1. Introduction

Let $p$ be an odd prime. Among the nonzero numbers in $\mathbb{F}_p$, half are squares and half are nonsquares. The former are called quadratic residues and the latter are called quadratic nonresidues. We do not consider 0 to be a quadratic residue or nonresidue, even though it is of course a square.

If $a$ is a quadratic residue in $\mathbb{F}_p^\times$, is $a + 1$ more or less likely to be a quadratic residue? If $a$ is a quadratic nonresidue in $\mathbb{F}_p^\times$, is $a + 1$ more or less likely to be a quadratic nonresidue?

Let’s look at some data.

**Example 1.1.** Taking $p = 19$, the 9 quadratic residues are 1, 4, 5, 6, 7, 9, 11, 16, 17, and the 9 quadratic nonresidues are 2, 3, 8, 10, 12, 13, 14, 15, 18. In the table below we indicate when $a$ and $a + 1$ are quadratic residues (QR) for $a \in \mathbb{F}_19^\times$.

<table>
<thead>
<tr>
<th>$a$</th>
<th>QR?</th>
<th>$a + 1$ is QR?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>7</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>9</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>11</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>12</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>13</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>14</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>15</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>16</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>17</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>18</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

There are 17 pairs $(a,a + 1)$ where $a$ and $a + 1$ are nonzero in $\mathbb{F}_19$ (all $a$ aside from 0 and 18). The table above tells us that 4 pairs have $a$ and $a + 1$ as quadratic residues ($a = 4, 5, 6, 16$), 5 pairs have $a$ as a quadratic residue and $a + 1$ as a quadratic nonresidue ($a = 1, 7, 9, 11, 17$), 4 pairs have $a$ as a quadratic nonresidue and $a + 1$ as a quadratic residue ($a = 3, 8, 10, 15$), and 4 pairs have $a$ and $a + 1$ as quadratic nonresidues ($a = 2, 12, 13, 14$, noting 18 doesn’t count since $18 + 1 = 0$). The four options for $a$ and $a + 1$ to be quadratic residues or nonresidues are approximately equally likely (around 25% each).

**Example 1.2.** When $p = 101$, there are 99 pairs $(a,a + 1)$ where $a$ and $a + 1$ are nonzero in $\mathbb{F}_{101}$ (all $a \neq 0, 100$). Among these pairs, $a$ and $a + 1$ are quadratic residues 24 times, $a$ is a quadratic residue and $a + 1$ is a quadratic nonresidue 25 times, $a$ is a quadratic nonresidue and $a + 1$ is a quadratic residue 25 times, and $a$ and $a + 1$ are quadratic nonresidues 25 times. These counts are equal or nearly equal.

There are 98 triples $(a,a + 1,a + 2)$ where $a$, $a + 1$, and $a + 2$ are nonzero in $\mathbb{F}_{101}^\times$: all $a$ aside from 0, 99, and 100. Using + to denote a quadratic residue and − to denote a quadratic nonresidue, the following table says the frequency of the quadratic residue patterns among the triples $(a,a + 1,a + 2)$ in $\mathbb{F}_{101}^\times$ is nearly uniform.

<table>
<thead>
<tr>
<th>$(a,a + 1,a + 2)$</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>(+,+,+)</td>
<td>12</td>
</tr>
<tr>
<td>(+,+,−)</td>
<td>12</td>
</tr>
<tr>
<td>(+,−,+),−</td>
<td>12</td>
</tr>
<tr>
<td>(−,+)+</td>
<td>12</td>
</tr>
</tbody>
</table>

