Distinct residues of Lucas polynomials over $\mathbb{F}_p$

Matthew Litman
Joint with Thomas Brazelton, Joshua Harrington, Tony Wong

March 27th-28th, 2021
MASON V(irtual)

Outline of the Talk

1. Background on residue sums and Lucas polynomials

Outline of the Talk

1. Background on residue sums and Lucas polynomials
2. Hyperbolic, elliptic, & parabolic elements and their images

Outline of the Talk

1. Background on residue sums and Lucas polynomials
2. Hyperbolic, elliptic, & parabolic elements and their images
3. $p \equiv 3 \pmod 4$ case - sum and image size

Outline of the Talk

1. Background on residue sums and Lucas polynomials
2. Hyperbolic, elliptic, & parabolic elements and their images
3. $p \equiv 3 \pmod 4$ case - sum and image size
4. $p \equiv 1 \pmod 4$ case - sum and image size

Key Definitions

For an integral polynomial f and prime p, let

$$\begin{aligned}
\mathfrak{R}_p(f) &= \text{the image set of } f \text{ modulo } p \\
&= \{y \in \mathbb{F}_p : \exists x \in \mathbb{F}_p \text{ s.t. } f(x) \equiv y \pmod{p}\}, \\
S_p(f) &= \text{the sum over distinct residues of } f \text{ modulo } p \\
&= \sum_{y \in \mathfrak{R}_p(f)} y \pmod{p}
\end{aligned}$$

Key Definitions

For an integral polynomial f and prime p, let

$$\begin{aligned}
\mathfrak{R}_p(f) &= \text{the image set of } f \text{ modulo } p \\
&= \{y \in \mathbb{F}_p : \exists x \in \mathbb{F}_p \text{ s.t. } f(x) \equiv y \pmod{p}\}, \\
S_p(f) &= \text{the sum over distinct residues of } f \text{ modulo } p \\
&= \sum_{y \in \mathfrak{R}_p(f)} y \pmod{p}
\end{aligned}$$

- If f is odd, $S_p(f) = 0 \Rightarrow$ study $S_p(f)$ when f is not odd

Key Definitions

For an integral polynomial f and prime p, let

$$\begin{aligned}\mathfrak{R}_p(f) &= \text{the image set of } f \text{ modulo } p \\ &= \{y \in \mathbb{F}_p : \exists x \in \mathbb{F}_p \text{ s.t. } f(x) \equiv y \pmod{p}\}, \\ S_p(f) &= \text{the sum over distinct residues of } f \text{ modulo } p \\ &= \sum_{y \in \mathfrak{R}_p(f)} y \pmod{p}\end{aligned}$$

- If f is odd, $S_p(f) = 0 \Rightarrow$ study $S_p(f)$ when f is not odd
- For a general polynomial, understanding $\mathfrak{R}_p(f)$ can be quite difficult (e.g. how does $|\mathfrak{R}_p(f)|$ behave as $p \to \infty$?)

Key Definitions

For an integral polynomial f and prime p, let

$$\begin{aligned}\mathfrak{R}_p(f) &= \text{the image set of } f \text{ modulo } p \\ &= \{y \in \mathbb{F}_p : \exists x \in \mathbb{F}_p \text{ s.t. } f(x) \equiv y \pmod{p}\}, \\ S_p(f) &= \text{the sum over distinct residues of } f \text{ modulo } p \\ &= \sum_{y \in \mathfrak{R}_p(f)} y \pmod{p}\end{aligned}$$

- If f is odd, $S_p(f) = 0 \Rightarrow$ study $S_p(f)$ when f is not odd
- For a general polynomial, understanding $\mathfrak{R}_p(f)$ can be quite difficult (e.g. how does $|\mathfrak{R}_p(f)|$ behave as $p \to \infty$?)
- For some polynomials f, certain properties of $\mathfrak{R}_p(f)$ are invariant for all primes p (including $S_p(f)$)

