

## キーワード

符号のゼータ関数、不変式環、リーマン予想、原始根分布、剰余位数分布

Zeta function for code, invariant polynomial ring, Riemann hypothesis, distribution of primitive roots, distribution of residual orders

## 研究内容

### [1] 剰余位数分布に関する研究

・ $a$  を 2 以上の自然数とし、 $p$  を素数とする。このとき  $a^m \equiv 1 \pmod{p}$  を満たす最小の自然数  $m$  を  $a$  の  $\text{mod } p$  での剰余位数という。これを以下  $D_a(p)$  で表す。これは整数論においてきわめて自然に現れる重要な量であるが、 $a$  を固定して  $p$  を動かしたときの  $D_a(p)$  の挙動は、数論的にきわめて扱いづらい。

・ここでいう剰余位数分布の問題とは、 $D_a(p)$  の値を  $\text{mod } k$  で分類する問題である。つまり、

$$Q_a(x; k, l) = \{p \leq x; D_a(p) \equiv l \pmod{k}\}$$

という素数集合を考え、その自然密度を求めるのである。 $l=0$  の場合は比較的易しく、Hasse, Odoni らの結果がある。しかし、 $l$  が 0 でないときは非常に難しく、過去にこの場合を扱った研究はなかった。

・筆者はかつて、村田玲音氏 (明治学院大学) との共同研究において、 $k=4, l=1,3$  の場合に、 $a$  に関する軽い制限と、一般リーマン予想 (以下 GRH) の仮定の下で、 $Q_a(x; k, l)$  の自然密度を剰余項付きで決定することに成功した。ついで  $k=q^i$  ( $q$  は素数) の場合を扱い、同様の仮定のもとで  $Q_a(x; q^i, j)$  ( $0 \leq j \leq q^i - 1$ ) の自然密度を決定した。さらに一般の  $k, l$  の組に対して、GRH のもとで  $Q_a(x; k, l)$  の密度を計算するアルゴリズムが存在することを示した。これらの結果は 2004 年から 2006 年にかけて 4 編の査読付き論文として発表した。その最後のものは [1] である。

・この方向の筆者の最新の結果は [3] である。これは田村知佳子氏 (筆者が指導した大学院生) との共同研究である。これは上記  $Q_a(x; k, l)$  に、さらに条件  $(b/p)=1$  を付け加えた集合  $S_{a,b}(x; k, l)$  を考えるものである。ただし、 $b$  はあらかじめ選んだ整数、 $(b/p)$  はルジャンドル記号である。この条件を付け加えることで集合  $Q_a(x; k, l)$  は二分されるが、 $a, b$  が代数的に影響を与えることで、等分されない場合がある。本結果は、 $l=0$  の場合に、どのような場合に二等分されるか、あるいはされないか、されないとすると密度はどうなるかを決定したものである。

### [2] 線型符号および不変式のゼータ関数とそのリーマン予想

・線型符号のゼータ関数は、1999 年に I. Duursma によって定義された、比較的新しい概念である。そ

れは代数曲線のゼータ関数と非常によく似た性質をもっている。大きく異なるのはそのリーマン予想で、符号のゼータ関数の場合、リーマン予想を満たす符号とそうでない符号の両方が実在する。実在の自己双対符号に関しては、「extremal 符号はリーマン予想を満たすか」という問題があり、一部しか解決されていない。

- ・筆者らは、このテーマの新しい方向の研究として、まず符号のゼータ関数の定義を formal weight enumerator と呼ばれる一群の不変式に拡張し、extremal なものはリーマン予想を満たすことを示唆するいくつかの数値実験例を提示した。
- ・ついで、扱う不変式の範囲を、MacWilliams 変換で不変な斉次多項式全体まで拡張し、そこにリーマン予想を満たす不変式がかなり多く存在することを示した ([2])。ここでは、任意の線型符号の重み多項式から不変式を構成する一般的方法も与えている。この結果により、リーマン予想を満たす不変式をさらに多く構成できる可能性が生じ、このテーマに関する 1 つの新しい研究方法が開発されたと言ってよい。

## 最近の業績

- [1] Chinen, K. and Murata, L. : On a distribution property of the residual order of  $a \pmod{p}$  – IV, in *Number Theory: Tradition and Modernization*, W. Zhang and Y. Tanigawa, eds., Developments in Math. 15, 11-22, Springer Verlag, 2006.
  - [2] Chinen, K. : An abundance of invariant polynomials satisfying the Riemann hypothesis, *Discrete Math.* 308 (2008), 6426-6440.
  - [3] Chinen, K. and Tamura, C. : On a distribution property of the residual order of  $a \pmod{p}$  with a quadratic residue condition, *Tokyo J. Math.* 35-2 (2012), 441-459.
- 科学研究費 基盤研究 (C) 代表 (平成 20-22 年度 230 万円)
  - 科学研究費 基盤研究 (C) 代表 (平成 23-25 年度 190 万円)
  - 科学研究費 基盤研究 (C) 分担 (平成 19-20 年度 20 万円)
  - 科学研究費 基盤研究 (C) 分担 (平成 21-22 年度 22.5 万円)
  - 京都大学数理解析研究所 解析的整数論研究集会 研究代表者 (2012.10.29-31)
  - 上の研究集会が文部科学省「平成 24 年度 数学・数理科学と諸科学・産業との連携研究ワークショップ」に採択 (助成額 76020 円)