ヴィーフェリッヒ素数の多項式の類似

Polynomial analogues of Wieferich primes

東京理科大学大学院理学研究科　　長田龍青 [*1]
Ryusei Osada
Graduate School of Science
Tokyo University of Science

東京理科大学理学部第一部　　武田渉 [*2]
Wataru Takeda
Faculty of Science Division I
Tokyo University of Science

東京理科大学理学部第一部　　関川浩 [*3]
Hiroshi Sekigawa
Faculty of Science Division I
Tokyo University of Science

Abstract

We consider polynomial analogues of Wieferich primes and call them Wieferich irreducible polynomials. For polynomials over $\mathbb{F}_2$, we obtain the following results: if g is the square of a polynomial, then there are infinitely many Wieferich irreducible polynomials in base g; if polynomials g or $g+1$ is divisible by the derivative of g, then there are only finitely many Wieferich irreducible polynomials in base g.

1　はじめに

ヴィーフェリッヒ素数はフェルマーの最終定理や素数判定法の一種であるフェルマーテストに関連した素数で、2 を底とする擬素数の平方因子は全てヴィーフェリッヒ素数である。ヴィーフェリッヒ素数は現在 1093 と 3511 の 2 つのみ見つかっているが、それ以外にヴィーフェリッヒ素数が存在するか、さらに、ヴィーフェリッヒ素数が無限に存在するかどうかについてはまだ分かっていない。本研究ではヴィーフェリッヒ素数の多項式の類似物を考え、それがどのような多項式であるか、さらに、無限に存在するかどうかについて考察する。

[*1] 〒 162-8601 東京都新宿区神楽坂 1 − 3　E-mail: 1422509@alumni.tus.ac.jp
[*2] 〒 162-8601 東京都新宿区神楽坂 1 − 3　E-mail: w.takeda@rs.tus.ac.jp
[*3] 〒 162-8601 東京都新宿区神楽坂 1 − 3　E-mail: sekigawa@rs.tus.ac.jp

2　フェルマーテストとヴィーフェリッヒ素数

まず、フェルマーテストとヴィーフェリッヒ素数についての説明をする。フェルマーテストとは確率的素数判定法の一種であり、フェルマーの小定理を利用して素数判定をする。ある自然数 n が与えられたときに n と互いに素な a を一つ選び、

$$a^{n-1} \equiv 1 \pmod{n}$$

を満たさないならば n は合成数、満たすならば n はおそらく素数であると判定をする。この式を満たすにもかかわらず n が合成数のとき、n を a を底とする擬素数であるという [1]。

2 を底とする擬素数を調べると、341 や 561 のようにほとんど平方因子を持たないことが分かる。2 を底とする擬素数が素数 p の平方を因子として持つならば

$$2^{p-1} \equiv 1 \pmod{p^2}$$

を満たす。このような素数をヴィーフェリッヒ素数という。

現在、ヴィーフェリッヒ素数は 1093 と 3511 の 2 つのみ見つかっている。この 2 つ以外にヴィーフェリッヒ素数が存在するかどうか、さらに、ヴィーフェリッヒ 素数が無限に存在するかどうかについてはまだ分かっていない。また、ヴィーフェリッヒ素数の一般化として、底が 2 以外のものについても考えることがある。

3　ヴィーフェリッヒ既約多項式

3.1　ヴィーフェリッヒ既約多項式の定義

本研究ではヴィーフェリッヒ素数の多項式の類似物を考える。

フェルマーテストは $\mathbb{F}_p$ 上の多項式が既約かどうかについても判定することができ、f と g が互いに素、$N(f) = p^{\deg f}$ としたとき、

$$g^{N(f)-1} \equiv 1 \pmod{f}$$

を満たさないならば f は既約多項式でない、満たすならば f はおそらく既約多項式である、と判定できる [2]。

そこで、フェルマーテストとヴィーフェリッヒ素数の定義の類似点に注目して、

$$g^{N(f)-1} \equiv 1 \pmod{f^2}$$

を満たす既約多項式 f を、底を g とするヴィーフェリッヒ既約多項式と呼ぶことにする。

本研究では $\mathbb{F}_2$ 上の多項式を対象とし、底 g を動かしたときにどのような既約多項式がヴィーフェリッヒ既約多項式となるかについて考察する。つまり、以下の問題を考える。

