数理解析研究所講究録 1274 巻 2002 年 219-229

素数を変数とするいくつかの加法的問題について

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

1. 序 — 3つのべき乗数の和

今回報告させていただく結果は、Stuttgart 大学の Jörg Brüdern 先生との共同研究 [3] である。これは、名古屋大学の松本耕二先生が研究代表者となられた 1999 年の数理解析研究所での研究集会の期間中になされたものであり、この論文 [3] はその会議の Proceeding に掲載していただくことになっている。この論文の最初の原稿の作成は私が引き受けたのだが、ひとえに私の仕事の遅さのため、結局投稿したのは Proceeding の締め切りを半年近く過ぎた 2000 年の 8 月に入ってからとなってしまった。松本先生を筆頭に、ご迷惑、ご心配をお掛けした皆様には、この場で改めてお詫び申し上げたい。自分でも、論文を書く能力の低さにがっかりしている。

それはともかく、数学の話に進ませていただこう。Waring 問題の拡張や変形は数多いが、3つのべき乗数の和によって自然数を表す問題もひときわ注目を集めたものの一つといえよう。これについては、3つの自然数 k_1, k_2, k_3 が (どれかが 1 だとつまんないからみんな 2 以上として)

$$\frac{1}{k_1}+\frac{1}{k_2}+\frac{1}{k_3}>1 \tag{1}$$

をみたすならば、自然に要求される合同式条件をみたす十分大きい自然数 n はすべて、ある自然数 x, y, z によって

$$n=x^{k_1}+y^{k_2}+z^{k_3} \tag{2}$$

と表せる、と予想されていた。ここで、「n に自然に要求される合同式条件」というのは、すべての自然数 q について合同式

$$n\equiv x^{k_1}+y^{k_2}+z^{k_3} \pmod{q} \tag{3}$$

が解をもつ、といった感じの条件なのだが、すべての場合に明確に書くのは結構めんどくさい。言うまでもなく、あるqに対してこの合同式(3)が解をもたなければ、nを(2)の形で表すことはもちろんできない。こういった条件は加法的問題にはいつでも暗黙のうちに付きまとうもので、全く初等的な考察で処理できることであるのだが、それに触れるのはいつも億劫である。それが表面化しないときは黙っていればいいわけだが、表面化するときはさすがに何も言わないわけにはいかない。

実際、上の場合はk_1, k_2, k_3がすべて偶数、ということでなければ、すべての自然数q, nに対して合同式(3)は解をもち、nに要求される合同式条件はなにもない。つまり、k_1, k_2, k_3のうちの少なくとも一つが奇数で、(1)をみたすときは、上述の予想は単に、十分大きいnはすべて(2)の形で表される、ということになる。

k_1, k_2, k_3がすべて偶数なら、例えば$n = 4^r(8m+7)$ (r, mは0以上の整数)の形のnは3つの平方数の和で表されないことが知られているから、nは(2)の形で表されることはない。したがって、nは少なくともその形ではない、という条件が必要になることは明らかである。この場合には$n \not\equiv 0, 4, 7 \pmod 8$であれば$n$に要求される合同式条件はみたされ、よって上の予想によれば、そういうnは十分大きければ(2)の形で表される、と思われる。数行前に触れた通り、$n \equiv 7 \pmod 8$ならnは(2)の形で表されないからいいが、$n \equiv 0, 4 \pmod 8$のときは、(2)の形で表されることもあるし、ある2のべきのqに対して(3)が解をもたないことから(2)の形で表されないと分かることもある。この最後の$4|n$なる場合に、前出の予想において実際nに課される条件をきちんと書くのはちょっとめんどうなことで、しかもここで必要なこととも思えないので、省略させていただく。

