様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月　 ８ 日現在

機関番号：３２６０６
研究種目：基盤研究(C)（一般）
研究期間：2014～2018
課題番号：２６４０００２０

研究課題名（和文）素数ベキ分体の類数の素因子の分布

研究課題名（英文）Distribution of prime factors of the class numbers of prime-power cyclotomic fields

研究代表者
中島　匠一（NAKAJIMA, SHOICHI）

学習院大学・理学部・教授

研究者番号：９０１７２３１１

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：　円分体の類数（特に、そのマイナスパート）は整数論において重要な研究対象であるが、従来は素数分体についての計算が主眼となっていた。本研究では、その計算を素数ベキ分体にまで拡大し、類数のマイナスパートの性質を研究した。そして、素数ベキ分体の類数については、そのニューパート（＝ベキを上げるときに新しく登場する部分）達が互いに素なのではないか？という予測が（市村文男氏により）なされていて、その予測の検証が本研究の主たる目標となった。
　本研究での大規模な数値計算の結果、上記の予測は「ほとんど」成り立ちそうだが、一部の例外がある、という状況を明らかにすることができた。

研究成果の学術的意義や社会的意義
　フェルマーの最終定理への応用があることからも分かるように、円分体の類数は、代数的整数論において非常に重要な役割を果たす数である。しかし、従来の類数の計算においては、素数分体の場合が主眼であったし、類数の素因数について考察されることも少なかった。本研究では、素数ベキ分体の場合に研さん範囲を広げ、類数の素因子について新しい仮説の検証を行った。これは、類数の素因子、というテーマについて新しい局面を切り開くものである。

研究成果の概要（英文）：　Class numbers of cyclotomic fields are important object of research in Algebraic Number Theory. As to the computation of them, cyclotomic fields of prime conductors were main target of research. In this project, we enlarged the area of computation to (minus parts of) class numbers of cyclotomic fields of prime power conductors. We focused on the Hypothesis, posed by Prof. H.Ichimura, that the relative minus-part class numbers of the prime power cyclotomic fields are relatively prime to each other for all prime powers.
　On our project, we performed an extensive computation of the class numbers for prime-power cyclotomic fields, and verified that the above Hypothesis is (almost) valid in the range of our computation, finding only one exception to the Hypothesis.

研究分野：代数的整数論

キーワード：円分体　類数

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

19 世紀の E.Kummer による研究以来、円分体の（イデアル類群の）類数は代数的整数論の基本的研究対象となっている。
また、円分体の類数は「プラスパート」と「マイナスパート」の積に分解されることが（Kummer により）示されていた。
具体的には、自然数 m に対して、m 分体（＝有理数体に 1 の原始 m 乗根を添加した体）の類数（＝イデアル類群の位数）を h(m) とし、m 分体の最大総実部分体の類数を $h^+(m)$ とするとき $h^-(m) = h(m)/h^+(m)$ が整数になることがわかっていて、$h^+(m)$ と $h^-(m)$ をそれぞれプラスパートとマイナスパートと呼ぶ。
そして、Kummer 自身の研究とその後の多くの数学者の計算と考察によって、「プラスパート」と「マイナスパート」の両者は非常に対照的な性質を持っていることが明らかにされている；すなわち、類数のプラスパート $h^+(m)$ は比較的小さい値を取るのに対して、マイナスパート $h^-(m)$ は、m の増大に伴って急激に増大する。
　円分体の類数は整数論において重要な役割を果たすため、Kummer により類数が発見されて以来、多くの数学者によって類数の数値計算が行われてきた。
類数の計算は Dirichlet によって開発され、Kummer によって発展させられた「解析的類数公式」を用いて行われるのが一般的である。
特に、マイナスパートについては、一般ベルヌイ数による初等的な表示があり、そのことによって広い範囲での計算が可能となっていて、多くの数値データが得られている。
また、m 分体の考察では m が素数である場合（この場合、m = p と書くことにする）が特に重要なので、素数 p に対して、類数のマイナスパート $h^-(p)$ を計算する数値実験が広範に行われている。
しかし、数値例が多いとはいえ、$h^-(p)$ は桁数の非常に大きな整数となるため、p がある程度大きくなってしまうと、$h^-(p)$ を完全に素因数分解するのは困難な現状である。
　一方、類数のプラスパート $h^+(m)$ については、解析的類数公式を適用する場合に m 分体の基本単数系を求める必要がある。
その作業は、m が素数である場合に限定しても非常に困難であり、類数のプラスパート $h^+(p)$ の値が決定されている素数 p は限定されている。
ただし、R.Schoof などによる計算で、$h^+(p)$ の「推定値」はある程度の範囲で求められており、その「推定値」が実際の値である確率はかなり高いと思われているのは確かである。
　類数のプラスパートの計算は素数分体の場合に限定しておこなわれるのが一般的であったが、吉野健一先生（発表当時、金沢医科大学所属）により、素数ベキ分体の計算が実行され、これまで予測されていなかった現象が発見された。
その結果とは、

