# SUMS OF DISTINCT POLYNOMIAL RESIDUES

**Carrie Finch-Smith**
*Department of Mathematics, Washington and Lee University, Lexington, Virginia,*
finchc@wlu.edu

**Joshua Harrington**
*Department of Mathematics, Cedar Crest College, Allentown, Pennsylvania*
joshua.harrington@cedarcrest.edu

**Tony W. H. Wong**
*Department of Mathematics, Kutztown University of Pennsylvania, Kutztown, Pennsylvania*
wong@kutztown.edu

*Received: 4/11/23, Accepted: 8/12/23, Published: 8/25/23*

**Abstract**

Let $p \geq 5$ be a prime. In 1801, Gauss proved that the sum of distinct quadratic residues modulo $p$ is congruent to 0 modulo $p$. A study by Stetson in 1904 showed that the sum of distinct triangular residues modulo $p$ is congruent to $-1/16$ modulo $p$. Both of these results were extended in 2017 by Gross, Harrington, and Minott, who studied the sum of distinct quadratic polynomial residues modulo $p$. In this article, we determine the sum of distinct cubic polynomial residues modulo $p$ and prove a conjecture of Gross, Harrington, and Minott. We further consider the sum of distinct residues modulo $p$ for polynomials of higher degree.

## 1. Introduction

Throughout this paper, let $p \geq 5$ be a prime, and let $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. In 1801, Gauss [1] proved that the sum of distinct quadratic residues modulo $p$ is congruent to 0 modulo $p$. Then in 1904, Stetson [4] showed that the sum of distinct triangular residues modulo $p$ is congruent to $-1/16$ modulo $p$. Both of these results were extended by Gross, Harrington, and Minott [2] in 2017, who considered the sum of distinct $s$-gonal numbers, and more generally the sum of distinct quadratic polynomial residues, modulo $p$.

For every polynomial $f \in \mathbb{Z}_p[x]$, we define

$$\mathfrak{R}(f) = \{f(x) \in \mathbb{Z}_p : x \in \mathbb{Z}_p\},$$

DOI: 10.5281/zenodo.8283157

and define

$$S(f) = \sum_{y \in \mathfrak{R}(f)} y.$$

To generalize the results of Gauss and Stetson, Gross, Harrington, and Minott provided the following theorem.

**Theorem 1** ([2]). *Let $f(x) = ax^2 + bx + c \in \mathbb{Z}_p[x]$ be a quadratic polynomial. If $a \neq 0$, then*

$$S(f) = -\frac{b^2 - 4ac}{8a}.$$

In this article, we provide a formula for $S(f)$ when $f \in \mathbb{Z}_p[x]$ is a cubic polynomial, thus proving a conjecture of Gross, Harrington, and Minott. We then discuss $S(f)$ when $f \in \mathbb{Z}_p[x]$ has degree larger than 3, with a special emphasis on certain families of cyclotomic polynomials.

## 2. Determining $S(f)$ for Cubic Polynomials

We begin this section with the following lemma.

**Lemma 1.** *Let $h \in \mathbb{Z}_p[x]$ be an odd polynomial, i.e., $h(-x) = -h(x)$. Let $g(x) = h(x) + k$, where $k \in \mathbb{Z}_p$. Then*

$$S(g) \equiv |\mathfrak{R}(g)| \cdot k \pmod{p}.$$

*Proof.* Suppose $y \in \mathfrak{R}(h) \setminus \{0\}$. Then there exists an $x \in \mathbb{Z}_p$ such that $h(x) = y$. Since $h$ is an odd polynomial, we have $h(-x) = -h(x) = -y$. Thus, $-y \in \mathfrak{R}(h)$. Since $p > 2$, we have $y \neq -y$. It follows that $S(h) = 0$. Now, suppose $z \in \mathfrak{R}(g)$. Then $z = y + k$ for some $y \in \mathfrak{R}(h)$. Hence, $S(g)$ is given by

$$\sum_{z \in \mathfrak{R}(g)} z = \sum_{y \in \mathfrak{R}(h)} (y + k) = \sum_{y \in \mathfrak{R}(h)} y + \sum_{y \in \mathfrak{R}(h)} k \equiv |\mathfrak{R}(h)| \cdot k \equiv |\mathfrak{R}(g)| \cdot k \pmod{p}.$$

