アーベル曲面の $\mathrm{mod}\ p$ 巡回性

山内卓也 (広島大学大学院理学研究科)

1. はじめに ••• :

暗号理論

⇓

大きな位数を持つ巡回群がほしい.

巡回群:

1. $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$, 生成元は自明

2. $(\mathbb{Z}/p\mathbb{Z})^* = \langle \overline{a} \rangle$, 生成元の決定は非自明

原始根分布問題 (Artin, R.Murty,..., 知念, 村田..)

3. A: $\mathbb{Q}$上定義されたアーベル多様体.

   $\widetilde{A}$: 素数pにおける法p還元.

法p還元$\widetilde{A}$が良い還元

$\Downarrow$

有限群$\widetilde{A}(\mathbb{F}_p)$を得る.

問題:

$\widetilde{A}(\mathbb{F}_p)$が巡回群となるような素数$p$はどのくらいあるか？:

アーベル多様体Aが与えられたとき,

$$C_A = \lim_{X\to\infty} \frac{\sharp\{p \leq X \mid \tilde{A}(\mathbb{F}_p) \text{ is cyclic}\}}{\sharp\{p \leq X\}}$$

を計算したい.

2. 諸結果:

$A = E$: $\mathbb{Q}$ 上の楕円曲線.

Theorem (Serre, R.Murty) GRHの仮定の下で,

$$C_E = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} = \prod_{l} (1 - \frac{1}{[\mathbb{Q}(E[l]) : \mathbb{Q}]})$$

$\mathbb{Q}(E[m])$: $\mathbb{Q}$ に E の m 等分点を添加した体.

$\mu(m)$:メービウス関数.

Theorem (Serre)

E がnon-CM 楕円曲線ならば, ほとんどすべてのl に対して、

$$(*)\ [\mathbb{Q}(E[l]) : \mathbb{Q}] = \sharp \mathrm{GL}_2(\mathbb{F}_l) = (l^2 - 1)(l - 1).$$

例: $E : y^2 + y = x^3 - x$, $\mathrm{cond}(E) = 37$. この場合すべての素数l に対して、$(*)$が成立. 特に、

$$C_E = 0.81375190 \cdots\cdots .$$

Theorem (R.Gupta)

$E_1 : y^2 = x^3 - ax, a \in \mathbb{Z}\backslash\{0\}$ は squarefree .

$$C_{E_1} = \frac{1}{4} + \begin{cases} \dfrac{1}{2}\delta_{E_1} & (a \text{ is even}) \\ \dfrac{1}{2}(1 - A_{E_1}(a))\delta_{E_1} & (\text{otherwise}) \end{cases}$$

$$A_{E_1}(a) = \prod_{\substack{p|a \\ p \equiv 1 (\mathrm{mod} 4)}} \frac{1}{p(p-2)} \prod_{\substack{p|a \\ p \equiv -1 (\mathrm{mod} 4)}} \frac{1}{p^2 - 2}$$

$$\delta_{E_1} := \prod_{p\equiv 1(\mathrm{mod}4)} (1-\frac{1}{(p-1)^2}) \prod_{p\equiv -1(\mathrm{mod}4)} (1-\frac{1}{p^2-1})$$

$$= 0.388745\cdots .$$

aを動かしたとき、E_1の巡回性密度の動く範囲:

$$0.42<C_{E_1}<0.44$$

Theorem (竹内)

$E_2 : y^2 = x^3 - a, a \in (\mathbb{Z}\backslash\{0\})$ + conditions .

$$C_{E_2} = \frac{1}{2} + \begin{cases} \frac{1}{2}(1 - B_{E_2}(a))\lambda_{E_2} & (a \equiv \pm 1 \bmod 9) \\ \\ \frac{1}{2}(1 + \frac{1}{5}B_{E_2}(a))\lambda_{E_2} & (\text{otherwise}) \end{cases}$$

$$B_{E_2}(a) = \prod_{\substack{p|a \\ p \equiv 1 (\mathrm{mod} 3)}} \frac{1}{p(p-2)} \prod_{\substack{p|a \\ p \equiv -1 (\mathrm{mod} 3)}} \frac{1}{p^2 - 2}$$

$$\lambda_{E_2} := \frac{5}{6} \prod_{p\equiv 1(\mathrm{mod}3)} (1-\frac{1}{(p-1)^2}) \prod_{p\equiv -1(\mathrm{mod}3)} (1-\frac{1}{p^2-1})$$

$$= 0.5011126\cdots .$$

aを動かしたとき、E_2の巡回性密度の動く範囲:

$$0.43<C_{E_2}<0.44$$

Open case:

$$\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}),$$
$$\mathbb{Q}(\sqrt{-43})\mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163})$$

3. アーベル曲面の場合:

