Paper

Regular sequences of power sums in the polynomial ring in three variables

Satoru Isogawa[1,*], Tadahito Harima[2]

In this article, we provide a partial result concerning the conjecture given by Conca, Krattenthaler and Watanabe in (1) on regular seqence of symmetric polynomials.

Keywords : Regular sequences, Power sums, Resultant of polynomials.

1. Intorduction

In (1), Conca, Krattenthaler and Watanabe stated the following conjecture:

Conjecture 1.1. *Any sequence of three power sums* $p_a := X^a + Y^a + Z^a$, $p_b := X^b + Y^b + Z^b$ *and* $p_c := X^c + Y^c + Z^c$, *where* a, b *and* c *are distinct positive integers with* $abc \equiv 0 \pmod 6$ *and* $\gcd(a,b,c) = 1$, *forms a regular sequence in the polynomial ring* $K[X,Y,Z]$ *in three variables* X, Y *and* Z *over a field* K *of characteristic zero.*

This conjecture has been studied by several authors (e.g., (2)-(5)) and is still an open problem. The purpose of this paper is to prove the following result which gives an affirmative answer to Conjecture 1.1 under some conditions.

Theorem 1.2. *If* $c = 1$ *and* $a = 2^n, 3^n, 5^n, 7^n, 10$ $(n = 1, 2, \cdots)$, *then Conjecture 1.1 is true.*

2. Proof of Theorem 1.2

Let a,b integers with $2 \le a,b$ and $a \ne b$. Since the sequence of three power sums p_a, p_b and $p_1 = X + Y + Z$ is a regular sequence in $K[X,Y,Z]$ if and only if the sequence of two polynomials $(X+Y)^a + (-1)^a (X^a + Y^a)$ and $(X+Y)^b + (-1)^b (X^b + Y^b)$ is a regular sequence in $K[X,Y]$ if and only if $\gcd(F,G) = 1$ in $K[X]$, where $F := (x+1)^a + (-1)^a (x^a + 1)$ and $G := (x+1)^b + (-1)^b (x^b + 1)$ are polynomials in $\mathbb{Z}[x] (\subseteq K[x])$. Therefore, if $c = 1$, we can reduce Conjecture 1.1 to the following statement:

Conjecture 2.1. *If* $ab \equiv 0 \pmod 6$, *then* $\gcd(F,G) = 1$.

Hence we have only to prove the following proposition:

Prop. 2.2. *If* $a = 2^n, 3^n, 5^n, 7^n, 10 (n = 1, 2, \cdots)$, *then Conjecture* 2.1 *is true.*

1 Faculty of Liberal Studies
2627 Hirayamashinmachi Yatsushiro-shi Kumamoto, Japan 866-8501
2 Department of Mathematics Education, Niigata University
8050 Ikarashi-2no-chou Nishi-ku Niigata-shi Niigata, Japan 950-2181
* Corresponding author:
E-mail address: isogawa@kumamoto-nct.ac.jp (S. Isogawa)

Before going into the proof of this proposition, we need some preparations. We denote the resultant of two polynomials f and g by $\mathrm{res}(f,g)$. If $f \in \mathbb{Z}[x]$, then we denote $\overline{f} \in \mathbb{Z}/p\mathbb{Z}[x]$ the image of f in $\mathbb{Z}/p\mathbb{Z}[x]$, where p is a prime number, and let $\mathrm{LC}(f) \in \mathbb{Z}$ be the leading coefficient of f.

Lemma. 2.3. *Let* $f, g \in \mathbb{Z}[x]$ *with* $\deg f, \deg g \geq 1$. *If* $\deg f = \deg \overline{f}$ *(i.e.* $\overline{\mathrm{LC}(f)} \neq 0 \bmod p$*) and* $\deg \overline{g} \geq 1$*, then*

$$\mathrm{res}(f,g) \equiv \mathrm{LC}(f)^{\delta}\, \mathrm{res}(\overline{f},\overline{g}) \bmod p, \text{ where } \delta = \deg g - \deg \overline{g}.$$

Proof Let denote $f = a_n x^n + \cdots + a_0$ and $g = b_m x^m + \cdots + b_0$, where $\deg f = n$, $\deg g = m$. By the definition of the resultant,

$$\overline{\mathrm{res}(f,g)} = \begin{vmatrix} \overline{a_n} & \cdots & & & \\ & \overline{a_n} & \cdots & & \\ & & \vdots & & \\ \overline{b_m} = 0 & \cdots & & & \\ & \overline{b_m} = 0 & \cdots & & \\ & & \vdots & & \end{vmatrix} = \left(\overline{a_n}\right)^{\delta} \mathrm{res}(\overline{f},\overline{g}).$$

This implies $\mathrm{res}(f,g) \equiv \mathrm{LC}(f)^{\delta}\, \mathrm{res}(\overline{f},\overline{g}) \bmod p$. □

From Lemma 2.3, we have the following corollary.