さて、べきの組(k_1, k_2, k_3)には$2 \le k_1 \le k_2 \le k_3$という条件をつけて一般性を失わないが、その下で(1)をみたす組は

$$\text{I型:} \qquad (k_1, k_2, k_3) = (2, 2, k), \quad (k \text{は2以上の整数})$$

または

$$\text{II型:} \qquad (k_1, k_2, k_3) = (2, 3, k), \quad (k = 3, 4, 5)$$

のいずれかとなることが容易に分かる。ここに書いたように、本文では便宜上前者をI型、後者をII型と呼ぶことにする*。

*これは一般に通用しているものではなく、本文内に限った呼び方である。

上の問題については、I型で$k=2$のときは完璧な結果が古典的に知られている。即ち、$4^r(8m+7)$ (r, mは0以上の整数)の形の自然数は3つの平方数の和で表せないが、それ以外の自然数は3つの平方数の和となる、というもので、1798年にLegendreが証明した。それ以外の場合については、今のところ“ほとんどすべてのnは”(2)の形で表せる、というタイプの結果しか得られていない。この“ほとんどすべて”というのは解析的整数論においてはよく使われる用語だから大体お分かりいただけることと思うが、ここでは上で触れたような合同式条件を考慮する必要がある。つまり先程の命題は、N以下の自然数nのうち、必要な合同式条件(これはI型でkが偶数のときしか現われない)をみたし、かつ(2)の形で表せないnの個数は、$o(N)$ $(N\to\infty)$である、という意味である。本文中ではこのように、必要な合同式条件を込みにして、“ほとんどすべての”という用語を使うことにする。この$o(N)$の部分を実際にどのくらいまで精密に評価できるか、については、あとで報告する我々の結果に関してのみ言及することにする。

ではここで、3つの平方数の和の場合以外に、ほとんどすべてのnが(2)の形で表せることを証明した論文を紹介しておく。

I型, $k\geq 3$: Davenport-Heilbronn [6], 1937.
II型, $k=3$: Davenport-Heilbronn [5], 1937.
II型, $k=4$: Roth [14], 1949.
II型, $k=5$: Vaughan [15], 1980; Hooley [10], 1981.

最後のVaughanとHooleyの仕事は独立で、方法も全く異なる。

ところでこの問題に関する予想を上で述べたが、今ではその予想に対する反例が知られている。I型で$k=9$の場合、十分大きいnはすべて(2)の形で表されるだろうと予想されていたわけだが、Jagy-Kaplansky [12]は1995年、2つの平方数と1つの9乗数の和で表されない自然数が無限個あることを示した。筆者はまだこの論文を読んでいないが、是非とも読まなければならないと思っている。これはかなり衝撃的な結果だと思う。

2. 素数のべき乗数への制限

さて、我々の今回の問題意識は、(2)におけるx, y, zを素数に制限できるか、ということである。これについては、「ほとんどすべてのnは3つの素数x, y, zによって(2)の形で表せる」ということを示すことが、当面の目標になる。前節で見たことから、現在ではそれ以上のことは期待で

ここで、“ほとんどすべての”という中に暗黙のうちに合同式条件も含むことは先に約束したが、変数を素数に制限することでnに課される合同式条件もちょっと変わる。そのnの条件は、「すべての自然数qに対して、合同式(3)は、xyzがqと互いに素になるような解をもつ」というものとなる。実際この条件をみたさない(少なくとも)ほとんどすべてのnは、素数x, y, zによって(2)の形で表されないことが分かるから、この条件を課すのは自然なことである。このことを確認しておこう。

前節でも触れた通り合同式(3)が解をもつことが必要なのは自明である。ある自然数qに対して、合同式(3)が、xyzがqと互いに素でないような解しかもたないとしよう。中国の余りの定理なんかがあるから、このqを素数のべき乗としてよい。仮に、$q = p^l$ (pは素数、$l \geq 1$)としよう。すると、そのようなnが素数x, y, zによって(2)の形で表せたなら、いまの合同式に関する仮定から$p|xyz$となるから、x, y, zのうちの少なくとも一つはpでなければならない。変数を素数に制限する場合は、ここがミソである。一方、Nを大きい実数とし、N以下の自然数nを(2)の形で書けば、もちろんx, y, zはそれぞれN^{1/k_1}, N^{1/k_2}, N^{1/k_3}以下である。したがって、少なくとも一つがpであるような3つの素数x, y, zによって、(2)の形で表されるnのうち、N以下のものの個数は、

$$\ll (N^{1/k_1}(\log N)^{-1})(N^{1/k_2}(\log N)^{-1}) \ll N(\log N)^{-2}$$

(ここで$2 \leq k_1 \leq k_2 \leq k_3$に注意した)となる。この意味で、先の合同式条件をみたさないほとんどすべてのnは素数x, y, zによって(2)の形で表されない。

ここで述べたnについての条件は、合同式に関する初等的な考察により、もっと直接的な条件に書き直すことができる。ここでは後で述べる我々の結果と関係する、II型の場合についてのみ、書いておく。実際、nに要求される条件は、次のようになる。

II型, $k = 3$ のとき： $n \equiv 1 \pmod 2$ かつ $n \not\equiv 5 \pmod 7$.

