7}{24}$$

ということがわかる．

$\mathcal{A}$ が $(Q,2Q]$ 内の自然数から成るどんな部分集合であっても $\delta=0$ とできるだろうと予想されるわけだが，例えば $\mathcal{A}$ を $(Q,2Q]$ 内のすべての素数の集合としたときに現時点で得られる一番いい結果は，$\delta=1/2$ にすぎない．従って今のところ定理 4 は予想 1 を解決するものではない．

Brüdern や筆者は，[2], [6], [3] において，篩を使って予想 1 に近づく結果を示したが，篩って素数のみを残すことはできない（parity 現象と呼ばれる) ことが知られている．つまり，これまでの手法では，予想 1 に近づけても，その解決に至る道筋を見ることはできなかった．しかし今回の定理 4 は，例えば $\mathcal{A}$ を $(Q, 2Q]$ 内のすべての素数の集合としたときに，本当は $\delta = 0$ で成立するであろう (6) を，7/24 よりほんのちょっとでも小さい δ に対して証明出来たら，予想 1 が解決する，という道筋を見せた．このことも定理 4 の意義であると言えよう．

5．定理 4 から定理 2，定理 3 を導くには．

前節の説明だけでは不十分かもしれないが，実際定理 4 は，次の 2 つの条件を満たすような自然数の集合 $\mathcal{A}$ に対してのみ有効な評価を与える；

(i) 7/24 より真に小さい δ に対して $I_0 \ll Q^{3+\delta}$ が証明できる．

(ii) $\mathcal{A} \subset (Q, 2Q]$ だが，ある正定数 c に対して，$\sharp\mathcal{A} \gg QL^{-c}$．

現在知られている，これらの条件を両方満たす集合 $\mathcal{A}$ は，素因数の大きさに都合の良い制限を加えた数の集合，というタイプのものだけで，次の集合 $\mathcal{A}$ はその一例である；

$$\mathcal{A} = \{p_1 p_2 \ : \ (2Q)^{1/7} < p_1 \leq 2(2Q)^{1/7},\ Q/p_1 < p_2 \leq 2Q/p_1\}. \qquad (7)$$

この $\mathcal{A}$ に対しては $I_0 \ll Q^{3+2/7+\varepsilon}$ が示されていて，$2/7 < 7/24$ である．この I_0 の評価の形は Brüdern[1] にあるが，その評価だけなら本質的には Vaughan[10] の Theorem A と言える．いずれにしろ，定理 4 を (7) の $\mathcal{A}$ に対して使うことで，定理 2 および定理 3 が従うことになる．

もし $\mathcal{A}$ を素数だけからなる集合として定理 4 を使えれば，8 個の素数変数に関する不定方程式 (5) の解の個数が数えられるということになり，予想 1 も解決する，というのは納得していただけようが，$\mathcal{A}$ を (7) とすると，(5) は 8 変数のうち 4 つが P_2 だから，それが P_2 が 1 つだけしかない定理 2 や定理 3 と直結することは，説明を要するだろう．

大きい自然数 n が 8 個の素数の 3 乗の和で表せることを circle method で証明したいと思うと，まず最初に，$2P = n^{1/3}$ くらいに P を設定し，

$$\int_0^1 f_P(\alpha)^8 e(-n\alpha)d\alpha$$

という積分を計算できるか，ということを考える．この積分は (4) により，$n = p_1^3 + \cdots + p_8^3$ $(P < p_j \leq 2P)$ という形の n の表現の数を数える．その

積分に対する major arc $\mathfrak{N}$ の寄与は今では容易に計算され，

$$n\text{ が十分大きい偶数なら}\quad \int_{\mathfrak{N}} f_P(\alpha)^8 e(-n\alpha)d\alpha \gg P^5L^{-8}$$

となる．よって，対応する minor arc $\mathfrak{n}$ の寄与が $o(P^5L^{-8})$ だともし証明できれば十分大きい偶数は 8 個の素数の和となり，予想 1 が解決する．

