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

Satoru Isogawa\textsuperscript{1,*}, Tadahito Harima\textsuperscript{2}

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

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

1. Introduction

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

**Conjecture 1.1.** Any sequence of three power sums $p_\alpha := X^\alpha + Y^\alpha + Z^\alpha$, $p_\beta := X^\beta + Y^\beta + Z^\beta$ and $p_\gamma := X^\gamma + Y^\gamma + Z^\gamma$, where $\alpha, \beta$ and $\gamma$ are distinct positive integers with $\alpha \beta \gamma \equiv 0 \pmod{6}$ and $\gcd(\alpha, \beta, \gamma) = 1$, 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 $a = 2^n, 3^n, 5^n, 7^n, 10^n \ (n = 1, 2, \cdots)$, then Conjecture 1.1 is true.

2. Proof of Theorem 1.2

Let $a, b$ integers with $2 \leq a, b$ and $a \neq b$. Since the sequence of three power sums $p_\alpha, p_\beta$ and $p_\gamma = X + Y + Z$ is a regular sequence in $K[X,Y,Z]$ if and only if the sequence of two polynomials $(X + Y)^\alpha + (X + Y)^\beta$ and $(X + Y)^\gamma$ is a regular sequence in $K[X,Y]$ if and only if $\gcd(F,G) = 1$ in $K[X]$, where $F := (x + 1)^\alpha + (x + 1)^\beta$ and $G := (x + 1)^\gamma$ 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 $a b \equiv 0 \pmod{6}$, then $\gcd(F,G) = 1$.

Hence we have only to prove the following proposition:

**Prop. 2.2.** If $a = 2^n, 3^n, 5^n, 7^n, 10^n (n = 1, 2, \cdots)$, then Conjecture 2.1 is true.
Before going into the proof of this proposition, we need some preparations. We denote the resultant of two polynomials \( f \) and \( g \) by \( \text{res}(f, g) \). 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 \( \text{LC}(f) \in \mathbb{Z} \) 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. \( \text{LC}(f) \not\equiv 0 \pmod{p} \)) and \( \deg g \geq 1 \), then 
\[
\text{res}(f, g) = \text{LC}(f) \delta \text{res}(\overline{f}, \overline{g}) \pmod{p^e},
\]
where \( \delta = \deg g - \deg \overline{g} \).

**Proof.** Let denote 
\[ f = a_n x^n + \cdots + a_0 \quad \text{and} \quad g = b_m x^m + \cdots + b_0, \]
where \( \deg f = n \), \( \deg g = m \). By the definition of the resultant,
\[
\text{res}(f, g) = \begin{vmatrix}
\overline{a_n} & \cdots & \overline{a_0} \\
\overline{b_m} & \cdots & \overline{b_0} \\
\vdots & \cdots & \vdots
\end{vmatrix} = (\overline{a_0})^e \text{res}(\overline{f}, \overline{g}).
\]
This implies \( \text{res}(f, g) = \text{LC}(f)^\delta \text{res}(\overline{f}, \overline{g}) \pmod{p^e} \). \( \square \)

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 \( \text{res}(\overline{f}, \overline{g}) \neq 0 \), then \( \text{res}(f, g) \neq 0 \).

On the other hand, for two polynomials \( f, g \in K[x] \), it is well known that \( \text{res}(f, g) \neq 0 \) if and only if \( f \) and \( g \) have no common zeros in \( K \) if and only if \( K[x]/(f + g) = K[x]/(f \cap g) \) (i.e. \( \text{gcd}(f, g) = 1 \)) 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 \( \text{gcd}(\overline{f}, \overline{g}) = 1 \) in \( (\mathbb{Z}/p\mathbb{Z})[x] \), then 
\( \text{gcd}(f, g) = 1 \) in \( K[x] \).