II型, $k = 4$ のとき： $n \equiv 1 \pmod 2$ かつ $n \not\equiv 2 \pmod 3$.

II型, $k = 5$ のとき： $n \equiv 1 \pmod 2$.

I型の場合についてはBrüdern-Kawada [3] のIntroductionには脚注として書いてあるが、ここでは不要と思うから省略する。

上で当面の目標と書いたものは、しかし、I型の場合には既に終わっている。つまり、I型のべきの組に対しては、ほとんどすべてのnは3つの素

数 x, y, z によって(2)の形で表せる。これは今となっては、circle method に関するやや進んだ演習問題、といったくらいのものである。実際に誰の結果か、と聞かれるとちょっと難しいが、I.M. Vinogradov, Hua らの名前を挙げるべきだろう。Hua は1938年にほとんどすべての自然数は3つの素数の平方の和で表せることをはじめ、Additive prime number theory における結果をいくつか示しており、技術的にはこの時点でI型の場合はみんな処理可能となっていたといえる。もちろんHuaの議論には、その前年の Vinogradov の Ternary Goldbach Problem に関する有名な仕事が極めて重要な役割を果たしている。

ではII型に移ろう。II型の場合はこの当面の目標は達成できていない。が、それに向かっていくつかの結果が証明されているので、それらをここで紹介しておこう。次のように、それぞれの場合に x, y, z を記されている通りに制限した上で、ほとんどすべての n が

$$n = x^2 + y^3 + z^k \tag{4}$$

の形で表されることが証明されている (下で制限が明示されてない変数は、単に、自然数、ということである)。

II型, $k = 4$ のとき;	z: 素数	(Halberstam [7], 1950)
II型, $k = 3$ のとき;	x: 素数, z:素数	(Halberstam [8], 1951)
II型, $k = 5$ のとき;	z: 素数	(Hooley [10], 1981)
II型全て ($k = 3, 4, 5$);	y: 素数, z: 素数	(Brüdern [1], 1988)

年代順に書いたが、1番目の Halberstam [7] と3番目の Hooley [10] の結果は、最後の Brüdern [1] に含まれているから、この方向で今最もよいといえるのは、2番目の Halberstam [7] と最後の Brüdern [1] の結果である。

いずれにしても2つまでは素数にできているわけだが、3つ全部素数にすることはできていないし、残念ながら我々もできなかった。しかし、篩の方法を使って残りの一つの変数を almost prime(概素数、と和訳される)にすることはできる。これが今回報告させていただく主な結果であり、次節で詳しく述べる。

なんだ、almost prime にするのか、じゃあ「素数を変数とする加法的問題」とタイトルにあるのは、看板に偽りありじゃないか、と怒ってJARO[†]に言いつける方はさすがにいないと思うが、不適切だ、というご意見はあるかもしれない。これについては、誤解を与えたとしたら反省したいと

[†]Japan Advertising Review Organization, Inc.; 社団法人 日本広告審査機構

は思うが、一応「〜について」と付いているから問題はないと認識している[‡]。

まじめな話に戻って、例えばある種の Hasse-Weil L 関数に対する Riemann 予想の成立を仮定すれば、k が 3 か 4 のときは、ほとんどすべての n が素数 x, y, z によって(4)の形で表せることを証明できる。これは Hooley や Heath-Brown による 3 乗数の Waring 問題に関連した研究から比較的容易に導かれることだが、ここでは深入りしない。$k = 5$ のときはその仮定だけでは不足で、加えて別の、当分証明されなそうだけど正しいと予想されている命題を仮定すれば、同様の結論は従う。いずれにしても、II 型の場合、3 つの変数を全部素数にするという前述の当面の目標を達成することは、現状でははっきり無理にみえる。

