様式 C-19

科学研究費補助金研究成果報告書

平成 20 年　5 月 31 日現在

研究種目：　基盤研究（C）
研究期間：　２００６～２００８
課題番号：　１８５４００５４
研究課題名（和文）　一般の剰余類群における剰余位数・剰余指数の分布

研究課題名（英文）　On the distribution of the residual order/index of the residual class a(mod n) in the residual group with composite moduli.

研究代表者
村田　玲音（MURATA LEO）
明治学院大学　経済学部　教授
３０１５７７８９

研究成果の概要：
素数 p を法とする剰余類群は、位数 p－1 の単純な巡回群になる。自然数 a を固定し、素数 p を動かして剰余類 a(mod p)の位数の分布を調べる問題は、すでに村田-知念によってほぼ解決している。ところが二つの異なる素数の積 pq を法とする剰余類群は、群構造が複雑になり、例えば原始根の分布問題等は、素数 p の剰余類群の場合と大きく異なった様相を呈する。今回は剰余類 a(mod pq)の位数の分布を p,q を動かした場合に調べ、この問題の場合、現象としては素数 p を法とする場合と大きな違いはなさそうだという結論を得た。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,000,000	0	1,000,000
2007 年度	800,000	240,000	1,040,000
2008 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	2,800,000	540,000	3,340,000

研究分野：　数物系科学
科研費の分科・細目：　数学、代数学、数論、解析的整数論
キーワード：　剰余位数、剰余指数、原始根、Code 理論

１．研究開始当初の背景

自然数 n を法とする剰余類群（Z/nZ）* は整数論の色々なところで現れる非常に重要な研究対象である。n＝p が素数の場合、これは単純な p－1 次の巡回群になる。ここで「自然数 a を固定し､素数 p を動かしたとき、剰余類 a(mod p)の剰余位数はどのような分布を示すか？」という問題を考える。

この問題は 2003 年頃より村田-知念によって研究され、詳しい成果が得られている。それによれば「一般リーマン予想を仮定し、a(mod p)の剰余指数を自然数 k を法とする剰余によって分類すると、各剰余類には自然密度 Δ(a,k)が存在する」のである。この密度 Δ(a,k)の値も、完全に決定するアルゴリズムが与えられている。

この問題を、法が合成数の場合に考えてみたいというのが一番大きな動機であった。

２．研究の目的

今回は法 n (modulus)として合成数の場合を考えるが、特に「n が二つの異なる素数の積 pq の場合」、これは暗号の世界で有名な RSA 公開鍵暗号の理論とも関連すると思われる。

また、剰余位数と剰余指数の積が(p－1)(q－1)になることから、剰余指数の分布とも関連する。興味深いのは、剰余指数の分布問題で一番良く研究されている「原始根に関する Artin 予想」では、法が合成数になると法が素数の場合とまったく違った現象が起きることで(Pomerance 達の結果による)、剰余位数の場合も違った現象が見られるかどうか、これが一つの焦点であった。

さらに剰余位数の分布問題を解析数論の立場から研究する場合、数論的関数の利用が重要な鍵になる。そこでもっと広い観点から、数論的関数と Code 理論の関係を研究するのも目的の一つである。

３．研究の方法

本研究は、理論的・実験的の双方向から進めた。

実験的方法とは、計算機実験を積み重ねて、その中から法則性を見つけようという立場で、これは素数を法とする剰余類群の場合に、村田-知念が用いて成功した方法である。具体的には、base と呼ばれる自然数 a (これは小さく取っておく)を固定し、二つの素数 p,q を選んで a(mod pq)の類の剰余位数を計算し、p,q をかなり先まで(どちらも 10^8 位まで)動かしてみて、剰余位数の、４を法とした各類への分布状態を調べた。

理論的な方向では、まず「a(mod pq)の類の剰余位数」を「a(mod p)の類の剰余位数」と「a(mod q)の類の剰余位数」によって書き表わすことを考え、これを実現する数論的関数を構成した。これによって、法が素数 p の場合の議論に帰着させる方向を試みた。

４．研究成果

今回の研究成果は大きく二つの方向に分けることができる。

１　剰余位数の分布に関するもの

上記の『研究の方向』で述べたように、ここでは「a(mod pq)の類の剰余位数を、４を法とする剰余によって分類し、その各々の類での自然密度」を問題にした。法として４を選んだのは、経験的に「面白い現象は既に法４で見られる」からである。一般的に言って、自然密度を持つ現象は、分布がかなり“均一”でなくてはならない。法が合成数の場合にこの均一性があるかどうかが焦点である。