Previous Studies of $\mathfrak{R}_p(f)$ and $S_p(f)$

Towards $\mathfrak{R}_p(f)$:

1. It's well known that $|\mathfrak{R}_p(x^2)| = \frac{p+1}{2}$, and for all quadratics one has $|\mathfrak{R}_p(ax^2+bx+c)| = \frac{p+1}{2}$ $(p \geq 3)$
2. von Sterneck (1908) proved that if $b^2 \not\equiv 3c \pmod{p}$, then

$$\left|\mathfrak{R}_p\left(x^3+bx^2+cx+d\right)\right| = \frac{2p+\left(\frac{p}{3}\right)}{3}$$

Previous Studies of $\mathfrak{R}_p(f)$ and $S_p(f)$

Towards $\mathfrak{R}_p(f)$:

1. It's well known that $|\mathfrak{R}_p(x^2)| = \frac{p+1}{2}$, and for all quadratics one has $|\mathfrak{R}_p(ax^2+bx+c)| = \frac{p+1}{2}$ $(p \geq 3)$
2. von Sterneck (1908) proved that if $b^2 \not\equiv 3c \pmod{p}$, then

$$\left|\mathfrak{R}_p\left(x^3+bx^2+cx+d\right)\right| = \frac{2p+\left(\frac{p}{3}\right)}{3}$$

Towards $S_p(f)$:

1. Gauss (1801) showed $S_p(x^2) = 0$
2. For $a \not\equiv 0 \pmod{p}$, Gross–Harrington–Minnott (2017) showed $S_p(ax^2+bx+c) \equiv -\frac{b^2-4ac}{8a}$
3. The cubic polynomial case was handled by Finch-Smith–Harrington–Wong (2019) with a formula depending on $p \pmod 6$

Lucas Polynomials

Definition

The Lucas polynomials $L_n(x)$ for $n \geq 0$ are defined recursively by $L_0(x) = 2$, $L_1(x) = x$, and $L_n(x) = x \cdot L_{n-1}(x) + L_{n-2}(x)$ for all $n \geq 2$.

The Lucas polynomials admit a Binet formula expansion: for

$$\omega(x) = \frac{x + \sqrt{x^2+4}}{2}, \quad \omega^{-1}(x) = \frac{-x + \sqrt{x^2+4}}{2},$$

one has the closed form expression

$$L_n(x) = \omega(x)^n + (-\omega(x)^{-1})^n.$$

Furthermore, $L_n(x)$ is even/odd $\iff$ n is even/odd.

Example – $S_7(L_n)$

Investigation of $S_7(L_n)$ for $1 \leq n \leq 48$

n	$S_7(L_n)$	n	$S_7(L_n)$	n	$S_7(L_n)$	n	$S_7(L_n)$
1	0	13	0	25	0	37	0
2	1	14	1	26	1	38	1
3	0	15	0	27	0	39	0
4	1	16	1	28	1	40	6
5	0	17	0	29	0	41	0
6	2	18	2	30	2	42	2
7	0	19	0	31	0	43	0
8	6	20	1	32	1	44	1
9	0	21	0	33	0	45	0
10	1	22	1	34	1	46	1
11	0	23	0	35	0	47	0
12	2	24	0	36	2	48	2

Example – $S_7(L_n)$

Investigation of $S_7(L_n)$ for $1 \leq n \leq 48$

n	$S_7(L_n)$	n	$S_7(L_n)$	n	$S_7(L_n)$	n	$S_7(L_n)$
1	0	13	0	25	0	37	0
2	1	14	1	26	1	38	1
3	0	15	0	27	0	39	0
4	1	16	1	28	1	40	6
5	0	17	0	29	0	41	0
6	2	18	2	30	2	42	2
7	0	19	0	31	0	43	0
8	6	20	1	32	1	44	1
9	0	21	0	33	0	45	0
10	1	22	1	34	1	46	1
11	0	23	0	35	0	47	0
12	2	24	0	36	2	48	2

Observation: the only values that appear for $S_7(L_n)$ are -1, 0, 1, 2

Main Result – $S_p(L_n)$

Theorem (Brazelton, Harrington, L., Wong '21)

Let p be an odd prime, n a natural number. Then

$$S_p(L_n) \in \{-1, 0, 1, 2\}$$

and we can say exactly when each value will occur.

