Kitaoka, Y.
Osaka J. Math.
49 (2012), 393–420

A STATISTICAL RELATION OF ROOTS OF A POLYNOMIAL IN DIFFERENT LOCAL FIELDS III

YOSHIYUKI KITAOKA

(Received March 2, 2010, revised November 5, 2010)

Abstract

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. We have observed a statistical relation of roots of $f(x) \bmod p$ for different primes p, where $f(x)$ decomposes completely modulo p. We could guess what happens if $f(x)$ is irreducible and has at most one decomposition $f(x) = g(h(x))$ such that g, h are monic polynomials over $\mathbb{Z}$ with $h(0) = 0$, $1 < \deg h < \deg f$. In this paper, we study cases that f has two different such decompositions. Besides, we construct a series of polynomials f which have two non-trivial different decompositions $f(x) = g(h(x))$.

1. Introduction

Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be a monic polynomial with integer coefficients. We put

$$Spl(f) = \{p \mid f(x) \bmod p \text{ is completely decomposable}\},$$

where p denotes prime numbers. Let $r_1, \dots, r_n$ $(r_i \in \mathbb{Z},\ 0 \leq r_i \leq p-1)$ be solutions of $f(x) \equiv 0 \bmod p$ for $p \in Spl(f)$; then $a_{n-1} + \sum r_i \equiv 0 \bmod p$ is clear. Thus there exists an integer $C_p(f)$ such that

$$a_{n-1} + \sum_{i=1}^{n} r_i = C_p(f)p. \tag{1}$$

If $f(x)$ has no rational roots, then we have $1 \leq C_p(f) \leq n-1$ with finitely many exceptional primes p.

2010 Mathematics Subject Classification. 11N64, 11C08.

The author was partially supported by Grant-in-Aid for Scientific Research (C), The Ministry of Education, Science, Sports and Culture.

By defining the natural density

$$Pr(k,\ f,\ X) = \frac{\#\{p \mid p \in Spl(f),\ p \le X,\ C_p(f) = k\}}{\#\{p \mid p \in Spl(f),\ p \le X\}}, \tag{2}$$

the limit

$$Pr(k,\ f) = \lim_{X \to \infty} Pr(k,\ f,\ X)$$

seems to exist ([1], [2]).

If a polynomial f is of a form $f(x) = g(h(x))$ for polynomials $g(x), h(x)$ with $\deg h = 2$, then $C_p(f) = (\deg f)/2$ holds with finitely many exceptions $p \in Spl(f)$ ([1]). They and linear forms seem exceptional polynomials for which $Pr(k,\ f)$ can be evaluated explicitly. Hereafter we exclude such polynomials and assume that f is irreducible.

First, suppose that f does not have a decomposition such that $f(x) = g(h(x))$, where g, h are polynomials over $\mathbb{Q}$ with $1 < \deg h < \deg f$. We call it non-reduced. Let $r_1, \ldots, r_n$ be roots of f mod p for a prime $p \in Spl(f)$; then the relation (1) implies that $\sum r_i/p$ tends to an integer $C_p(f)$ if $p \to \infty$, hence points $(r_1/p, \ldots, r_n/p) \in [0,1)^n$ are not distributed uniformly. However, by considering $n!$ points $(r_{i_1}/p, \ldots, r_{i_{n-1}}/p) \in [0,\ 1)^{n-1}$ for all $n-1$ ordered choices of roots impartially, it is likely that these are uniformly distributed in $[0,\ 1)^{n-1}$ when $p(\in Spl(f)) \to \infty$. Here the definition of the uniform distribution is an ordinary one, numbering points in numerical order of $p \in Spl(f)$ with arbitrary numbering for the same p. If it is true, it is known ([2]) that

$$Pr(k,\ f) = \frac{A(n-1,\ k)}{(n-1)!} \quad (= E_n(k) \text{ say}), \tag{3}$$

where $A(m, k)$ is the Eulerian number defined by the following rules:

$$\begin{cases} A(m,\ k) = 0 \text{ unless } 1 \le k \le m, \quad \text{and} \\ A(1,\ 1) = 1,\ A(m,\ k) = (m-k+1)A(m-1,\ k-1) + kA(m-1,\ k). \end{cases}$$

In fact, numerical data by computer support (3). (See [1, 2])

Next, suppose that there is a decomposition

$$f(x) = g(h(x)) \quad (2 < \deg h(x) < \deg f(x)), \tag{4}$$

where we normalize the decomposition so that g, h are monic and $h(0) = 0$. We call $h(x)$ a reduced kernel of $f(x)$ and the degree of $h(x)$ a reduced degree of $f(x)$. Although there may be several reduced kernels, a reduced degree determines a reduced kernel uniquely (cf. Proposition 3 below). Put $m = \deg g$, $r = \deg h$ $(n = \deg f = mr)$

in (4). For a prime $p \in Spl(f)$, we group the roots $r_1, \ldots, r_n$ of $f(x) \equiv 0 \bmod p$ as follows:

$$\begin{aligned}\{r_i \mid 1 \le i \le n\} &= \{x \bmod p \mid f(x) = g(h(x)) \equiv 0 \bmod p\}\\ &= \bigcup_{i=1}^{m} \{r_{i,1}, \ldots, r_{i,r}\},\end{aligned}$$

where $r_{i,j}$ satisfies

$$h(r_{i,j}) \equiv s_i \bmod p \quad (1 \le \forall j \le r),$$

where s_i $(1 \le i \le m)$ are all roots of $g(x) \equiv 0 \bmod p$. Let us arrange any $r-1$ roots of $h(x) \equiv s_i \bmod p$ $(i = 1, \ldots, m)$ impartially. Denoting the permutation group of $\{1, \ldots, a\}$ by $\mathfrak{S}_a$, we put, for permutations $\mu \in \mathfrak{S}_m$ and $\sigma_k \in \mathfrak{S}_r$

$$\boldsymbol{r}_k(\mu, \sigma_k) = \left(\frac{r_{\mu(k),\sigma_k(1)}}{p}, \ldots, \frac{r_{\mu(k),\sigma_k(r-1)}}{p}\right) \quad (1 \le k \le m).$$

So, $p\boldsymbol{r}_k(\mu, \sigma_k)$ is an arrangement of $r - 1$ roots of $h(x) \equiv s_{\mu(k)} \bmod p$. As in [2], if points

$$(5) \qquad (\boldsymbol{r}_1(\mu, \sigma_1), \ldots, \boldsymbol{r}_m(\mu, \sigma_m)) \in [0, 1)^{m(r-1)} \quad \text{for} \quad \forall \mu \in \mathfrak{S}_m,\ \forall \sigma_i \in \mathfrak{S}_r$$

are distributed uniformly when $p \to \infty$, then we have

$$(6) \qquad Pr(f) = E_r^m \quad (f(x) = g(h(x)),\ m = \deg g,\ r = \deg h),$$

where the convolution E_r^m is defined inductively by the following:

$$E_r^1 = E_r, \quad E_r^{k+1}(l) = \sum_{i+j=l} E_r^k(i) E_r(j).$$

We note that it does not happen that all elements of a subset

$$\{x \bmod p \mid h(x) \equiv h(r_{i,j}) \bmod p\} \quad (\subset \{x \bmod p \mid f(x) \equiv 0 \bmod p\})$$

for i, j appear in an vector in (5) at the same time.

Now, let us assume that there is only one reduced degree, that is the decomposition (4) is unique; then numerical data in [1, 2] support (6), and we may expect that the points in (5) are distributed uniformly.

Before referring to examples in [2], which have two reduced degrees, let us give two non-trivial examples that have plural reduced degrees, and discuss the non-uniformity of points (5). A trivial example means $f(x) = g((h \circ k)(x)) = (g \circ h)(k(x))$ for three polynomials g, h, k. We consider all over $\mathbb{C}$ if we do not refer.

First, we treat the case that a reduced kernel is a monomial.

Theorem 1. *Let n be a natural number and l (≥ 2) a divisor of n. Let $f(x)$ be a monic polynomial of degree n and assume that there are monic polynomials $g(x), h(x)$ with $\deg h = r$, $h(0) = 0$ such that*

$$f(x) = g(x^l) = \sum_{k=0}^{m} b_k h(x)^k \quad (mr = n,\ b_m = 1). \tag{7}$$

Then, putting

$$h(x) = \sum_{k=1}^{r} c_k x^k \quad (c_r = 1),$$

we have

$$h(x) = \sum_{j \equiv r \bmod l} c_j x^j = x^{r_0} \times (a \text{ polynomial in } x^l)$$

where r_0 is the least non-negative residue of r modulo l and

$$f(x) = \sum_{\substack{0 \leq k \leq m,\\ rk \equiv 0 \bmod l}} b_k h(x)^k.$$

Proofs of this theorem and subsequent theorems are given from the next section on.

To state the next example, we introduce notations. For a natural number m and a constant $D \in \mathbb{C}$, we put

$$h(x, m, D) = x^m + m \sum_{1 \leq k \leq (m-1)/2} \binom{m-k}{k} \frac{D^k}{m-k} x^{m-2k},$$

where k is supposed to be integers, and for an odd natural number n and an even natural number m

$$H(x, n, m, D) = x^{(n-1)/2} + n \sum_{0 \leq j \leq (n-1)/2-1} \binom{(n-1)/2 + j}{2j+1} \frac{D^{m(n-(2j+1))/4}}{(n-1)/2 - j} x^j.$$

For example, $h(x, 1, D) = x$, $h(x, 2, D) = x^2$, $h(x, 3, D) = x^3 + 3Dx$, and we see that above two polynomials $h(x, m, D)$, $H(x, n, m, D)$ are polynomials in D, x with integer coefficients, computing p-factors for

$$\frac{m}{m-k}\binom{m-k}{k} = m \cdot \frac{(m-k-1)!}{(m-2k)!k!},$$

$$\frac{n}{(n-1)/2 - j}\binom{(n-1)/2 + j}{2j+1} = n \cdot \frac{((n-1)/2 + j)!}{((n-1)/2 - j)!(2j+1)!},$$

respectively.