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

1. \( v_p(0) = \infty \) (This is a part of the definition of \( v_p \)).
2. \( v_p(ab) = v_p(a) + v_p(b) \) and \( v_p(a/b) = v_p(a) - v_p(b) \).
3. \( v_p(a+b) \geq \min\{v_p(a), v_p(b)\} \) and \( v_p(a+b) = v_p(a) + v_p(b) \) if \( v_p(a) \neq v_p(b) \).

The following lemma is our key result.

熊本高等学校 研究紀要 第10号 (2018) —61—
Lemma 2.6. Let \( n, r \) integers with \( n \geq 1 \) and \( p^s > r > 0 \). Then the following hold:

1. \( v_p \left( \frac{p^s}{r} \right) = v_p(p^s) - v_p(r) \left( = n - v_p(r) \right) \).

2. \( v_p \left( \frac{p^s}{r} \right) \geq 1 \).

3. \( v_p \left( \frac{p^s}{r} \right) = 1 \) if and only if \( r = ip^{s-1} \) with \( i = 1, \ldots, p-1 \).

4. \( \frac{1}{p} \left( \frac{p^s}{r} \right) = \frac{(-1)^{s-1}}{r} \) for \( i = 1, \ldots, p-1 \) in \( \mathbb{Z}/p\mathbb{Z} \subseteq (\mathbb{Z}/p\mathbb{Z})[x] \).

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

**Proof**

(1) First we remark that \( v_p \left( \frac{p^s}{r} - i \right) = \min \left\{ v_p \left( p^s \right), v_p(-i) \right\} = v_p(i) \) for integers \( p^s > i > 0 \). Hence we have

\[
v_p \left( \frac{p^s}{r} \right) = v_p \left( \frac{p^s \cdot (p^s - 1) \cdots (p^s - r + 1)}{p^s - 1} \right) = v_p \left( \frac{p^s}{r} \right) + v_p \left( \frac{p^s - 1}{r} \right) + \cdots + v_p \left( \frac{p^s - (r-1)}{r} \right) = v_p \left( \frac{p^s}{r} \right) - v_p(r).
\]

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

(3) Since \( v_p \left( \frac{p^s}{r} \right) = n - v_p(r) = 1 \), we have \( v_p(r) = n - 1 \) if and only if \( r = ip^{s-1} \) with \( i = 1, \ldots, p-1 \).

(4) If we denote \( j = c_i p^{s-1} \) for \( 1 \leq j \leq p^{s-1} - 1 \) and \( i = 1, \ldots, p-1 \), then we have

\[
\frac{p^s - j}{p^s - c_i} = \frac{p^{s-1} - c_i}{c_j} \quad \text{and} \quad \frac{p^{s-1} - c_i}{c_j} = -c_j \neq 0.
\]

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

So, we have

\[
\frac{1}{p} \left( \frac{p^s}{p^{s-1}} \right) = \frac{1}{p} \left( \prod_{j=1}^{p^{s-1} - 1} \left( \frac{p^s - j}{p^s - c_i} \right) \right) = \frac{1}{p} \left( \prod_{j=1}^{p^{s-1} - 1} \frac{p^{s-1} - c_i}{c_j} \right) = \frac{1}{p} \left( \prod_{j=1}^{p^{s-1} - 1} \frac{(-1)^{j-1}}{r} \right) = \frac{(-1)^{s-1} (x^{s-1})}{r}.
\]

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

\[
\frac{1}{p} \left( (x+1)^r - (x^r + 1) \right) \equiv \sum_{i=1}^{s-1} \frac{(-1)^{i-1}}{r} x^i \right)^{s-1} \) in \( (\mathbb{Z}/p\mathbb{Z})[x] \).