□

In 1908, von Sterneck [3] proved that for all $x^3 + a_1x^2 + a_2x + a_3 \in \mathbb{Z}_p[x]$ such that $a_1^2 \neq 3a_2$,

$$|\mathfrak{R}(x^3 + a_1x^2 + a_2x + a_3)| = \frac{2p + \left(\frac{p}{3}\right)}{3}, \tag{1}$$

where $\left(\frac{p}{3}\right)$ is the Legendre symbol. With von Sterneck's result and Lemma 1, we can now prove our main result.

**Theorem 2.** *Let $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Z}_p[x]$ be a cubic polynomial. If $a \neq 0$, then*

$$S(f) = \begin{cases} \dfrac{27a^2d - 9abc + 2b^3}{81a^2} & \text{if } b^2 \neq 3ac \text{ and } p \equiv 1 \pmod 6 \\ -\dfrac{27a^2d - 9abc + 2b^3}{81a^2} & \text{if } b^2 \neq 3ac \text{ and } p \equiv 5 \pmod 6 \\ \dfrac{2(27a^2d - 9abc + 2b^3)}{81a^2} & \text{if } b^2 = 3ac \text{ and } p \equiv 1 \pmod 6 \\ 0 & \text{if } b^2 = 3ac \text{ and } p \equiv 5 \pmod 6. \end{cases}$$

*Proof.* We begin by letting $g(x) = f(x - b/(3a))/a$, i.e.,

$$g(x) = x^3 + \left(\frac{3ac - b^2}{3a^2}\right)x + \frac{27a^2d - 9abc + 2b^3}{27a^3}.$$

Notice that the coefficients of $g$ are well-defined in $\mathbb{Z}_p$ since $p \geq 5$. Therefore, $S(g)$ is defined, and it can easily be seen that $S(f) = a \cdot S(g)$. Thus, we will study $S(g)$ to obtain the proof.

Since $g(x) = h(x) + k$, where

$$h(x) = x^3 + \left(\frac{3ac - b^2}{3a^2}\right)x$$

is an odd polynomial and

$$k = \frac{27a^2d - 9abc + 2b^3}{27a^3},$$

we have from Lemma 1 that $S(g) = |\mathfrak{R}(g)| \cdot k$.

If $3ac - b^2 \neq 0$, then Equation (1) implies

$$|\mathfrak{R}(g)| = \frac{2p + \left(\frac{p}{3}\right)}{3} \equiv \begin{cases} 1/3 \pmod p & \text{if } p \equiv 1 \pmod 6 \\ -1/3 \pmod p & \text{if } p \equiv 5 \pmod 6. \end{cases}$$

Otherwise, if $3ac - b^2 = 0$, then $g(x) = x^3 + k$ and

$$\begin{aligned} |\mathfrak{R}(g)| &= \begin{cases} (p+2)/3 & \text{if } p \equiv 1 \pmod 6 \\ p & \text{if } p \equiv 5 \pmod 6 \end{cases} \\ &\equiv \begin{cases} 2/3 \pmod p & \text{if } p \equiv 1 \pmod 6 \\ 0 \pmod p & \text{if } p \equiv 5 \pmod 6. \end{cases} \end{aligned}$$

The theorem follows since $S(f) = a \cdot S(g) \equiv a \cdot |\mathfrak{R}(g)| \cdot k \pmod p$. $\square$

