様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年　6 月　1 日現在

機関番号：　３２６８３
研究種目：　基盤研究（C）
研究期間：　２００９　～　２０１１
課題番号：　２１５４００２７
研究課題名（和文）　数論的関数と Code 理論・剰余位数の分布

研究課題名（英文）　Arithmetical Functions, Code Theory and Distribution properties of the Residual Order

研究代表者
村田 玲音　(Murata Leo)
明治学院大学・経済学部・教授
研究者番号：　３０１５７７８９

研究成果の概要（和文）：
Code の Sum of digits と呼ばれる関数があって、複雑な挙動を示すことで知られている。本研究では《Code の Sum of digits と数論的関数の間に 1 対 1 の対応関係がある》ことを示した。これによって Code の Sum of digits 関数（複雑な関数）を、（単純な）数論的関数によって調べることができる。成果として、Gray code から得られる Sum of digits の精密な平均値を求めたり、Sum of digits とオートマトンその他の対象との関連を明らかにすることができた。

研究成果の概要（英文）：
From a code C, we can define the “sum of digits function” f_C(n), usually f_C(n) fluctuates quite irregularly. In this research, we proved “a one-to-one correspondence between arithmetical functions and the sum of digits function of code C’s”. This result enables us to control complex sum-of-digits functions by simple arithmetical functions. As an application, we can obtain the Delange-type average of sum-of-digits function of Gray code. We also consider relations between sum-of-digits function and Automaton etc.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,000,000	300,000	1,300,000
２０１０年度	800,000	240,000	1,040,000
２０１１年度	900,000	270,000	1,170,000
年度			
年度			
総　計	2,700,000	810,000	3,510,000

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：　解析的整数論、数論的関数、Code 理論、剰余位数

１．研究開始当初の背景

数論的関数と Code 理論の関係を、明確に論じた研究はこれまで特には知られていない。村田-神谷は《通常の q 進数の Sum of digits function の平均値》に関する Delange

の古典的な研究を詳しく調べた結果、この研究の背後には数論的関数と Code の間の深い関係があることに気づいていた。今回の研究の最初の目的は、この両者の関係を明確にし、さらには Delange による《平均値定理》がどこまで広く成立するのか、その拡張を考えることであった。

剰余位数の分布問題は直接 Code とは関連しないが、現代暗号の中心的存在である。RSA 公開鍵暗号では、異なる素数の積 pq を法とする剰余類群の性質が使われる。そこでその基礎研究の一つとして、pq を法とする剰余位数の分布を研究すること、特に法 p の剰余位数の持っている分布的特性が、法 pq でも同様に成立するかどうか、これが研究したい第二の目的である。

２．研究の目的

(1) Code とは、有限個の記号によって自然数に一律に番号付けをする方法のことと解し、これと数論的関数の関係を明らかにすることが第一の目的である。Code をなるべく単純な数論的関数と関連づけて、その Code に関する多くの事柄が数論的関数によってコントロールされている様子を明らかにしたい。

(2) p,q を異なる素数とする。これを $p \leqq x$ かつ $q \leqq x$ の条件下で独立に動かしたとき、固定しておいた剰余類 a(mod pq)の剰余位数が「k を法とする剰余類にどのように分布するか」その分布特性を調べる。

３．研究の方法

(1) 上述の Delange による先駆的な《q 進数の Sum of digits function の平均値》定理の証明を見直し、我々が気づいた《数論的関数と Code の間の関係》を反映させた別証明を与える。この証明に必要な要素を吟味することによって、より広い範囲の Code について、Delange 流の平均値定理を得ることができる。

(2) 既に村田-知念の一連の研究によって、素数 p を法とする場合の a(mod p)の剰余位数の分布については、「k を法とする剰余類にどのように分布するか」が、かなりの範囲まで解明されている（主要な結果は《主な発表論文等》の後半に挙げてある）。この方法を元にして、これを mod pq の場合にどのように進めれば同様の結論が得られるのか、証明のテクニックを開発する。

４．研究成果

数論的関数と Code 理論の間の関係については、十分な成果が得られた。詳細は私と神谷氏（研究分担者）の共著論文①②に詳しくまとめられている。

(1) Code C から自然に、その Sum of digits function f_C(n) を定義することができる。この差分数列 { f_C(n)－f_C(n－1) }_{n=1}^{∞} と数論的関数の間には密接な関係があり、これを定式化することにより、{Code の Sum of digits（複雑な関数)} と {(単純な)数論的関数} の間に《１対１写像》を定義することができた（雑誌論文①の Theorem 1.1)。この定理が、今回の研究テーマである《数論的関数と Code 理論》への基本的な解答である。