一方，Hua の補題により，ある正定数 C に対して，

$$\int_0^1 |f_P(\alpha)|^8 d\alpha \ll P^5L^C \tag{8}$$

である．普通はこの (8) の右辺を $P^{5+\varepsilon}$ とした形が Hua の補題として引用されるが，Hua[5] の Theorem 4 にある (8) の形にできることも古くから知られていた．さらに Vaughan[10] により，(8) における C の値は 0 どころか負の値 ($|C|$ は小さめだが) にできることも示されている．そして，(8) の左辺の積分区間を $\mathfrak{n}$ に制限したら C を -8 より小さくできる，ともし証明できれば，予想 1 は解決するのである．そういう意味では，元々 L のべきの話にはなっていたわけで，予想 1 の解決まではそもそもほんのちょっと足りないだけ，とも言えるのかもしれない．

もっと雑な，違う言い方をすると，(5) において集合 $\mathcal{A}$ を素数だけからなる集合にして 8 個の素数変数の方程式にすると，その解の個数を正確に計算することはできていないものの，(真の大きさと比べて L の何乗かの分だけ大きい，という意味で) わりと正確に近い上からの評価は得られている，ということである．こういう事情があるため，(5) において $\mathcal{A}$ の元は 1 個以上あるなら何個でもあまり関係はないのである．

具体的には，定理 4 から定理 2 を導くには，(7) の $\mathcal{A}$ に対し，例えば

$$\int_0^1 f_P(\alpha)^6 f_Q(\alpha) g(\alpha) e(-n\alpha) d\alpha \tag{9}$$

を計算する．この積分は $n = p_1^3 + \cdots + p_7^3 + x^3$ $(p_1, \cdots, p_6 \in (P, 2P]$, $p_7 \in (Q, 2Q]$, $x \in \mathcal{A})$ という n の表現を数える．その積分に対する $\mathfrak{N}$ の寄与は問題なく計算でき，$\mathfrak{n}$ の寄与に対して十分な評価が得られれば定理 2 が従うことになる．そこで，まず Hölder の不等式を使って，

$$\left|\int_{\mathfrak{n}} f_P(\alpha)^6 f_Q(\alpha) g(\alpha) e(-n\alpha) d\alpha\right| \ll \left(\int_0^1 |f_P(\alpha)|^8 d\alpha\right)^{5/8} \times \\ \left(\int_0^1 |f_P(\alpha)|^4 |f_Q(\alpha)|^4 d\alpha\right)^{1/8} \left(\int_{\mathfrak{n}} |f_P(\alpha)^2 f_Q(\alpha)^2 g(\alpha)^4| d\alpha\right)^{1/4}$$

とすると，右辺の1番目の積分には(8)を使えばいいし，右辺2番目の積分もまあ似たようなもので，どちらに対しても上記のように真の大きさからLの何乗かの分だけ損した形の上からの評価が得られる．そして，(7)の$\mathcal{A}$に対しては(6)が$\delta = 2/7 + \varepsilon\ (< 7/24)$で成立するから，最後の不等式の右辺の3番目の積分には定理4そのものを使えば，Bの値を大きくとることで，必要な評価からLのべき乗ならいくらでもへこませられるので，全体として(9)の積分に対する$\mathfrak{n}$の寄与は，$\mathfrak{N}$の寄与に比べて十分小さいことが示される．このようにして定理4から定理2が導かれる．

定理3を示すには，Nを大きい実数として$P \asymp N^{1/3}$と設定し，(7)の$\mathcal{A}$に対し，

$$\int_0^1 f_P(\alpha)^2 f_Q(\alpha) g(\alpha) e(-n\alpha) d\alpha$$

という積分を考える．これは$n = p_1^3 + p_2^3 + p_3^3 + x^3$ ($P < p_1$, $p_2 \leq 2P$, $Q < p_3 \leq 2Q$, $x \in \mathcal{A}$)というnの表現を数える．その積分に対する$\mathfrak{N}$の寄与は，$n \in \mathcal{N} \cap (N, 2N]$に対してやはり大きな問題なく処理できて，$\mathfrak{n}$の寄与については，Besselの不等式により，

$$\sum_{N<n\leq 2N} \left| \int_{\mathfrak{n}} f_P(\alpha)^2 f_Q(\alpha) g(\alpha) e(-n\alpha) d\alpha \right|^2 \ll \int_{\mathfrak{n}} \left| f_P(\alpha)^4 f_Q(\alpha)^2 g(\alpha)^2 \right| d\alpha,$$