We have explicit formulas for $S_p(L_n)$ for every prime p and natural number n, the formulas are a bit too large to fit together on this slide. We will see these formulas later in the talk.

Notation and Conventions

- n is an even natural number
- $d := \gcd(n, p-1)$
- $\delta := \gcd(n, 2(p+1))$
- 2^h is the highest power of 2 dividing $p-1$
- 2^r is the highest power of 2 dividing $2(p+1)$

Notation and Conventions

- n is an even natural number
- $d := \gcd(n, p-1)$
- $\delta := \gcd(n, 2(p+1))$
- 2^h is the highest power of 2 dividing $p-1$
- 2^r is the highest power of 2 dividing $2(p+1)$

Each of these conventions gives us a way to simplify things:

- n even $\Rightarrow L_n(x) = \omega(x)^n + \omega(x)^{-n}$
- $\{\zeta_{p-1}^{an}\} = \{\zeta_{p-1/d}^{a}\}$, ζ_{p-1} = primitive $(p-1)^{st}$ root of unity
- $\{\zeta_{2(p+1)}^{bn}\} = \{\zeta_{2(p+1)/\delta}^{b}\}$
- If $p \equiv 1 \pmod 4$, $\frac{p-1}{d}$ is odd $\iff 2^h \mid n$.
- If $p \equiv 3 \pmod 4$, $\frac{2(p+1)}{\delta}$ is odd $\iff 2^r \mid n$.

Main Result – $\mathfrak{R}_p(L_n)$

Theorem (Brazelton, Harrington, L., Wong '21)

Let n, d, δ, r be as previously defined. For $p \equiv 3 \pmod 4$,

$$|\mathfrak{R}_p(L_n)| = \left\lceil \frac{p-1}{2d} \right\rceil + \begin{cases} \left\lfloor \frac{p+1}{\delta} \right\rfloor & \text{if } 2^r \mid n; \\ \left\lceil \frac{p+1}{2\delta} \right\rceil & \text{if } 2^r \nmid n, \end{cases}$$

and for $p \equiv 1 \pmod 4$,

$$|\mathfrak{R}_p(L_n)| = \begin{cases} \frac{p-1}{2d} + 1 & \text{if } 2 \,||\, d \text{ and } d \neq 2; \\ \left\lceil \frac{p-1}{2d} \right\rceil & \text{if } 4 \mid d \text{ or } d = 2, \end{cases} + \begin{cases} \left\lfloor \frac{p+1}{\delta} \right\rfloor & \text{if } 2 \,||\, \delta; \\ \left\lfloor \frac{p+1}{2\delta} \right\rfloor & \text{if } 4 \mid \delta, \end{cases} + \begin{cases} 1 & \text{if } d = 2; \\ 0 & \text{if } d \neq 2. \end{cases}$$

Hyperbolic, Elliptic, and Parabolic elements of $\mathbb{F}_p$

We partition $\mathbb{F}_p$ into subsets depending on the value of x^2+4 present under the square-root in $\omega(x) = \frac{x+\sqrt{x^2+4}}{2}$:

$$\mathcal{H}_p = \{x \in \mathbb{F}_p : x^2+4 \text{ is a quadratic residue mod } p\},$$
$$\mathcal{E}_p = \{x \in \mathbb{F}_p : x^2+4 \text{ is a quadratic non-residue mod } p\},$$
$$\mathcal{P}_p = \{x \in \mathbb{F}_p : x^2+4 \equiv 0 \pmod{p}\}.$$

Elements of $\mathcal{H}_p$, $\mathcal{E}_p$, and $\mathcal{P}_p$ are called **hyperbolic**, **elliptic**, and **parabolic**, respectively.

