科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１２　日現在

機関番号：３４４１９
研究種目：基盤研究(C)
研究期間：2011～2013
課題番号：２３５４００３４

研究課題名（和文）ゼータ関数を軸とした線型符号および数論的関数の研究

研究課題名（英文）Study on linear codes and arithmetic functions by way of zeta functions

研究代表者
知念　宏司（CHINEN, Koji）

近畿大学・理工学部・准教授

研究者番号：３０４１９４８６

交付決定額（研究期間全体）：（直接経費）　　1,900,000円、（間接経費）　　570,000円

研究成果の概要（和文）：本研究においては、研究代表者が以前から関係している「剰余位数分布問題」において成果が得られた。これは、整数 a （2 以上で完全 h 乗数ではない）を固定し、素数 p に対して a の mod p での位数 D_a(p) の分布を調べる、より具体的には、D_a(p) を k で割ると l 余るような素数 p の自然密度を調べる問題である。この問題の拡張として、平方剰余の条件を付加した場合 (Chinen-Tamura, 2012)、および、mod p のかわりに mod pq とした場合 (Murata-Chinen, 2013) について成果が得られた。

研究成果の概要（英文）：In this research, some results are obtained in the subject "distribution of the residual orders", in which the author has been involved. This is to investigate the distribution of D_a(p), where D_a(p) is the order of a mod p (a is an integer greater than 1, which is not a h-th power and p is a prime). More precisely, the problem of determining the natural density of p such that D_a(p) is congruent to l mod k. As generalizations of this problem, we obtained some results in the case where a quadratic residue condition is added (Chinen-Tamura, 2012), and where mod pq instead of mod p (Murata-Chinen, 2013).

研究分野：数物系科学

科研費の分科・細目：数学・代数学

キーワード：数論　ゼータ関数

１．研究開始当初の背景

符号理論は情報伝達時の誤りをできるだけ訂正するための機構を支える数学理論である。また、解析数論は整数の性質を、解析学を用いて解明する分野で、長い歴史をもっている。両分野に登場する対象として種々のゼータ関数がある。とくに、符号のゼータ関数は比較的新しい対象で、解明が待たれる部分が多いものである。また、剰余位数のような、解析数論に登場する数論的関数にも、未解明な現象がまだ多いのが現状であった。

２．研究の目的

上記のような状況において、符号のゼータ関数や種々の数論的関数について新しい知見を得るとともに、さらには符号理論と解析数論の境界領域開拓を目指すことを目標とした。

３．研究の方法

本研究期間は、主として数論的関数の一種である剰余位数について、剰余類に沿った分布を考える問題（剰余位数分布問題）に取り組んだ。最も基本的な場合をすでに代表者らは過去に解決しているため、その種々の拡張を考えるという方向に進んだ。方法としては、目標とする素数集合を、ある種の篩の考え方を用いて分解し、分解後の集合の自然密度を計算する、という方法であり、これは基本的な場合と共通であるが、次項でも述べる本研究期間における問題は、基本的な場合には現れなかった集合を考察する必要もあって、新しい手法の開発も必要であった。また、本研究においては、数値実験を行なうことも非常に重要で、その役割も決して無視することができない。つまり、数値実験によって傾向をつかみ，結果を予想して理論的計算の指針とするのである。こうした方法は本研究のもつ、研究方法としての大きな特色の一つと言える。本問題における数値実験の特徴としては、主として自然数を扱うものであること、そして、桁数が大きな数を扱うことはないが、その代わりに扱うべき自然数のデータ量が非常に多いことである。実際、本研究のためのある数値実験においては、２２００億個ものデータを扱う必要があった。このような特徴のため、数値実験には専ら C 言語を用いた。というのも、自前で書く必要のある関数がそれほど多くなく、一般に流布している数式処理ソフトを用いるよりもはるかに計算速度が速いからである。

４．研究成果

本研究期間における成果は２種類ある。１つは平方剰余の条件を付加した剰余位数分布問題であり、もう１つは「２変数版」剰余位数分布問題である。これらはいずれも、整数論において古くから重要な役割を果たしているデデキントゼータ関数が関連する問題である。