3. 我々の結果と証明の概要

自然数 r に対して、高々 r 個の(必ずしも相異ならない)素数の積となる 1 より大きい自然数を P_r と呼ぶ。P_1 とは、したがって、素数である。篩の方法に関連して広く通用しているこの記号の下、前節の問題に関して我々が [3] で得た結果は、次の通りである。

定理 1 (II 型, $k = 3$) ほとんどすべての n は

$$n = x^2 + y^3 + z^3 \qquad (x\text{: } P_3,\ y\text{: 素数},\ z\text{: 素数})$$

と表される。また、ほとんどすべての n は

$$n = x^2 + y^3 + z^3 \qquad (x\text{: 素数},\ y\text{: } P_3,\ z\text{: 素数})$$

とも表される。

定理 2 (II 型, $k = 4$) ほとんどすべての n は

$$n = x^2 + y^3 + z^4 \qquad (x\text{: } P_6,\ y\text{: 素数},\ z\text{: 素数})$$

と表される。また、ほとんどすべての n は

$$n = x^2 + y^3 + z^4 \qquad (x\text{: 素数},\ y\text{: } P_4,\ z\text{: 素数})$$

とも表される。

[‡]こんな、政治家か官僚みたいな言い訳も一興かな、と思ったんですが、どうでしょ

定理 3 (II型, $k=5$) ほとんどすべての n は

$$n = x^2 + y^3 + z^5 \qquad (x\text{: } P_{15},\ y\text{: 素数},\ z\text{: 素数})$$

と表される。

それぞれの定理において暗黙のうちに仮定されている n についての合同式条件は、3ページ前に明示してある。いずれの場合も、それぞれの形で表せない例外的な n の密度について、我々の証明は次の評価を与える。任意に(大きく)固定した正数 A に対して、N 以下の自然数 n のうち、対応する合同式条件をみたすのに指定された形で表せない n の個数は、$O(N(\log N)^{-A})$ である。ここで O 記号に含まれる定数は高々 A にのみ依存する。この例外の n の個数に対する評価は、すごく小さいだろうが原理的に計算可能なある正数 δ に対して、$O(N^{1-\delta})$ の形にできるのは確実だろう。こういうのは、この方面でよく知られている Montgomery-Vaughan の方法によって得られると思われるが、筆者はその細部の検討はしていない。そこの評価を改良するより、almost prime P_r を良くする(添え字の数字を小さくする)方が大事だと思うからである。

これらの結果の証明には、篩の方法と circle method を用いる。この2つを融合するアイディアを初めて用いたのは Heath-Brown [9] であり、それを Waring タイプの問題に初めて応用したのは Brüdern [2] である。

我々の証明の概要をそれなりに筋が通って理解されるように述べるには、記号の定義などのためどうしても相当数の頁を要することとなる。敢えて言葉だけで概要を述べるようがんばれば、次のようになろうか。どの場合でも n が必要な合同式条件をみたしていれば、linear sieve の問題となり、linear sieve を使う際の誤差項は circle method によって表現できる。しかし、個々の n についてその誤差項をちゃんと押さえることが、今のところはできない。そこで、この分野では常套手段なのだが、Bessel の不等式に基づいて n についての2乗平均を評価する。これにより、いわゆる篩の "level of distribution" がそんなに大きくない限りは、ほとんどすべての n について篩をかけた際の誤差項は小さい、という形の結果が導かれる。あとは篩の理論の話だが、それぞれの場合の "level of distribution" に応じて上記のように P_r の添え字の大きさが決められることになる、というわけである。

まあ、無理にこんなことを書いてもあまり意味はなかったような気もするが、証明についてこれ以上の内容を書くとなると、適当な長さで収

める書き方を思い付くことができなかったので、お許しいただきたい。もちろんちゃんとした証明は、Brüdern-Kawada [3] にある。

この節の結びに、蛇足ではあるが、篩についてそれなりにご存知の方向けに、さらにもう2点について付け加えさせていただく。まず1つめとして、定理1の前半、定理2の前半、および定理3では、2次の項の変数 x に篩をかけているが、これらの場合では、Iwaniec の linear sieve の誤差項の bilinear form が威力を発揮していることを注意しておきたい。

