

背景と動機

- 有限体上の楕円曲線：暗号理論の重要な一対象
- 二元四次形式：
 - 楕円曲線と付加データの組を圧縮表現できる
 - 特異な形式：圧縮データに対応しない形式

研究目的： 二元四次形式を通じて、
楕円曲線を統計的に理解する基礎研究

→ まず特異な形式の分布を解析する

設定と記号

- 二元四次形式：次の形の多項式（係数は有限体）

$$v(x, y) = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4$$
 - 方程式 $z^2 = v(x, 1)$ ：楕円曲線を含む「曲線」
 - $z^2 = v(1, 0)$ の解：付加データ
- V ：二元四次形式全体の集合
- Φ ： V のなかで重根を持つ形式を判定する関数

$$\Phi(v) = \begin{cases} 1 & (v \text{ が重根を持つ} = \text{特異な形式}) \\ 0 & (\text{その他}) \end{cases}$$

主定理とその帰結

- Φ のフーリエ係数 $\hat{\Phi}$

$$\hat{\Phi}(w) = \underbrace{\frac{1}{|V|}}_{\text{正規化}} \underbrace{\sum_{v \in V} \Phi(v) \exp\left(\frac{2\pi i w \cdot v}{p}\right)}_{\text{離散フーリエ変換}}$$

- 重根を持つ形式の頻度・偏りを考察できる

定理： $\hat{\Phi}(w)$ の値の具体的な決定

- 特異形式は例外的にほぼ一様に分布
- 以前は一般論から得られる不等式評価のみ
(波及：有理数体上の楕円曲線の統計的性質)

手法：組合せ論 × 不変式論

$$\hat{\Phi}(w) \xrightarrow{(1)} \underbrace{\quad}_{(2)} \quad \text{〔代数方程式の有限体での解の個数〕}$$

- 多重集合の組合せ論で数え上げ問題に再解釈
- 古典的不変式論でその値を決定

参考文献：Y. Ishitsuka, T. Taniguchi, F. Thorne and S. Y. Xiao,
Exponential sums over singular binary quartic forms and applications.
arXiv: 2404.00541