（１）平方剰余の条件を付加した剰余位数分布問題において一定の成果が得られた。まずどのような問題かを述べる。1 より大きい整数 a と素数 p（p は a を割らない）を取る。またとくに a は平方因子をもたないとする。乗法群 Z/pZ^* における a の（群論的意味での）位数を D_a(p) で表すことにする。これは広い意味で数論的関数の一種と捉えることができる。他に整数 b を取ってルジャンドル記号を (b/p) で表す。このとき、集合 S_{a,b}(k,l)={p は素数; p は a,b を割らない、D_a(p)≡l (mod k)、(b/p)=1} の自然密度を考察するのがこの問題である。これは、集合 Q_a(k,l)={p は素数; p は a を割らない、D_a(p)≡l (mod k)} の自然密度を考察する剰余位数分布問題の自然な拡張である。ここで、条件 (b/p)=1 のみを考えた場合、これを満たす素数 p の自然密度は 1/2 であることが知られている。つまり、素数全体が条件 (b/p)=1 によってちょうど二分されるということである。したがって、Q_a(k,l) に条件 (b/p)=1 を付加することで、Q_a(k,l) は確率的にはちょうど二分されるはずである。しかし、a と b が互いに何らかの代数的影響を与え合う場合には、そのような確率的推論が成り立たない場合がある可能性がある。本研究では、S_{a,b}(k,l) の自然密度を、いくつかの場合に決定し、どういった場合に確率的推論通りになるか、あるいは逆にならないか、ということを調べることが目的である。とくに本研究では、k=q が素数であり、l=0 の場合を主に考察した。その結果、多くの場合は S_{a,b}(q,0) の自然密度は Q_a(q,0) のそれの 1/2 となるが、ある場合には確率的推論通りにならない場合があることが判明した。それは（条件が複雑なので詳細は述べられないが、荒く言えば）a または b が素因子として 2 を含み、かつ q=2 の場合に起こることである。その中で最も特徴的なのは、S_{a,a}(2,0) (a は 2 でない)の場合で、この集合の密度は 1/6 であることがわかった。確率的推論通りであれば 1/3 となるべきであるが、そのさらに半分の密度となっている。そしてその場合は、ごく間接的ではあるものの、原始根の動きを観察できていると考えることもでき、大変興味深い結果が得られたと考えている。またこのほか、(k,l)=(2,0), (2,1), (4,0), (4,2) に対して S_{a,b}(k,l) を求めることができた。

証明にあたっては、まず S_{a,b}(q,0) を、この集合に含まれるべき素数 p の mod q での合同条件および (b/p)=1 で表される素数集合の和集合の形に分解する。分解されたあとの集合の自然密度は、有理数体上のある種のクンマー拡大を、さらに 2 次拡大したものの拡大次数で表される。この自然密度の表示にあたっては、いわゆる素イデアル定理が用いられるが、それはデデキントゼータ関数の解析からもたらされるものである。そして

最後に、剰余項の評価を行ない、S_{a,b}(q,0) の自然密度を表す無限級数を得てその値を計算すると結論が得られる。なお、この結果に関しては、デデキントゼータ関数に対するリーマン予想（一般リーマン予想、略して GRH）を用いる必要はない。

関連する数値実験としては、実際に集合 S_{a,b}(q,0) に含まれる素数のうち、10^9 以下であるものの個数を計測する実験を、いろいろな a, b の組合せに対して行なった。以下いくつかの数値例を示す。以下の表は、x=10^7 から 10^9 まで 3 段階で # S_{a,b}(x;q,0)/π(x) （π(x) は x 以下の素数の個数、S_{a,b}(x;q,0) は S_{a,b}(q,0) に含まれる素数のうち x 以下のものの集合）を計算したものである。

x	(a,b,q)=(3,2,3)	(a,b,q)=(5,3,5)
10^7	0.187309	0.104101
10^8	0.187495	0.104099
10^9	0.187474	0.104185

これは標準的な（確率的推論通りの）分布と考えられるもので、(a,b,q)=(3,2,3) の場合の理論値は 3/16=0.1875, (a,b,q)=(5,3,5) の場合は 5/48=0.104166... である。いずれも、平方剰余の条件をつけない場合のちょうど半分となっている。

x	(a,b,q)=(10,3,2)	(a,b,q)=(3,3,2)
10^7	0.333408	0.166599
10^8	0.333218	0.166595
10^9	0.333338	0.166652

これは標準的な場合とそうでない場合の比較である。つまり、(a,b,q)=(10,3,2) の場合、密度の理論値は 1/3 で、平方剰余の条件をつけない場合のちょうど半分である。しかし、(a,b,q)=(3,3,2) の場合は、確率的には 1/3 になるはずであるが、それより少ない 1/6 が理論値である。