Corollary 2.4. *Let* $f, g \in \mathbb{Z}[x]$. *If* $\deg f = \deg \overline{f} \geq 1$, $\deg \overline{g} \geq 1$ *and* $\mathrm{res}(\overline{f},\overline{g}) \neq 0$, *then* $\mathrm{res}(f,g) \neq 0$.

On the other hand, for two polynomials $f, g \in K[x]$, it is well known that $\mathrm{res}(f,g) \neq 0$ if and only if f and g have no common zeros in $\overline{K}$ the algebraic closure of K if and only if $K[x]f + K[x]g = K[x]$ (i.e. $\gcd(f,g) = 1$) by the Hilbert's Nullstellensatz. Hence we also have the following corollary as a variant of Corollary 2.4.

Corollary 2.5. *Let* $f, g \in \mathbb{Z}[x] \subseteq K[x]$. *If* $\deg f = \deg \overline{f} \geq 1$, $\deg \overline{g} \geq 1$ *and* $\gcd(\overline{f},\overline{g}) = 1$ *in* $(\mathbb{Z}/p\mathbb{Z})[x]$, *then* $\gcd(f,g) = 1$ *in* $K[x]$.

We denote $\binom{n}{r} := \dfrac{n!}{r!(n-r)!}$ the binomial coefficient with $n \geq r \geq 0$. Let p be a prime number, we denote $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ the p-adic valuation. We use the following properties of the p-adic valuation:

(0) $v_p(0) = \infty$ (This is a part of the definition of v_p).

(1) $v_p(ab) = v_p(a)v_p(b)$ and $v_p(a/b) = v_p(a) - v_p(b)$.

(2) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$ and $v_p(a+b) = \min\{v_p(a), v_p(b)\}$ if $v_p(a) \neq v_p(b)$.

The following lemma is our key result.

Lemma 2.6. *Let* n, r *integers with* $n \geq 1$ *and* $p^n > r > 0$. *Then the following hold:*

(1) $v_p\binom{p^n}{r} = v_p(p^n) - v_p(r) (= n - v_p(r))$.

(2) $v_p\binom{p^n}{r} \geq 1$.

(3) $v_p\binom{p^n}{r} = 1$ *if and only if* $r = ip^{n-1}$ *with* $i = 1, \cdots, p-1$.

(4) $\overline{\frac{1}{p}\binom{p^n}{ip^{n-1}}} = \frac{\left(-\overline{1}\right)^{i-1}}{\overline{i}}$ *for* $i = 1, \cdots, p-1$ *in* $\mathbb{Z}/p\mathbb{Z} \subseteq (\mathbb{Z}/p\mathbb{Z})[x]$.

(5) *If* $a = p^n$, *then* $\overline{\frac{1}{p}\left((x+1)^a - (x^a+1)\right)} = \left(\sum_{i=1}^{p-1} \frac{\left(-\overline{1}\right)^{i-1}}{\overline{i}} x^i\right)^{p^{n-1}}$ *in* $(\mathbb{Z}/p\mathbb{Z})[x]$.

Proof (1) First we remark that $v_p(p^n - i) = \min\{v_p(p^n), v_p(-i)\} = v_p(i)$ for integers $p^n > i > 0$.
Hence we have

$$v_p\binom{p^n}{r} = v_p\left(\frac{p^n \cdot (p^n - 1) \cdots (p^n - r + 1)}{r \cdots 1}\right)$$

$$= v_p(p^n) + v_p(p^n - 1) + \cdots + v_p(p^n - (r-1)) - \{v_p(1) + \cdots + v_p(r-1) + v_p(r)\} = v_p(p^n) - v_p(r).$$

(2) Since $p^n > r > 0$, we have $v_p(r) < n$. By (1), $v_p\binom{p^n}{r} = n - v_p(r) \geq 1$.