**Example 1.3.** The tables below count how many pairs $(a,a + 1)$ and triples $(a,a + 1,a + 2)$ in $\mathbb{F}_{1009}^\times$ have different quadratic residue patterns. The counts look nearly uniform in each case.
\[
\begin{array}{c|cccc}
(a, a+1) & (+,+) & (+,-) & (-,+) & (-,-) \\
\hline
\text{Count} & 251 & 252 & 252 & 252 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
(a, a+1, a+2) & (+,+,+) & (+,+-) & (-,+-) & (-,+,+) \\
\hline
\text{Count} & 128 & 122 & 122 & 122 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
(a, a+1, a+2) & (+,-,-) & (-,+-) & (-,-+) & (-,-,-) \\
\hline
\text{Count} & 130 & 130 & 130 & 122 \\
\end{array}
\]

These examples suggest that the possible quadratic residue patterns of a fixed length in \(F_p^\times\) are approximately equally likely. For a set of \(r\) consecutive numbers in \(F_p^\times\), allowing for \(2^r\) choices of their quadratic residue or nonresidue status, we will show the frequency of each quadratic residue pattern is nearly \(p/2^r\), which is what we’d expect if we were discussing \(r\) independent random variables on \(F_p\) that each have two outcomes.

2. The main theorem

For \(r \geq 1\) and an odd prime \(p > r\), we want to count how many \(r\)-tuples of consecutive numbers \(a, a+1, \ldots, a+r-1\) in \(F_p^\times\) have predetermined quadratic residue or nonresidue behavior. (We need \(p > r\) so that \(F_p^\times\) contains at least \(r\) elements.) We will use the Legendre symbol. For a choice of \(r\) signs \(\varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}\), set

\[
N_p(\varepsilon_1, \ldots, \varepsilon_r) = \left| \left\{ a \in F_p^\times : \left( \frac{a}{p} \right) = \varepsilon_1, \left( \frac{a+1}{p} \right) = \varepsilon_2, \ldots, \left( \frac{a+r-1}{p} \right) = \varepsilon_r \right\} \right|
\]

In the tables in Examples 1.2 and 1.3, the + corresponds to Legendre symbol 1 and the − corresponds to Legendre symbol −1. For instance, Example 1.2 tells us that \(N_{101}(1, 1, 1) = 12\) and \(N_{101}(1, -1, -1) = 13\). Here is the main result.

**Theorem 2.1.** For \(r\) signs \(\varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}\) and an odd prime \(p > r\), \(N_p(\varepsilon_1, \ldots, \varepsilon_r) = p/2^r + O_r(\sqrt{p})\). More precisely,

\[
\left| N_p(\varepsilon_1, \ldots, \varepsilon_r) - \frac{p}{2^r} \right| < (r-1)\sqrt{p} + \frac{r}{2}.
\]

**Proof.** We will write down a formula for \(N_p(\varepsilon_1, \ldots, \varepsilon_r)\) in terms of a sum of Legendre symbol products, extract the main term \(p/2^r\), and bound what is left.

We begin with a counting formula. For \(b \in F_p^\times\) and \(\varepsilon = \pm 1\),

\[
1 + \varepsilon \left( \frac{b}{p} \right) = \begin{cases} 
2, & \text{if } \left( \frac{b}{p} \right) = \varepsilon, \\
0, & \text{if } \left( \frac{b}{p} \right) \neq \varepsilon,
\end{cases}
\]

so

\[
\frac{1}{2} \left( 1 + \varepsilon \left( \frac{b}{p} \right) \right) = \begin{cases} 
1, & \text{if } \left( \frac{b}{p} \right) = \varepsilon, \\
0, & \text{if } \left( \frac{b}{p} \right) \neq \varepsilon.
\end{cases}
\]