## 3. Addressing $S(f)$ for Polynomials of Degree Greater than 3

Theorems 1 and 2 provide formulae for calculating $S(f)$ when $f$ is a quadratic polynomial or cubic polynomial, respectively. A natural direction for further study is to consider $S(f)$ for quartic or higher degree polynomials $f \in \mathbb{Z}_p[x]$. Preliminary work in this direction suggests that $|\mathfrak{R}(f)|$ plays an important role in understanding $S(f)$. Unfortunately, the study of $|\mathfrak{R}(f)|$ seems very limited; interested readers are referred to Sun's article for results concerning $|\mathfrak{R}(f)|$ for quartic polynomials $f$ [5]. Nonetheless, in this section, we study $S(f)$ for certain families of polynomials of arbitrarily high degree.

A polynomial $f \in \mathbb{Z}_p[x]$ is called a permutation polynomial if $\mathfrak{R}(f) = p$. Clearly, for an odd prime $p$, if $f$ is a permutation polynomial, then $S(f) = 0$. The following lemma shows that the converse of this statement is not true.

**Lemma 2.** *For a positive integer $r$,*

$$S(x^r) = \begin{cases} 1 & \text{if } (p-1) \mid r \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* For a positive integer $r$, let $g_r \in \mathbb{Z}_p[x]$ with $g_r(x) = x^r$. Recall that $\mathfrak{R}(g_r) \setminus \{0\}$ forms a group under multiplication with $|\mathfrak{R}(g_r) \setminus \{0\}| = (p-1)/\gcd(p-1, r)$. Thus, if $p-1$ divides $r$, then $|\mathfrak{R}(g_r) \setminus \{0\}| = 1$. We then deduce that $\mathfrak{R}(g_r) = \{0, 1\}$ and $S(g_r) = 1$. On the other hand, if $p-1$ does not divide $r$, then $\mathfrak{R}(g_r) \setminus \{0\}$ contains an element $\beta \neq 1$. Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be the elements of $\mathfrak{R}(g_r) \setminus \{0\}$. Since $\mathfrak{R}(g_r) \setminus \{0\}$ forms a group under multiplication,

$$S(g_r) = 0 + \alpha_1 + \alpha_2 + \cdots + \alpha_t = \beta \cdot 0 + \beta \cdot \alpha_1 + \beta \cdot \alpha_2 + \cdots + \beta \cdot \alpha_t = \beta \cdot S(g_r).$$

Since $\beta \neq 1$, we deduce that $S(g_r) = 0$. $\square$

For the rest of this article, let $g_r \in \mathbb{Z}_p[x]$ such that $g_r(x) = x^r$. The next theorem determines $S(f)$ for a particular class of binomials $f \in \mathbb{Z}_p[x]$.

**Theorem 3.** *Let $f(x) = ax^r + b \in \mathbb{Z}_p[x]$. Then*

$$S(f) = \begin{cases} a + 2b & \text{if } (p-1) \mid r \\ b\left(\dfrac{p-1}{\gcd(r, p-1)} + 1\right) & \text{otherwise.} \end{cases}$$

*Proof.* Let $\alpha$ be the generator of the multiplicative group $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. Then the order of $\alpha^r$ is $\mathrm{ord}_p(\alpha^r) = (p-1)/\gcd(r, p-1)$. By Lemma 2,

$$\begin{aligned} S(f) &= a \cdot S(g_r) + b \cdot (\mathrm{ord}_p(\alpha^r) + 1) \\ &= \begin{cases} a \cdot 1 + b \cdot (1+1) & \text{if } (p-1) \mid r \\ a \cdot 0 + b \cdot (\mathrm{ord}_p(\alpha^r) + 1) & \text{otherwise} \end{cases} \\ &= \begin{cases} a + 2b & \text{if } (p-1) \mid r \\ b \cdot (\mathrm{ord}_p(\alpha^r) + 1) & \text{otherwise.} \end{cases} \end{aligned}$$

□

Let $\Phi_n(x) \in \mathbb{Z}_p[x]$ denote the $n$-th cyclotomic polynomial. Recall that $\Phi_{2^t}(x) = x^{2^{t-1}} + 1$. Thus, letting $a = b = 1$ and $r = 2^{t-1}$ in Theorem 3 yields the following corollary.