Code の中に特殊な条件を満たす Gray code というものが知られているが、これに上記の定理を応用すると、これらに対応する数論的関数が“周期性”“Zero sum 性”といったきれいな条件を満たすことが示せる。この帰結の一つとして、Gray code から得られる Sum of digits function についても Delange 型の平均値定理が得られることが示せた。これは

Delange の定理の大幅な拡張になっている。

(2) 上の研究の一つの帰結として、「Reflected binary code (RBC, Gray code の一つ)の Sum of digits function の差分数列と regular paper-folding sequence が一致する」という興味ある結果が得られた。これの拡張を試みて、目的通りの成果を得た。

RBC を参考にして新たに一般的な Code C を導入すると、「Code C の Sum of digits function の差分数列と Generalized paper-folding sequence が一致する」という結果が得られた。ここで新たに導入された Code C の性質も、ある程度まで調べてある。最も大きい特徴は、この code が自然数集合Nから整数集合Ｚへの全単射になっていることであろう。Generalized paper-folding sequence は超越数論などでも用いられる極めて興味ある研究対象である。これと code, Sum of digits function が結びついたのは面白い現象である。

数論的関数と Code 理論については、今回の研究によってオートマトンや超越数論など、様々な分野との接点が顕われてきたので、今後の発展が期待できる。

(3) 剰余位数の研究については、目的であった「k を法とする剰余類にどのように分布するか」までは到達できなかったが、「a に多少の条件を付け、かつ k＝４の場合」に限って、十分満足すべき結果を得た。法が pq の場合にも、法 p の場合同様、《剰余位数≡i (mod 4)》で(p, q)を分類すると、i＝0, 1, 2, 3 に対してそれぞれの集合は自然密度を持ち、それは《均一分布》ではなかった。なお、この証明の一部には一般リーマン予想を使っている。自然密度の存在や仮定の使い方などは mod p の場合と同じで、要するに《法 pq の剰余位数も、法 p の剰余位数と極めて似た分布状態を示す》ことが示せた。このことは、剰余位数に関する限り、mod p から mod pq への移行は、そんなに複雑ではないことを示唆している。

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４件）

① Yuichi KAMIYA and Leo MURATA, Certain codes related to generalized paper-folding sequences, Journal de Theorie des Nombres de BORDEAUX, Vol. 25 (2013), (to appear). 査読有

② Yuichi KAMIYA and Leo MURATA, Relations among arithmetical functions, automatic sequences and sum of digits functions induced by certain Gray codes, Journal de Theorie des Nombres de BORDEAUX, Vol. 24 (2012), pp 307-337. 査読有

③ 村田玲音、剰余位数の分布について、経済研究(明治学院大学)、第 145 号 (2012)、pp 55-66. 査読なし

④ 村田玲音、原始根や剰余位数にまつわる話、数学セミナー、査読なし、2013 年 7 月号

⑤ Koji Chinen and Leo Murata, On a distribution property of the residual order of a (mod p) IV, “Number Theory, Tradition and Modernization”, Springer Science (2006), pp 11-22. 査読有

⑥ Koji Chinen and Leo Murata, On a distribution property of the residual order of a (mod p) III, J. of Mathematical Society of Japan, Vol. 58 (2006), pp 693-720. 査読有

⑦ Leo Murata and Koji Chinen, On a distribution property of the residual order of a (mod p) II, J. of Number Theory, Vol. 105 (2004), pp 82-100. 査読有

⑧ Koji Chinen and Leo Murata, On a distribution property of the residual order of a (mod p), J. of Number Theory, Vol. 105 (2004), pp 60-81. 査読有

〔学会発表〕（計２件）

① 村田玲音、(Z/pZ)* や (Z/pqZ)* での剰余位数・剰余指数の分布について、日本数学会、2011 年春の学会（特別講演）、2011.10.1 信州大学

② Leo Murata, On a distribution property of the multiplicative order of a(mod p) and a(mod pq), Colorado Kempner Colloquium, 2010.9.30, Colorado Univ. in Boulder, Colorado, USA（アメリカ）

６．研究組織

(1)研究代表者

村田 玲音（Murata Leo）
明治学院大学・経済学部・教授
研究者番号：　３０１５７７８９

(2)研究分担者

知念 宏司（Chinen Koji）
近畿大学・理工学部・准教授
研究者番号：　３０４１９４８６

神谷 諭一（Kamiya Yuichi）
大東文化大学・経済学部・講師
研究者番号：　９９５５３４１２

(3)連携研究者

なし