Theorem 2. *Let m, n be natural numbers. If mn is odd, then we put*

$$h_1(x) = h(x, m, D), \quad h_2(x) = h(x, n, D),$$
$$g_1(x) = h(x, n, D^m), \quad g_2(x) = h(x, m, D^n).$$

If m is even and n is odd, then we put

$$h_1(x) = h(x, m, D), \qquad h_2(x) = h(x, n, D),$$
$$g_1(x) = xH(x, n, m, D)^2, \quad g_2(x) = h(x, m, D^n).$$

Then we have

$$g_1(h_1(x)) = g_2(h_2(x)).$$

With respect to these theorems, let us state some expectations. Suppose $f(x) = g_i(h_i(x))$ with $1 < \deg h_i < n = \deg f$ $(i = 1, 2)$, and we normalize them by a transformation $x \to x + a$ so that the second leading coefficient of f vanishes and moreover $h_i(0) = 0$. Put $d = (\deg h_1, \deg h_2)$. Then we expect
(i) if $d = 1$, then such pairs are of the form in the theorems above,
(ii) there are polynomials $H_1(x), H_2(x)$ such that $\deg H_i = (\deg h_i)/d$ $(i = 1, 2)$ which satisfy $h_i(x) = H_i(p(x))$ for an appropriate polynomial $p(x)$, and
(iii) there are polynomials G_1, G_2 with $\deg G_1 = (\deg h_2)/d$ and $\deg G_2 = (\deg h_1)/d$ which satisfy $G_1(h_1(x)) = G_2(h_2(x))$.

Now, let us give examples of polynomials $f(x)$ for which it has two decompositions and points in (5) are not distributed uniformly.

Theorem 3. *Let $G(x)$ be a monic polynomial with integer coefficients and let integers j, r satisfy $r > 1$, $j \geq 1$, $(j, r) = 1$, and we assume that either $G(x) = 1$, $j > 1$ or $\deg G > 0$. Then for a polynomial*

$$f = (x^j G(x^r))^r - d \quad (d \in \mathbb{Z}), \tag{8}$$

it has polynomials x^r and $x^j G(x^r)$ as reduced kernels, and points in (5) *are not distributed uniformly for $g(x) = x^j G(x)^r - d$, $h(x) = x^r$.*

In particular, points (5) do not distributed uniformly for a polynomial $f(x) = x^{jr} - d$, $g(x) = x^j - d$, $h(x) = x^r$ with $j > 1$, $r > 1$, $(j, r) = 1$.

Theorem 4. *Let m, n be odd integers such that $m > 1$, $n > 1$ and $dm \nmid n$ and $n > d$ for $d = (m, n)$, and we put*

$$f(x) = h(h(x, m, D), n, D^m) + c = h(h(x, n, D), m, D^n) + c,$$

where c, D $(\neq 0)$ are integers. Then for points in (5) *are not distributed uniformly for $g(x) = h(x, n, D^m), h(x) = h(x, m, D)$.*

Note that if m divides n, then $h(x, n, D)$ itself is a polynomial in $h(x, m, D)$ by Proposition 2, i.e. of a trivial type.

Now with these preparations, let us consider examples in [2]. First, let deg $f = 12$. Put

$$f(x) = (x(x^3 + c))^3 - d \quad (j = 1,\ G = x + c,\ r = 3 \text{ at } (8)),$$

and let p ($\neq 3$) be a prime number for which f mod p is completely decomposable. It is likely

$$\begin{aligned} &[Pr(1, f), \dots, Pr(11, f)] \\ &= \left[0, 0, 0, \frac{1}{15}, \frac{7}{30}, \frac{2}{5}, \frac{7}{30}, \frac{1}{15}, 0, 0, 0\right], \end{aligned} \tag{9}$$

which is equal neither to E_3^4 nor to E_4^3. In [2], the cases $c = -3$, $d = -3$ and $c = -1$, $d = -3$ are referred to as f_5, f_6, respectively. As above, points (5) for $g = x(x+c)^3 - d$, $h = x^3$ are not distributed uniformly. Thus $Pr(f) \neq E_3^4, E_4^3$ is not strange. Take an integer D such that $D^3 \equiv d$ mod p, and let $r_1, \dots, r_4$ be roots of $x^4 + cx - D \equiv 0$ mod p, and put

$$\prod_{i=1}^{4}(x - r_i) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4.$$

Then we have, besides a fundamental linear relation $s_1 \equiv 0$ mod p, non-linear relations among r_i

$$s_2 \equiv 0, \quad s_3 \equiv -c, \quad s_4 \equiv -D \quad \text{mod } p. \tag{10}$$

In this case, we have more relations as follows.

Theorem 5. *Let ω be an integer such that $\omega^2 + \omega + 1 \equiv 0$ mod p; then symmetric polynomials $S_1, \dots, S_4$ of $r_1, r_2, \omega r_3, \omega r_4$ defined by*

$$(x + r_1)(x + r_2)(x + \omega r_3)(x + \omega r_4) = x^4 + S_1x^3 + S_2x^2 + S_3x + S_4$$

satisfy

$$\begin{cases} 6S_3 - S_1^3 - 3c \equiv 0 \quad \text{mod } p, \\ S_1S_2 - 3S_3 \equiv 0 \quad \text{mod } p, \\ 36S_1^2S_4 - S_1^6 - 27c^2 \equiv 0 \quad \text{mod } p. \end{cases} \tag{11}$$

The author does not know whether non-linear relations (10) and (11) contribute to (9).

Next, let us consider the case of deg $= 15$. For

$$f = (x^3)^5 + 2 \quad (j = 3,\ G = 1,\ r = 5,\ d = -2), \tag{12}$$

numerical data in [2] suggest that $Pr(f)$ is (not E_5^3 but) E_3^5 as if $h = x^3$ were a unique reduced kernel. But, for the polynomial (12), points defined by (5) for $g = x^5 + 2$, $h = x^3$ are not distributed uniformly by Theorem 3. The data might be too few to recognize the difference between $Pr(f)$ and E_3^5. By contrast, we can recognize easily the difference between $Pr(f)$ and E_3^4, E_4^3 in the case of degree 12 as above, where data in the same range of primes p are enough.

For polynomials $f(x) = (x^3)^7 + 2, (x^5)^7 + 2, (x^3)^{35} + 2$, $Pr(f)$ looks like E_3^7, E_5^7, E_3^{35}, respectively ([2]).

We can add one more example. Put $f = (x^2(x^6 + x^3 + 1))^3 + 2$, which is of the type (8) like examples of degree 12 above. The difference

$$\begin{aligned} &E_3^8 - Pr(f) \\ &= [0, 0, 0, 0, 0, 0, 0, 0.00032, -0.00041, -0.00125, 0.00314, \\ &\quad 0.00170, -0.00568, 0.00169, 0.00095, -0.00045, 0, 0, 0, 0, 0, 0, 0, 0] \end{aligned}$$

within the range of $p < 10^{11}$.

The situations resemble the case of deg $= 15$. What differs between these and the case of degree 12? Are points (5) not distributed uniformly if there are distinct reduced degrees?

2. Proof of Theorem 1

We keep notations in Theorem 1, and let us introduce a notation $O(x^k)$, which denotes a polynomial in x whose degree is less than or equal to k.

Decompose $h(x)$ as

$$h(x) = \sum_{j \equiv r \bmod l} c_j x^j + \sum_{j \not\equiv r \bmod l} c_j x^j = h_0(x) + h_1(x) \quad \text{(say).}$$

We have to prove $h_1(x) = 0$ first. Assume that $h_1(x) \neq 0$ and denote the degree by s; then $s \not\equiv r \bmod l$ and $0 < s < r$ are obvious.

$f(x) = h(x)^m + O(x^{(m-1)r})$ follows from (7), and $h^m = \sum_{k=0}^m \binom{m}{k} h_0^k h_1^{m-k}$ and $\deg(h_0^k h_1^{m-k}) = rk + s(m-k) = sm + (r-s)k$ imply

$$h^m = h_0^m + m h_0^{m-1} h_1 + O(x^{sm+(r-s)(m-2)}).$$

Therefore we have

$$f = h_0^m + m h_0^{m-1} h_1 + O(x^{sm+(r-s)(m-2)}) + O(x^{(m-1)r}).$$

It is easy to see that the condition $0 < s < r$ implies $\deg(h_0^{m-1} h_1) = (m-1)r + s > \max((m-1)r, sm + (r-s)(m-2))$. Hence the degree of the right-hand side of

$$f - h_0^m = m h_0^{m-1} h_1 + O(x^{(m-1)r+s-1}) \tag{13}$$

is equal to $\deg(mh_0^{m-1}h_1)$. Since $mr_0 \equiv mr = n \equiv 0 \bmod l$, $h_0^m = (x^{r_0}\cdot$(a polynomial in $x^l))^m = x^{mr_0}\cdot$ (a polynomial in x^l) is a polynomial in x^l. Thus $f - h_0^m$ is a polynomial in x^l, hence the degree of the left-hand side polynomial in (13) is divisible by l. On the other hand, for the right-hand side of (13), we have $\deg(mh_0^{m-1}h_1) = (m-1)r + s \equiv -(r-s) \not\equiv 0 \bmod l$. This contradicts (13). Thus we have $h_1 = 0$ and there is a polynomial h_2 such that $h(x) = x^{r_0}h_2(x^l)$, and so we have $f(x) = g(x^l) = \sum_{k=0}^m b_k x^{r_0 k} h_2(x^l)^k$. This implies $b_k = 0$ unless $rk \equiv r_0 k \equiv 0 \bmod l$. □

3. Proof of Theorem 2 and miscellaneous results

We still keep notations in the introduction. To prove Theorem 2, we prepare lemmas.