Hyperbolic, Elliptic, and Parabolic elements of $\mathbb{F}_p$

We partition $\mathbb{F}_p$ into subsets depending on the value of x^2+4 present under the square-root in $\omega(x) = \frac{x+\sqrt{x^2+4}}{2}$:

$$\mathcal{H}_p = \{x \in \mathbb{F}_p : x^2+4 \text{ is a quadratic residue mod } p\},$$
$$\mathcal{E}_p = \{x \in \mathbb{F}_p : x^2+4 \text{ is a quadratic non-residue mod } p\},$$
$$\mathcal{P}_p = \{x \in \mathbb{F}_p : x^2+4 \equiv 0 \pmod{p}\}.$$

Elements of $\mathcal{H}_p$, $\mathcal{E}_p$, and $\mathcal{P}_p$ are called **hyperbolic**, **elliptic**, and **parabolic**, respectively.

By studying the images of each of these sets under L_n, we are able to get a handle on $S_p(L_n)$ and $\mathfrak{R}_p(L_n)$

$\mathcal{H}_p, \mathcal{E}_p, \mathcal{P}_p$ and their relation to $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$

- If $x \in \mathcal{H}_p$, then $\omega(x) \in \mathbb{F}_p$ and $\omega(x)^{p-1} = 1 \Rightarrow$ $\omega(x) = \zeta_{p-1}^a$, for some a, where ζ_{p-1} is a primitive $(p-1)$st root of unity.

$\mathcal{H}_p, \mathcal{E}_p, \mathcal{P}_p$ and their relation to $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$

- If $x \in \mathcal{H}_p$, then $\omega(x) \in \mathbb{F}_p$ and $\omega(x)^{p-1} = 1 \Rightarrow \omega(x) = \zeta_{p-1}^a$, for some a, where ζ_{p-1} is a primitive $(p-1)$st root of unity.
- If $y \in \mathcal{E}_p$, then $\omega(y) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$, $\Rightarrow \omega(y)^{p^2-1} = 1$.

$\mathcal{H}_p, \mathcal{E}_p, \mathcal{P}_p$ and their relation to $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$

- If $x \in \mathcal{H}_p$, then $\omega(x) \in \mathbb{F}_p$ and $\omega(x)^{p-1} = 1 \Rightarrow$ $\omega(x) = \zeta_{p-1}^a$, for some a, where ζ_{p-1} is a primitive $(p-1)$st root of unity.
- If $y \in \mathcal{E}_p$, then $\omega(y) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$, $\Rightarrow \omega(y)^{p^2-1} = 1$.
- If $z \in \mathcal{P}_p$, then $\omega(z) = z/2 \in \mathbb{F}_p$ and $z = \sqrt{-4}$ $\Rightarrow \;\; z = \pm 2i$, where $i = \sqrt{-1}$.

$\mathcal{H}_p, \mathcal{E}_p, \mathcal{P}_p$ and their relation to $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$

- If $x \in \mathcal{H}_p$, then $\omega(x) \in \mathbb{F}_p$ and $\omega(x)^{p-1} = 1 \Rightarrow$ $\omega(x) = \zeta_{p-1}^a$, for some a, where ζ_{p-1} is a primitive $(p-1)$st root of unity.
- If $y \in \mathcal{E}_p$, then $\omega(y) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$, $\Rightarrow \omega(y)^{p^2-1} = 1$.
- If $z \in \mathcal{P}_p$, then $\omega(z) = z/2 \in \mathbb{F}_p$ and $z = \sqrt{-4}$ $\Rightarrow \;\; z = \pm 2i$, where $i = \sqrt{-1}$.

$$\mathcal{P}_p \text{ is nonempty } \iff \; p \equiv 1 \pmod 4$$

In this situation, we see that

$$L_n(z) = \omega(z)^n + \omega(z)^{-n} = i^n + i^{-n} = 2\,(-1)^{n/2}$$

Explicit Description of $\mathcal{H}_p, \mathcal{E}_p, \mathcal{P}_p$

Proposition

For $y \in \mathcal{E}_p$, we have that $\omega(y)^{p+1} = -1$ in $\mathbb{F}_p$. In particular, we may write $\omega(y) = \zeta_{2(p+1)}^{b}$, where b is some odd number, and $\zeta_{2(p+1)}$ is a primitive $2(p+1)$th root of unity in $\mathbb{F}_{p^2}$.