Hence, using (4), we have

\[
\frac{1}{p} \left( (x+1)^r - (x^r + 1) \right) \equiv \sum_{i=1}^{s-1} \frac{(-1)^{i-1}}{r} x^i \right)^{s-1} \) in \( (\mathbb{Z}/p\mathbb{Z})[x] \). \( \Box \)

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 \( n \geq 1 \), then \( \overline{\frac{1}{2}F} = \left( x^2 + x + 1 \right)^{\frac{n}{2}} \) in \( \left( \mathbb{Z}/2\mathbb{Z} \right)[x] \). Especially, \( \deg \left( \frac{1}{2}F \right) = \deg \left( \overline{\frac{1}{2}F} \right) = a \).

(2) If \( b = 3m \) with an integer \( m \geq 1 \), then \( G = 3m x^{\left(3^{m-1}\right)} + \cdots \mod 2 \) where \( m = 2^m m' \) with \( m' \) odd and \( G \equiv 1 \mod (2, x^2 + x + 1) \). Especially, \( \deg G \geq 1 \) and \( \gcd \left( \overline{\frac{1}{2}F}, G \right) = 1 \) in \( \left( \mathbb{Z}/2\mathbb{Z} \right)[x] \).

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

(2) \( G = \left( x + 1 \right)^{3^{n-1}} + (-1)^{3^{n-1}} \left( x^{3^{n-1}} + 1 \right) = x^{3^{n-1}} + (x^{3^{n-1}} + 1) = 3m' \left( x^{3^{n-1}} + \cdots + 3m' x^{3^{n-1}} + \cdots \mod 2 \right). \)

Since \( x^2 = x + 1 \mod (2, x^2 + x + 1) \) and \( x^3 = 1 \mod (2, x^2 + x + 1) \), we have
\[
G = \left( x + 1 \right)^{3^{n-1}} + (-1)^{3^{n-1}} \left( x^{3^{n-1}} + 1 \right) = 1^{\frac{n}{2}} + (1^{n+1} + 1) \mod (2, x^2 + x + 1) = 1^{n+1} + 1 \mod (2, x^2 + x + 1). \quad \square
\]

Proof of Prop. 2.2 for \( a = 2^n \):

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

Lemma 2.8. The following hold:

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

(2) If \( b = 2m \) with an integer \( m \geq 1 \), then we have
\[
\text{LC}(G) \equiv 2 \mod 3, \quad G = \left( x + 1 \right)^n + x^{n+1} = 2 \mod (3, x) \quad \text{and} \quad G = \left( x + 1 \right)^n + x^{n+1} = 2 \mod (3, x + 1).
\]

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

Proof (1) Since \( \overline{\frac{1}{3}} = \overline{1} \) in \( \mathbb{Z}/3\mathbb{Z} \subseteq \left( \mathbb{Z}/3\mathbb{Z} \right)[x] \), by Lemma 2.6 (5), we have
\[
\overline{\frac{1}{3}F} = \frac{1}{3} \left( \left( x + 1 \right)^n - (x^{n+1}) \right) = \frac{1}{3} \cdot \frac{\left( x - (x^{n+1}) \right)}{\overline{1}} = x^\left(\frac{n}{3}\right) \left( x + 1 \right)^{\frac{n}{3}} \text{ in } \left( \mathbb{Z}/3\mathbb{Z} \right][x].
\]

(2) Obviously \( \text{LC}(G) = 2 \mod 3 \). Since \( x + 1 = x^2 + 1 = 1 \mod (3, x) \) and \( x + 1 = (-1)^n + 1 = 2 \mod (3, x + 1) \), we have
\[
G = \left( x + 1 \right)^n + (x^{n+1}) = 2 \mod (3, x) \quad \text{and} \quad G = (x + 1)^n + (x^{n+1}) = 2 \mod (3, x + 1). \quad \square
\]
Proof of Prop. 2.2 for $a = 3^r$:

Since $ab = 0 \pmod{6}$, we can assume that $b = 2m$ with an integer $m \geq 1$. From Lemma 2.8, $\deg (G) = \deg \left( \frac{1}{3} G \right)$, $\deg \left( \frac{1}{3} F \right) \geq 1$ and $\gcd \left( \frac{1}{3} F, G \right) = 1$ in $(\mathbb{Z}/3\mathbb{Z})[[x]]$, which 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 $a = 5^r$ with $n = 1, 2, \cdots$, then $\frac{1}{5} F = \frac{1}{5} \left( x^3 + \frac{x}{3} \right)^{r} \left( x + \frac{x}{3} \right)^{r} \in (\mathbb{Z}/5\mathbb{Z})[[x]]$.