さらにHölderの不等式によって

$$\ll \left(\int_0^1 |f_P(\alpha)|^8 d\alpha \right)^{1/4} \left(\int_0^1 |f_P(\alpha)|^4 |f_Q(\alpha)|^4 d\alpha \right)^{1/4} \times \left(\int_{\mathfrak{n}} |f_P(\alpha)^2 f_Q(\alpha)^2 g(\alpha)^4| d\alpha \right)^{1/2}$$

とすれば，先程と同様に定理4によって十分な評価が得られ，定理3の主張中のAに応じてBを大きくとることにより，$\mathfrak{n}$の寄与が$\mathfrak{N}$のそれに匹敵するくらい大きくなってしまう$n \in \mathcal{N} \cap (N, 2N]$の個数が$O(NL^{-A})$という評価が従う．このようにして定理3は定理4から従うことになる．

6. Vaughanの方法とZhaoの方法．

最後に，定理4の証明において重要な役割を果たす2つのアイディアについて触れて，本稿を終える．1つは，minor arc上に制限されたVaughanのdiminishing range methodと呼ばれるもので，その方法はVaughan[11]が$G(6) \leq 31$を証明する際に初めて使われている．もう1つは，Zhao[13]のアイディアである．

まずは前者の話をするために，定理 4 を書いた直後に (3) で定義した記号 $I(\mathfrak{B})$ を思い出していただく．定理 4 は $I(\mathfrak{n})$ の評価だが，$I([0,1))$ は (5) の解の個数であった．その (5) の等式を

$$p_1^3 - p_3^3 = p_4^3 + x_3^4 + x_4^3 - p_2^3 - x_1^3 - x_2^3 \tag{10}$$

と書いて，各変数の大きさの条件に注意すると右辺の絶対値は $24Q^3$ を越えず，一方 $|p_1^3 - p_3^3| = |p_1 - p_3|(p_1^2 + p_1p_3 + p_3^2) \geq 3P^2|p_1 - p_3|$ だから，

$$|p_1 - p_3| < 8Q^3P^{-2} \ (= H \text{ とおく}). \tag{11}$$

よって，積分 $I(\mathfrak{n})$ に現れている $|f_P(\alpha)|^2$ を

$$F(\alpha) = \sum_{\substack{P<p_1,\, p_3 \leq 2P \\ |p_1 - p_3| \leq H}}\sum e((p_1^3 - p_3^3)\alpha) \tag{12}$$

という，条件 (11) を込みにした指数和で置き換えてもいいだろう，というのが基本的な思想である．区間 $(P, 2P]$ 内の 2 つの素数 p_1, p_3 の組の個数は $\asymp P^2L^{-2}$ だが，そのうち (11) を満たす組は $O(PHL^{-2})$ しかないから，$|f_P(\alpha)|^2$ を $F(\alpha)$ で置き換えられれば得することが期待できる．

そこで $\mathfrak{B} \subset [0,1)$ に対し，

$$J(\mathfrak{B}) = \int_{\mathfrak{B}} F(\alpha)|f_Q(\alpha)^2 g(\alpha)^4| d\alpha$$