2つめは、証明に使う篩の方法に関することである。不定方程式 $n = x^2 + y^3 + z^4$ において、2次の項の x と3次の項の y とどちらに篩をかける方が簡単だろうか、と考えてみると、やはり2次の x の方に篩をかけるほうが楽にみえるのではないかと思う。とすると、定理2で、前半の x は P_6 で後半の y が P_4 なのは、ちょっと不思議にみえるかもしれない。これは使う篩の方法が違うためなのである。

実際2次の方が楽、というのはその通りで、実は先の方程式で、x, z を素数に限定して y に篩をかける、というのは直接はできないのである§。定理2の後半のためには、都合の良い大きさの素数 p を導入して、かつ x, z を素数として、$n = x^2 + (pw)^3 + z^4$ という表示を考える。すると3乗数の Waring 問題に関する Vaughan の結果が使えて、この w に篩をかけることができるようになる。しかもこの x の方にも篩はかけられる。このようなときには、switching principle あるいは reversal rôle technique¶と呼ばれるアイディアを応用できる。そして結果として w を P_3 にとることができ、定理2の後半が従うのである‖。

一方の定理2の前半の状況では、x にしか篩がかからないから、switching principle は使えず、こういうときは weighted sieve に頼るしかない。篩の方法に詳しい方々には既によく知られていることかもしれないが、switching principle と weighted sieve が両方使える状況のときは、前者の方がいい結果を与える、そして level of distribution が悪い (小さい) ほどその差は

---

§正確に言うと、大きい実数 N 以下の n を扱う際に、現状ではがんばっても level of distribution を $\log N$ のある程度小さいべきの程度にしかできない、ということである。

¶"switching principle" という用語は Iwaniec [11] に、"reversal rôle" という用語は Chen [4] に、それぞれよるようである。筆者は個人的には "reversal rôle" の方がなんとなく好きである。あまりうだうだ言うつもりはないが歴史的な事情を考えても Chen の用語を使うほうがいいように思うのだが、現実には "switching principle" が使われることの方が圧倒的に多いようである。これは多分、[11] の方が [4] よりも先に出版されているからではないか、と想像している。

‖前節の(4) の直後に紹介した II 型に関するこれまでの仕事を見れば分かる通り、II 型の $k = 4$ のときに x, z を素数に限定できる、というのは、それ自身新しい結果であ

は大きい、といえるようである。これ以上の深入りは止めるが、それはそれなりの理由のあることである。上の結果のうち、定理2の前半と定理3ではweighted sieve**を使っている。それら以外のものたちについてはswitching principleが使えるので、それを用いた。

4. Prachar の問題など

最後に、前節の結果と深く関係する問題に言及する。以下、添え字付きの文字pは常に素数を表すとする。

1953年、Prachar [13] は十分大きい奇数nはすべて

$$n = p_1 + p_2^2 + p_3^3 + p_4^4 + p_5^5$$

と表せることを示した。この最後の項のべきは、5に限らず任意の自然数としても同様の結論が得られることを、Prachar [13] は指摘している。ということは、最後の項を落とした$p_1 + p_2^2 + p_3^3 + p_4^4$の形で、十分大きいすべての偶数が表されることを、もうちょっとで証明できるところまできている、といえるかもしれない。少なくとも、それを証明することがこの方向の次の目標だといえるだろう。が、これは第2節の終わりに述べたのと同様に、ある種のHasse-Weil L関数に対するRiemann予想を認めれば、HooleyやHeath-Brownの仕事を基に証明できるが、そういった仮定なしでは、今のところは手が届かなそうな目標なのである。