このように、いずれも実験値と理論値はよい一致を示している。

（２）「２変数版」剰余位数分布問題における成果を次に説明する。1 より大きい整数 a と、異なる奇素数 p, q（p, q は a を割らない）を取る。またとくに a の square-free 部分は完全 h 乗数でないとする（h>1）。乗法群 Z/pqZ^* における a の（群論的意味での）位数を D_a(pq) で表す。本研究は、この位数 D_a(pq) が k で割って l 余るような素数の組 (p,q) の集合 R_a(k,l) の自然密度を調べるものである。以前、研究代表者らが取り組んで成果を上げた問題は、群が Z/pZ^* であったため、本研究はその「２変数版」への拡張と言えるものである。また、Z/pqZ^* は、RSA 暗号の構成に用いられる群と同一であることにも注意を要する。

素数は組 (p,q) の形になっているため、従来の素数 p のみの場合に比べるといろいろと考えるべきこと、困難なことが数多くある。まず (p,q) の動く範囲であるが、十分大きな実数 x をとり、p, q とも x 以下という範囲の (p,q) に対して D_a(pq) を考える。言わば、(p,q) は正方形状の領域にあると考える。そして x を無限に大きくしたときの集合 R_a(k,l) の自然密度を考える。本研究では主に a が奇数で k=4 の場合を扱った。R_a(k,l) の自然密度を Γ_a(k,l) で表す。本研究の主結果を述べる。上の仮定を満たす a に対して、まずΓ_a(4,0)=5/9, Γ_a(4,2)=1/3 が得られた。これには GRH の仮定は不要である。次に、GRH を仮定すると Γ_a(4,1)= Γ_a(4,3)=1/18 という結果が得られた。l=0 の場合には、k=4 以外の場合にも結果を得ている。それは、r を奇素数とするとき

Γ_a(r,0)=r(2r^2-r-2)/(r^2-1)^2

というものである。他に k=r^h (h>1) の場合にも密度が求まっている。なお、この l=0 の場合には GRH は不要である。

次に、R_a(4,l) (l=1,3) の場合の証明について述べる。まず D_a(pq) を D_a(p) と D_a(q) の式で表すことから始まる。これにはメービウス関数を用いたかなり複雑な篩の一種が必要であった。そして結果として、R_a(x;4,l)（これは R_a(4,l) に含まれる素数 p に条件 p<=x を追加したもの ）の元の個数は、Q_a(x; 4D, D) および Q_a(x; 4D, 3D) の元の個数の、かなり複雑な形の和で表されることがわかった。ここで、Q_a(x; k, l) は、位数 D_a(p) が k で割って l 余る素数 p で、x 以下であるものの集合である。また、D は正の奇数で、R_a(x;4,l) は D を渡る和として表される。ところで、Q_a(x; k, l) は以前研究代表者らが取り扱い、成果を上げた素数集合と同じである。しかしながら、以前の結果をそのまま利用することはできない。というのも、第一に、Q_a(x; k, l) の密度が剰余項つきで求められていた（ある場合は GRH のもと、またある場合は無条件で）のは k が素数あるいは素数べきの場合だけであり、k と l が互いに素でないような場合には、密度の存在と、密度を計算するアルゴリズムの存在（いずれも GRH のもと）が示されていただけであるため、第二に、R_a(x;4,l) は D を渡る和であるため、Q_a(x; 4D, lD) の個数について和を取るにあたっては、剰余項に D の依存が明示されている必要があるが、以前の研究ではその必要はなく、そうした結果は得ていなかったためである。

そこで、集合 Q_a(x; 4D, lD) をさらに分解する計算をあらためて行なう。すると、集合 Q_a(x; 4D, lD) は、剰余指数、すなわち、D_a(p)I_a(p)=p-1 となる I_a(p) の条件、および p の合同条件を組み合わせた集合の和に分解される。その集合の漸近挙動を素イデアル定理を用いて表すことで、ようやく

Q_a(x; 4D, lD) の漸近挙動を書き下すことができる。それは、ある種の代数体の拡大次数と、関連する代数体の自己同型写像の存在、非存在によって定まる係数によって表される、複雑な無限級数が主要項係数に現れるようなものである。この計算によって、集合 Q_a(x; 4D, lD) の自然密度の存在、そして自然密度の値を級数の形で表示することができたことになる。

次に、自己同型写像の存在、非存在によって定まる係数を決定しなければならない。類似の計算は以前の研究でも行なっているが、本研究においては、新しいパラメータ D が加わるため難度が上がり、困難を極めたが解決に成功した。最終的に示せたことは、a の square-free 部分が奇数のとき、Q_a(x; 4D, D) の自然密度を表す級数と Q_a(x; 4D, 3D) のそれが同じ形であることである。したがって両者の自然密度は一致することになる。これは本研究のための言わば補題に当たる結果であるが、それ自体としても興味深いものである。