**Corollary 1.** *Let $j$ be an integer such that $2^j \mid\mid (p-1)$. Then*

$$S(\Phi_{2^t}) = \begin{cases} 3 & \textit{if } (p-1) \mid 2^{t-1} \\ \dfrac{p-1}{2^{min\{t-1,j\}}} + 1 & \textit{otherwise.} \end{cases}$$

The following lemma is an easy exercise in elementary number theory, and can by verified by considering the multiplicative group $\mathbb{Z}_p^*$.

**Lemma 3.** *Let $q$ be a prime and let $j$ satisfy $q^j \mid\mid (p-1)$. For every integer $t \geq j$,*

$$\mathfrak{R}(g_{q^t}) = \mathfrak{R}(g_{q^j}).$$

*Consequently, for all $h \in \mathbb{Z}_p[x]$,*

$$S(h \circ g_{q^t}) = S(h \circ g_{q^j}).$$

**Remark 1.** Lemma 3 shows that for all $h \in \mathbb{Z}_p[x]$, $S(h \circ g_{q^t}) = S(h)$ for any positive integers $t$ and prime $q$ with $\gcd(q, p-1) = 1$. In combination with Theorems 1 and 2, if $\gcd(q, p-1) = 1$ and $f = h \circ g_{q^t}$, where $\deg(h) \in \{2, 3\}$, we can determine $S(f)$ as $S(h)$.

To make use of Lemma 3 in studying $S(\Phi_n)$, we present the following well-known cyclotomic identity.

**Lemma 4.** *For any prime $q$ and positive integer $n$ divisible by $q$, $\Phi_{qn} = \Phi_n \circ g_q$.*

The following theorem is an immediate consequence of Lemmas 3 and 4.

**Theorem 4.** *Let $q$ be a prime and let $j$ satisfy $q^j \mid\mid (p-1)$. Then for any positive integer $m$ not divisible by $q$ and integer $t > j$,*

$$S(\Phi_{q^t m}) = S(\Phi_{q^{j+1} m}).$$

## 4. Concluding Remarks

In their article, Gross, Harrington, and Minott gave the following conjecture.

**Conjecture 1.** Let $f(x) = ax^3 + bx^2 \in \mathbb{Z}_p[x]$. If $a \neq 0$, then

$$S(f) = \begin{cases} \dfrac{2b^3}{81a^2} & \text{if } p \equiv 1 \pmod 6 \\ -\dfrac{2b^3}{81a^2} & \text{if } p \equiv 5 \pmod 6). \end{cases}$$

Theorem 2 of this paper proves Conjecture 1 and generalizes it to all cubic polynomials.

Although it would be nice to obtain a theorem analogous to Theorems 1 and 2 for quartic or higher degree polynomials, such a result seems beyond our reach. For instance, let $f_c(x) = x^4 + cx^2 \in \mathbb{Z}_p[x]$. In view of Theorems 1 and 2, it is natural to conjecture that $S(f_c)$ is a polynomial of $c$. However, for selected primes $p$, when we apply the method of successive differences on the sequence $(S(f_c))_{c=1}^{p-1}$, the resulting sequences do not become constant after several iterations, indicating that the conjecture fails.

In the following, we provide a conjecture related to $S(f_c)$.