From the definition of $\omega(x)$, we have $x = \omega(x) - \omega^{-1}(x) \Rightarrow$

- $\mathcal{H}_p = \left\{ \zeta_{p-1}^{a} - \zeta_{p-1}^{-a} : 0 \leq a \leq p-1,\ a \neq \frac{p-1}{4}, \frac{3(p-1)}{4} \right\}$
- $\mathcal{E}_p = \left\{ \zeta_{2(p+1)}^{b} - \zeta_{2(p+1)}^{-b} : 1 \leq b \leq 2(p+1) \text{ odd}, \right.$
  $\left. b \neq \frac{2(p+1)}{4}, \frac{3(2(p+1))}{4} \right\}$
- $\mathcal{P}_p = \{\pm 2i\}$

Explicit Description of $\mathcal{H}_p, \mathcal{E}_p, \mathcal{P}_p$

Proposition

For $y \in \mathcal{E}_p$, we have that $\omega(y)^{p+1} = -1$ in $\mathbb{F}_p$. In particular, we may write $\omega(y) = \zeta_{2(p+1)}^{b}$, where b is some odd number, and $\zeta_{2(p+1)}$ is a primitive $2(p+1)$th root of unity in $\mathbb{F}_{p^2}$.

From the definition of $\omega(x)$, we have $x = \omega(x) - \omega^{-1}(x) \Rightarrow$

- $\mathcal{H}_p = \left\{ \zeta_{p-1}^{a} - \zeta_{p-1}^{-a} : 0 \leq a \leq p-1,\ a \neq \frac{p-1}{4}, \frac{3(p-1)}{4} \right\}$
- $\mathcal{E}_p = \left\{ \zeta_{2(p+1)}^{b} - \zeta_{2(p+1)}^{-b} : 1 \leq b \leq 2(p+1) \text{ odd}, \right.$
  $\left. b \neq \frac{2(p+1)}{4}, \frac{3(2(p+1))}{4} \right\}$
- $\mathcal{P}_p = \{\pm 2i\}$

For an element of the form $t = \zeta_m^a - \zeta_m^{-a}$ $(m | p^2 - 1)$, one has

$$L_n(t) = \zeta_m^{na} + \zeta_m^{-na}$$

$p \equiv 3 \pmod 4$ – Images of $\mathcal{H}_p, \mathcal{E}_p$

For $p \equiv 3 \pmod 4$, one has

$$L_n(\mathcal{H}_p) = \left\{ \zeta_{\frac{p-1}{d}}^{a} + \zeta_{\frac{p-1}{d}}^{-a} : 0 \leq a \leq \frac{1}{2}\left(\frac{p-1}{d} - 1\right) \right\}$$

$$L_n(\mathcal{E}_p) = \left\{ (-1)^{n/2}\left(\zeta_{\frac{2(p+1)}{\delta}}^{b} + \zeta_{\frac{2(p+1)}{\delta}}^{-b}\right) : 1 \leq b \leq \frac{2(p+1)}{\delta} \text{ odd} \right\}$$

and their intersection satisfies

$$L_n(\mathcal{H}_p) \cap L_n(\mathcal{E}_p) = \begin{cases} \{2\} & \text{if } 2^r \mid n; \\ \emptyset & \text{otherwise.} \end{cases}$$