Lemma 1. *For a natural number $n \geq 2$, we have*

$$\begin{aligned} &h(x, n+1, D^2) - xh(x, n, D^2) - D^2 h(x, n-1, D^2) \\ &= (1 + (-1)^n) D^n h(x, 1, D^2) \end{aligned} \tag{14}$$

and for $x = D(t - t^{-1})$,

$$h(x, 1, D^2) = D(t - t^{-1}), \quad h(x, 2, D^2) = D^2(t^2 + (-t^{-1})^2 - 2).$$

Proof. Since $h(x,1,D^2) = x$, $h(x,2,D^2) = x^2$, the last two equations are obvious. Before the proof of the induction formula (14), we note two equalities

$$\begin{aligned} &(n+1)\binom{n+1-k}{k}\frac{1}{n+1-k} - n\binom{n-k}{k}\frac{1}{n-k} \\ &= \binom{n-1-k}{k-1}\frac{n-1}{n+1-2k}, \end{aligned}$$

and

$$\binom{n-k-2}{k}\frac{1}{n-1-2k} = \binom{n-k-1}{k}\frac{1}{n-1-k}.$$

The first follows from

$$\begin{aligned} &(n+1)\binom{n+1-k}{k}\frac{1}{n+1-k} - n\binom{n-k}{k}\frac{1}{n-k} \\ &= \frac{(n+1)\cdot(n-k)!}{k!(n+1-2k)!} - \frac{n\cdot(n-1-k)!}{k!(n-2k)!} \\ &= \frac{(n-1-k)!}{k!(n-2k)!}\left\{\frac{(n+1)(n-k)}{n+1-2k} - n\right\} \\ &= \frac{(n-1-k)!}{k!(n-2k)!}\frac{kn-k}{n+1-2k} \\ &= \binom{n-1-k}{k-1}\frac{n-1}{n+1-2k}, \end{aligned}$$

and the second is direct.

Suppose that n is odd; then the left-hand side of (14) is equal to

$$\begin{aligned}
&(n+1)\sum_{1\le k\le (n-1)/2}\binom{n+1-k}{k}\frac{D^{2k}}{n+1-k}x^{n+1-2k}\\
&-n\sum_{1\le k\le (n-1)/2}\binom{n-k}{k}\frac{D^{2k}}{n-k}x^{n+1-2k}\\
&-D^2x^{n-1}-(n-1)\sum_{1\le k\le (n-1)/2-1}\binom{n-1-k}{k}\frac{D^{2k+2}}{n-1-k}x^{n-1-2k}\\
&=\sum_{1\le k\le (n-1)/2}\binom{n-1-k}{k-1}\frac{n-1}{n+1-2k}D^{2k}x^{n+1-2k}\\
&\quad -D^2x^{n-1}-(n-1)\sum_{1\le k\le (n-1)/2-1}\binom{n-1-k}{k}\frac{D^{2k+2}}{n-1-k}x^{n-1-2k}\\
&=\sum_{1\le K\le (n-1)/2-1}\binom{n-2-K}{K}\frac{n-1}{n-1-2K}D^{2K+2}x^{n-1-2K}\\
&\quad -(n-1)\sum_{1\le k\le (n-1)/2-1}\binom{n-1-k}{k}\frac{D^{2k+2}}{n-1-k}x^{n-1-2k}\\
&=0.
\end{aligned}$$

Next, suppose that n is even; then the right-hand side of (14) is equal to

$$\begin{aligned}
&(n+1)\sum_{1\le k\le n/2}\binom{n+1-k}{k}\frac{D^{2k}}{n+1-k}x^{n+1-2k}\\
&-n\sum_{1\le k\le n/2-1}\binom{n-k}{k}\frac{D^{2k}}{n-k}x^{n+1-2k}\\
&-D^2x^{n-1}-(n-1)\sum_{1\le k\le n/2-1}\binom{n-1-k}{k}\frac{D^{2k+2}}{n-1-k}x^{n-1-2k}\\
&=(n+1)\binom{n/2+1}{n/2}\frac{D^{n}}{n/2+1}x\\
&\quad +\sum_{1\le k\le n/2-1}\binom{n-1-k}{k-1}\frac{n-1}{n+1-2k}D^{2k}x^{n+1-2k}\\
&\quad -D^2x^{n-1}-(n-1)\sum_{1\le k\le n/2-1}\binom{n-1-k}{k}\frac{D^{2k+2}}{n-1-k}x^{n-1-2k}
\end{aligned}$$

$$
\begin{aligned}
&= (n+1)D^n x + D^2 x^{n-1} \\
&\quad + \sum_{2\le k\le n/2-1} \binom{n-1-k}{k-1} \frac{n-1}{n+1-2k} D^{2k} x^{n+1-2k} \\
&\quad - D^2 x^{n-1} - (n-1) \sum_{1\le k\le n/2-1} \binom{n-1-k}{k} \frac{D^{2k+2}}{n-1-k} x^{n-1-2k} \\
&= (n+1)D^n x \\
&\quad + \sum_{1\le K\le n/2-2} \binom{n-2-K}{K} \frac{n-1}{n-1-2K} D^{2K+2} x^{n-1-2K} \\
&\quad - (n-1) \sum_{1\le k\le n/2-1} \binom{n-1-k}{k} \frac{D^{2k+2}}{n-1-k} x^{n-1-2k} \\
&= (n+1)D^n x - (n-1)D^n x \\
&= 2D^n x \\
&= 2D^n h(x, 1, D^2),
\end{aligned}
$$

which completes a proof. □

Lemma 2. *Put*

$$c_n = D^n(t^n + (-t^{-1})^n - 1 - (-1)^n).$$

Then we have

$$c_{n+1} - D(t - t^{-1})c_n - D^2 c_{n-1} = D^n(1 + (-1)^n)c_1 \tag{15}$$

and

$$c_1 = D(t - t^{-1}), \quad c_2 = D^2(t^2 + (-t^{-1})^2 - 2).$$

Proof. The equalities for c_1, c_2 are obvious. The first follows from

$$
\begin{aligned}
&c_{n+1} - D(t - t^{-1})c_n - D^2 c_{n-1} \\
&= D^{n+1}(t^{n+1} + (-t^{-1})^{n+1} - 1 - (-1)^{n+1}) \\
&\quad - D(t - t^{-1}) \cdot D^n(t^n + (-t^{-1})^n - 1 - (-1)^n) \\
&\quad - D^2 \cdot D^{n-1}(t^{n-1} + (-t^{-1})^{n-1} - 1 - (-1)^{n-1}) \\
&= D^{n+1}(1 + (-1)^n)(t - t^{-1}) \\
&= D^n(1 + (-1)^n)c_1.
\end{aligned}
$$

□

Proposition 1. *For a natural number n, we have*

$$h(D(t-t^{-1}), n, D^2) = D^n(t^n + (-t^{-1})^n - 1 - (-1)^n)$$
$$= \begin{cases} D^n(t^n - t^{-n}) & \textit{if} \quad 2 \nmid n, \\ (D^{n/2}(t^{n/2} - t^{-n/2}))^2 & \textit{if} \quad 2 \mid n. \end{cases}$$

Proof. $h(D(t-t^{-1}), k, D^2) = c_k$ holds for $k = 1, 2$ and their induction formulas (14), (15) coincide for $x = D(t-t^{-1})$. Therefore they are the same. □

Proof of Theorem 2. We put $x = D_1(t-t^{-1})$ for $D_1 = \sqrt{D}$.

Let m, n be odd; then we have

$$\begin{aligned} h_1(x) &= h(D_1(t-t^{-1}), m, D_1^2) = D_1^m(t^m - t^{-m}), \\ g_1(h_1(x)) &= h(D_1^m(t^m - t^{-m}), n, D_1^{2m}) = D_1^{mn}(t^{mn} - t^{-mn}), \end{aligned} \tag{16}$$

which is symmetric with respect to m, n. Therefore we have $g_1(h_1(x)) = g_2(h_2(x))$ for $x = D_1(t-t^{-1})$, and so the assertion in this case.

Next, suppose that m is even and n is odd. First, we can see easily

$$xH(x^2, n, m, D_1^2) = h(x, n, D_1^m).$$

Hence, putting $x = D_1(t-t^{-1})$, we have

$$g_1(x^2) = x^2 H(x^2, n, m, D_1^2)^2 = h(x, n, D_1^m)^2$$

and

$$h_1(x) = h(x, m, D_1^2) = (D_1^{m/2}(t^{m/2} - t^{-m/2}))^2,$$

and so

$$\begin{aligned} &g_1(h_1(x)) \\ &= h(D_1^{m/2}(t^{m/2} - t^{-m/2}), n, D_1^m)^2 \\ &= (D_1^{mn/2}(t^{mn/2} + (-t^{-m/2})^n))^2 \\ &= D_1^{mn}(t^{mn} + t^{-mn} - 2). \end{aligned}$$

On the other hand, we have

$$\begin{aligned} &g_2(h_2(D_1(t-t^{-1}))) \\ &= h(h(D_1(t-t^{-1}), n, D_1^2), m, D_1^{2n}) \\ &= h(D_1^n(t^n + (-t^{-1})^n), m, D_1^{2n}) \\ &= D_1^{mn}(t^{mn} + (-t^{-1})^{mn} - 2), \end{aligned}$$

which implies

$$g_1(h_1(x)) = g_2(h_2(x)).$$

This completes a proof of Theorem 2. □

Let us give miscellaneous results.