問題 1
g を $\mathbb{F}_2$ 上の多項式とする。それぞれの g に対してどのような既約多項式 f が

$$g^{N(f)-1} \equiv 1 \pmod{f^2}$$

を満たすか。

3.2 実験

問題を考察するため以下の実験を行なった。

1. $x^{2^n-1}+1$ の x に 1 次以上 5 次以下の全ての多項式 g を代入する。
2. それぞれの g に対して n を 1 から 6 まで変えて $g^{2^n-1}+1$ を因数分解し、重複因子の現れ方を観察する。

なお、平方因子が現れてもそれがヴィーフェリッヒ既約多項式とは限らない。ヴィーフェリッヒ既約多項式であるかは以下の補題による。

補題 1
g を $\mathbb{F}_2$ 上の多項式とする。$g^{2^n-1}+1$ に平方因子 f^2 が存在し、f が n 次既約多項式なら、f は g を底とするヴィーフェリッヒ既約多項式である。

証明 もし $g^{2^n-1}+1$ に平方因子 f^2 が存在し、f が n 次既約多項式なら、$n=\deg f$ より

$$g^{2^n-1}+1 \equiv g^{2^{\deg f}-1}+1 \equiv g^{N(f)-1}+1 \equiv 0 \pmod{f^2}$$

を満たす。よって、

$$g^{N(f)-1} \equiv 1 \pmod{f^2}$$

となるので、f は g を底とするヴィーフェリッヒ既約多項式である。 ∎

結果としては、以下の 4 パターンの重複因子の現れ方を確認できた。

1. 重複因子が現れない。

   例: $g=x+1$ のとき

   $$\begin{aligned}
   g^{2^1-1}+1 &= x \\
   g^{2^2-1}+1 &= x(x^2+x+1) \\
   g^{2^3-1}+1 &= x(x^3+x+1)(x^3+x^2+1) \\
   g^{2^4-1}+1 &= x(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)
   \end{aligned}$$

   考えられる原因: $g^{2^n-1}+1$ が無平方であるから。

2. 重複因子の数が一定となる。

   例: $g=x^3+x+1$ のとき

   $$\begin{aligned}
   g^{2^1-1}+1 &= x(x+1)^2 \\
   g^{2^2-1}+1 &= x(x+1)^2(x^2+x+1)(x^4+x^3+1) \\
   g^{2^3-1}+1 &= x(x+1)^2(x^3+x^2+1)(x^6+x^5+1)(x^9+x^7+x^5+x+1) \\
   g^{2^4-1}+1 &= x(x+1)^2(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) \\
   &\quad (x^8+x^4+x^3+x^2+1)(x^8+x^7+x^3+x^2+1)(x^{12}+x^9+x^7+x^5+x^4+x^3+1)
   \end{aligned}$$

   考えられる原因: $g^{2^n-1}+1=(g+1)(g^{2^n-2}+\cdots+g+1)$ の $g^{2^n-2}+\cdots+g+1$ が無平方であるから。

3. 全てが重複因子となる。

   例: $g = x^2$ のとき

$$
\begin{aligned}
g^{2^1-1}+1 &= (x+1)^2 \\
g^{2^2-1}+1 &= (x+1)^2(x^2+x+1)^2 \\
g^{2^3-1}+1 &= (x+1)^2(x^3+x+1)^2(x^3+x^2+1)^2 \\
g^{2^4-1}+1 &= (x+1)^2(x^2+x+1)^2(x^4+x+1)^2(x^4+x^3+1)^2(x^4+x^3+x^2+x+1)^2
\end{aligned}
$$