$p \equiv 3 \pmod 4$ – Images of $\mathcal{H}_p, \mathcal{E}_p$

For $p \equiv 3 \pmod 4$, one has

$$L_n(\mathcal{H}_p) = \left\{ \zeta_{\frac{p-1}{d}}^{a} + \zeta_{\frac{p-1}{d}}^{-a} : 0 \leq a \leq \frac{1}{2}\left(\frac{p-1}{d} - 1\right) \right\}$$

$$L_n(\mathcal{E}_p) = \left\{ (-1)^{n/2}\left(\zeta_{\frac{2(p+1)}{\delta}}^{b} + \zeta_{\frac{2(p+1)}{\delta}}^{-b}\right) : 1 \leq b \leq \frac{2(p+1)}{\delta} \text{ odd} \right\}$$

and their intersection satisfies

$$L_n(\mathcal{H}_p) \cap L_n(\mathcal{E}_p) = \begin{cases} \{2\} & \text{if } 2^r \mid n; \\ \emptyset & \text{otherwise.} \end{cases}$$

From these descriptions, we can directly work out $S_p(L_n)$ and $\mathfrak{R}_p(L_n)$ for every prime p and even natural number n.

First step towards $S_p(L_n)$ – $S_p^{\mathcal{H}_p}(L_n)$ and $S_p^{\mathcal{E}_p}(L_n)$

Proposition (Brazelton, Harrington, L., Wong '21)

Suppose that $p \equiv 3 \pmod 4$. Then the hyperbolic and elliptic sums are given by

$$S_p^{\mathcal{H}_p}(L_n) = \begin{cases} 2 & \text{if } (p-1) \mid n; \\ 1 & \text{otherwise.} \end{cases}$$

$$S_p^{\mathcal{E}_p}(L_n) = \begin{cases} 1 & \text{if } \frac{2(p+1)}{\delta} \neq 1 \text{ is odd}; \\ -1 & \text{if } \left(2 \mid\mid \frac{2(p+1)}{\delta} \text{ and } \frac{2(p+1)}{\delta} \neq 2\right); \\ 2 & \text{if } \delta = 2(p+1); \\ -2 & \text{if } \delta = p+1; \\ 0 & \text{if } 4 \mid \frac{2(p+1)}{\delta}. \end{cases}$$

We'll outline the elliptic case as the hyperbolic case is similar and simpler.

Proof of $S_p^{\mathcal{E}_p}(L_n)$

$$L_n(\mathcal{E}_p) = \left\{ (-1)^{n/2} \left(\zeta_{\frac{2(p+1)}{\delta}}^{b} + \zeta_{\frac{2(p+1)}{\delta}}^{-b} \right) : 1 \leq b \leq \frac{2(p+1)}{\delta} \text{ odd} \right\}$$

1. $\left(2 \nmid \frac{2(p+1)}{\delta}\right)$: $\frac{2(p+1)}{\delta}$ is odd, hence $4 \mid \delta$, and therefore $4 \mid n$, so $(-1)^{n/2} = 1$. The collection $\zeta_{\frac{2(p+1)}{\delta}}^{b} + \zeta_{\frac{2(p+1)}{\delta}}^{-b}$ runs over all powers of $\zeta_{\frac{2(p+1)}{\delta}}$, with $\zeta_{\frac{2(p+1)}{\delta}}^{\frac{2(p+1)}{\delta}}$ twice, hence

$$S_p^{\mathcal{E}_p}(L_n) = \left(\sum_{1 \leq a \leq \frac{2(p+1)}{\delta}} \zeta_{\frac{2(p+1)}{\delta}}^{a} \right) + \zeta_{\frac{2(p+1)}{\delta}}^{\frac{2(p+1)}{\delta}}$$

$$= \begin{cases} 0+1 & \text{if } \frac{2(p+1)}{\delta} \neq 1; \\ 1+1 & \text{if } \frac{2(p+1)}{\delta} = 1, \end{cases}$$

$$= \begin{cases} 1 & \text{if } \delta \neq 2(p+1); \\ 2 & \text{if } \delta = 2(p+1). \end{cases}$$