Proposition 2. *Let k, m be natural numbers. Then $h(x, mk, D)$ is a polynomial of $h(x, m, D)$.*

Proof. The assertion follows from Proposition 1 and that $x^{mk} + y^{mk}$ is a polynomial in $x^m + y^m$, $x^m y^m$, hence $t^{mk} + (-t^{-1})^{mk}$ is a polynomial in $t^m + (-t^{-1})^m$ □

A polynomial $h(x,mk,D)$ is not necessarily a polynomial in $h(x,m,D)$ with integer coefficients as $h(x, 2, D) = x^2$, $h(x, 4, D) = x^4 + 4Dx^2$.

Proposition 3. *Let $f(x),y,z$ be monic polynomials in x and suppose that* $\deg(y) = \deg(z)$ *and $y(0) = z(0) = 0$. If $f(x)$ is a polynomial both in y and in z, then we have $y = z$.*

Proof. Put

$$\begin{aligned} f(x) &= y^m + a_{m-1}y^{m-1} + \cdots + a_1 y + a_0 \\ &= z^m + c_{m-1}z^{m-1} + \cdots + c_1 z + a_0, \\ y &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x \quad (b_n = 1), \\ z &= d_n x^n + d_{n-1}x^{n-1} + \cdots + d_1 x \quad (d_n = 1). \end{aligned}$$

We have only to conclude a contradiction under the assumption that there is an integer s with $1 \le s \le n-1$ such that $b_s \ne d_s$ and $b_k = d_k$ for $k \ge s+1$. Put

$$X = \sum_{i=s+1}^{n} b_i x^i, \quad Y = \sum_{i=1}^{s} b_i x^i, \quad Z = \sum_{i=1}^{s} d_i x^i;$$

then we have

$$y = X + Y, \quad z = X + Z, \quad \deg(Y - Z) = s.$$

Since $\deg(X^{m-k}Y^k) \le n(m-k) + sk = nm - (n-s)k$ and $\deg(X^{m-k}Z^k) \le nm - (n-s)k$, we have

$$y^m = X^m + mX^{m-1}Y + O(x^{nm-2(n-s)}), \quad z^m = X^m + mX^{m-1}Z + O(x^{nm-2(n-s)}).$$

Thus we have

$$\begin{aligned} f(x) &= y^m + O(x^{n(m-1)}) = z^m + O(x^{n(m-1)}) \\ &= X^m + mX^{m-1}Y + O(x^{nm-2(n-s)}) + O(x^{n(m-1)}) \\ &= X^m + mX^{m-1}Z + O(x^{nm-2(n-s)}) + O(x^{n(m-1)}) \end{aligned}$$

and so

$$mX^{m-1}(Y - Z) = O(x^{nm-2(n-s)}) + O(x^{n(m-1)}). \tag{17}$$

On the other hand, the definition of s implies $\deg(mX^{m-1}(Y-Z)) = n(m-1)+s$. The inequalities of degrees $\{n(m-1)+s\}-\{nm-2(n-s)\} = n-s > 0$ and $\{n(m-1)+s\}-\{n(m-1)\} = s > 0$ imply that the degree of the right hand side of the above equation (17) is less than the degree of the left hand side. Thus we have a contradiction. □

By this proposition, a reduced degree determines a reduced kernel uniquely.

Proposition 4. *Let $h_1(x), h_2(x)$ be monic polynomials with $(\deg(h_1), \deg(h_2)) = d$. Suppose that there are monic polynomials $g_1(x)$, $g_2(x)$ such that*

$$g_1(h_1(x)) = g_2(h_2(x)), \quad \deg(g_1) = \frac{\deg(h_2)}{d} \quad \textit{and} \quad \deg(g_2) = \frac{\deg(h_1)}{d}.$$

If polynomials G_1, G_2 satisfy $G_1(h_1(x)) = G_2(h_2(x))$, then there exists a polynomial $G(x)$ so that $G_i(x) = G(g_i(x))$ for $i = 1, 2$.

Proof. We note that $G_1(h_1(x)) = G_2(h_2(x))$ implies $\deg(G_1)\deg(h_1) = \deg(G_2)\deg(h_2)$, hence $\deg(G_1)$ is divisible by $\deg(h_2)/d = \deg(g_1)$. We prove the assertion by induction on $m = \deg(G_1)/\deg(g_1)$. Suppose $m = 1$; denoting the leading coefficient of G_1 by a, we have

$$\deg(G_1 - ag_1) < \deg(g_1)$$

and $(G_1 - ag_1)(h_1(x)) = G_1(h_1(x)) - ag_1(h_1(x)) = G_2(h_2(x)) - ag_2(h_2(x)) = (G_2 - ag_2)(h_2(x))$. Therefore $\deg(G_1 - ag_1)$ is divisible by $\deg(g_1)$ as above, and hence we have $G_1 - ag_1 = c$ for some constant $c \in \mathbb{C}$. Then $G_2(h_2(x)) = G_1(h_1(x)) = ag_1(h_1(x)) + c = ag_2(h_2(x)) + c = (ag_2 + c)(h_2(x))$, which means $G_2(x) = ag_2(x) + c$. Thus we can take a polynomial $ax + c$ as $G(x)$.

Suppose that the assertion is true for $m \le k$ and $\deg(G_1) = (k+1)\deg(g_1)$. Denoting the leading coefficient of G_1 by a as above, we have $\deg(G_1 - ag_1^{k+1}) < (k+1)\deg(g_1)$ and $(G_1 - ag_1^{k+1})(h_1(x)) = G_1(h_1(x)) - ag_1(h_1(x))^{k+1} = (G_2 - ag_2^{k+1})(h_2(x))$. Hence $\deg(G_1 - ag_1^{k+1})$ is divisible by $\deg(g_1)$ and so $\deg(G_1 - ag_1^{k+1}) = l\deg(g_1)$ with $l \le k$. Thus the induction assumption to $G_1 - ag_1^{k+1}$ and $G_2 - ag_2^{k+1}$ completes a proof. □

4. Case of $\deg h = 3$

In this section, we discuss the expectation in the introduction in the case of $h_1 = h(x, 3, D^2)$. Through this section, we put

$$y = h(x, 3, D^2) = x^3 + 3D^2x \quad (D \neq 0).$$

Then a polynomial h in x can be written as $v_0(y) + v_1(y)x + v_2(y)x^2$ for polynomials v_i in y uniquely. We will give two theorems in this section, which support the expectation.

Lemma 3. *Let*

$$y = x^3 + 3D^2x, \quad h = v_0 + v_1x + v_2x^2,$$

where v_i $(i = 0, 1, 2)$ *are polynomials in* y *with* $\deg v_0 > \max(\deg v_1, \deg v_2)$ *and put*

$$A = v_1^3 + 3D^2v_1v_2^2 - v_2^3y. \tag{18}$$

Put $d_0 = \deg v_0$ *as a polynomial in* y *and let* c_0, c_1, c_2, u, w *be polynomials in* y *which satisfy*

$$c_0 = v_0^n + O(x^{3d_0n-3}),$$
$$c_1 = O(x^{3d_0n-3}),$$
$$c_2 = nv_0^{n-1}v_2 + O(x^{3d_0n-6}) = O(x^{3d_0n-3}),$$
$$c_1A + v_2^2y(c_1v_2 - c_2v_1) = uv_1A, \tag{19}$$
$$c_1v_2 - c_2v_1 = wA, \tag{20}$$
$$u = nv_0^{n-1} + O(x^{3d_0(n-1)-3}),$$
$$w = -\frac{n(n-1)}{2} \cdot v_0^{n-2} + O(x^{3d_0(n-2)-3}).$$

For

$$H = c_0 + c_1x + c_2x^2,$$

we put

$$hH = C_0 + C_1x + C_2x^2,$$

where C_i $(i = 0, 1, 2)$ *are polynomials in* y. *Then we have*

$$C_0 = v_0^{n+1} + O(x^{3d_0(n+1)-3}),$$
$$C_1 = O(x^{3d_0(n+1)-3}),$$
$$C_2 = (n+1)v_0^nv_2 + O(x^{3d_0(n+1)-6}),$$
$$C_1A + v_2^2y(C_1v_2 - C_2v_1) = Uv_1A,$$
$$C_1v_2 - C_2v_1 = WA \quad \text{if} \quad v_1 \neq 0,$$

where

$$U = c_0 - 3D^2c_2 + (v_0 - 3D^2v_2)u - yv_1v_2w = (n+1)v_0^n + O(x^{3d_0n-3}),$$
$$W = v_0w - u = -\frac{n(n+1)}{2} \cdot v_0^{n-1} + O(x^{3d_0(n-1)-3}).$$

Proof. Since hH is equal to

$$\begin{aligned}
&c_2v_2x^4 + (c_1v_2 + c_2v_1)x^3 + (c_0v_2 + c_1v_1 + c_2v_0)x^2 + (c_0v_1 + c_1v_0)x + c_0v_0\\
&= (c_0v_2 + c_1v_1 + c_2v_0 - 3D^2c_2v_2)x^2\\
&\quad + (c_0v_1 + c_1v_0 - 3D^2(c_1v_2 + c_2v_1) + c_2v_2y)x + c_0v_0 + (c_1v_2 + c_2v_1)y,
\end{aligned}$$

we have

$$\begin{aligned}
C_0 &= c_0v_0 + (c_1v_2 + c_2v_1)y,\\
C_1 &= c_0v_1 + c_1v_0 - 3D^2(c_1v_2 + c_2v_1) + c_2v_2y,\\
C_2 &= c_0v_2 + c_1v_1 + c_2v_0 - 3D^2c_2v_2.
\end{aligned}$$