(3) Since $v_p\binom{p^n}{r} = n - v_p(r) = 1$, we have $v_p(r) = n - 1$ if and only if $r = ip^{n-1}$ with $i = 1, \cdots, p-1$.

(4) If we denote $j = c_j p^{v_p(j)}$ for $1 \leq j \leq p^{n-1} - 1$ and $i = 1, \cdots, p-1$, then we have

$$\frac{p^n - j}{j} = \frac{p^{n - v_p(j)} - c_j}{c_j} \quad \text{and} \quad \overline{p^{n - v_p(j)} - c_j} = -\overline{c_j} \neq 0.$$

Here we remark that for any integers a, b, if $\frac{a}{b}$ is an integer and $\overline{b} \neq 0$, then $\overline{\left(\frac{a}{b}\right)} = \frac{\overline{a}}{\overline{b}}$ in $\mathbb{Z}/p\mathbb{Z} \subseteq (\mathbb{Z}/p\mathbb{Z})[x]$.

So, we have

$$\overline{\frac{1}{p}\binom{p^n}{ip^{n-1}}} = \overline{\frac{1}{i}\prod_{j=1}^{ip^{n-1}-1} \frac{(p^n - j)}{j}} = \overline{\frac{1}{i}\prod_{j=1}^{ip^{n-1}-1} \frac{\left(p^{n-v_p(j)} - c_j\right)}{c_j}} = \frac{1}{\overline{i}}\prod_{j=1}^{ip^{n-1}-1} \frac{-\overline{c_j}}{\overline{c_j}} = \frac{\left(-\overline{1}\right)^{(ip^{n-1}-1)}}{\overline{i}} = \frac{\left(-\overline{1}\right)^{(i-1)}}{\overline{i}}.$$

(5) By (2) and (3), we have

$$\overline{\frac{1}{p}\left((x+1)^a - (x^a+1)\right)} = \sum_{i=1}^{p-1} \overline{\frac{1}{p}\binom{p^n}{ip^{n-1}}} \left(x^i\right)^{p^{n-1}} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[x].$$

Hence, using (4), we have

$$\overline{\frac{1}{p}\left((x+1)^a - (x^a+1)\right)} = \sum_{i=1}^{p-1} \frac{\left(-\overline{1}\right)^{(i-1)}}{\overline{i}} \left(x^i\right)^{p^{n-1}} = \left(\sum_{i=1}^{p-1} \frac{\left(-\overline{1}\right)^{(i-1)}}{\overline{i}} x^i\right)^{p^{n-1}} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[x]. \quad \square$$

Here we start proof of Theorem 1.2 by dividing into five cases. We prove them each after the supportive lemma.

Lemma 2.7. *The following hold:*

(1) *If* $a=2^n$ *with an integer* $n\ge 1$, *then* $\overline{\frac{1}{2}F}=\left(x^2+x+\overline{1}\right)^{\frac{a}{2}}$ *in* $(\mathbb{Z}/2\mathbb{Z})[x]$. *Especially,* $\deg\left(\frac{1}{2}F\right)=\deg\left(\overline{\frac{1}{2}F}\right)=a$.

(2) *If* $b=3m$ *with an integer* $m\ge 1$, *then* $G\equiv 3m'x^{2^{\nu}(3m'-1)}+\cdots \bmod 2$ *where* $m=2^{\nu}m'$ *with* m' *odd*

and $G\equiv 1 \bmod\left(2,\, x^2+x+1\right)$. *Especially,* $\deg\overline{G}\ge 1$ and $\gcd\left(\overline{\frac{1}{2}F},\overline{G}\right)=1$ *in* $(\mathbb{Z}/2\mathbb{Z})[x]$.