Proof of $S_p^{\mathcal{E}_p}(L_n)$ – Continued

2. $\left(2 \,||\, \frac{2(p+1)}{\delta}\right)$: In this case, $\frac{2(p+1)}{\delta}$ is even and since $2(p+1)$ is divisible by 8, we must have $4 \mid \delta$ again yielding $(-1)^{n/2} = 1$. This time we have only odd powers of $\zeta_{\frac{2(p+1)}{\delta}}$, including $\zeta_{\frac{2(p+1)}{\delta}}^{\frac{(p+1)}{\delta}} = -1$ twice. This yields

$$S_p^{\mathcal{E}_p}(L_n) = \left(\sum_{\substack{1 \le a \le \frac{2(p+1)}{\delta} \\ a \text{ odd}}} \zeta_{\frac{2(p+1)}{\delta}}^{a} \right) + \zeta_{\frac{2(p+1)}{\delta}}^{\frac{p+1}{\delta}} = \begin{cases} 0 + (-1) & \text{if } \frac{2(p+1)}{\delta} \neq 2; \\ -1 + (-1) & \text{if } \frac{2(p+1)}{\delta} = 2, \end{cases}$$

$$= \begin{cases} -1 & \text{if } \delta \neq p+1; \\ -2 & \text{if } \delta = p+1. \end{cases}$$

3. $\left(4 \mid \frac{2(p+1)}{\delta}\right)$: Neither $\frac{2(p+1)}{\delta}$ nor $\frac{(p+1)}{\delta}$ are odd. After a lemma on summing odd powers of ROU, the sum at hand is

$$S_p^{\mathcal{E}_p}(L_n) = \sum_{\substack{1 \le a \le \frac{2(p+1)}{\delta} \\ a \text{ odd}}} (-1)^{n/2} \zeta_{\frac{2(p+1)}{\delta}}^{a} = 0. \qquad \square$$

$p \equiv 3 \pmod 4$ – $S_p(L_n)$

Theorem (Brazelton, Harrington, L., Wong)

For $p \equiv 3 \pmod 4$,

$$S_p(L_n) = \begin{cases} 2 & \text{if } d = p-1 \text{ and } \left(\delta = 2(p+1) \text{ or } 4 \mid \frac{2(p+1)}{\delta}\right); \\ 1 & \text{if } d = p-1 \text{ and } \left(\frac{2(p+1)}{\delta} \neq 1 \text{ is odd or } \left(2 \mid\mid \frac{2(p+1)}{\delta} \text{ and } \frac{2(p+1)}{\delta} \neq 2\right)\right), \text{or } d \neq p-1 \text{ and } \left(\delta = 2(p+1) \text{ and } 4 \mid \frac{2(p+1)}{\delta}\right); \\ 0 & \text{if } d = p-1 \text{ and } \delta = p+1, \\ & \quad \text{or } d \neq p-1 \text{ and } \left(\frac{2(p+1)}{\delta} \neq 1 \text{ is odd} \right. \\ & \quad \left. \text{or } \left(2 \mid\mid \frac{2(p+1)}{\delta} \text{ and } \frac{2(p+1)}{\delta} \neq 2\right)\right); \\ -1 & \text{if } d \neq p-1 \text{ and } \delta = p+1. \end{cases}$$

$p \equiv 3 \pmod 4$ – $S_p(L_n)$

Theorem (Brazelton, Harrington, L., Wong)