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

\[
\text{LC}(G) = 2 \pmod{5},
\]

\[
G = (x+1)^r + (x^3+1)^r = 2 \pmod{5, x},
\]

$G = (x+1)^r + (x^3+1)^r = 2 \pmod{5, x+1}$ and

\[
G = (x+1)^r + (x^3+1)^r = 3 \pmod{5, x^2+x+1}.
\]

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

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

\[
\frac{1}{5} F = \frac{1}{5} \left( \frac{x}{3} + \frac{x}{2} + \frac{x}{3} + \frac{x}{4} \right) = \left( x + 2x^3 + 2x^3 + x^3 \right)^{r} \left( x + 3 \right)^{r} \left( x + 1 \right)^{r} \in (\mathbb{Z}/5\mathbb{Z})[[x]].
\]

(2) Obviously $\text{LC}(G) = 2 \pmod{5}$. Since $x+1 = x^2+1 = 1 \pmod{(5, x)}$ and $x^3+1 = (-1)^{2m} + 1 = 2 \pmod{(5, x+1)}$, we have

\[
G = (x+1)^r + (x^3+1)^r = 2 \pmod{5, x} \quad \text{and} \quad G = (x+1)^r + (x^3+1)^r = 2 \pmod{5, x+1}.
\]

Moreover, since $x^3 = 1 \pmod{(5, x^2+x+1)}$ and $x+1 = x^2 \pmod{(5, x^2+x+1)}$, we have

\[
G = (x+1)^r + (x^3+1)^r = (-1)^{2m} + (x^{2m}+1) = 3 \pmod{(5, x^2+x+1)}. \quad \square
\]

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

Since $ab = 0 \pmod{6}$, we can assume that $b = 6m$ with an integer $m \geq 1$. From Lemma 2.9, $\deg (G) = \deg \left( \frac{1}{5} G \right)$, $\deg \left( \frac{1}{5} F \right) \geq 1$ and $\gcd \left( \frac{1}{5} F, G \right) = 1$ in $(\mathbb{Z}/5\mathbb{Z})[[x]]$, which 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 $a = 7^r$ with $n = 1, 2, \cdots$, then $\frac{1}{7} F = \frac{1}{7} \left( x^3 + \frac{x}{3} \right)^{r} \left( x^2 + \frac{x}{3} \right)^{r} \left( x + \frac{x}{3} \right)^{r} \left( x + 5 \right)^{r} \in (\mathbb{Z}/7\mathbb{Z})[[x]]$.

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

\[
\text{LC}(G) = 2 \pmod{7},
\]

\[
G = (x+1)^r + (x^3+1)^r = 2 \pmod{(7, x)},
\]

Especially, $\deg (G) = \deg \left( \frac{1}{7} G \right) = b$ and $\gcd \left( \frac{1}{7} F, G \right) = 1$ in $(\mathbb{Z}/7\mathbb{Z})[[x]]$. □
\[ G = (x + 1)^3 + (x^3 + 1) = 2 \mod (7, x + 1), \]
\[ G = (x + 1)^3 + (x^3 + 1) = 3 \mod (7, x + 3) \quad \text{and} \quad G = (x + 1)^3 + (x^3 + 1) = 3 \mod (7, x + 5). \]