Proof (1) Since $\overline{\frac{1}{2}\left((x+1)^a-\left(x^a+1\right)\right)}=\overline{\frac{1}{2}\left((x+1)^{2^n}-\left(x^{2^n}+1\right)\right)}=x^{2^{n-1}}=x^{\frac{a}{2}}$ in $(\mathbb{Z}/2\mathbb{Z})[x]$ by Lemma 2.6 (5), we have

$$\overline{\frac{1}{2}F}=\overline{\frac{1}{2}\left((x+1)^a+\left(x^a+1\right)\right)}=\overline{\left\{\frac{(x+1)^a-\left(x^a+1\right)}{2}+\left(x^a+1\right)\right\}}=x^a+x^{\frac{a}{2}}+\overline{1}=\left(x^2+x+\overline{1}\right)^{\frac{a}{2}}\quad\text{in }(\mathbb{Z}/2\mathbb{Z})[x].$$

(2) $G=(x+1)^{3\cdot 2^{\nu}m'}+(-1)^{3\cdot 2^{\nu}m'}\left(x^{3\cdot 2^{\nu}m'}+1\right)\equiv\left(x^{2^{\nu}}+1\right)^{3m'}-\left(x^{3\cdot 2^{\nu}m'}+1\right)\equiv 3m'\left(x^{2^{\nu}}\right)^{3m'-1}+\cdots=3m'x^{2^{\nu}(3m'-1)}+\cdots \bmod 2$.

Since $x^2\equiv x+1 \bmod\left(2,\, x^2+x+1\right)$ and $x^3\equiv 1 \bmod\left(2,\, x^2+x+1\right)$, we have

$$\begin{aligned}G=(x+1)^{3m}+(-1)^{3m}\left(x^{3m}+1\right)&\equiv\left(x^2\right)^{3m}+\left(x^{3m}+1\right) \bmod\left(2,\, x^2+x+1\right)\\&\equiv 1^{2m}+\left(1^m+1\right)\equiv 1 \bmod\left(2,\, x^2+x+1\right).\quad\square\end{aligned}$$

Proof of Prop. 2.2 for $a=2^n$:

Since $ab\equiv 0\ (\bmod 6)$, we can assume that $b=3m$ with an integer $m\ge 1$. From Lemma 2.7, $\deg\left(\frac{1}{2}F\right)=\deg\left(\overline{\frac{1}{2}F}\right)$, $\deg\overline{G}\ge 1$ and $\gcd\left(\overline{\frac{1}{2}F},\overline{G}\right)=1$ in $(\mathbb{Z}/2\mathbb{Z})[x]$, this implies $\gcd(F,G)=\gcd\left(\frac{1}{2}F,G\right)=1$ by Corollary 2.5. $\square$

Lemma 2.8. *The following hold:*

(1) *If* $a=3^n$ *with* $n=1,2,\cdots$, *then* $\overline{\frac{1}{3}F}=x^{\frac{a}{3}}\left(x+\overline{1}\right)^{\frac{a}{3}}$ *in* $(\mathbb{Z}/3\mathbb{Z})[x]$.

(2) *If* $b=2m$ *with an integer* $m\ge 1$, *then we have*

$$\begin{aligned}&\mathrm{LC}(G)\equiv 2 \bmod 3,\\&G=(x+1)^b+\left(x^b+1\right)\equiv 2 \bmod(3,\, x)\ \text{ and}\\&G=(x+1)^b+\left(x^b+1\right)\equiv 2 \bmod(3,\, x+1).\end{aligned}$$

Especially, $\deg(G)=\deg\left(\overline{G}\right)=b$ *and* $\gcd\left(\overline{\frac{1}{3}F},\overline{G}\right)=1$ *in* $(\mathbb{Z}/3\mathbb{Z})[x]$.

Proof (1) Since $\frac{\overline{-1}}{2}=\overline{1}$ in $\mathbb{Z}/3\mathbb{Z}\subseteq(\mathbb{Z}/3\mathbb{Z})[x]$, by Lemma 2.6 (5), we have

$$\overline{\frac{1}{3}F}=\overline{\frac{1}{3}\left((x+1)^a-\left(x^a+1\right)\right)}=\left(\sum_{i=1}^{2}\frac{\left(\overline{-1}\right)^{(i-1)}}{\overline{i}}x^i\right)^{3^{n-1}}=\left(\frac{\overline{1}}{\overline{1}}x+\frac{\overline{-1}}{\overline{2}}x^2\right)^{\frac{a}{3}}=x^{\frac{a}{3}}\left(x+\overline{1}\right)^{\frac{a}{3}}\quad\text{in }(\mathbb{Z}/3\mathbb{Z})[x].$$

