数理解析研究所講究録
第155巻 1972年 14-30

14

多項式の既約性について

岡山大理　　内山三郎
京大数理研　　一松　信

§1. Chowla の予想

この話は，ある多項式が mod p の素体の上で既約であるような素数 p をさがす話であるが，まず問題の背景を解説する。

p を素数，n を正の整数とする。有理整数を係数とする多項式

(1)　$$f(x)=\sum_{m=0}^{n} a_m x^m \qquad (a_0=1)$$

を，GF[p, x]（GF(p) 上の多項式）の元とみなす。$n\geq 2$ で，f(x) が mod p に関して既約，すなわち GF[p, x] の多項式として既約ならば，

$$\sum_{j=0}^{n-1} c_j \theta^j \qquad (f(\theta)=0,\ c_j\in GF(p),\ 0\leq j\leq n-1)$$

は，p^n 個の元をもつ有限体 $GF(p^n)$ をなす。

$GF[p,x]$ において，任意の次数 n の既約な多項式 $f(x)$ が存在することは，よく知られている。それを作りだすアルゴリズムも知られている．その個数は

$$\frac{1}{n}\sum_{d|n}\mu(d)p^{n/d} \sim \frac{p^n}{n} \quad (n\text{を固定し，}p\to\infty\text{としたとき})$$

である。ここに μ は，Möbius の関数（$\mu(1)=1$，d が素数の2乗で割り切れるときは0，r 個の相異なる素数の積であるときには $(-1)^r$）である。

既約な n 次多項式 $f(x)$ で，その係数のうち，はじめのほうと，終りの方の若干個があらかじめ指定されているときでも，その個数に対して，同様の漸近式を与えることができる。しかし与えられた p と n とに対して，具体的にこのような $f(x)$ をみつけることは，必ずしも容易ではない。

たとえば $p=101$，$n=5$ とすると，(1) の形の多項式は（x^5 の係数を1と固定しても）$101^5 > 10^{10}$ 個もある。そのうちただちに可約とわかるものも多いが，この中から mod 101 で既約なものを1つ探すとしたら，相当の手間である。

これに関して S. Chowla [1] は，つぎのような予想をした。

Chowla の予想　n に対して定まるある限界 $p_0(n)$ があって，　$p > p_0(n)$ ならば

$$f(x) = x^n + x + a \qquad (1 \leqq a \leqq p-1)$$

の形の多項式の中に，mod p で既約なものが存在する。そのような $f(x)$ の個数 N は，n を固定し，$p \to \infty$ とするとき，漸近式

$$N \sim \frac{p}{n}$$

をみたす。

この予想は，$n=1$ のときは自明であり，$n=2$ のときも，容易に正しいことがわかる。Chowla 自身は，$n=3$ のときを証明し，一般のときを予想したが，後に P. A. Leonard [4] と，K. S. Williams [8] は，$n=4$ のときを証明した。さらに最近になって，R. Ree [5] が，A. Weil の密度定理（[1], [3] 参照）を用いて，この予想を，一般の $n \geqq 2$ について，完全に証明した。── したがって，いまや定理というべきである。

この Ree の方法によって，さらにつぎのような事実を証明することができる。

$n \geqq 2$ のとき，多項式

$$f(x) = x^n + x + a$$

が，mod p で既約となるような，最小の正の整数 $a = a_n(p)$ は，$p \to \infty$ のとき，評価

$$a_n(p) \leqq C_n \cdot p^{1/2} \log p \quad (C_n \text{は定数})$$

をみたす．ただし係数 C_n は，n に依存する。

§2. Williams の予想と修正

そこで，以下

(2) $$f(x) = x^n + x + a$$

の形の三項多項式を考える．上記のように mod p で $f(x)$ が既約になる最小の $a = a_n(p)$ （p が十分大きければ存在する）をとり，

$$a_n = \liminf_{p \to \infty} a_n(p)$$

とおく。

K. S. Williams [8] は，すべての $n \geqq 2$ に対して

$$a_n = 1$$

であることを予想し，$n = 2, 3$ については証明した。しかし，この予想は，一般の n については正しくない。$n \equiv 2 \pmod 3$ ならば，$x^n + x + 1$ は $x^2 + x + 1$ で割り切れるから，$n \geqq 5$ については既約ではない。

Williams の予想は，つぎのように修正されるべきものと考えられる：

$$\begin{cases} n=2 \text{ および } n\not\equiv 2 \pmod 3 \text{ のとき} & a_n=1 \\ n\equiv 2 \pmod 3,\ n \text{ が奇のとき} & a_n=3 \\ n\equiv 2 \pmod 3,\ n>2 \text{ で偶のとき} & a_n=2 \end{cases}$$

