

# 有限体上の方程式の解の個数の研究

石川 恒男 (いしかわ つねお)  
工学部 一般教育科 教授

用途・応用分野：数学、離散数論、計算理論

## ■ 研究概要

素数  $p$  に対して整数全体  $Z$  を  $p$  で割った余り全体は普通の計算で有限体  $F_p = Z/pZ$  となるが、 $F_p$  上で方程式を考えると各素数  $p$  について様々な性質を持つ。

例えば、 $e$  を自然数として、 $p$  を  $e$  を法として 1 となる素数とすると、方程式

$$X_1^e + X_2^e + X_3^e + \cdots + X_n^e = 0$$

の解の個数  $T_e(n)$  は、 $e=3$  のとき

$$\sum_{n=1}^{\infty} T_3(n)x^n = \frac{x}{1-px} + \frac{x^2(p-1)(2+dx)}{1-3px-pdx^2}$$

と表される。ここで  $d$  は

$$4p = d^2 + 27b^2, \quad d \equiv 1 \pmod{3}$$

をみだす。自然数  $e=3, 4, 5, 6, 7, 8$  についてガウス和とヤコビ和を用いて完全な計算結果を得た。

## ■ 研究の特徴

ガウス和とヤコビ和を用いることで数列の母関数を与える。

- ① ガウス和
- ② ヤコビ和
- ③ 母関数