これまでに我々の得た計算結果によれば、「自然密度」はほぼ間違いなく存在するようである。これは、「一般の剰余類群において剰余指数の分布は偏りが大きく、自然密度が存在しない」という Pomerance 達の結果と好対照をなす現象である。

理論的な方向では、特殊な剰余類での分布密度を求めることができた。a(mod pq)の類の剰余位数が自然数 k で割り切れる場合の密度は、一般の k に対して求めることができ、しかもこの部分に一般リーマン予想の仮定は不必要である。ただ、一般の剰余類での自然密度の存在は、まだ完全な証明を得るところまでは至らなかった。

２　数論的関数と Code 理論の関係に関するもの

Code 理論では２進数表示が重要であるが、神谷論一氏と村田による共同研究で、「数の２進法表示(Binary Code)から作った Sum of digits 関数と非常に単純な数論的関数の間に、非常に深い繋がりがある」ことが分かってきた。こうした興味ある繋がりが出てくる理由を調べると同時に、別の Code と数論的関数の間に、同種の関係がないかどうか調べ、Gray Code と呼ばれる特殊な Code と数論的関数の間にも似たような関係が成り立つことが分かった。この興味ある関係は、今後更に色々な Code と数論的関数の間に成り立つと思われる。

また主として知念宏司氏の研究であるが、Code からゼータ関数を構成し、その関数論的な性質を調べることによって、Code の研究を進めるという面でも成果があった。ゼータ関数の理論では　リーマン予想という未解決の予想が重要であるが、Code から作ったゼータ関数のあるものはリーマン予想を満たすことが示されている。

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　6件）

[1]
L. Murata, K. Chinen,
On a distribution property of the residual order of a (mod p), part III,
J. of Math. Soc. Japan,
Vol. 58-3 (2006) pp. 693-720.
査読：有

[2]
L. Murata, K. Chinen,
On a distribution property of the residual order of a (mod p), part IV,
"Number Theory: Tradition and Modernization",
Edited by Y. Tanigawa and W. Zhang,
Springer Science, (2006) pp. 11-22.
査読：有

[3]
Leo Murata, Yuichi Kamiya,
On the average of some q-additive functions,
Annales Univ. Sci. Budapest., Sect. Comp.,
Vol. 29 (2008) pp.39-63.
査読：有

[4]
T. Hadano, Y. Kitaoka, T. Kubota, M. Nozaki
Densities of sets of primes related to decimal expansion of rational numbers,
"Number Theory: Tradition and Modernization",
Edited by Y. Tanigawa and W. Zhang,
Springer Science, (2006) pp. 67-80.
査読：有

[5]
Y. Kitaoka,
A statistical relation of roots of a polynomial in different local fields,
Mathematics of Computation,
Vol. 78 (2009), pp. 523-536.
査読：有

[6]
K. Chinen,
An abundance of invariant polynomials satisfying the Riemann hypothesis,
Discrete Math.,
Vol. 308 (2008), pp. 6426-6440.
査読：有

〔学会発表〕（計　3件）

(1)
村田　玲音,
On a property of the multiplicative order of a(mod p),
The 4th Japan-China Seminar on Number Theory,
2006年9月3日, 中国・山東大学.

(2)
村田　玲音,
Some q-additive functions and related topics,
The 5th Japan-China Seminar on Number Theory,
2008年8月28日, 近畿大学・理工学部.

(3)
北岡　良之,
A statistical relation of roots of a polynomial in different local fields,
The 5th Japan-China Seminar on Number Theory,
2008年 8月30日, 近畿大学・理工学部.

〔図書〕（計　0件）

なし

〔産業財産権〕
○出願状況（計　0件）

なし

○取得状況（計　0件）

なし

〔その他〕

なし

６．研究組織

(1)研究代表者
村田　玲音
明治学院大学・経済学部・教授
３０１５７７８９

(2)研究分担者
北岡　良之
名城大学・理工学部・教授
４００２２６８６

岡崎　龍太郎
同志社大学・工学部・専任講師
２０２６８１１３

知念　宏司
近畿大学・理工学部・准教授
３０４１９４８６

(3)連携研究者

特になし