素数 p と自然数 n に対して、類数のプラスパートの比を
$h^+(p, n) = h^+(p^{n+d}) / h^+(p^{n+d-1})$ とおくとき、n が 2 以上ならば、 $h^+(p, n)$ の推定値はすべて 1 である

ということである。
（ここで、d は p=2 のとき 1 で、それ以外は 0 を表している；そして、この $h^+(p, n)$ が整数になることが知られている。
また、データの計算方法は下記の文献参照；計算結果は private communication により伝えられた。）
　以上が、本研究の構想に至るまでの円分体の類数計算の状況である。
この事態を踏まえて、研究を開始することになった。

文献：Y.Koyama, K.Yoshino, “Prime divisors of the class number of the real p^r th cyclotomic field and characteristic polynomials attached to them”, RIMS Kokyuroku Bessatsu, B12, 2009.

２．研究の目的

　上記の「背景」で述べたように、円分体の類数のプラスパートとマイナスパートは、数値としては対照的な振る舞いをしている。
しかし、それにも関わらず、両者の間にはある意味での「類似現象」が存在することが観察できることがある。
（プラスパートとマイナスパートは、「1 つの現象の表と裏に対応している」と見なせる場合がある。）
茨城大学・理学部数学科の市村文男氏は、類数のマイナスパートに関する過去の計算例も考慮して、プラスパートに関する上記の「$n > 1$ なら $h^+(p, n) = 1$？」という推測に対するマイナスパートでの対応物（＝類似）として、次の主張を提示した；

予測：自然数 n に対して $h\text{-}(p, n) = h\text{-}(p^n) / h\text{-}(p^{n-1})$ とおく（注：この h-(p, n) も整数であることが知られている）とき、すべての素数 p と自然数 $n > 1$ に対して h-(p, n) の素因数はすべて異なるのではないか？

本研究は、この予測の（数値実験による）検証を行うことと、予測が成立した場合の応用を探ることを目的としている。
具体的には、

1：可能な限り広範囲に h-(p, n) （p は素数で $n > 1$）の計算を実行すること
2：h-(p, n) の数値データの素因数分解への応用

を目標とした。
（正確には、当初は 1：のみを目的として研究を開始し、その後に 2：という応用に着目した。）
1：については、h-(p, n) を計算して求めてもそれを素因数分解して（市村氏の）予測を検証することはできないのだが、「素因子がすべて異なる」ことを「互いに素である」と言い換えて、ユークリッドの互除法を活用することで、この困難を回避できることに注目した。
2：の「応用」は、次のことを指している；
一般に、与えられた 2 つの自然数が互いに素になる確率は $6 / \pi^2 = 0.607\ldots$ である、という発見的推測がある。
したがって、ただランダムに自然数を選ぶだけでは、すべてが互いに素である多数の自然数の集団を見いだすことは困難であり、その結果、市村氏の推測が成り立つなら、h-(p, n) から作られる自然数の集団は、共通素因子を 1 つも持たない大きな集団、ということになる。
つまり、h-(p, n) の集団には非常に多くの（互いに異なる）素因子が含まれていることになるので、「因数分解をしたい自然数と h-(p, n) との公約数を求める」という操作によって、大きな自然数の因数分解が可能になる可能性がある。