**Conjecture 2.** Let $\mathcal{S} = \{S(f_c) : c \in \mathbb{Z}_p\}$. If $p > 5$, then

$$\mathcal{S} = \begin{cases} \mathbb{Z}_p & \text{if } p \equiv 3 \pmod 4 \text{ and } -1 \in \mathcal{S} \\ \mathfrak{R}(g_2) & \text{if } p \equiv 3 \pmod 4 \text{ and } -1 \notin \mathcal{S}, \\ & \quad \text{or } p \equiv 1 \pmod 4 \text{ and } -1 \in \mathcal{S} \\ \mathfrak{R}(g_4) & \text{if } p \equiv 5 \pmod 8 \text{ and } -1 \notin \mathcal{S} \\ \mathfrak{R}(g_2) \setminus \mathfrak{R}(g_4) & \text{if } p \equiv 1 \pmod 8 \text{ and } -1 \notin \mathcal{S}. \end{cases}$$

Furthermore, $S(f_8) = 1$ if $p \equiv 3 \pmod 4$.

**Theorem 5.** *Let $f(x) = \sum_{\ell=0}^{k} a_\ell x^{m_\ell} \in \mathbb{Z}_p[x]$, where $0 < m_0 < m_1 < m_2 < \cdots < m_k$ and $a_\ell \neq 0$ for all $0 \leq \ell \leq k$. Let $\delta > 1$ be a common factor of $\{m_\ell - m_0 : 1 \leq \ell \leq k\}$ such that $\gcd(\delta, m_0) = 1$ and $\delta \mid (p-1)$. Then $S(f) = 0$.*

*Proof.* Since $m_0 > 0$, $f(0) = 0 \in \mathfrak{R}(f)$. Let $\alpha$ be a generator of $\mathbb{Z}_p^*$, and let $\omega = \alpha^{\frac{p-1}{\delta}}$. For each $0 \leq i \leq \frac{p-1}{\delta} - 1$, let $\mathfrak{C}_i = \{f(\alpha^i \omega^j) : 0 \leq j \leq \delta - 1\}$. Note that

$$\begin{aligned} f(\alpha^i \omega^j) &= \alpha^{im_0} \omega^{jm_0} \sum_{i=0}^{k} a_\ell \alpha^{i(m_\ell - m_0)} \omega^{j(m_\ell - m_0)} \\ &= \alpha^{im_0} \omega^{jm_0} \sum_{i=0}^{k} a_\ell \alpha^{i(m_\ell - m_0)} \\ &= \omega^{jm_0} f(\alpha^i), \end{aligned}$$

since $\omega^{m_\ell - m_0} = \alpha^{\frac{p-1}{\delta}(m_\ell - m_0)} = 1$. Together with the condition that $\gcd(\delta, m_0) = 1$, it follows that for each $0 \le i \le \frac{p-1}{\delta} - 1$, the elements of $\mathfrak{C}_i$ are all distinct unless $f(\alpha^i) = 0$, and the sum of the elements of $\mathfrak{C}_i$ is

$$\sum_{j=0}^{\delta-1} \omega^{jm_0} f(\alpha^i) = f(\alpha^i) \sum_{j=0}^{\delta-1} \omega^{jm_0} = f(\alpha^i) \sum_{j=0}^{\delta-1} \omega^j = 0$$

since $\delta - 1 > 0$. Finally, since $\mathfrak{R}(f) = \{0\} \cup \bigcup_{i=0}^{\frac{p-1}{\delta}-1} \mathfrak{C}_i$, and $\mathfrak{C}_i$ and $\mathfrak{C}_{i'}$ are either equal or disjoint for any $0 \le i < i' \le \frac{p-1}{\delta} - 1$, we conclude that $S(f) = 0$. $\square$

For example, if $p = 71$, then it follows that $S(a_3x^{62} + a_2x^{42} + a_1x^{22} + a_0x^2) = 0$ by taking $\delta = 5$ in Theorem 5. By taking $\delta = 3$, we have the following corollary.