(2) Obviously $\mathrm{LC}(G)\equiv 2 \bmod 3$. Since $x+1\equiv x^b+1\equiv 1 \bmod(3,\, x)$ and $x^b+1\equiv(-1)^{2m}+1\equiv 2 \bmod(3,\, x+1)$, we have

$$G=(x+1)^b+\left(x^b+1\right)\equiv 2 \bmod(3,\, x)\ \text{ and }\ G=(x+1)^b+\left(x^b+1\right)\equiv 2 \bmod(3,\, x+1).\quad\square$$

Proof of Prop. 2.2 for $a = 3^n$:

Since $ab \equiv 0 \pmod 6$, we can assume that $b = 2m$ with an integer $m \geq 1$. From Lemma 2.8, $\deg(G) = \deg(\overline{G})$, $\deg\left(\overline{\frac{1}{3}F}\right) \geq 1$ and $\gcd\left(\overline{\frac{1}{3}F}, \overline{G}\right) = 1$ in $(\mathbb{Z}/3\mathbb{Z})[x]$, this implies $\gcd(F, G) = \gcd\left(\frac{1}{3}F, G\right) = 1$ by Corollary 2.5. □

Lemma 2.9. *The following hold:*

(1) *If* $a = 5^n$ *with* $n = 1, 2, \cdots$, *then* $\overline{\frac{1}{5}F} = x^{\frac{a}{5}}\left(x^2 + x + \overline{1}\right)^{\frac{a}{5}}\left(x + \overline{1}\right)^{\frac{a}{5}}$ *in* $(\mathbb{Z}/5\mathbb{Z})[x]$.

(2) *If* $b = 6m$ *with an integer* $m \geq 1$, *then we have*

$$\mathrm{LC}(G) \equiv 2 \bmod 5,$$

$$G = (x+1)^b + \left(x^b + 1\right) \equiv 2 \bmod (5, x),$$

$$G = (x+1)^b + \left(x^b + 1\right) \equiv 2 \bmod (5, x+1) \quad \text{and}$$

$$G = (x+1)^b + \left(x^b + 1\right) \equiv 3 \bmod \left(5, x^2 + x + 1\right).$$

Especially, $\deg(G) = \deg(\overline{G}) = b$ *and* $\gcd\left(\overline{\frac{1}{5}F}, \overline{G}\right) = 1$ *in* $(\mathbb{Z}/5\mathbb{Z})[x]$.

Proof (1) Since $\frac{\overline{-1}}{\overline{2}} = \overline{2}, \frac{\overline{1}}{\overline{3}} = \overline{2}$ and $\frac{\overline{-1}}{\overline{4}} = \overline{1}$ in $\mathbb{Z}/5\mathbb{Z} \subseteq (\mathbb{Z}/5\mathbb{Z})[x]$, by Lemma 2.6 (5), we have

$$\overline{\frac{1}{5}F} = \left(\frac{\overline{1}}{\overline{1}}x + \frac{\overline{-1}}{\overline{2}}x^2 + \frac{\overline{1}}{\overline{3}}x^3 + \frac{\overline{-1}}{\overline{4}}x^4\right)^{5^{n-1}} = \left(x + 2x^2 + 2x^3 + x^4\right)^{\frac{a}{5}} = x^{\frac{a}{5}}\left(x^2 + x + \overline{1}\right)^{\frac{a}{5}}\left(x + \overline{1}\right)^{\frac{a}{5}} \quad \text{in} \quad (\mathbb{Z}/5\mathbb{Z})[x].$$

(2) Obviously $\mathrm{LC}(G) \equiv 2 \bmod 5$. Since $x + 1 \equiv x^b + 1 \equiv 1 \bmod (5, x)$ and $x^b + 1 \equiv (-1)^{6m} + 1 \equiv 2 \bmod (5, x+1)$, we have

$$G = (x+1)^b + \left(x^b + 1\right) \equiv 2 \bmod (5, x) \quad \text{and} \quad G = (x+1)^b + \left(x^b + 1\right) \equiv 2 \bmod (5, x+1).$$

Moreover, since $x^3 = 1 \bmod \left(5, x^2 + x + 1\right)$ and $x + 1 = -x^2 \bmod \left(5, x^2 + x + 1\right)$, we have

$$G = (x+1)^b + \left(x^b + 1\right) \equiv \left(-x^2\right)^{6m} + \left(x^{6m} + 1\right) \equiv 3 \bmod \left(5, x^2 + x + 1\right). \quad \square$$