Therefore if \(b_1, \ldots, b_r \in F_p^\times\) and \(\varepsilon_1, \ldots, \varepsilon_r \in F_p^\times\),

\[
\prod_{i=1}^r \frac{1}{2} \left( 1 + \varepsilon_i \left( \frac{b_i}{p} \right) \right) = \begin{cases} 
1, & \text{if } \left( \frac{b_i}{p} \right) = \varepsilon_i \text{ for all } i \in \{1, \ldots, r\}, \\
0, & \text{if } \left( \frac{b_i}{p} \right) \neq \varepsilon_i \text{ for some } i \in \{1, \ldots, r\}.
\end{cases}
\]
\[ N_p(\varepsilon_1, \ldots, \varepsilon_r) = \left| \left\{ a \in \mathbb{F}_p^\times : \left( \frac{a + i - 1}{p} \right) = \varepsilon_i \text{ for } i = 1, \ldots, r \right\} \right| \]

\[ = \sum_{a \in \mathbb{F}_p} \prod_{i=1}^{r} \frac{1}{2} \left( 1 + \varepsilon_i \left( \frac{a + i - 1}{p} \right) \right). \]

What can we say about missing terms in the outer sum, where \( a + j - 1 = 0 \) in \( \mathbb{F}_p \) for some \( j \in \{1, \ldots, r\} \)? Then \( \frac{1}{2} \left( 1 + \varepsilon_j \left( \frac{a + j - 1}{p} \right) \right) = \frac{1}{2} \) while \( \frac{1}{2} \left( 1 + \varepsilon_i \left( \frac{a + i - 1}{p} \right) \right) \) is 0 or 1 for \( i \neq j \), so

\[ \left| \prod_{i=1}^{r} \frac{1}{2} \left( 1 + \varepsilon_i \left( \frac{a + i - 1}{p} \right) \right) \right| \leq \frac{1}{2}. \]

There are \( r \) such terms (corresponding to \( a = 0, a = -1, \ldots, a = -(r - 1) \) in \( \mathbb{F}_p \)), so

\[ N_p(\varepsilon_1, \ldots, \varepsilon_r) = \sum_{a \in \mathbb{F}_p} \prod_{i=1}^{r} \frac{1}{2} \left( 1 + \varepsilon_i \left( \frac{a + i - 1}{p} \right) \right) + \frac{e_r}{2}, \quad \text{where } |e_r| \leq r, \]

\[ = \frac{1}{2^r} \sum_{a \in \mathbb{F}_p} \prod_{i=1}^{r} \left( 1 + \varepsilon_i \left( \frac{a + i - 1}{p} \right) \right) + \frac{e_r}{2}. \]

Let’s expand the product inside the sum: for each \( a \in \mathbb{F}_p \),

\[ \prod_{i=1}^{r} \left( 1 + \varepsilon_i \left( \frac{a + i - 1}{p} \right) \right) = 1 + \sum_{S \subseteq \{1, \ldots, r\}} \left( \prod_{i \in S} \varepsilon_i \right) \left( \frac{f_S(a)}{p} \right), \]

where \( f_S(x) = \prod_{i \in S} (x + i - 1) \). The polynomial \( f_S(x) \in \mathbb{F}_p[x] \) is separable with degree \( |S| \). Feeding the above expression for the product into the formula for \( N_p(\varepsilon_1, \ldots, \varepsilon_r) \) and swapping the order of summation,

\[ N_p(\varepsilon_1, \ldots, \varepsilon_r) = \frac{1}{2^r} \sum_{a \in \mathbb{F}_p} \left( 1 + \sum_{S \subseteq \{1, \ldots, r\}} \left( \prod_{i \in S} \varepsilon_i \right) \left( \frac{f_S(a)}{p} \right) \right) + \frac{e_r}{2}, \]

\[ = \frac{p}{2^r} + \frac{1}{2^r} \sum_{S \subseteq \{1, \ldots, r\}} \left( \prod_{i \in S} \varepsilon_i \right) \sum_{a \in \mathbb{F}_p} \left( \frac{f_S(a)}{p} \right) + \frac{e_r}{2}. \]

We have found the desired term \( p/2^r \) in the formula for \( N_p(\varepsilon_1, \ldots, \varepsilon_r) \) and want to show the rest of the formula is small.\(^1\)