   底が平方のときのみ見られた。

   このパターンではヴィーフェリッヒ既約多項式は無限に存在する。証明は次節に記述する。

4. 特定の n のときに重複因子が現れる。

   例: $g = x^5 + x^3 + x^2 + x + 1$ のとき

$$
\begin{aligned}
g^{2^1-1}+1 &= x(x+1)(x^3+x^2+1) \\
g^{2^2-1}+1 &= x(x+1)(x^2+x+1)^2(x^3+x^2+1)(x^6+x^4+x^2+x+1) \\
g^{2^3-1}+1 &= x(x+1)(x^3+x+1)(x^3+x^2+1)(x^6+x^5+1) \\
&\qquad (x^9+x^8+x^6+x^5+x^3+x^2+1)(x^{12}+x^5+x^4+x^2+1) \\
g^{2^4-1}+1 &= x(x+1)(x^2+x+1)^2(x^3+x^2+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) \\
&\qquad (x^6+x^4+x^2+x+1)(x^8+x^5+x^3+x+1)(x^8+x^5+x^4+x^3+1) \\
&\qquad (x^{12}+x^9+x^8+x^6+x^5+x^4+1)(x^{20}+x^{12}+x^8+x^5+x^4+x^3+x^2+x+1)
\end{aligned}
$$

   考えられる原因: $x^{2^n-1}+1$ を因数分解したときの特定の因子の x に多項式を代入すると重複因子が現れるから。例えば、x^2+x+1 という因子の x に $x^5+x^3+x^2+x+1$ を代入して因数分解すると $(x^2+x+1)^2$ という因子が現れる。$x^{2^n-1}+1$ を因数分解すると n が 2 の倍数のときのみ、x^2+x+1 という因子が現れるので、特定の n のときに重複因子が現れる。

なお、どのような底で全てが重複因子となるパターンになるかは証明することができたが、それ以外はまだ推測のままである。

以下の表は、それぞれの g で重複因子の現れ方がどのパターンだったかを示した物である。

表 1: 1 次以上 5 次以下の全ての多項式 g に対して $g^{2^n-1}+1$ に現れる重複因子のパターン

g	パターン
x	1
$x+1$	1
x^2	3
$(x+1)^2$	3
$x(x+1)$	1
x^2+x+1	1
x^3	1
$(x+1)(x^2+x+1)$	2
$x(x+1)^2$	1
x^3+x+1	2
$x^2(x+1)$	1
x^3+x^2+1	2
$x(x^2+x+1)$	2
$(x+1)^3$	1
x^4	3
$(x+1)^4$	3
$x(x+1)(x^2+x+1)$	1
x^4+x+1	1
$x^2(x+1)^2$	3
$(x^2+x+1)^2$	3
$x(x^3+x+1)$	1
$(x+1)(x^3+x^2+1)$	1
$x^3(x+1)$	1
x^4+x^3+1	2
$x(x^3+x^2+1)$	2
$(x+1)^2(x^2+x+1)$	1
$x^2(x^2+x+1)$	1
$(x+1)(x^3+x+1)$	2
$x(x+1)^3$	1
$x^4+x^3+x^2+x+1$	2
x^5	1

g	パターン
$(x+1)(x^4+x^3+x^2+x+1)$	2
$x(x+1)^4$	1
$(x^2+x+1)(x^3+x^2+1)$	2
$x^2(x+1)(x^2+x+1)$	1
x^5+x^2+1	2
$x(x^4+x+1)$	2
$(x+1)^2(x^3+x+1)$	1
$x^3(x+1)^2$	1
x^5+x^3+1	2
$x(x^2+x+1)^2$	1
$(x+1)(x^4+x^3+1)$	2
$x^2(x^3+x+1)$	2
$(x+1)^3(x^2+x+1)$	2
$x(x+1)(x^3+x^2+1)$	4
$x^5+x^3+x^2+x+1$	4
$x^4(x+1)$	1
$(x^2+x+1)(x^3+x+1)$	2
$x(x^4+x^3+1)$	2
$(x+1)^5$	1
$x^2(x^3+x^2+1)$	1
$(x+1)(x^4+x+1)$	2
$x(x+1)^2(x^2+x+1)$	1
$x^5+x^4+x^2+x+1$	2
$x^3(x^2+x+1)$	2
$(x+1)^2(x^3+x^2+1)$	2
$x(x+1)(x^3+x+1)$	4
$x^5+x^4+x^3+x+1$	4
$x^2(x+1)^3$	1
$x^5+x^4+x^3+x^2+1$	2
$x(x^4+x^3+x^2+x+1)$	2
$(x+1)(x^2+x+1)^2$	1