Proof of Prop. 2.2 for $a = 5^n$:

Since $ab \equiv 0 \pmod 6$, we can assume that $b = 6m$ with an integer $m \geq 1$. From Lemma 2.9, $\deg(G) = \deg(\overline{G})$, $\deg\left(\overline{\frac{1}{5}F}\right) \geq 1$ and $\gcd\left(\overline{\frac{1}{5}F}, \overline{G}\right) = 1$ in $(\mathbb{Z}/5\mathbb{Z})[x]$, this implies $\gcd(F, G) = \gcd\left(\frac{1}{5}F, G\right) = 1$ by Corollary 2.5. □

Lemma 2.10. *The following hold:*

(1) *If* $a = 7^n$ *with* $n = 1, 2, \cdots$, *then* $\overline{\frac{1}{7}F} = x^{\frac{a}{7}}\left(x + \overline{1}\right)^{\frac{a}{7}}\left(x + \overline{3}\right)^{\frac{2a}{7}}\left(x + \overline{5}\right)^{\frac{2a}{7}}$ *in* $(\mathbb{Z}/7\mathbb{Z})[x]$.

(2) *If* $b = 6m$ *with an integer* $m \geq 1$, *then we have*

$$\mathrm{LC}(G) \equiv 2 \bmod 7,$$

$$G = (x+1)^b + \left(x^b + 1\right) \equiv 2 \bmod (7, x),$$

$$G=(x+1)^b+(x^b+1)\equiv 2 \bmod (7,\, x+1),$$

$$G=(x+1)^b+(x^b+1)\equiv 3 \bmod (7,\, x+3) \quad \text{and} \quad G=(x+1)^b+(x^b+1)\equiv 3 \bmod (7,\, x+5).$$

Especially, $\deg(G)=\deg(\overline{G})=b$ *and* $\gcd\left(\overline{\frac{1}{7}F},\overline{G}\right)=1$ *in* $(\mathbb{Z}/7\mathbb{Z})[x]$.

Proof (1) Since $\frac{\overline{-1}}{\overline{2}}=\overline{3},\ \frac{\overline{1}}{\overline{3}}=\overline{5},\ \frac{\overline{-1}}{\overline{4}}=\overline{5},\ \frac{\overline{1}}{\overline{5}}=\overline{3},\ \frac{\overline{-1}}{\overline{6}}=\overline{1}$ and

$$x(x+\overline{1})(x+\overline{3})^2(x+\overline{5})^2\equiv x+\overline{3}x^2+\overline{5}x^3+\overline{5}x^4+\overline{3}x^4+x^5 \quad \text{in} \quad \mathbb{Z}/7\mathbb{Z}\subseteq(\mathbb{Z}/7\mathbb{Z})[x],$$

by Lemma 2.6 (5), we have

$$\overline{\left(\frac{1}{7}F\right)}=\left(x+\overline{3}x^2+\overline{5}x^3+\overline{5}x^4+\overline{3}x^4+x^5\right)^{7^{n-1}}=x^{\frac{a}{7}}(x+\overline{1})^{\frac{a}{7}}(x+\overline{3})^{\frac{2a}{7}}(x+\overline{5})^{\frac{2a}{7}}.$$

(2) Obviously $\mathrm{LC}(G)\equiv 2 \bmod 7$ and $G=(x+1)^b+(x^b+1)\equiv 2 \bmod (7,\, x)$. Since $x^b+1\equiv(-1)^{6m}+1\equiv 2 \bmod (7,\, x+1)$, $(x+1)^b\equiv(5^6)^m\equiv 1 \bmod (7,\, x+3)$, $x^b\equiv(4^3)^{2m}\equiv 1 \bmod (7,\, x+3)$, $(x+1)^b\equiv(3^6)^m\equiv 1 \bmod (7,\, x+5)$ and $x^b\equiv(2^3)^{2m}\equiv 1 \bmod (7,\, x+5)$, we have $G=(x+1)^b+(x^b+1)\equiv 2 \bmod (7,\, x+1)$, $G=(x+1)^b+(x^b+1)\equiv 3 \bmod (7,\, x+3)$ and $G=(x+1)^b+(x^b+1)\equiv 3 \bmod (7,\, x+5)$. □

