一般三浦曲線の算術種数について

On the arithmetic genus of a Miura curve

中央大学大学院　理工学研究科　数学専攻　田中翔太
ＴＡＮＡＫＡ　Ｓｈｏｔａ

１９７６年にＤｉｆｆｉｅとＨｅｌｌｍａｎによって提案された有限体の乗法群を用いた離散対数問題を使った公開鍵暗号アルゴリズムにより不特定多数間の秘密通信が容易になった。その後、これを暗号方式に使えるように変形したＥｌＧａｍａｌ暗号、整数の素因数分解を用いたＲＳＡ暗号などが提案された。これらはインターネット通信の急速な発達により需要が増加し、特にＲＳＡ暗号が広く利用されていった。しかし、それと同時に、コンピュータ自体の急速な進歩により、これら暗号の解読時間は急激に短くなり、暗号の核ともいえる安全性が劣化していくこととなった。そこで登場したのが楕円曲線の群演算を用いた楕円曲線暗号である。

楕円曲線暗号は、１９８５年に発明された暗号であり、ＲＳＡ暗号に比べ、より短い長さの鍵で、ＲＳＡ暗号と同等の安全性をもつ暗号として注目を浴びていった。鍵が短い事で、以前よりも高速な処理が可能となった。この基盤ともなる楕円曲線は、谷山・志村定理を通じて、フェルマーの大定理の証明にも使われるなど、１９世紀以降数学において非常に重要な位置を占めるものとなった。

本論文は、三浦曲線についての考察である。三浦曲線とは、三浦晋示氏によってモデル化された代数曲線の定義方程式の表現方法であり、双有理同値を除いて全ての代数曲線は三浦曲線で表現できる。一般の特異点を持つ代数曲線を考え、その幾何種数と算術種数の関係性、そして最終的に三浦曲線において算術種数公式を与える事を目標とする。

尚、本論文は２００９年度中央大学大学院修士卒業生三ツ石直矢氏が修士論文として書かれた「Ｃａｂ曲線の算術種数について」の一般化である。三ツ石氏が用いた、０次コホモロジー群同士の射が全射である事を仮定した議論の展開を使用せず、代数曲線が射影曲線で局所完全交叉である事を仮定した上で、算術種数公式を導いていく。

１．リーマン・ロッホの定理

この章では、リーマン面の位相的な性質を代数的な性質と結び付けるリーマン・ロッホの定理について述べ、そして、一般代数曲線の幾何種数と算術種数を、コホモロジー群を用いて定義する。

Ｃを種数ｇの非特異代数曲線、ＤをＣ上の因子とする。この時、オイラーポアンカレ指標を用いた、以下の等式

$$\chi(C,\mathcal{O}(D)) = degD + 1 - g$$

をリーマン・ロッホの定理という。

Ｃの１次コホモロジー群の次元をＣの算術種数、Ｃの正規化Ｃ’の１次コホモロジー群の次元をＣの幾何種数と定義する。次章において、このＣの算術種数と幾何種数の関係性、また一般化されたリーマン・ロッホの定理とＳｅｒｒｅ双対を用いて得られる０次コホモロジー群の次元と算術種数の関係式を示していく。

２．代数曲線と算術種数

Ｃを射影曲線で局所的完全交叉と仮定し、Ｃ上のＳｅｒｒｅ双対を与える層をWとする。また、Ｃの算術種数をｇａとおく。この時、以下の等式、

$$\chi(C,W) = degW + 1 - g_a$$

を一般化されたリーマン・ロッホの定理という。

また、代数曲線のオイラーポアンカレ指標から

$$\chi(C,W) = h^0(C,W) - h^1(C,W)$$

が成り立ち、Ｓｅｒｒｅ双対の性質から、

$$\chi(C,W) = g_a - 1$$

が成り立つ。

よって、ＰをＣの特異点でない点、ｎを０以上の整数とすると、ｎＰは因子となり、以下の等式

$$h^0(C,\mathcal{O}_C(nP)) = n + 1 - g_a$$

が成り立つ。

三ツ石氏の論文において、０次コホモロジー群の射の全射性を仮定したのはこの等式を証明の議論の中であり、本論文ではこの等式を全射性を仮定せず、一般化されたリーマン・ロッホの定理とＳｅｒｒｅ双対を用いる事で導く事が出来た。

ここで、ｎ＝２ｇａ－１とおくと、

$$\begin{aligned} h^0(C,\mathcal{O}_C((2g_a-1)P)) &= (2g_a-1)+1-g_a \\ &= g_a \end{aligned}$$

を得る。

以下の列

$$1 = h^0(C,\mathcal{O}_C(0P)) \leq \cdots \leq h^0(C,\mathcal{O}_C((2g_a-1)P)) = g_a$$

から、次の式、

$$\sharp\{m | h^0(C,\mathcal{O}_C((m-1)P)) = h^0(C,\mathcal{O}_C(mP))\} = g_a$$

が得られる。

３．三浦モデル

２章までの議論を三浦曲線へ応用し、以下の三浦曲線の算術種数公式を導く。

$A_t = (a_1, \cdots, a_t) \quad a_i \in \mathbb{Z} > 0 \quad t > 0$

$< A_t >= \{ \quad \sum_{i=1}^{t} a_i n_i \quad , \quad n_i \in \mathbb{Z}\}$ とおく。

$gcd\{A_t\} = 1$ と仮定する。

この時、以下の公式が成立する。

(算術種数公式)

$$\begin{aligned} g_a &= \sharp\{\mathbb{N} \cup \{0\} \setminus < A_t >\} \\ &= \sum_{i=1}^{a_1 - 1} [b_i/a_1] \end{aligned}$$

但し、

$$\begin{aligned} [b_i/a_1] &= max\{s \in \mathbb{Z}, s \leq b_i/a_i\} \\ b_i &= min\{b \in < A_t >, b \equiv i \mod a_1\} \quad i = 1, \cdots, a_1 - 1 \end{aligned}$$

とおく。

４．結論

本論文では、三浦曲線の算術種数公式は証明されているが、代数曲線Ｃを局所完全交叉の射影曲線と限定した上での議論である。この局所完全交叉という仮定を取り除いた上での一般的な算術種数公式を考察していく事が本論文の課題となる。

５．参考文献

［1］有田正剛：Ｃａｂ曲線のヤコビアン群加算アルゴリズムとその離散対数型暗号への応用
電子情報通信学会論文誌Ａ，Ｖｏｌ．Ｊ８２－Ａ，Ｎｏ．８，１９９９
［2］川原修一郎：楕円曲線に関するＰｉｃａｒｄ 群の演算アルゴリズムについて
中央大学大学院理工学研究科数学専攻２００５年度修士論文集，２００６
［3］三ツ石直矢：Ｃａｂ 曲線の算術種数について
中央大学大学院理工学研究科数学専攻２００９年度修士論文集，２０１０
［4］三浦晋示：代数曲線のＣＡモデルについて
電子情報通信学会論文誌Ａ，Ｖｏｌ．Ｊ８１－Ａ，Ｎｏ．１０，１９９８
［5］宮西正宜：数学選書１０　代数幾何学
裳華房，１９９０
［6］Ｒ．ハーツホーン：代数幾何学１
シュプリンガー・フェアラーク東京，２００４