For $p \equiv 3 \pmod 4$,

$$S_p(L_n) = \begin{cases} 2 & \text{if } d = p-1 \text{ and } \left(\delta = 2(p+1) \text{ or } 4 \mid \frac{2(p+1)}{\delta}\right); \\ 1 & \text{if } d = p-1 \text{ and } \left(\frac{2(p+1)}{\delta} \neq 1 \text{ is odd or } \left(2 \mid\mid \frac{2(p+1)}{\delta} \text{ and } \frac{2(p+1)}{\delta} \neq 2\right)\right), \text{or } d \neq p-1 \text{ and } \left(\delta = 2(p+1) \text{ and } 4 \mid \frac{2(p+1)}{\delta}\right); \\ 0 & \text{if } d = p-1 \text{ and } \delta = p+1, \\ & \quad \text{or } d \neq p-1 \text{ and } \left(\frac{2(p+1)}{\delta} \neq 1 \text{ is odd } \text{or } \left(2 \mid\mid \frac{2(p+1)}{\delta} \text{ and } \frac{2(p+1)}{\delta} \neq 2\right)\right); \\ -1 & \text{if } d \neq p-1 \text{ and } \delta = p+1. \end{cases}$$

To calculate $|\mathfrak{R}_p(L_n)|$, calculate the sizes of $L_n(\mathcal{H}_p)$, $L_n(\mathcal{E}_p)$, $L_n(\mathcal{H}_p) \cap L_n(\mathcal{E}_p)$ and use inclusion-exclusion

$p \equiv 1 \pmod 4$ – Images of $\mathcal{H}_p, \mathcal{E}_p, \mathcal{P}_p$

For $p \equiv 1 \pmod 4$, one has

$$L_n(\mathcal{H}_p) = \left\{ \zeta_{\frac{p-1}{d}}^{a} + \zeta_{\frac{p-1}{d}}^{-a} : 0 \leq a \leq \frac{p-1}{d},\ a \neq \frac{p-1}{4} \right\}$$

$$L_n(\mathcal{E}_p) = \left\{ \zeta_{\frac{2(p+1)}{\delta}}^{a} + \zeta_{\frac{2(p+1)}{\delta}}^{pa} : 1 \leq a \leq 2(p+1),\ a \text{ odd}, \right.$$
$$\left. a \neq \frac{p+1}{2}, \frac{3(p+1)}{2} \right\}$$

$$L_n(\mathcal{P}_p) = \begin{cases} \{-2\} & \text{if } n \equiv 2 \pmod 4; \\ \{2\} & \text{if } n \equiv 0 \pmod 4. \end{cases}$$

$p \equiv 1 \pmod 4$ – $S_p(L_n)$

Theorem (Brazelton, Harrington, L., Wong '21)

Let p be an odd prime, n an even natural number, $d = \gcd(p-1, n)$, $\delta = \gcd(2(p+1), n)$, and 2^h the highest power of 2 dividing $p-1$. For $p \equiv 1 \pmod 4$,

$$S_p(L_n) = \begin{cases} 2 & \text{if } (p^2-1) \mid n; \\ 1 & \text{if } (2 \,||\, \delta \text{ and } \delta \neq p+1), \\ & \quad \text{or } (d = p-1 \text{ and } \delta \neq 2(p+1)), \\ & \quad \text{or } \left(2^h \mid d,\ d \neq p-1 \text{ and } \delta = 2(p+1)\right); \\ 0 & \text{if } \delta = p+1, \\ & \quad \text{or } \left(2^h \mid d,\ d \neq p-1 \text{ and } \delta \neq 2(p+1)\right), \\ & \quad \text{or } \left(4 \mid d,\ 2^h \nmid d,\ \text{and } \delta = 2(p+1)\right); \\ -1 & \text{if } 4 \mid d,\ 2^h \nmid d,\ \text{and } \delta \neq 2(p+1). \end{cases}$$

Thank You!

Possible values for $S_7(L_n)$ and $S_{29}(L_n)$

d	δ	$S_7(L_n)$
2	2	1
2	4	1
2	8	-1
2	16	1

d	δ	$S_7(L_n)$
6	2	2
6	4	2
6	8	0
6	16	2

d	δ	$S_{29}(L_n)$
2	2	1
2	6	1
2	10	1
2	30	0
4	4	0
4	12	0
4	20	0
4	60	1

d	δ	$S_{29}(L_n)$
14	2	1
14	6	1
14	10	1
14	30	0
28	4	1
28	12	1
28	20	1
28	60	2