このような修正をする一つの理由は，ここで定義された $a_n=a$ が，$\mathbb{Z}[x]$ の多項式として，x^n+x+a が既約であるような最小の正の整数であることである。

この修正された Williams の予想は，かなりもっともらしい。じっさい内山[6]は，これを

$$n=4,\ 6,\ 8,\ 9 \text{ および任意の素数}$$

について証明した。また Williams [9] は，Gleason-Marsh の定理（[11]参照）を用いて，$x^{15}+x+1$ が mod 2 で既約であることを示し，$a_{15}=1$ （$n=15$ のとき）を証明した。

つぎの目標は $n=10$ のときである。ここに多項式

(3) $\quad f(x)=x^{10}+x+1$

が既約になる p を探す問題が生じてくる。じっさい $a_n=a$ を証明するためには，無限に多くの素数 p に対して，$f(x)=x^n+x+a$ が mod p で既約となるような最小の正の整数 a であることを示さなければならない。

ところで，F. G. Frobenius の密度定理（[2], [6] 参照）によれば，このことは，その a が $f(x)$ の判別式

$$(-1)^{n(n-1)/2}\left(n^n a^{n-1}+(-1)^{n-1}(n-1)^{n-1}\right)$$

を割らない少なくとも1つの素数 p に対して，$f(x)$ が $\bmod p$ で既約となるような最小の正の整数 a であること，と同値であることがわかる。

したがって，(2) が $\bmod p$ で既約となるような素数 p を少なくとも1つみつけることが当面の問題となる。もっとも $f(x)$ が $\bmod p$ で既約となる素数 p がただちにみつからなくても，いくつかの p についての $f(x)$ $(\bmod p)$ の分解の様子から，$f(x)$ のガロア群の構造が定まり，それによって，Frobenius の密度定理から，$f(x)$ が $\bmod p$ で既約となる p が無限に存在することが示されることもある。*) とくに $f(x)$ の次数 n が素数のときには，素数次の任意の推移置換群は，その次数に等しい長さの巡回置換を含むから，Frobenius の密度定理により，上記の結果（内山[6]）をうる。（*) じっさいにそうであった。§4の末尾参照）。

§3. 実験とその結果（当初）

当面の $x^{10}+x+1$ についてのべる。

内山[6]は，これが $\bmod 2$ で既約であるとして，$a_{10}=1$

を主張したが，これは誤りであった．Williams [9] によると，mod 2 で可約であって，じつは

$$x^{10}+x+1 \equiv (x^3+x+1)(x^7+x^5+x^4+x^3+1) \pmod 2$$

となる．この因子はいずれも既約であり，これから，Galois 群が原始的（primitive）な置換群になることがわかる。

mod 3 で可約なことは，$x=1$ を代入すれば 0 になることからわかるが，$x+2$ のほかにも，x^3+2x^2+2x+2 という因子もあって，3個の既約多項式の積に分解される。

一松は，当初計算機によるテストにもとづき，mod 5，mod 7 で「既約である」とのべたが，これはプログラムの不備による誤りであった。Williams [10] は，計算機によって

$$x^{10}+x+1 \equiv (x^2+4x+2)(x^8+x^7+4x^6+2x^5+4x^4+2x^2+2x+3) \pmod 5$$

$$x^{10}+x+1 \equiv (x^2+6x+6)(x^8+x^7+2x^6+3x^5+5x^4+x^3+6x^2+6) \pmod 7$$

を示した。（一松もその後やり直して，これを確認した。）じつは後述の Swan の定理 [12] から，$p=5,7$ に対して可約なことは，計算してみなくても，すぐにわかることであった（§4 参照）。

一松はその後，計算機によって，つぎのような順序で探索をつづけた：

1° 1次因数をもつ p をしらべる。これは $a=1,2,\cdots,p-1$ を代入して，$\bmod p$ で0になるかどかをしらべる。じっさいには，$a \leqq (p-1)/2$ までとし，$a^{10}+1 \equiv \pm a \pmod p$ をしらべた．結果を表1に示す．ここにはみつかった限りの1次因数をあげてある。

2.° 1次因数をもたない p について，2次因数を求める。(表2)．ただし表2は，概算もかねて試みたもののみで，すべての2次因数を網羅してはいない。

3.° 残ったものについて，3次因数を求める（表3)。これも網羅していない。2.°, 3.°は $\bmod p$ でできるすべての多項式（定数項＝0のものを除く）で順次割ってみて，剰余が0になるかいなかをためした。

ここで残ったのは $p=41$ である。このときは，さらに4次因数をさがして，$x^4+bx^3+\cdots$ $(b \leqq 27)$ までは因数がないことをたしかめたが，これまでに3時間近くかかったため，中断して，研究集会で報告した．じつは Swan の定理によれば，$p=41$ のときは，可約であることがすぐにわかるので，むだな努力であった。