$C_1A + v_2^2y(C_1v_2 - C_2v_1)$ is equal to

$$\begin{aligned}
&(c_0 - 3D^2c_2)v_1A + (v_0 - 3D^2v_2)c_1A\\
&+ c_2v_2yA + c_1v_0v_2^3y + c_2v_2^4y^2 - 3D^2c_1v_2^4y - c_2v_0v_1v_2^2y - c_1v_1^2v_2^2y,
\end{aligned}$$

and by replacing c_1A by $uv_1A - v_2^2y(c_1v_2 - c_2v_1)$ (cf. 19) in the second term, it is equal to

$$\begin{aligned}
&(c_0 - 3D^2c_2)v_1A + (v_0 - 3D^2v_2)(uv_1A - v_2^2y(c_1v_2 - c_2v_1))\\
&+ c_2v_2yA + c_1v_0v_2^3y + c_2v_2^4y^2 - 3D^2c_1v_2^4y - c_2v_0v_1v_2^2y - c_1v_1^2v_2^2y
\end{aligned}$$

and replacing the third A by the definition (18),

$$= (c_0 - 3D^2c_2 + (v_0 - 3D^2v_2)u)v_1A - yv_1^2v_2(c_1v_2 - c_2v_1)$$

and using (20), we have the final form

$$(c_0 - 3D^2c_2 + (v_0 - 3D^2v_2)u - yv_1v_2w)v_1A = Uv_1A.$$

Now, by using (19), (20), it is easy to see that

$$(C_1v_2 - C_2v_1)v_1 - (v_0w - u)v_1A = -3D^2c_1v_1v_2^2 - c_1v_1^3 + c_1v_2^3y + c_1A = 0.$$

If $v_1 \neq 0$, then we have $C_1v_2 - C_2v_1 = (v_0w - u)A$. And the other assertions are easy, noting $\deg v_1, \deg v_2 \leq d_0 - 1$ as polynomials in y. □

Lemma 4. *Let $h = v_0(y) + v_1(y)x + v_2(y)x^2$ with $y = x^3 + 3D^2x$ and $d_0 = \deg v_0 > \max(\deg v_1, \deg v_2)$, and put $A = v_1^3 + 3D^2v_1v_2^2 - v_2^3y$. For a natural number n, write $h^n = c_0 + c_1x + c_2x^2$ with polynomials c_i in y. We have $c_2 = nv_0^{n-1}v_2 + O(x^{3d_0n-6})$, and if $v_1 \neq 0$, then $c_1v_2 - c_2v_1$ is a multiple of A by a polynomial $(-n(n-1)/2) \cdot v_0^{n-2} + O(x^{3d_0(n-2)-3})$.*

Proof. We use the induction on n. In case of $n = 1$, $c_i = v_i$ $(i = 0, 1, 2)$ and $u = 1$ imply $c_1 v_2 - c_2 v_1 = 0$, and $c_1 A + v_2^2 y(c_1 v_2 - c_2 v_1) = u v_1 A$ is clear. Thus the assertion for $n = 1$ is obvious. Then Lemma 3 completes the induction. □

Theorem 6. *Let $h(x), g(x)$ be monic polynomials in x with $h(0) = g(0) = 0$, and suppose that $f(x) = g(h(x))$ is a polynomial in $y = x^3 + 3D^2 x$ $(D \neq 0)$. If $\deg h(x)$ is a multiple of 3, then $h(x)$ itself is a polynomial in y.*

Proof. We write $h = v_0 + v_1 x + v_2 x^2$, where v_0, v_1, v_2 are polynomials in y. Since $\deg h$ is a multiple of 3 by the assumption and $\deg v_k x^k \equiv k \bmod 3$ $(k = 0, 1, 2)$, we have $\deg h = \deg v_0 > \deg v_1 + 1, \deg v_2 + 2$. Put $f(x) = c_0 + c_1 x + c_2 x^2$ for polynomials c_i in y. Then we have $c_1 = c_2 = 0$ by the assumption. On the other hand, applying Lemma 4 to the expression of $f(x)$ as a sum of powers of $h(x)$, we have $c_2 = n v_0^{n-1} v_2 + O(x^{3d_0 n - 6})$ for $n = \deg g(x)$ and the degree d_0 of v_0 as a polynomial in y, and so $v_2 = 0$. Suppose $v_1 \neq 0$; Lemma 4 implies that

$$c_1 v_2 - c_2 v_1 = (v_1^3 + 3D^2 v_1 v_2^2 - v_2^3 y)\left(-\frac{n(n-1)}{2} \cdot v_0^{n-2} + O(x^{3d_0(n-2)-3})\right),$$

which is equal to 0 by $c_1 = c_2 = 0$. Since $(-n(n-1)/2) \cdot v_0^{n-2} + O(x^{3d_0(n-2)-3}) \neq 0$, we have $v_1^3 + 3D^2 v_1 v_2^2 - v_2^3 y = 0$. This implies $v_1 = 0$ by $v_2 = 0$, which is a contradiction. Thus we have $v_1 = 0$ and hence $h = v_0$ is a polynomial in y. □

The next result supports the expectation, although it is a very special case of $\deg g = 3$. Our proof is technical and an intrinsic proof is desirable.

Theorem 7. *Let $h(x)$ be a monic polynomial in x with $h(0) = 0$, and $f(x) = g(h(x))$ $(g(x) = x^3 + b_2 x^2 + b_1 x)$ $(b_1, b_2 \in \mathbb{C})$. Then $f(x)$ is a polynomial in y if and only if either $h(x)$ itself is a polynomial in y, or for an integer M, $h(x) = h(x, M, D^2)$ and*

$$\begin{aligned} b_2 &= 0, & b_1 &= 3D^{2M} \quad \text{if} \quad M \equiv 1 \mod 2,\\ b_2 &= 6D^M, & b_1 &= 9D^{2M} \quad \text{if} \quad M \equiv 0 \mod 2. \end{aligned}$$

The proof of the sufficiency is easy as follows: If $h(x)$ is a polynomial in y, then $f(x)$ is clearly a polynomial in y. To show the other case, we put $x = D(t - t^{-1})$. Since we have, by Proposition 1

$$h(x) = h(x, M, D^2) = D^M \begin{cases} t^M - t^{-M} & \text{if} \quad M \equiv 1 \mod 2,\\ t^M + t^{-M} - 2 & \text{if} \quad M \equiv 0 \mod 2, \end{cases}$$

it is easy to see

$$\begin{aligned} h^3 \phantom{{}+ 6D^M h^2} + 3D^{2M} h &= D^{3M}(t^{3M} - t^{-3M}) \quad \text{if} \quad M \equiv 1 \mod 2,\\ h^3 + 6D^M h^2 + 9D^{2M} h &= D^{3M}(t^{3M/2} - t^{-3M/2})^2 \quad \text{if} \quad M \equiv 0 \mod 2. \end{aligned}$$

They are polynomials in $y = D^3(t^3 - t^{-3})$ by the theory of symmetric polynomials. Thus $f(x)$ is a polynomial in y, containing D in coefficients in general.

To prove the converse, we need preparations.

Lemma 5. *For a non-negative integer m, we put*

$$u_m(x) = x^m + \sum_{1\le k\le m/2} \frac{\binom{m-k}{m-2k}}{2^{2k}} x^{m-2k},$$

$$p_m(x) = x^{m+1} + (m+1) \sum_{1\le k\le m/2} \frac{\binom{m-k}{m-2k}}{2^{2k}(m-2k+1)} x^{m-2k+1} + (1+(-1)^{m-1})2^{-(m+1)},$$

where k is supposed to be integers. Then we have

$$u_{m+2}(x) = \frac{x}{2} p_m(x) + \left(\frac{x^2}{2} + \frac{1}{4}\right) u_m(x), \tag{21}$$

$$p_{m+2}(x) = \left(\frac{x^2}{2} + \frac{1}{4}\right) p_m(x) + \frac{x}{2}(x^2+1) u_m(x). \tag{22}$$

Proof. If m is even, then we see

$$\begin{aligned}
&\frac{x}{2} p_m(x) + \left(\frac{x^2}{2} + \frac{1}{4}\right) u_m(x) \\
&= \frac{x^{m+2}}{2} + \frac{m+1}{2} \sum_{k=1}^{m/2} \frac{\binom{m-k}{m-2k}}{2^{2k}(m-2k+1)} x^{m-2k+2} \\
&\quad + \frac{x^{m+2}}{2} + \frac{1}{2} \sum_{k=1}^{m/2} \frac{\binom{m-k}{m-2k}}{2^{2k}} x^{m-2k+2} + \frac{x^m}{4} + \frac{1}{4} \sum_{k=1}^{m/2} \frac{\binom{m-k}{m-2k}}{2^{2k}} x^{m-2k} \\
&= x^{m+2} + \frac{x^m}{4} + \frac{1}{2} \sum_{k=1}^{m/2} \frac{\binom{m-k}{m-2k}}{2^{2k}} \left(\frac{m+1}{m-2k+1} + 1\right) x^{m-2k+2} \\
&\quad + \sum_{K=1}^{m/2} \frac{\binom{m-K+1}{m-2K+2}}{2^{2K}} x^{m-2K+2} + \frac{1}{2^{m+2}} - \frac{x^m}{4} \\
&= x^{m+2} + \sum_{k=1}^{m/2} \frac{1}{2^{2k}} \left\{ \binom{m-k}{m-2k} \frac{m-k+1}{m-2k+1} + \binom{m-k+1}{m-2k+2} \right\} x^{m-2k+2} \\
&\quad + \frac{1}{2^{m+2}} \\
&= x^{m+2} + \sum_{k=1}^{m/2+1} \frac{1}{2^{2k}} \binom{m+2-k}{m-2k+2} x^{m-2k+2} \\
&= u_{m+2}(x),
\end{aligned}$$

and similarly we have (21) for an odd integer m. Next, let us see (22). For even m, we have