Proof of Prop. 2.2 for $a=7^n$:

Since $ab\equiv 0 \pmod 6$, we can assume that $b=6m$ with an integer $m\geq 1$. From Lemma 2.9, $\deg(G)=\deg(\overline{G})$, $\deg\left(\overline{\frac{1}{7}F}\right)\geq 1$ and $\gcd\left(\overline{\frac{1}{7}F},\overline{G}\right)=1$ in $(\mathbb{Z}/7\mathbb{Z})[x]$, this implies $\gcd(F,G)=\gcd\left(\frac{F}{7},G\right)=1$ by Corollary 2.5. □

Lemma 2.11. *The following hold:*

(1) *If* $a=10$, *then* $\overline{F}=\overline{2}(x^2+x+\overline{1})^5$ *in* $(\mathbb{Z}/5\mathbb{Z})[x]$. *Especially,* $\deg(F)=\deg(\overline{F})=10$.

(2) *If* b *is even, then* $G\equiv 2x^b+\cdots \bmod 5$ *and if* b *is odd, then* $G\equiv b'x^{5^v(b'-1)}+\cdots \bmod 5$ *where* $b=5^v b'$ *with* $\overline{b'}\neq 0$ *in* $\mathbb{Z}/5\mathbb{Z}$.

(3) *If* $b=3m$ *with an integer* $m\geq 1$, *then* $G\equiv 3\cdot(-1)^b \bmod (5,\, x^2+x+1)$. *Especially,* $\gcd(\overline{F},\overline{G})=1$ *in* $(\mathbb{Z}/5\mathbb{Z})[x]$.

Proof (1) $F=(x+1)^{10}+(x^{10}+1)\equiv(x^5+1)^2+(x^{10}+1)\equiv 2(x^{10}+x^5+1)\equiv 2(x^2+x+1)^5 \bmod 5$.

(2) If b is odd, then $G=(x+1)^{5^v b'}-(x^{5^v b'}+1)\equiv(x^{5^v}+1)^{b'}-(x^{5^v b'}+1)\equiv b'(x^{5^v})^{b'-1}+\cdots=b'x^{5^v(b'-1)}+\cdots \bmod 5$. If b is even, then the assertion is clear.

(3) Since $x^3\equiv 1$ and $x+1\equiv -x^2 \bmod (5,\, x^2+x+1)$, we have

$$G=(x+1)^b+(-1)^b(x^b+1)\equiv(-x^2)^{3m}+(-1)^{3m}(x^{3m}+1)\equiv(-1)^{3m}(x^{6m}+x^{3m}+1)=3\cdot(-1)^b \bmod (5,\, x^2+x+1). \quad \square$$

Proof of Prop. 2.2 for $a=10$:

Since $a=10$, we can assume that $b=3m$ with an integer $m\geq 1$. From Lemma 2.9, $\deg(F)=\deg(\overline{F})$, $\deg(\overline{G})\geq 1$ and $\gcd(\overline{F},\overline{G})=1$ in $(\mathbb{Z}/5\mathbb{Z})[x]$, this implies $\gcd(F,G)=1$ by Corollary 2.5. □

Acknowledgement. This work was supported by Grant-in-Aid for Scientific Research (C) (15K04812).

(Received: Sep. 25, 2018)
(Accepted: Dec. 5, 2018)

References

(1) Aldo Conca, Christian Krattenthaler, and Junzo Watanabe: “Regular sequences of symmetric polynomials”, *Rend. Semin. Mat. Univ. Padova*, Vol.121, pp.179-199 (2009).
(2) Ri-Xiang Chen: “On two classes of regular sequences ”, *J. Commut. Algebra*, Vol.8, No.1, pp.29-42 (2016).
(3) Federico Galetto, Anthony V. Geramita, and David L. Wehlau: “Degrees of regular sequences with a symmetric group action”, *arXiv:1610.06610 [math.AC]*, pp.1-14 (2016).
(4) Neeraj Kumar and Ivan Martino: “Regular sequences of power sums and complete symmetric polynomials”, *Matematiche (Catania)* , Vol.67, No.1, pp. 103-117 (2012).
(5) Heather Topping: “The zero locus of symmetric polynomials”, *Master Thesis (Queen’s University)* , pp.1-73 (2017).