§4. その後の進展（追加）

研究集会の席で，名城大の太田喜一郎先生から，非常に重要な，つぎの御注意をいただいた（[12], [13]）。

Swanの定理　整係数のn次モニックな多項式$f(x)$が，mod pで重根をもたないとする。このとき$f(x)$のmod pでの既約因数の個数をrとすると，つぎの関係がある。

$r \equiv n \pmod 2$ $\Longleftrightarrow$ $D(f)$がmod pの素体で平方剰余

（pは奇素数とする。）

$D(f)$はfの判別式であり，fの根を$\alpha_1, \alpha_2, \cdots, \alpha_n$；$f$の導関数を$f'$とすると，つぎの式で表わされる：

$$D(f) = (-1)^{n(n-1)/2} \prod_i f'(\alpha_i)。$$

当面の(3)では，判別式は

$$D(f) = (-1)^{45}(10^{10} - 9^9) = -9612579511$$
$$= -29 \cdot 4127 \cdot 80317$$

である（この最後の因数分解は，内田典二氏[14]による）。

そして，上記の定理を書き下すと，mod pに対して，

Dが平方剰余 $\Longleftrightarrow$ rが偶数 $\longrightarrow$ 可約！

Dが平方非剰余 $\Longleftrightarrow$ rが奇数 $\longrightarrow$ 既約 かまたは少なくとも3つの因数，したがってたかだか3次の因数をもつ。

となる。

この注意にしたがい、$D(f) \pmod p$ が平方剰余かどうかをためしたところ、表4のようになった。表1とあわせると、(3)が既約である可能性のある p は、$p \leqq 113$ の範囲で、

17, 71, 73

しかない。この検査で、大幅に可能性がへらされた。

$p=17, 71$ については、表3, 2のように3次、2次の因数がそれぞれみつかったから、残る可能性は、$p=73$ のみである。そこで再度前記の2°3°のプログラムでさがしたところ、$p=73$ のときには、2次、3次の因数とも存在せず、したがって既約であることがたしかめられた（この計算に、約52分を要した）。したがって、$n=10$ のときの Williams の予想(の修正)がたしかめられたことになる。

ところが、じつは、この探索の成功以前に、$n=10$ の場合の Williams の予想が正しいことが、内田興二氏([14])によって証明されていた。その概要はつぎのとおりである:

この目的のためには、(2)の $\mathbb{Q}$ 上の Galois 群が、長さ n のサイクルを含むことをいえばよい。一般の n については不明であるが、$n=10$ のときには、Galois 群は対称群 S_{10} となる([14])。このことから、$x^{10}+x+1$ が $\bmod p$ で既約である p は無数にあり、その Dirichlet 密度は 1/10 であることが、Frobenius の密度定理からわかる。もっとも、

上記の探索から、そのような p が、はじめの30個の素数（113まで）のうち、ただ一つしかないという実験結果は別の意味で興味深い。

その後この稿の印刷直前にWilliamsから重要な注意([15])をいただいたので、とりあえず追加する：

1° $n=10$ のとき、$p=73$ について $x^{10}+x+1$ が既約であることは、すでにWilliamsとB. Mortimaがたしかめた。

2° 論文[6]にある $n=8$ の場合の議論は誤りであった。x^8+x+2 は $(\mathrm{mod}\ 3)$ で既約でなく、

$$(x^3+2x^2+2x+2)(x^5+x^4+2x^3+x^2+x+1)$$

である。ただし、$p=17$ に対して既約であることがたしかめられたので、$n=8$ のときの結果は正しい。

3° $n=20$ までは、Williamsの予想の修正は正しい。各 n に対する既約になる最小の p を右の表に示す。

n	p
12	19
13	19
14	3
15	2
16	79
17	7
18	5
19	59
20	19

4° $n=10$ に対し、$x^{10}+x+1$ は $\mathrm{mod}\ 41$ で可約であるが、その具体的な因子はみつかっていない。

5° Williamsの予想の修正は、n が奇素数、および $n\leqq 20$ の

ほか，Zierler による mod 2 に対する既約性の研究([16])により，少なくとも，下記の n については正しい．

22, 28, 30, 46, 60, 63, 153, 172, 303, 471,
532, 865, 900, 1366, 2380, 3310, 4495, 6321, 7447,
10198, 11425, 21846, 24369, 27286, 28713.