$$\begin{aligned}
&\left(\frac{x^2}{2}+\frac{1}{4}\right)p_m(x)+\frac{x}{2}(x^2+1)u_m(x)\\
&=\frac{x^{m+3}}{2}+\frac{m+1}{2}\sum_{k=1}^{m/2}\frac{\binom{m-k}{m-2k}}{2^{2k}(m-2k+1)}x^{m-2k+3}\\
&\quad+\frac{x^{m+1}}{4}+\frac{m+1}{4}\sum_{k=1}^{m/2}\frac{\binom{m-k}{m-2k}}{2^{2k}(m-2k+1)}x^{m-2k+1}\\
&\quad+\frac{x^{m+3}}{2}+\frac{1}{2}\sum_{k=1}^{m/2}\frac{\binom{m-k}{m-2k}}{2^{2k}}x^{m-2k+3}\\
&\quad+\frac{x^{m+1}}{2}+\frac{1}{2}\sum_{k=1}^{m/2}\frac{\binom{m-k}{m-2k}}{2^{2k}}x^{m-2k+1}\\
&=x^{m+3}+\frac{3x^{m+1}}{4}+\frac{1}{2}\sum_{k=1}^{m/2}\frac{\binom{m-k}{m-2k}}{2^{2k}}\left\{\frac{m+1}{m-2k+1}+1\right\}x^{m-2k+3}\\
&\quad+\sum_{k=1}^{m/2}\frac{\binom{m-k}{m-2k}}{2^{2k}}\left\{\frac{m+1}{4(m-2k+1)}+\frac{1}{2}\right\}x^{m-2k+1}\\
&=x^{m+3}+\frac{3x^{m+1}}{4}+\sum_{k=1}^{m/2}\frac{\binom{m-k}{m-2k}}{2^{2k}}\frac{m-k+1}{m-2k+1}x^{m-2k+3}\\
&\quad+\sum_{K=1}^{m/2}\frac{\binom{m-K+1}{m-2K+2}}{2^{2K}}\left\{\frac{m+1}{m-2K+3}+2\right\}x^{m-2K+3}-\frac{3}{4}x^{m+1}+\frac{m+3}{2^{m+2}}x\\
&=x^{m+3}+\sum_{k=1}^{m/2}\frac{1}{2^{2k}}\left\{\binom{m-k}{m-2k}\frac{m-k+1}{m-2k+1}\right.\\
&\qquad\qquad\left.+\binom{m-k+1}{m-2k+2}\left(\frac{m+1}{m-2k+3}+2\right)\right\}x^{m-2k+3}\\
&\quad+\frac{m+3}{2^{m+2}}x\\
&=x^{m+3}+\sum_{k=1}^{m/2}\frac{1}{2^{2k}}\binom{m+2-k}{m+2-2k}\frac{m+3}{m-2k+3}x^{m-2k+3}+\frac{m+3}{2^{m+2}}x\\
&=p_{m+2}(x),
\end{aligned}$$

and similarly we have (22) for odd m. □

We note $u_m(x) = p'_m(x)/(m+1)$.

Proposition 5. *If monic polynomials* $u(x)$, $p(x)$ *satisfy*

$$(x^2+1)u(x)^2 + c = p(x)^2 \quad (c \in \mathbb{C}), \tag{23}$$

then we have, for $m = \deg(u(x))$

$$u(x) = u_m(x), \quad p(x) = p_m(x), \quad c = c_m = \frac{(-1)^{m-1}}{2^{2m}}. \tag{24}$$

Proof. We prove the assertion by induction on m.

The case of $m = 0$: In this case, $u(x) = 1$ and $p(x) = x + b$ for some $b \in \mathbb{C}$. The equation (23) implies

$$x^2 + 1 + c = x^2 + 2bx + b^2,$$

which means $b = 0$, $c = -1$. Since $u_0(x) = 1$, $p_0(x) = x$, $c_0 = -1$, the assertion is true for $m = 0$.

The case of $m = 1$: We put $u(x) = x + b$, $p(x) = x^2 + dx + e$; then we have

$$(x^2+1)u(x)^2 + c = x^4 + 2bx^3 + (b^2+1)x^2 + 2bx + b^2 + c,$$
$$p(x)^2 = x^4 + 2dx^3 + (d^2+2e)x^2 + 2dex + e^2,$$

hence $b = d$, $b^2 + 1 = d^2 + 2e$, $b = de$, $b^2 + c = e^2$. Thus we have $b = d = 0$, $e = 1/2$, $c = 1/4$, which implies (24) for $m = 1$, since $u_1(x) = x$, $p_1(x) = x^2 + 1/2$.

The case of $m \geq 2$: Since $p(x), u(x)$ are monic and $\deg(p(x)) = \deg(u(x)) + 1 = m + 1$, putting

$$r(x) = p(x) - xu(x) \tag{25}$$

we have $\deg(r(x)) \leq m$. The equation (23) implies $(x^2+1)u(x)^2 + c = p(x)^2 = r(x)^2 + 2xr(x)u(x) + x^2u(x)^2$ and so

$$u(x)^2 + c = r(x)^2 + 2xr(x)u(x). \tag{26}$$

Next, we will show

$$r(x) = \frac{1}{2}x^{m-1} + O(x^{m-2}). \tag{27}$$

As above, we know $\deg(r(x)) \leq m$. Suppose $\deg(r(x)) = m$; then the degree of the right-hand side of (26) is $2m+1$, but the left-hand side is of degree $2m$. Hence we have a contradiction and so $\deg(r(x)) < m$. Suppose $\deg(r(x)) \leq m-2$; the degree of the right-hand side of (26) is less than $\max(2(m-2), 1+(m-2)+m) = 2m-1$, which is less than the degree $2m$ of the left-hand side, which is a contradiction. Thus we have $\deg(r(x)) = m-1$, and then comparing the leading terms of the both sides of (26), we have (27). Next, we show

$$u(x) = 2xr(x) + r_1(x), \quad \deg(r_1(x)) = m-2. \tag{28}$$

Write

$$u(x) = (bx+d)r(x) + r_1(x), \quad \deg(r_1(x)) \le m-2.$$

Comparing the leading coefficients of the both sides, we have $b = 2$ easily. Substituting the above to (26), we have

$$(4dx + d^2 - 1)r(x)^2 + 2(x+d)r(x)r_1(x) + r_1(x)^2 + c = 0. \tag{29}$$

Since the degree of $2(x+d)r(x)r_1(x) + r_1(x)^2 + c$ is less than or equal to $2m-2$, we have $\deg((4dx + d^2 - 1)r(x)^2) \le 2m-2$, hence $d = 0$, and then (29) implies $0 = r(x)^2 - 2xr(x)r_1(x) - r_1(x)^2 - c = (r(x) - xr_1(x))^2 - x^2 r_1(x)^2 - r_1(x)^2 - c$, i.e.

$$(r(x) - xr_1(x))^2 = (x^2+1)r_1(x)^2 + c. \tag{30}$$

If $\deg(r_1(x)) \le m-3$ holds, then the degree of the left-hand side of (30) is $2(m-1)$ and the right-hand side is of degree less than or equal to $2 + 2(m-3)$, which is a contradiction. Thus we have proved $\deg r_1(x) = m-2$ and so (28).

Denote the leading coefficient of $r_1(x)$ by a; then comparing the leading coefficients of (30) we have $(1/2 - a)^2 = a^2$ and so $a = 1/4$. Therefore we have

$$r_1(x) = \frac{1}{4}x^{m-2} + O(x^{m-3})$$

and then (27) implies

$$r(x) - xr_1(x) = \frac{1}{4}x^{m-1} + O(x^{m-2}). \tag{31}$$

Now, (30) is nothing but

$$(x^2+1)(4r_1(x))^2 + 16c = (4r(x) - 4xr_1(x))^2,$$

and $4r_1(x), 4r(x) - 4xr_1(x)$ are monic polynomials of degree $m-2, m-1$, respectively. Hence by the induction assumption, we have

$$4r_1(x) = u_{m-2}(x), \quad 16c = c_{m-2}, \quad 4r(x) - 4xr_1(x) = p_{m-2}(x). \tag{32}$$

This implies $c = c_m$. We can show the assertion as follows:

$$\begin{aligned} u(x) &= 2xr(x) + r_1(x) \quad \text{(by (28))} \\ &= \frac{x}{2} p_{m-2}(x) + \left(\frac{x^2}{2} + \frac{1}{4}\right) u_{m-2}(x) \quad \text{(by (32))} \\ &= u_m(x) \quad \text{(by Lemma 5)} \end{aligned}$$

and

$$\begin{aligned} p(x) &= r(x) + xu(x) \quad \text{(by (25))} \\ &= \frac{x}{4} \cdot u_{m-2}(x) + 4^{-1} p_{m-2}(x) + xu_m(x) \quad \text{(by (32))} \\ &= \left(\frac{x^2}{2} + \frac{1}{4}\right) p_{m-2}(x) + \frac{x}{2} \cdot (x^2+1) u_{m-2}(x) \quad \text{(by Lemma 5)} \\ &= p_m(x). \end{aligned}$$

□

Proposition 6. *For a non-negative integer m, we have*

$$\begin{aligned} p_m\left(\frac{t-t^{-1}}{2}\right) &= 2^{-(m+1)}(t^{m+1} + (-t)^{-(m+1)}), \\ u_m\left(\frac{t-t^{-1}}{2}\right) &= \frac{t^{m+2} + (-t)^{-m}}{2^m(t^2+1)}. \end{aligned}$$

Proof. By denoting the right-hand sides of p_m, u_m in the assertion by P_m, U_m, respectively, it is easy to see

$$\begin{aligned} U_{m+2} &= \frac{t-t^{-1}}{4} P_m + \frac{t^2+t^{-2}}{8} U_m, \\ P_{m+2} &= \frac{t^2+t^{-2}}{8} P_m + \frac{(t-t^{-1})(t+t^{-1})^2}{2^4} U_m. \end{aligned}$$