A: $\mathbb{Q}$ 上定義された主偏極アーベル曲面

密度C_Aの確率論的解釈：

素数lに対して,

$$T_l := \{\sigma \in \mathrm{Gal}(\mathbb{Q}(A[l])/\mathbb{Q}) |\ \dim_{\mathbb{F}_l}(A[l])^\sigma \geq 2\}$$

$$S_l := \{p : \text{素数} \mid {}^{\exists}\mathfrak{p} | p : \mathbb{Q}(A[l])\text{の素点} \text{s.t } \mathrm{Frob}_{\mathfrak{p}} \in T\}$$

$$S_l\text{の密度} = \frac{\sharp T_l}{\sharp \mathrm{Gal}(\mathbb{Q}(A[l])/\mathbb{Q})}$$

(by Čhevotarev の密度定理)

$$S_l \approx \{p : \text{素数} \mid \widetilde{A}(\mathbb{F}_p) \supset (\mathbb{Z}/l\mathbb{Z})^{\oplus 2}\}$$

$$\widetilde{A}(\mathbb{F}_p)\text{が非巡回的} \Longleftrightarrow \widetilde{A}(\mathbb{F}_p) \not\supset (\mathbb{Z}/l\mathbb{Z})^{\oplus 2}$$
$$\text{for } {}^{\forall} l = 2, 3, 5, 7, 11, \ldots.$$

よって、確率論的密度は

$$P_A = \prod_l (1 - (S_l\text{の密度}))$$
$$= \prod_l (1 - \frac{\sharp T_l}{\sharp \mathrm{Gal}(\mathbb{Q}(A[l])/\mathbb{Q})}) \text{ となる.}$$

確率論的密度P_Aの計算は$\sharp T_l, \sharp \mathrm{Gal}(\mathbb{Q}(A[l])/\mathbb{Q})$の計算に帰着された.

Theorem. Aを主偏極アーベル曲面とする.
$\mathrm{Gal}(\mathbb{Q}(A[l])/\mathbb{Q}) \simeq \mathrm{GSp}(4, \mathbb{F}_l), l \geq 3$のとき、

$$\sharp T_l = l^2(2l^5 - l^4 - l^3 - l^2 - 3l - 1)$$

数値実験: $C : y^2 = x^5 - x + 1$, $\mathrm{End}_{\mathbb{Q}}(J(C)) = \mathbb{Z}$

Fact: (1) $\mathrm{Gal}(\mathbb{Q}(J(C)[l])/\mathbb{Q} = \mathrm{GSp}(4, \mathbb{F}_l)$ for $l \geq 3$

(ただし、GRHの仮定が必要)

(2) $\mathrm{Gal}(\mathbb{Q}(J(C)[2])/\mathbb{Q} = \mathfrak{S}_5$

$$\Longrightarrow 1 - \frac{\sharp T_2}{\sharp \mathrm{Gal}(\mathbb{Q}(J(C)[2])/\mathbb{Q}} = 1 - \frac{46}{5!} = \frac{37}{60}$$

$$P_{J(C)} = 0.5945673\cdots$$

期待:

$$C_A = \lim_{X\to\infty} \frac{\sharp\{p \le X \mid \tilde{A}(\mathbb{F}_p) \text{ is cyclic}\}}{\sharp\{p \le X\}} = P_{J(C)}$$

TABLE 1. $J(C)(\mathbb{F}_p)$ が巡回群である p の密度について

範囲	素数の個数	Type1	Type2	Type3	巡回率 1	巡回率 2
$1 < p < 1000$	163	62	91	10	0.5947712	0.5582822
$1 < p < 2000$	298	108	176	14	0.6197183	0.5906040
$1 < p < 3000$	425	151	258	16	0.6068702	0.6070588
$1 < p < 4000$	544	206	318	20	0.6068702	0.5845588
$1 < p < 5000$	663	243	393	27	0.6179245	0.5927602
$1 < p < 6000$	777	295	453	29	0.6056150	0.5830116
$1 < p < 7000$	894	340	524	30	0.6064815	0.5861298
$1 < p < 8000$	1001	389	578	34	0.5977249	0.5774226

ただし，$p = 2, 3, 5$ と $19, 151$(bad prime) を除く．

Type 1：$J(C)(\mathbb{F}_p)$ が巡回群でない p　　巡回率 1 := $\frac{\#\{\text{Type 2 の素数}\}}{(\text{素数の総数})}$

Type 2：$J(C)(\mathbb{F}_p)$ が巡回群である p　　巡回率 2 := $\frac{\#\{\text{Type 2 の素数}\}}{(\text{素数の総数}) - \#\{\text{Type 3 の素数}\}}$

Type 3：$J(C)(\mathbb{F}_p)$ の巡回性不明な p (高い確率で非巡回であることが予想される)

(* この計算は電通大の金山氏に協力して頂きました.)

広島大学大学院理学研究科数学専攻
山内卓也
e-mail:yamauchi@math.sci.hiroshima-u.ac.jp