3.3 理論的な結果

前節の結果を元に二つの定理が得られた。はじめに本研究で得られた定理の証明に必要な、よく知られた定理を示す。定理 2 の証明は [3] の 5.3.1 節など、定理 4 の証明は [3] の 3.5 節などを参照のこと。

定理 2
h を $\mathbb{F}_q$ 上の既約多項式とすると、h が $x^{q^n} - x$ を割り切るための必要十分条件は $\deg h$ が n の約数であることである。

系 3
$\mathbb{F}_2$ 上で $x^{2^n} + x$ は全ての n 次既約多項式を因子に持つ。

定理 4
体 $\mathbb{F}$ 上の多項式 f の導関数を f' とするとき、f が無平方であるための必要十分条件は $\gcd(f,\ f') = 1$ が成り立つことである。

以下が本研究で得られた定理である。

定理 5
$\mathbb{F}_2$ 上の多項式 h が存在して $g = h^2$ のとき、底を g とするヴィーフェリッヒ既約多項式は無限に存在する。

証明 $h \in \mathbb{F}_2[x]$ を $h = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0\ (a_i \in \mathbb{F}_2)$ とすると

$$\begin{aligned}
h^{2^n} + h &= (x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0)^{2^n} + (x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0) \\
&= ((x^m)^{2^n} + (a_{m-1}x^{m-1})^{2^n} + \cdots + (a_1x)^{2^n} + (a_0)^{2^n}) + (x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0) \\
&= ((x^m)^{2^n} + x^m) + ((a_{m-1}x^{m-1})^{2^n} + a_{m-1}x^{m-1}) + \cdots + ((a_1x)^{2^n} + a_1x) \\
&= ((x^{2^n})^m + x^m) + a_{m-1}((x^{2^n})^{m-1} + x^{m-1}) + \cdots + a_1(x^{2^n} + x) \\
&= (x^{2^n} + x)h_m + a_{m-1}(x^{2^n} + x)h_{m-1} + \cdots + a_1(x^{2^n} + x) \\
&= (x^{2^n} + x)h_{sum}
\end{aligned}$$

が成り立つ。ただし、h_i は $(x^{2^n})^i + x^i$ から $x^{2^n} + x$ をくくり出した残りの因子、h_{sum} は

$$(x^{2^n} + x)h_m + a_{m-1}(x^{2^n} + x)h_{m-1} + \cdots + a_1(x^{2^n} + x)$$

から $x^{2^n} + x$ をくくり出した残りの因子である。$g = h^2$ ならば

$$\begin{aligned}
g^{2^n-1} + 1 &= (h^2)^{2^n-1} + 1 \\
&= (h^{2^n-1})^2 + 1 \\
&= (h^{2^n-1} + 1)^2 \\
&= \left(\frac{h^{2^n} + h}{h}\right)^2 \\
&= \left(\frac{(x^{2^n} + x)h_{sum}}{h}\right)^2
\end{aligned}$$

系 3 より $\mathbb{F}_2$ 上で $x^{2^n} + x$ は全ての n 次既約多項式を因子に持つので、少なくとも h の因子以外の n 次既約多項式の平方は $g^{2^n-1} + 1$ の因子となる。