とおいてみると，まず今の観察から $I([0,1)) = J([0,1))$ である．ここでは計算には深入りしないから雑に書くが，$\mathfrak{N}$ と $\mathfrak{n}$ の定義における P^3 を Q^3 で置き換えたものを $\mathfrak{M}$, $\mathfrak{m}$ とし，$J([0,1))$ を計算するときの major arc と minor arc はこの $\mathfrak{M}$, $\mathfrak{m}$ とする．これは，(10) の両辺の大きさが $\asymp Q^3$ であることが影響しているのだが，いずれにしろ，

$$\begin{aligned} I(\mathfrak{n}) &= I([0,1)) - I(\mathfrak{N}) \\ &= J([0,1)) - I(\mathfrak{N}) = J(\mathfrak{m}) + J(\mathfrak{M}) - I(\mathfrak{N}) \end{aligned} \tag{13}$$

と書く．やはり major arc 上の積分 $I(\mathfrak{N})$, $J(\mathfrak{M})$ は計算できて，どちらも同じものを数えているわけだから両方の主項は一致し，それらが打ち消し合うので $J(\mathfrak{M}) - I(\mathfrak{N})$ は小さいことが証明できる．そのため，(13) により，$I(\mathfrak{n})$ の評価が実質的に $J(\mathfrak{m})$ の評価に帰着されることになる．この意味で，定理 4 の不等式の左辺の積分において，$|f_P(\alpha)|^2$ を $F(\alpha)$ で置き換えられた ($\mathfrak{n}$ は $\mathfrak{m}$ に変わったが)．これが Vaughan[11] の方法である．

$F(\alpha)$ に置き換えてはみたが，α が minor arc に入るときに $F(\alpha)$ 自身に対して何らかの自明でない評価を示すことができるとはとても思えない．$F(\alpha)$ の定義 (12) は素数 p_1, p_3 についての 2 重和だが，p_3 についての和を内側とみると，p_3 は p_1 周辺の非常に狭い範囲の素数を動くわけで，そういう状況で充分な打ち消しあいの効果を引き出せるとはとても思えない．その際ネックとなるのは p_1, p_3 が「素数」ということで，それらが素数という制約なく指定された区間内の自然数を全部動いて良ければ話は違ってくる．その素数という制約を，もちろんただで外せるわけではないが，次のような手順でわりと簡単に，しかも効果的に外すことができる，というのが Zhao のアイディアである．

まず $F(\alpha)$ をその定義に戻して，$J(\mathfrak{m})$ を，

$$J(\mathfrak{m}) = \sum_{\substack{P<p_1,\, p_3\le 2P \\ |p_1-p_3|\le H}}\sum \int_{\mathfrak{m}} e((p_1^3-p_3^3)\alpha)\,|f_Q(\alpha)^2 g(\alpha)^4|d\alpha$$

と書いてみる．この右辺の 2 重和の内側の積分に絶対値を付ければ，それは $|J(\mathfrak{m})|$ の上界になるし，その状態でなら p_1, p_3 が素数という条件を外しても問題ない．つまり，

$$|J(\mathfrak{m})| \le \sum_{\substack{P<m_1,\, m_3\le 2P \\ |m_1-m_3|\le H}}\sum \left|\int_{\mathfrak{m}} e((m_1^3-m_3^3)\alpha)\,|f_Q(\alpha)^2 g(\alpha)^4|d\alpha\right|,$$

ここで m_1, m_3 はもはや素数でなく，示された条件を満たす奇数としておく．さらに，$m_1+m_3=2m$，$m_1-m_3=2h$ とおけば，

$$|J(\mathfrak{m})| \le \sum_{|h|\le H/2}\ \sum_{P<m\le 2P} \left|\int_{\mathfrak{m}} e((6hm^2+2h^3)\alpha)|f_Q(\alpha)^2 g(\alpha)^4|d\alpha\right|.$$

ここで $h=0$ の寄与は単純に $O(PI_0)$ で，$h>0$ の場合の寄与は，Cauchy の不等式を使って，そのあとで積分の絶対値の 2 乗を展開して，

$$\ll \left(PH \sum_{1\le h\le H/2}\ \sum_{P<m\le 2P}\left|\int_{\mathfrak{m}} e((6hm^2+2h^3)\alpha)|f_Q(\alpha)^2 g(\alpha)^4|d\alpha\right|^2\right)^{1/2}$$
$$= \left(PH\int_{\mathfrak{m}}\int_{\mathfrak{m}} \widetilde{F}(\alpha-\beta)\big|f_Q(\alpha)^2 g(\alpha)^4 f_Q(\beta)^2 g(\beta)^4\big|d\alpha d\beta\right)^{1/2}$$