そこで全部素数にするのをとりあえずあきらめて、どれか一つがalmost primeになることを許せば、似た形で十分大きい偶数がすべて表せることを示せる。実際前節の定理達の証明をみれば、この方向のいくつかの帰結がすぐに従う。例えば前節の定理2の後半とそのあとの例外集合の密度の評価によれば、十分大きいn以下で3を法として2と合同でない奇数のうち、素数の2乗とP_4の3乗と素数の4乗の和で表せないものの個数は$O(n(\log n)^{-2})$だが、一方で十分大きい偶数n以下の奇素数p_1で、$n - p_1 \not\equiv 2 \pmod 3$なるものの個数は$\gg n/(\log n)$だから、$n - p_1$の形の自然数で前述の形で表されるものがあることが分かる。つまり、十分大きい偶数nは

$$n = p_1 + p_2^2 + y^3 + p_4^4 \qquad (y \text{は} P_3)$$

と表せる。

前節の他の結果に関しても同様だが、場合によっては上のように直接従う帰結よりもよい結果を示せることもある。これは前節の3項の問題で

**これはRichertのweighted sieveで十分。

switching principle が使えず weighted sieve を用いていた場合でも、1 次の項が加わることで switching principle を使えるようになるからである。このような結果を次に述べる。

定理 4 十分大きい偶数 n は、

$$n = p_1 + x^2 + p_2^3 + p_3^4 \qquad (x \text{ は } P_3)$$

と表せる。また、十分大きい偶数 n は、

$$n = p_1 + x^2 + p_2^3 + p_3^5 \qquad (x \text{ は } P_4)$$

とも表せる。

この定理の直前で示唆されているように、1 次の項に篩をかけることもできて、次の結果を得る。

定理 5 $k = 3, 4$ または 5 とする。いずれの場合でも、十分大きい偶数 n は、

$$n = x + p_1^2 + p_2^3 + p_3^k \qquad (x \text{ は } P_2)$$

と表せる。

この節の定理も、両方とも Brüdern-Kawada [3] に含まれている。その証明の方針は、おおざっぱに言えば前節の定理達のそれと同じである。この節の結果の場合は、篩を使うときの誤差項が、n について平均的にではなく、個々の n についてうまく押さえることができる、というのが前節の 3 変数の問題達との差である。

参考文献

[1] J. Brüdern, *Iterationsmethoden in der additiven Zahlentheorie.* Thesis, Göttingen 1988.

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

[3] J. Brüdern and K. Kawada, *Ternary problems in additive prime number theory.* to appear in the joint Proceedings of the China-Japan Number Theory Conference (Beijing, September 1999) and the RIMS Analytic Number Theory Conference (Kyoto, November/December 1999), Kluwer Acad. Press.

[4] J.-R. Chen, *On the representation of a large even integer as the sum of a prime and the product of at most two primes.* Sci. Sinica 16 (1973), 157-176.

[5] H. Davenport and H. Heilbronn, *On Waring's problem: two cubes and one square.* Proc. London Math. Soc. (2) 43 (1937), 73-104.

[6] H. Davenport and H. Heilbronn, *Note on a result in additive theory of numbers.* Proc. London Math. Soc. (2) 43 (1937), 142-151.

[7] H. Halberstam, *Representations of integers as sums of a square, a positive cube, and a fourth power of a prime.* J. London Math. Soc. 25 (1950), 158-168.

[8] H. Halberstam, *Representations of integers as sums of a square of a prime, a cube of a prime, and a cube.* Proc. London Math. Soc. (2) 52 (1951), 455-466.

[9] D. R. Heath-Brown, *Three primes and an almost prime in arithmetic progression.* J. London Math. Soc. (2) 23 (1981), 396-414.

[10] C. Hooley, *On a new approach to various problems of Waring's type.* Recent progress in analytic number theory (Durham, 1979), vol. 1. Academic Press, London-New York, 1981, 127-191.

[11] H. Iwaniec, *Primes of the type $\phi(x,y) + A$, where ϕ is a quadratic form.* Acta Arith. 21 (1972), 203–224.

[12] W. Jagy and I. Kaplansky, *Sums of squares, cubes and higher powers.* Experiment. Math. 4 (1995), 169-173.

[13] K. Prachar, *Über ein Problem vom Waring-Goldbach'schen Typ II.* Monatsh. Math. 57 (1953) 113-116.

[14] K. F. Roth, *Proof that almost all positive integers are sums of a square, a cube and a fourth power.* J. London Math. Soc. 24 (1949), 4-13.

[15] R. C. Vaughan, *A ternary additive problem.* Proc. London Math. Soc. 41 (1980), 516-532.