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

**Proof (1)** Since \( \frac{-T}{2} = \frac{-3}{2}, \ \frac{T}{3} = \frac{-3}{3}, \ \frac{-T}{4} = \frac{-3}{3}, \ \frac{-T}{6} = \frac{-3}{3} \) and
\[ x(x + 1)\left(x + \frac{3}{3}\right)^2 + x(x + 1)\left(x + \frac{3}{3}\right)^2 = x + \frac{3}{3}x + \frac{3}{3}x + \frac{3}{3}x + x^2 + x^3 \text{ in } \mathbb{Z}/7\mathbb{Z} \triangleq (\mathbb{Z}/7\mathbb{Z})[x], \]
by Lemma 2.6 (5), we have
\[ \left(\frac{1}{7}F\right) = \left(x + \frac{3}{3}x + x^3 + x^3 + x^3 + x^3\right)^{n+1} = \left(x + \frac{3}{3}x + x^3 + x^3 + x^3 + x^3\right)^{n+1}. \]

(2) Obviously \( \text{LC}(G) = 2 \mod 7 \) and \( G = (x + 1)^3 + (x^3 + 1) = 2 \mod (7, x) \). Since \( x^3 + 1 = (-1)^{\frac{m}{2}} + 1 = 2 \mod (7, x + 1) \),
\( (x + 1)^3 = \left(5^m\right)^n = 1 \mod (7, x + 3) \), \( x^3 = \left(4^m\right)^n = 1 \mod (7, x + 3) \), \( (x + 1)^3 = \left(3^m\right)^n = 1 \mod (7, x + 5) \) and
\( x^3 = \left(2^m\right)^n = 1 \mod (7, x + 5) \), we have \( G = (x + 1)^3 + (x^3 + 1) = 2 \mod (7, x + 1) \), \( G = (x + 1)^3 + (x^3 + 1) = 3 \mod (7, x + 3) \) and \( G = (x + 1)^3 + (x^3 + 1) = 3 \mod (7, x + 5) \)

**Proof of Prop. 2.2 for \( a = 7^n \):**

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

**Lemma 2.11.** The following hold:

(1) If \( a = 10 \), then \( F = 2\left(x^2 + x + 1\right)^3 \) in \( (\mathbb{Z}/5\mathbb{Z})[x] \). Especially, \( \deg(F) = \deg(\overline{F}) = 10 \).

(2) If \( b \) is even, then \( G = 2x^6 + \cdots \mod 5 \) and if \( b \) is odd, then \( G = b'x^{b'(b'-1)} + \cdots \mod 5 \) where \( b = 5'b' \) with \( \overline{b} \neq 0 \) in \( \mathbb{Z}/5\mathbb{Z} \).

(3) If \( b = 3m \) with an integer \( m \geq 1 \), then \( G = 3\left(-1\right)^m \mod (5, x^2 + x + 1) \). Especially, \( \gcd(F, G) = 1 \) in \( (\mathbb{Z}/5\mathbb{Z})[x] \).

**Proof (1)** \( F = (x + 1)^{10} + (x^{10} + 1) = (x^2 + 1)^3 + (x^{10} + 1) = 2\left(x^6 + x + 1\right)^3 \mod 5 \).

(2) If \( b \) is odd, then \( G = (x + 1)^{b'} - (x^3 + 1)^{b'} = (x^2 + 1)^{b'} - (x^{b'} + 1)^{b'} = b'\left(x^2 + 1\right)^{b'} + \cdots = b'x^{b'(b'-1)} + \cdots \mod 5 \). If \( b \) is even, then the assertion is clear.

(3) Since \( x^3 = 1 \) and \( x + 1 = -x^2 \mod (5, x^2 + x + 1) \), we have
\[ G = (x + 1)^3 + (-1)^3 (x^3 + 1)^{m+1} + (-1)^m (x^{3m+1} + 1) = 3\left(-1\right)^m (x^6 + x^{3m} + 1) = 3\left(-1\right)^m \mod (5, x^2 + x + 1). \]

**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
\[ \gcd(F, G) = 1 \text{ in } (\mathbb{Z}/5\mathbb{Z})[x], \]
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