さらに、$g \equiv 0 \pmod{h}$ なので、

$$g^{2^n-1} \equiv 0 \pmod{h}$$
$$g^{2^n-1} + 1 \equiv 1 \pmod{h}$$

より、$g^{2^n-1}+1$ は h の因子で割り切れない。

以上のことは全ての n について成り立つので、補題 1 と合わせて h の因子以外の全ての既約多項式がヴィーフェリッヒ既約多項式となることが分かる。従って、底を g とするヴィーフェリッヒ既約多項式は無限に存在する。 ∎

定理 6

$\mathbb{F}_2$ 上の多項式 g の導関数を g' とするとき、$g \equiv 0 \pmod{g'}$ または $g \equiv 1 \pmod{g'}$ ならば、底を g とするヴィーフェリッヒ既約多項式は有限個しか存在しない。

証明 $f \in \mathbb{F}_2[x]$ とし、f の導関数を f' とする。

$$f = g^{2^n-2} + g^{2^n-3} + \cdots + g + 1$$

のとき、f' は

$$f' = g'(g^{2^n-4} + g^{2^n-6} + \cdots + g^2 + 1)$$

となる。ここで、

$$\begin{aligned} f &= \frac{g(g+1)}{g'} \cdot g'(g^{2^n-4} + \cdots + g^2 + 1) + 1 \\ &= \frac{g(g+1)}{g'} \cdot f' + 1 \end{aligned}$$

と書ける。$g \equiv 0 \pmod{g'}$ または $g \equiv 1 \pmod{g'}$ ならば $g(g+1)$ は g' で割り切れるので、f を f' で割ったときの商は $g(g+1)/g'$ で余りは 1 であり、ユークリッドの互除法から $\gcd(f,\ f') = 1$ であると分かる。

従って、定理 4 より $f = g^{2^n-2} + g^{2^n-3} + \cdots + g + 1$ は無平方である。

$g^{2^n-1}+1 = (g+1)(g^{2^n-2} + g^{2^n-3} + \cdots + g + 1)$ と因数分解できるので、$g \equiv 0 \pmod{g'}$ または $g \equiv 1 \pmod{g'}$ ならば、$g^{2^n-1}+1$ の因子のうち平方因子となるのは $g+1$ の因子のみ。これは任意の n について成り立つので、補題 1 と合わせてヴィーフェリッヒ既約多項式は有限個しか存在しないことが分かる。 ∎

4 おわりに

ヴィーフェリッヒ素数の多項式の類似物であるヴィーフェリッヒ既約多項式を定義し、それについて考察を行い、以下の結果を得た。

1. $\mathbb{F}_2$ 上の多項式 h が存在して $g = h^2$ のとき、h の因子以外の全ての既約多項式が底を g とするヴィーフェリッヒ既約多項式となる。よって、底を g とするヴィーフェリッヒ既約多項式は無限に存在する（定理 5）。

2. $\mathbb{F}_2$ 上の多項式 g の導関数を g' とするとき、$g \equiv 0 \pmod{g'}$ または $g \equiv 1 \pmod{g'}$ ならば、底を g とするヴィーフェリッヒ既約多項式は有限個しか存在しない（定理 6）。

ヴィーフェリッヒ素数が無限に存在するかどうかについてはまだ分かっていないが、多項式の類似物であるヴィーフェリッヒ既約多項式では、底がある条件を満たせば無限に存在し、別のある条件を満たせば有限個しか存在しないことが分かった。

参 考 文 献

[1] N. コブリッツ著, 櫻井幸一訳, 数論アルゴリズムと楕円暗号理論入門, シュプリンガー・フェアラーク東京, 1997.

[2] Keith Conrad, “IRREDUCIBILITY TESTS IN $\mathrm{F}_p[T]$”. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/irredtestFpT.pdf (参照 2024-01-07).

[3] 長坂耕作, 岩根秀直編著, 北本卓也ほか著, 計算機代数の基礎理論, 共立出版, 2019.