研　究　報　告　書

「符号・暗号のための代数曲線論」

研究タイプ：通常型
研究期間：　平成 21 年 10 月～平成 25 年 3 月
研 究 者：　川北　素子

1.　研究のねらい

情報通信技術が発達に、符号理論、暗号理論の重要性が益々高まって来た。1970 年、1980 年に、代数曲線を使って効率の良い符号、安全性の高い暗号を構成できることが発見された。ところが、具体的に使える代数曲線を決定しようとすると、代数曲線論でも未知の部分が多く残されていることが分かった。符号、暗号の視点から代数曲線論を研究し、情報通信に役に立つ数学の新しい発見を目指す。

2.　研究成果

（1）概要

有限体上で定義された代数曲線の有理点数は符号理論、暗号理論において大事なパラメータとなる。一方代数曲線論の中で、それは十分研究されたとは言えない。有理点数に関する Hasse-Weil 上界に達する代数曲線は最大曲線と呼ばれ、色々な性質が知られているが、最大曲線ではない Serre 上界に達する代数曲線は具体例が殆どなく、性質も分かっていない。私が以前発見した最大曲線でない Serre 上界に達する代数曲線の性質を調べ、さらに Wiman の曲線も Serre 上界に達することを発見した。

（2）詳細

研究テーマ A 「Serre 上界に達する Fermat 曲線の商曲線の性質」
Hasse-Weil 上界に達さず、Serre 上界に達する代数曲線は Fermat 曲線しか知られていなかったので、その性質を調べた。Jacobian が楕円曲線に完全分解し、それらの楕円曲線が虚数乗法を持つことが分かった。

研究テーマ B 「Serre 上界に達する新しい曲線の発見」
計算代数ソフト KASH を使って、色々な代数曲線について探索を行った結果、

Wiman 曲線(1897 年)　$x^6+y^6+1+\left(x^2+y^2+1\right)\left(x^4+y^4+1\right)-12x^2y^2=0$

Edge 曲線(1981 年)　$E_\alpha : T+\alpha S=0$

$$T := x^6 + y^6 + 1 + \left(x^2 + y^2 + 1\right)\left(x^4 + y^4 + 1\right) - 12x^2y^2 = 0$$

$$S := \left(y^2 - 1\right)\left(1 - x^2\right)\left(x^2 - y^2\right)$$

が Serre 上界に達することを発見した。
またデータベース http://www.manypoints.org/を多数更新出来た。
研究テーマ C「Wiman 曲線と Edge 曲線の性質」
Wiman 曲線は標数が 2; 3; 5 以外の体上で Jacobian が

$$J_w \sim \varepsilon^6$$

と完全分解する。ここで $\varepsilon : y^2 = x\left(5x^2 - 95x + 2^9\right)$。

命題 1. Wiman 曲線が有限体 F_{p^2} 上で最大曲線となる必要十分条件は

$$\sum_{i=0}^{\left\lfloor \frac{m}{2} \right\rfloor} \frac{m!}{(i!)^2 (m-2i)!} \cdot 2^{9i} \cdot 5^{m-i} \cdot (-19)^{m-2i} \equiv 0 \qquad \bmod p,$$

である。ここで $m := \dfrac{p-1}{2}$。

3. 今後の展開

Wiman 曲線、Edge 曲線が有理点を多数持ち、optimal 曲線となることも多くあることを発見できたが、その方向に沿ってより広い範囲で optimal 曲線が存在すると予想している。今後それを見つけ、性質を明らかにしたい。
また古典的な代数曲線の有理点数に関し、まだ研究されてないものも多くあり、コンピュータ探索でヒントを探し、論理的に解決させて行きたい。

4. 自己評価

代数幾何符号から提起された問題「optimal 曲線を全て決定せよ」に対して、最大曲線でない Serre 上界に達するものを発見できた。1897 年に Wiman が定義した曲線であるが、古い代数曲線に符号理論の視点を入れると斬新な新しい結果が得られたことが、本研究の最大の成果と考えている。またそれまで知られていたのは次数12と23の Fermat 曲線の商曲線のみでしたが、これらが暗号理論の視点では、どうなるのかまで研究できなかったのが心残りである。

5. 研究総括の見解

情報通信技術における符号理論、暗号理論の重要性はいうまでもない。とくに有限体上で定

義された代数曲線の有理点数は符号理論、暗号理論において大事なパラメータとなる。一方代数曲線論の中で、それは十分研究されたとは言えない。有理点数に関する Hasse-Weil 上界に達する代数曲線は最大曲線と呼ばれ、色々な性質が知られているが、川北氏による最大曲線でない Serre 上界に達する代数曲線の発見は今後、暗号理論においてどのような発展が見込まれるか期待をもって見ていきたい。これらの成果の発表も含め、関連分野とのより積極的な協働が必要であろう。

6. 主な研究成果リスト

（1）論文（原著論文）発表

なし

（2）特許出願

なし

（3）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）

紀要

1.代数幾何符号のための代数曲線論, 数理解析研究所講究録 1752「諸分野との協働による数理科学のフロンティア」(2011), 3—6.

講演

1. 安全・高速な情報通信のための代数曲線論, JST 数学領域 第 4 回領域シンポジウム「越境する数学」, 東京大学, 2012 年 11 月.
2. Wiman's and Edge's sextic attaining Serre's bound, Mini Workshop on Algebraic Curves for Coding Theory and Cryptography, 滋賀医科大学, 2012 年 7 月.
3. Wiman's and Edge's sextic attaining Serre's bound, 日本数学会, 東京理科大学, 2012 年 3 月.
4. 代数幾何符号のための代数曲線論, 諸分野との協働による数理科学のフロンティア, 京都大学, 2010 年 11 月.