**Corollary 2.** *Let $f(x) = x^4 + dx \in \mathbb{Z}_p[x]$. If $p \equiv 1 \pmod 3$, then $S(f) = 0$.*

**Proposition 1.** *Let $f_d(x) = x^4 + dx \in \mathbb{Z}_p[x]$. If $p \equiv 2 \pmod 3$, then $S(f_d) = d^{\frac{4}{3}} S(f_1)$.*

*Proof.* Note that if $p \equiv 2 \pmod 3$, then $x \mapsto x^3$ forms a permutation on $\mathbb{Z}_p$. Hence, every element $d \in \mathbb{Z}_p$ has a unique cube root $d^{\frac{1}{3}} \in \mathbb{Z}_p$. If $d \in \mathbb{Z}_p^*$, then $x \mapsto d^{\frac{1}{3}}x$ induces a permutation on $\mathbb{Z}_p$, so

$$\mathfrak{R}(f_d) = \{f_d(d^{\frac{1}{3}}x) : x \in \mathbb{Z}_p\} = \{d^{\frac{4}{3}}(x^4 + x) : x \in \mathbb{Z}_p\} = \{d^{\frac{4}{3}} f_1(x) : x \in \mathbb{Z}_p\}.$$

Furthermore, $x \mapsto d^{\frac{4}{3}}x$ also forms a permutation on $\mathbb{Z}_p$, so $\mathfrak{R}(f_d) = \{d^{\frac{4}{3}}y : y \in \mathfrak{R}(f_1)\}$, implying that $S(f_d) = d^{\frac{4}{3}} S(f_1)$. Finally, if $d = 0$, then by Theorem 3, $S(f_0) = 0$, which is equal to $0^{\frac{4}{3}} S(f_1)$. $\square$

**Conjecture 3.** Let $f(x) = x^4 + cx^2 + e \in \mathbb{Z}_p[x]$. Then

$$S(f) = \begin{cases} \dfrac{-9c^2 + 40e}{64} & \text{if } p \equiv 1 \pmod 8 \text{ and } c \text{ is a quadratic residue in } \mathbb{Z}_p \\ \dfrac{-c^2 + 40e}{64} & \text{if } p \equiv 1 \pmod 8 \text{ and } c \text{ is a quadratic nonresidue in } \mathbb{Z}_p \\ \dfrac{-7c^2 + 56e}{64} & \text{if } p \equiv 3 \pmod 8 \text{ and } c \text{ is a quadratic residue in } \mathbb{Z}_p \\ \dfrac{c^2 - 8e}{64} & \text{if } p \equiv 3 \pmod 8 \text{ and } c \text{ is a quadratic nonresidue in } \mathbb{Z}_p \\ \dfrac{-c^2 + 8e}{64} & \text{if } p \equiv 5 \pmod 8 \text{ and } c \text{ is a quadratic residue in } \mathbb{Z}_p \\ \dfrac{-9c^2 + 72e}{64} & \text{if } p \equiv 5 \pmod 8 \text{ and } c \text{ is a quadratic nonresidue in } \mathbb{Z}_p \\ \dfrac{c^2 + 24e}{64} & \text{if } p \equiv 7 \pmod 8 \text{ and } c \text{ is a quadratic residue in } \mathbb{Z}_p \\ \dfrac{-7c^2 + 24e}{64} & \text{if } p \equiv 7 \pmod 8 \text{ and } c \text{ is a quadratic nonresidue in } \mathbb{Z}_p. \end{cases}$$

## References

[1] C. Gauss, *Disquisitiones Arithmeticae*, Lipsiae : In commissis apud Gerh. Fleischer, Jun., 1801.

[2] S. Gross, J. Harrington, and L. Minott, Sums of polynomial residues, *Irish Math. Soc. Bull.* **79** (2017), 31-37.

[3] R. D. von Sterneck, Über die Anzahl inkongruenter Werte, die eine ganze Funktion dritten Grades annimmt, *Sitzungsber. Akad. Wiss. Wien (2A)* **114** (1908), 711-717.

[4] O. Stetson, Triangular residues, *Amer. Math. Monthly* **11** (1904), 106-107.

[5] Z.-H. Sun, On the number of incongruent residues of $x^4 + ax^2 + bx$ modulo $p$, *J. Number Theory* **119** (2006), 210-241.