§5. 反省

この問題の実験から，ささやかであるが，次のような反省を感じた．

1°. 計算機によるめくらまがしは，理論に及ばなかった．しかし途に手をこまねいていてはだめで，何でもやってみる必要があった．(たとえば，このあと一松は $n=12$ に対して探索をはじめ，$p=19$ に対して既約らしい，と見当をつけながら，うまい探索法を考えて時間を空費し，[15]に先をこされた．)

2°. 因子がみつかれば，それをためすことは手でもできる．しかし，みつからなかった場合，本当に正しいかどうかをたしかめるには，入念な検査が必要である．

3°. Background job としては，必ずしも適切でない．結果がわかるまでの時間が予測しにくいし，人間と機械との会話で進めてゆく必要がある．と同時に，どこは早くすみ，どこは時間がかかりそうだ，といった人間のかんも大事

ようである.

4° 長時間計算に対しては, 何らかの中間結果をメモして, どこまで進んだかを記録し, またときおり出力があるように工夫する必要がありそうである.

なおこの稿のうち, §§1, 2, §4 の後半は内山に, §3, §4の前半, §5 は一松が主に記した. 研究集会の折の予稿の内容を全面的に書きあらためたが, あちこち誤りが多く, みっともない報告になってしまった.

最後に有益な御注意を賜わった Williams, 太田喜一郎 内田興二の諸先生と, 長時間にわたる計算をやって下さった京都大学数理解析研究所計算機室の河野嘉治君に感謝の詞をのべたい.

表　1

p	因数
11	$x+2$
13	$x-2$
19	$x-9$
29	$x+14$ (重根)
31	$x+2$
37	$x-15$
43	$x+18$
53	$x+26$
59	$x+5$
67	$x-17$, $x+18$
79	$x-2$, $x-14$
83	$x+18$
97	$x+44$
101	$x-13$
103	$x+14$
107	$x-31$, $x-44$

表　2

p	因数
5	x^2+4x+2
7	x^2+6x+6
13	$x^2+8x+10$
23	$x^2+13x+20$
47	$x^2+3x+30$
61	$x^2+54x+5$
71	$x^2+14x+14$
79	$x^2+63x+28$

表　3

p	因数
13	x^3+6x^2+7x+6 $=(x+11)(x^2+8x+10)$
17	x^3+10x^2+4x+8
41	(3次までの因数なし) 可約だが具体的な因子未発見.

表 4

p	Dの値	√D	p	Dの値	√D
3	2	—	59	32	—
5	4	2	61	20	9
7	4	2	67	1	1
11	4	2	71	13	—
13	11	—	73	45	—
17	7	—	79	27	—
19	11	7	83	2	—
23	9	3	89	57	18
29	0	0	97	15	—
31	30	—	101	44	—
37	28	18	103	34	31
41	8	7	107	33	51
43	12	—	109	16	4
47	32	19	113	77	23
53	14	—			

— は平方非剰余であることを示す.

文　　献

[1] S. Chowla: A note on the construction of finite Galois fields $GF(p^n)$. J. Math. Anal. Appl., 15(1966), 53-54.

[2] F. G. Frobenius: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. Sitzungsberichte Kön. Preuss. Akad. Wiss. Berlin, 689-703 (1896).

[3] S. Lang: Sur les séries L d'une variété algébrique. Bull. Soc. Math. France, 84(1956), 385-407.

[4] P. A. Leonard: On constructing quartic extensions of GF(p). Norske Vid. Selsk. Forh., Trondheim, 40(1967), 96-97.

[5] R. Ree: Proof of a conjecture of S. Chowla. J. Number Theory, 3(1971), 210-212.

[6] S. Uchiyama: On a conjecture of K. S. Williams. Proc. Japan Acad., 46(1970), 755-757.

[7] A. Weil; Sur les courbes algébriques et les variétés qui s'en déduisent. Hermann, Paris, 1948.

[8] K. S. Williams: On two conjectures of Chowla. Canad. Math. Bull., 12(1969), 545-565.

[9] K. S. Williams: 内山への私信 (July 5, 1971).

[10] K. S. Williams: 内山への私信 (October 1, 1971).

[11] N. Zierler, On the theorem of Gleason and Marsh, Proc. Amer. Math. Soc., 9 (1958), 236-237.

[12] R.G.Swan, Factorization of polynomials over finite fields, Pacific J. of Math., 12 (1962), p. 1099-1106.

[13] 太田喜一郎, ガロア拡大体における素イデアル分解(I), 名城大学理工学部報告, 12 (1971), 381-387.

[14] K.Uchida, Unramified extensions of quadratic number fields, II, Tôhoku Math. J., ser. 2, 22 (1970), p. 220-224.

[15] B.C. Mortima & K.S.Williams, Note on a paper of S. Uchiyama, to be published (from preprint).

[16] N.Zierler, On x^n+x+1 over GF(2), Information and Control, 16 (1970), 502-505.