となる，ここで，

$$\widetilde{F}(\gamma) = \sum_{1 \le h \le H/2} \sum_{P < m \le 2P} e((6hm^2 + 2h^3)\gamma)$$

である．今は $h > 0$ の方だけ書いたが，$h < 0$ の方も同じことで，

$$|J(\mathfrak{m})| \ll PI_0 + \left(PH \int_{\mathfrak{m}} \int_{\mathfrak{m}} \widetilde{F}(\alpha - \beta) \left| f_Q(\alpha)^2 g(\alpha)^4 f_Q(\beta)^2 g(\beta)^4 \right| d\alpha d\beta \right)^{1/2}.$$

このようにして，いわば $F(\alpha)$ を，その定義 (12) における p_1, p_3 が「素数」という制約を外した指数和 $\widetilde{F}(\alpha)$ で置き換えることができる — 途中で Cauchy の不等式を使うから無償で置き換えたわけではないが，それでも結果として得るものがはるかに大きい — というのが Zhao[13] のアイディアである．

指数和 $\widetilde{F}(\alpha)$ は Vaughan[10] が扱っていて，わりと良い評価があるのでそれを使うのだが，この先の計算も実際には相当に長い．ここでは，定理 4 の証明には本節で紹介した Vaughan[11] の方法と Zhao[13] の方法が重要な役割を果たす，とだけ言うに留め，さらなる詳細は論文 [8] をご覧いただくこととし，本稿を終えることとする．

最後に，本稿の締め切りに関して非常に寛大なご対応をしてくださった，研究代表者の鈴木正俊氏に深い感謝の意を表する．

参考文献

[1] J. Brüdern, A note on cubic exponential sums, in: Séminaire de Théorie des nombres, Paris 1990-91, S. David (ed.), Progr. Math. 108, Birkhäuser, Basel, 1992, pp.23-34.

[2] J. Brüdern, “A sieve approach to the Waring-Goldbach problem, I: Sums of four cubes”, Ann. Sci. École Norm. Sup. (4) 28 (1995), 461-476.

[3] J. Brüdern and K. Kawada, “On the Waring-Goldbach problem for cubes”, Glasg. Math. J. 51 (2009), 703-712.

[4] L. K. Hua, “On the representation of numbers as the sum of the powers of primes,” Math. Z. (1938), 335–346.

[5] L. K. Hua, Additive Theory of Prime Numbers, Amer. Math. Soc., Providence, Rhode Island, 1965.

[6] K. Kawada, "Note on the sum of cubes of primes and an almost prime," Arch. Math. (Basel) 69 (1997), 13–19.

[7] K. Kawada, "On sums of seven cubes of almost primes," Acta Arith. 117 (2005), 213-245.

[8] K. Kawada and L. Zhao, "The Waring-Goldbach problem for cubes with an almost prime," Proc. London Math. Soc. (3) 119 (2019), 867-898.

[9] K. F. Roth, On Waring's problem for cubes, Proc. London Math. Soc. (2) 53 (1951), 268-279.

[10] R. C. Vaughan, On Waring's problem for cubes, J. Reine Angew. Math. 365 (1986), 122-170.

[11] R. C. Vaughan, On Waring's problem for sixth powers, J. London Math. Soc. (2) 33 (1986), 227-236.

[12] T. D. Wooley, "Slim exceptional sets for sums of cubes," Canad. J. Math. 54 (2002), 418–428.

[13] L. Zhao, On the Waring-Goldbach problem for fourth and sixth powers, Proc. London Math. Soc. (3) 108 (2014), 1593-1622.

Department of Mathematics
Faculty of Education
Iwate University
Morioka, Iwate Pref., 020-8550, JAPAN
E-mail address: kawada@iwate-u.ac.jp