３．研究の方法

「研究の目的」に挙げた目標のうち、1：の数値計算に関しては、p と n の増大とともに h-(p, n) が巨大な整数となってしまうことが大きな困難である。
この困難に対しては、以前から独自のプログラムにより h-(p) = h-(p, 0) の大規模な計算をおこなっていた谷口哲也氏（金沢工業大学）に協力を仰ぐこととした。
具体的には、谷口氏に本研究の連携研究者になって頂き、従来の素数分体に関する彼の計算プログラムを素数ベキ分体にも拡張して頂くことで市村氏の予測の実証計算を実行してもらった。
谷口氏のプログラムは、整数係数多項式の計算に 2 次元 FFT （高速フーリエ変換）を活用する、という独自のもので、巨大整数の高速演算と計算過程でのメモリー処理にオリジナルな手法が実装されていて、従来では不可能であった計算が実行できる。
「研究の目的」の 2：についても、谷口氏と共同で計算を行っている。
実際の計算では gmp （GNU の多倍長計算パッケージ）を利用し、1：において求めた h-(p, n) 達と因数分解したい自然数（一例は、$m > 11$ に対するフェルマー F_m ）との最大公約数を計算することで、目的の数の因数分解に挑戦している。

４．研究成果

「研究の方法」で述べたように、h-(p, n) の計算のために、従来の谷口氏のプログラムを拡張した。
そのプログラムの完成が本研究の 1 つの成果といえる。
（もちろん、計算の実行では、本研究の経費で導入した高性能計算機の果たした役割も大きいのは、当然である。）
「素数分体」から「素数ベキ分体」への拡張においては、p^n 分体から p^{n-1} 分体へのノルムの計算に当たって、従来は大規模な行列を使った複雑な計算を行っていたものを、1 のベキ根の跡に関する（数論的な）公式の活用によって、大幅に簡単化することができた。
そのことによって、p^n が 10^7 を（少し）越える値の範囲で h-(p, n) を計算することができた。
ちなみに、実行した計算の範囲での h-(p, n) の「最大値」は h-(17, 6) であり、これは（10 進で）637,620,997 桁の巨大な数となっている。
本研究の主題である市村氏の予測であるが、膨大なデータを集めた結果として、

現状：予測は「ほとんど」成り立っているが、「例外」も存在する

という、微妙な状態になっている。
具体的には、我々の計算した範囲で

例外：gcd(h-(2, 10), h-(2, 11)) = 83969 > 1

という「例外」が存在しているが、その他の h-(p, n) はすべて互いに素、となっている（gcd は最大公約数を表している）。
計算機資源の限界により我々の計算範囲を広げることができないため、この「例外」が真の（つまり、ただ 1 つの）例外であるのか、または、ある程度の割合で生じる「一般的な」数値例なのか、の判定が出来ていない。
市村氏の推測を理論的にサポートする方法も見つけることができないので、「推測」の正否を決定する決め手が全くない状態になっている。
このため、本研究で、従来行われなかった独自の計算を行ったにも関わらず、残念ながら、明確な「成果」を提示することはできていない。
しかし、計算機実験を行った広い範囲の数値について「推測」が成立している、という結果には大きな意義があると考えている。
　市村氏の予測の正否は確定できていないとはいえ、一部の例外を除けば、h-(p, n) 達がほとんど互いに素であることは確かである。
したがって、「研究の目的」で述べた 2：の（因数分解への）応用は、成果が得られる見込みがある。
この見込みのもと、本研究で得られた数値データを利用して、研究の最終年度から、フェルマー数の因数分解に挑戦している（そのためのプログラムを作成し、継続的に計算を行っている）。
しかし、やはりフェルマー数の因数分解は困難であり、残念ながら、まだ新しい素因数は発見できていない。
とはいえ、本研究において整備した計算機環境とソフトウェアは今後も利用可能なので、継続的にまだ素因数分解ができていない自然数の因数分解に挑んでいく計画である。

５．主な発表論文等

〔雑誌論文〕（計　　件）

〔学会発表〕（計　　件）

〔図書〕（計　　件）

〔産業財産権〕
○出願状況（計　　件）

○取得状況（計　　件）

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者

(2)研究協力者
研究協力者氏名：谷口 哲也
ローマ字氏名：Taniguchi Tetsuya