They coincide with the induction formula (21), (22) with $x = (t - t^{-1})/2$ in Lemma 5, noting that $x^2/2 + 1/4 = (t^2 + t^{-2})/8$ and $(x/2) \cdot (x^2+1) = 2^{-4}(t-t^{-1})(t+t^{-1})^2$. The definitions $p_0(x) = x$, $u_0(x) = 1$, $p_1(x) = x^2 + 1/2$ and $u_1(x) = x$ imply the assertion for $m = 0, 1$ easily. Thus we have the assertion of the proposition. □

Let us begin the proof of Theorem 7 with preparations above. We write

$$h(x) = v_0(y) + v_1(y)x + v_2(y)x^2,$$

and $a=3D^2$. It is not hard to see with $y=x^3+ax$

$$\begin{aligned}
f(x) &= h(x)^3 + b_2 h(x)^2 + b_1 h(x) \\
&= \{b_1 v_2 + b_2(v_1^2 + 2v_0 v_2 - a v_2^2) + 3v_1 v_2^2 y + 3v_0^2 v_2 + 3v_0 v_1^2 + a^2 v_2^3 \\
&\qquad - 3a v_0 v_2^2 - 3a v_1^2 v_2\} x^2 \\
&\quad + \{b_1 v_1 + b_2(v_2^2 y - 2v_1 v_2 a + 2v_0 v_1) + 3v_0 v_2^2 y + 3v_1^2 v_2 y - 6a v_0 v_1 v_2 - a v_1^3 \\
&\qquad + 3v_0^2 v_1 - 2a v_2^3 y + 3a^2 v_1 v_2^2\} x \\
&\quad + \{v_0^3 + b_2 v_0^2 + b_1 v_0 - 3a v_1 v_2^2 y + v_2^3 y^2 + (v_1^3 + 2b_2 v_1 v_2 + 6v_0 v_1 v_2) y\} \\
&= c_2 x^2 + c_1 x + c_0 \quad \text{(say)},
\end{aligned}$$

where we abbreviated $v_i(y)$ to v_i. Since $f(x)$ is a polynomial in $y=x^3+ax$ by the assumption, the coefficients of x and x^2 vanish and so we have

$$c_1 = c_2 = 0.$$

Then we have

$$c_2 v_1 - c_1 v_2 = (v_1^3 + a v_1 v_2^2 - v_2^3 y)(b_2 - 2a v_2 + 3v_0) = 0.$$

Suppose $v_1^3 + a v_1 v_2^2 - v_2^3 y = 0$; if $v_1 v_2 \neq 0$, the degree of the left-hand side is $3\deg v_1$, $3\deg v_2 + 1$ according to $\deg v_1 > \deg v_2$, $\deg v_1 \leq \deg v_2$, respectively. This is a contradiction and so we have $v_1 = v_2 = 0$. Thus in this case $h(x) = v_0(y)$ is a polynomial in y. Suppose $v_1^3 + a v_1 v_2^2 - v_2^3 y \neq 0$ and so $b_2 - 2a v_2 + 3v_0 = 0$. Since the determinant of the coefficients matrix of the simultaneous equations $c_1 = c_2 = 0$ with respect to b_1, b_2 is $-(v_1^3 + a v_1 v_2^2 - v_2^3 y) \neq 0$, we have

$$b_1 = -4a v_0 v_2 + 3v_0^2 + a^2 v_2^2 - 3v_1 v_2 y + a v_1^2, \tag{33}$$

$$b_2 = 2a v_2 - 3v_0. \tag{34}$$

Substituting $v_0 = (2a v_2 - b_2)/3$ to (33), we have

$$b_1 = -\frac{a^2 v_2^2}{3} + a v_1^2 + \frac{b_2^2}{3} - 3v_1 v_2 y$$

and so

$$\left(\left(\frac{y}{2D^3}\right)^2 + 1\right) v_2^2 + \frac{3}{a^2}\left(b_1 - \frac{b_2^2}{3}\right) = \left(\frac{v_1}{D} - \frac{y v_2}{2D^3}\right)^2$$

Since v_1, v_2 are polynomials in y, regarding them as a polynomial in $y/(2D^3)$, denote the leading coefficient of v_2 by A, and put $m = \deg(v_2)$. Proposition 5 yields

$$v_2 = Au_m\left(\frac{y}{2D^3}\right),$$
$$\frac{3}{a^2}\left(b_1 - \frac{b_2^2}{3}\right) = A^2 c_m,$$
$$\frac{v_1}{D} - \frac{yv_2}{2D^3} = Bp_m\left(\frac{y}{2D^3}\right) \quad (B = \pm A),$$

where u_m, p_m are polynomials in Lemma 5. Thus putting

$$Y = \frac{y}{2D^3},$$

we have

$$\begin{aligned} v_2 &= Au_m(Y), \\ v_1 &= D(AYu_m(Y) + Bp_m(Y)), \\ b_1 &= \frac{a^2 c_m A^2 + b_2^2}{3}, \\ v_0 &= \frac{2a}{3} Au_m(Y) - \frac{b_2}{3}. \end{aligned}$$

Therefore we have

$$\begin{aligned} h(x) &= v_0(y) + v_1(y)x + v_2(y)x^2 \\ &= \frac{2aA}{3} u_m(Y) - \frac{b_2}{3} + D(AYu_m(Y) + Bp_m(Y))x + Au_m(Y)x^2 \end{aligned}$$

and putting $\delta = A/B$ $(= \pm 1)$,

$$\begin{aligned} h(x) &= A(2D^2 + DYx + x^2)u_m(Y) + DBp_m(Y)x - \frac{b_2}{3} \\ &= \frac{A}{2D^2}\{(x^4 + 5D^2x^2 + 4D^4)u_m(Y) + 2D^3\delta p_m(Y)x\} - \frac{b_2}{3}, \end{aligned} \tag{35}$$

noting $Y = (2D^3)^{-1}(x^3 + 3D^2x)$. The following is the last lemma necessary to prove Theorem 2.

Lemma 6. *Putting*

$$g = (x^4 + 5D^2x^2 + 4D^4)u_m(Y) + 2D^3\delta p_m(Y)x,$$

we have

$$\begin{aligned} 2^{m-1}D^{3m}g - h(x, 3m+4, D^2) &= (1 + (-1)^m)D^{3m+4} \quad \textit{if} \quad \delta = 1, \\ 2^{m-1}D^{3m-2}g - h(x, 3m+2, D^2) &= (1 + (-1)^m)D^{3m+2} \quad \textit{if} \quad \delta = -1, \end{aligned}$$

and

$$h(x) = \kappa_1 h(x, 3m + 3 + \delta, D^2) + \kappa_2,$$

for some constants κ_1, κ_2.

Proof. Put $x = D(t - t^{-1})$, we have

$$Y = \frac{t^3 - t^{-3}}{2},$$
$$x^4 + 5D^2x^2 + 4D^4 = D^4(t^4 + t^{-4} + t^2 + t^{-2})$$

and then, noting $(t^4 + t^{-4} + t^2 + t^{-2})/(t^6 + 1) = (t^2 + 1)/t^4$, Proposition 6 implies

$$g = \begin{cases} \dfrac{D^4}{2^{m-1}}(t^{3m+4} + (-1)^m t^{-(3m+4)}) & \text{if} \quad \delta = 1, \\ \dfrac{D^4}{2^{m-1}}(t^{3m+2} + (-1)^m t^{-(3m+2)}) & \text{if} \quad \delta = -1. \end{cases}$$

Proposition 1 implies easily the assertion in the lemma. □

Since $h(x), h(x, m, D^2)$ are monic without constant term, Lemma 6 implies $\kappa_1 = 1$, $\kappa_2 = 0$, i.e.

$$h(x) = h(x, M, D^2) \quad \text{for} \quad M = 3m + 3 + \delta.$$

Hence, in case of m being odd, Proposition 1 implies

$$\begin{aligned} f(x) &= (D^M(t^M - t^{-M}))^3 + b_2(D^M(t^M - t^{-M}))^2 + b_1(D^M(t^M - t^{-M})) \\ &= D^{3M}(t^{3M} - t^{-3M}) + b_2D^{2M}(t^{2M} + t^{-2M} - 2) \\ &\quad + (-3D^{3M} + b_1D^M)(t^M - t^{-M}), \end{aligned}$$

which is a polynomial in $y = x^3 + 3D^2x = D^3(t^3 - t^{-3})$ $(x = D(t - t^{-1}))$ by the assumption. Therefore we have $b_2 = 0$ and $b_1 = 3D^{2M}$, since $(3, M) = 1$ and y is invariant by $t \to \sqrt[3]{1}t$.