以上の結果を総合し、剰余項の評価を終えれば冒頭で述べた主結果が得られる。

最後に数値実験について述べる。ここでも、集合 R_a(x;4,l) について、x=10^7 としたときの元の個数を計測するプログラムを準備した。計算速度を考慮して C 言語でプログラムを作成した。D_a(pq) を直接計算するより D_a(pq)=D_a(p)D_a(q)/(D_a(p), D_a(q)) という関係に着目する。つまり、D_a(p) の値のデータを準備し、あとはこの式によって、いわゆる GCD アルゴリズムを用いて D_a(pq) を計算するのである。10^7 までの素数の個数は 664579 個であるが、直積集合になっているので ((p,q) において p と q の役割を入れ替えても同じであることから、正方形状に取らなくても、正方形の半分に当たる三角形状に取れば十分である)、計算すべき (p,q) の組はおおよそ２２００億個に上る。計算に要する時間は、2.66 GHz の CPU において、１つの a について約２０時間であった。以下、いくつかの数値例を示す。以下の表は、x=10^5 から 10^7 まで３段階で #R_a(x;4,l)/π(x)^2 （π(x) は x 以下の素数の個数）を計算したものである。例としては a=13, 20, 11, 12 の場合を選んだ。初めの 2 つは a の square-free 部分が mod 4 で 1 に合同な場合、後半の 2 つはそれが mod 4 で 3 に合同な場合である。いずれの場合も、a が平方因子を含むもの、含まないものを 1 つずつ選んである。そしていずれの場合も理論値は

Γ_a(4,0)=5/9=0.555555...,
Γ_a(4,1)=1/18=0.055555...,
Γ_a(4,2)=1/3=0.333333...,
Γ_a(4,3)=1/18=0.055555...

である (l=0,2 は無条件、l=1,3 は GRH のもと)。

a=13

x	l=0	l=1	l=2	l=3
10^5	0.556690	0.055162	0.332985	0.055163
10^6	0.554714	0.055844	0.333596	0.055846
10^7	0.555568	0.055465	0.333504	0.055464

a=20

x	l=0	l=1	l=2	l=3
10^5	0.553677	0.056013	0.334307	0.056004
10^6	0.555689	0.055712	0.332883	0.055716
10^7	0.555655	0.055542	0.333261	0.055542

a=11

x	l=0	l=1	l=2	l=3
10^5	0.555764	0.055373	0.333472	0.055391
10^6	0.555451	0.055442	0.333664	0.055443
10^7	0.555532	0.055543	0.333380	0.055544

a=12

x	l=0	l=1	l=2	l=3
10^5	0.555208	0.055452	0.333889	0.055450
10^6	0.554873	0.055455	0.334217	0.055455
10^7	0.555667	0.055590	0.333154	0.055590

いずれの場合も、理論値とのよい一致を示している。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計３件）

① L. Murata and K. Chinen: On a distribution property of the residual order of a (mod pq), Annales Univ. Sci. Budapest., Sect. Comp. 41 (2013), 187-211, 査読あり.

② K. Chinen and C. Tamura: On a distribution property of the residual order of a (mod p) with a quadratic residue condition, Tokyo J. Math. 35-2 (2012), 441-459, 査読あり.

③ 知念 宏司, 田村 知佳子: 平方剰余の条件を付加した a (mod p) の剰余位数の分布について , 第 9 回 代数学と計算 研究集会 (AC2011, 首都大学東京) 報告集, pp. 93 - 101, 電子出版, 2012 年 4 月刊, 査読なし.

〔学会発表〕（計４件）

① K. Chinen: Zeta functions for linear codes and invariant polynomials, 2014 年 1 月 24 日, Workshop around algebraic combinatorics, 高知大学.

② 知念 宏司: 剰余位数の分布に関するいくつかの結果 (村田玲音氏との共同研究, および田村知佳子氏との共同研究), 2013 年 9 月 21 日, 数論研究集会, 明治学院大学.

③ K. Chinen: Zeta functions for linear

codes and their generalizations, 2012 年 3 月 3 日, Mathematical Coding Theory and its Industrial Applications, AMS Sectional Meeting 1078, University of Hawaii, Honolulu, March 3-4, 2012.
④ 知念 宏司, 田村 知佳子: 平方剰余の条件を付加した a (mod p) の剰余位数の分布について, 2011 年 11 月 9 日, 第 9 回 代数学と計算 研究集会 (AC2011), 首都大学東京.

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
知念　宏司（CHINEN, Koji）
近畿大学・理工学部・准教授
研究者番号：30419486

(2)研究分担者 なし

(3)連携研究者 なし