If m is even, then we have

$$\begin{aligned} &f(x) \\ &= (D^M(t^M + t^{-M} - 2))^3 + b_2(D^M(t^M + t^{-M} - 2))^2 + b_1D^M(t^M + t^{-M} - 2) \\ &= D^{3M}(t^{3M} + t^{-3M}) + (-6D^{3M} + b_2D^{2M})(t^{2M} + t^{-2M}) \\ &\quad + (-4b_2D^{2M} + 15D^{3M} + b_1D^M)(t^M + t^{-M}) + 6b_2D^{2M} - 20D^{3M} - 2b_1D^M \end{aligned}$$

which is a polynomial in $t^3 - t^{-3}$ by the assumption. Similarly we have $b_2 = 6D^M$ and $b_1 = 9D^{2M}$. Thus we have completed a proof of Theorem 7. □

5. Proof of Theorem 3

Put $X = X(x) = x^j G(x^r)$, and suppose that $f = X^r - d$ is completely decomposable modulo a prime p ($\nmid D$) without multiple roots; then there exists an integer D such that $D^r \equiv d \bmod p$, consequently we have

$$f \equiv X^r - D^r = (X - D)(X^{r-1} + X^{r-2}D + \cdots + D^{r-1}) \mod p.$$

Then, the second leading term of $X - D$ being 0 implies that the sum of roots r_i ($1 \leq i \leq m := \deg X$) of $X(x) - D \equiv 0 \bmod p$ vanishes, that is a linear relation

$$\sum_{i=1}^{m} r_i \equiv 0 \mod p \tag{36}$$

occurs. Let us see that $h(r_i) = r_i^r$ ($1 \leq i \leq m$, $h(x) = x^r$) are different, and roots of $f(x) \equiv 0 \bmod p$ are of the form $r_i \omega_0^k$ for a primitive r-th root ω_0 of unity in $\mathbb{Z}/p\mathbb{Z}$. First, suppose $r_i^r \equiv r_l^r \bmod p$; then $r_i \equiv r_l \omega \bmod p$ for an r-th root ω of unity and we have $D \equiv X(r_i) \equiv (r_l \omega)^j G(r_l^r) \equiv \omega^j X(r_l) \equiv \omega^j D \bmod p$, which implies $\omega \equiv 1 \bmod p$ by the assumption $(j, r) = 1$. Thus we have $r_i \equiv r_l \bmod p$, i.e. $i = l$. Second, let R be a root of $f(x) \equiv 0 \bmod p$; then $X(R)^r \equiv D^r \bmod p$ and so $X(R) \equiv D\omega_1 \bmod p$ for an r-th root ω_1 of unity in $\mathbb{Z}/p\mathbb{Z}$. By $(j, r) = 1$, $D \equiv \omega_1^{-1} X(R) \equiv X(\omega_2 R) \bmod p$ for an r-th root ω_2 of unity. Thus roots of $f(x) \equiv 0 \bmod p$ are of the form $r_i \omega$ for an r-th root ω of unity. Since the number of solutions of $f(x) \equiv 0 \bmod p$ is rm by the assumption, the number of r-th roots of unity in $\mathbb{Z}/p\mathbb{Z}$ is r, and so there is a primitive r-th root ω_0 of unity.

Then a point

$$\begin{aligned}(v_1, \ldots, v_{(r-1)m}) \\ := \left(\left(\frac{r_1\omega_0}{p}, \ldots, \frac{r_1\omega_0^{r-1}}{p}\right), \ldots, \left(\frac{r_m\omega_0}{p}, \ldots, \frac{r_m\omega_0^{r-1}}{p}\right)\right)\end{aligned} \tag{37}$$

in (5) for $g(x) = x^j G(x)^r - d$, $h(x) = x^r$ has a relation

$$\sum_{i=1}^{m} v_{k+(i-1)(r-1)} \in \mathbb{Z} \quad (1 \leq k \leq r-1), \tag{38}$$

which comes from (36). This breaks the uniformity of the distribution of points (5) when $p \to \infty$, since for a subset $\mathfrak{D} \subset [0, 1)^{m(r-1)}$ defined by

$$\left| \sum_{i=1}^{m} v_{k+(i-1)(r-1)} - a \right| < \epsilon \quad (a \in \mathbb{Z}),$$

the volume is arbitrarily small, but the point (37) is in $\mathfrak{D}$ for every prime. □

6. Proof of Theorem 4

Suppose that for a prime $p \nmid D$, $f(x) \bmod p$ is completely decomposable without multiple roots. Since $h(x, m, D)$ is a polynomial in x, D with integer coefficients, (16) holds over $F_p = \mathbb{Z}/p\mathbb{Z}$. We consider all over the algebraic closure $\overline{F_p}$ of the prime field F_p. Put $D_1 = \sqrt{D} \in \overline{F_p}$, and for $x \in \overline{F_p}$, we take an element $t \in \overline{F_p}$ so that $x = D_1(t - t^{-1})$, i.e. $t^2 - D_1^{-1}xt - 1 = 0$. Then by (16), $f(x) = h(h(x, m, D), n, D^m) + c = D_1^{mn}(t^{mn} - t^{-mn}) + c = 0$ is equivalent to $(t^{mn})^2 + cD_1^{-mn}t^{mn} - 1 = 0$. Taking a root $T_+ \in \overline{F_p}$ of $x^2 + cD_1^{-mn}x - 1 = 0$, we have $t = \sqrt[mn]{T_+}\zeta$ or $t = -\sqrt[mn]{T_+}^{-1}\zeta$ for an mn-th root of unity ζ in $\overline{F_p}$. Therefore, putting $T = \sqrt[mn]{T_+}$, the root of $f(x) = 0$ is written as $D_1(T\zeta - T^{-1}\zeta^{-1})$ for an mn-th root ζ of unity in $\overline{F_p}$. Since $f(x)$ has mn different roots over F_p by the assumption, the field $\overline{F_p}$ has mn roots for an equation $x^{mn} = 1$,

Let η be a primitive mn-th root of unity in $\overline{F_p}$, and put

$$x_k = D_1(T\eta^k - T^{-1}\eta^{-k}).$$

Then the roots of $f(x) = 0$ are $x_1, x_2, \dots, x_{mn}$. We have, for $1 \le k \le n$ and $0 \le r \le m-1$

$$\begin{aligned} h(x_{k+nr}, m, D) &= D_1^m((T\eta^{k+nr})^m - (T^{-1}\eta^{-k-nr})^m) \quad \text{(by (16))} \\ &= D_1^m((T\eta^k)^m - (T^{-1}\eta^{-k})^m) \\ &= h(x_k, m, D). \end{aligned}$$

Since, noting $f(x) = h(h(x, m, D), n, D^m) + c$, the equation $h(x, n, D^m) + c = 0$ has n distinct roots, $h(x_k, m, D)$ $(1 \le k \le n)$ are distinct, that is $h(x_k, m, D) \ne h(x_l, m, D)$ if $k \not\equiv l \bmod n$. Based on these, let us show the non-uniformity. Put $d = (m, n)$ and $N = n/d$; then we are assuming $N > 1$ and $dm \nmid n$. Put

$$S = \{x_l \mid l \equiv 0 \bmod dm\}.$$

Then we have $\#S = N > 1$ and

$$\sum_{x \in S} x = D_1 T \sum_{k \bmod N} \eta^{dmk} - D_1 T^{-1} \sum_{k \bmod N} \eta^{-dmk} = 0 \quad \text{in} \quad \overline{F_p}.$$

Since we suppose that $f(x) \bmod p$ is completely decomposable, all roots x_k of $f(x) \equiv 0 \bmod p$ are in F_p, that is we may consider $x_k \in \mathbb{Z}$ with $0 \le x_k < p$, and then the above means

$$\sum_{x \in S} \frac{x}{p} \in \mathbb{Z}. \tag{39}$$

Let us see

$$S \not\supset \{x \mid h(x, m, D) = h(x_k, m, D)\} \quad \text{for} \quad 1 \le \forall k \le mn. \tag{40}$$

If $S \supset \{x \mid h(x, m, D) = h(x_k, m, D)\}$ for some integer k, then we have

$$\{k + nr \mid r \in \mathbb{Z}\} \subset \{dml \mid l \in \mathbb{Z}\},$$

hence, $k = dml_0$ for an integer l_0, and so $n \equiv 0 \bmod dm$, which contradicts $dm \nmid n$.

By (40), we can arrange x/p for elements x in S into $\boldsymbol{r}_k(id, id)$ in (5), changing numbering, and then (39) means that an appropriate sum of coordinates in (5) is an integer. Thus points (5) are not distributed uniformly. $\square$

7. Proof of Theorem 5

We keep notations in Theorem 5. Since we assume that $f = x^3(x^3+c)^3 - d \bmod p$ is completely decomposable, the existence of ω in the theorem is clear. Let D be an integer such that $D^3 \equiv d \bmod p$. Since r_i are roots of $x(x^3 + c) - D \equiv 0 \bmod p$, we have

$$\prod_{i=1}^{4}(x - r_i) = x^4 + cx - D. \tag{41}$$

Put

$$(x - r_1)(x - r_2) = x^2 + a_1 x + a_2, \tag{42}$$

$$(x - r_3)(x - r_4) = x^2 + b_1 x + b_2. \tag{43}$$

Hence equations (41)–(43) imply

$$b_1 = -a_1, \quad b_2 = a_1^2 - a_2, \quad c = a_1^3 - 2a_1 a_2$$

and so

$$r_1 + r_2 = -a_1, \quad r_1 r_2 = a_2, \quad r_3 + r_4 = a_1, \quad r_3 r_4 = a_1^2 - a_2, \quad D = a_2^2 - a_1^2 a_2.$$

These imply

$$\begin{aligned}
S_1 &= r_1 + r_2 + \omega(r_3 + r_4) \\
&= a_1(\omega - 1), \\
S_2 &= r_1 r_2 + (r_1 + r_2)(r_3 + r_4)\omega + r_3 r_4 \omega^2 \\
&= -a_1^2(2\omega + 1) + a_2(\omega + 2), \\
S_3 &= (r_1 + r_2) r_3 r_4 \omega^2 + r_1 r_2 (r_3 + r_4)\omega \\
&= a_1^3(\omega + 1) - a_1 a_2, \\
S_4 &= r_1 r_2 r_3 r_4 \omega^2 = D(\omega + 1)
\end{aligned}$$

and easily relations (11), noting $(\omega-1)^3=6\omega+3$. $\square$

References

[1] Y. Kitaoka: *A statistical relation of roots of a polynomial in different local fields*, Math. Comp. **78** (2009), 523–536.

[2] Y. Kitaoka: *A statistical relation of roots of a polynomial in different local fields* II; in Number Theory, Ser. Number Theory Appl. **6** World Sci. Publ., Hackensack, NJ., 106–126, 2010.

Department of Mathematics
Meijo University
Tenpaku, Nagoya, 468-8502
Japan
e-mail: kitaoka@ccmfs.meijo-u.ac.jp