\(^1\)This technique of relating \( N_p(\varepsilon_1, \ldots, \varepsilon_r) \) to \( p/2^r \) goes back at least to Jacobsthal in 1906 when \( r = 2 \) [6, p. 27]. For a more recent account of it, see replies to the MathOverflow post “Consecutive non-quadratic residues” at [https://mathoverflow.net/questions/161271/consecutive-non-quadratic-residues].
The product $\prod_{i \in S} \epsilon_i$ is $\pm 1$, so by the triangle inequality

$$\left| N_p(\epsilon_1, \ldots, \epsilon_r) - \frac{p}{2^r} \right| \leq \frac{1}{2^r} \sum_{S \subseteq \{1, \ldots, r\}} \left| \sum_{a \in \mathbb{F}_p} \left( \frac{f_S(a)}{p} \right) \right| + \frac{r}{2}. \tag{2.2}$$

The inner sum over $\mathbb{F}_p$ on the right side can be estimated with Weil’s bound, which says in a special case that for nonconstant $f(x) \in \mathbb{F}_p[x]$ having no repeated roots (that is, are separable),

$$\left| \sum_{a \in \mathbb{F}_p} \left( \frac{f(a)}{p} \right) \right| \leq (\deg f - 1)\sqrt{p}. \tag{2.3}$$

(This inequality is an equality if $\deg f = 1$, and generally is a strict inequality if $\deg f \geq 2$.) Applying (2.3) to the polynomials $f_S(x)$, which each have no repeated roots, we get

$$\left| \sum_{a \in \mathbb{F}_p} \left( \frac{f_S(a)}{p} \right) \right| \leq (\deg f_S - 1)\sqrt{p} = (|S| - 1)\sqrt{p} \leq (r - 1)\sqrt{p}.$$  

This upper bound is independent of $S$, so feeding it into (2.2) gives us

$$\left| N_p(\epsilon_1, \ldots, \epsilon_r) - \frac{p}{2^r} \right| \leq \frac{1}{2^r} \sum_{S \subseteq \{1, \ldots, r\} \setminus \emptyset} ((r - 1)\sqrt{p}) + \frac{r}{2} = \frac{1}{2^r} (2^r - 1)(r - 1)\sqrt{p} + \frac{r}{2} < (r - 1)\sqrt{p} + \frac{r}{2}.$$  

For each $r$, the count $N_p(\epsilon_1, \ldots, \epsilon_r) = p/2^r + O_r(\sqrt{p})$ tends to $\infty$ as $p \to \infty$, so in particular $N_p(\epsilon_1, \ldots, \epsilon_r) \geq 1$ for all large $p$. We can determine the largest prime modulo which there are not $r$ consecutive quadratic residues mod $p$ by setting $N_p(1,1,\ldots,1) = 0$ in Theorem 2.1 to get an upper bound on the possible $p$.

**Example 2.2.** What is the largest prime $p$ for which there are not 3 consecutive quadratic residues mod $p$? This is asking when $N_p(1,1,1) = 0$. The bound in Theorem 2.1 implies $p/8 < 2\sqrt{p} + 3/2$, so $p < 16\sqrt{p} + 12$. That implies $p < 279.4$, so $p \leq 277$. Checking all primes up to 277, the last one without 3 consecutive quadratic residues is $p = 17$.

That there are three consecutive quadratic residues modulo $p$ for $p \geq 19$ is due to Jacobsthal [6, p. 30].

The proof of Theorem 2.1 can be used to count quadratic residue patterns with gaps that are not necessarily consecutive: if $p > r$ and $c_1, \ldots, c_r$ are distinct in $\mathbb{F}_p$, the set

$$\left\{ a \in \mathbb{F}_p^\times : \left( \frac{a + c_i}{p} \right) = \epsilon_i \text{ for } i = 1, \ldots, r \right\}$$

for each choice of signs $\epsilon_1, \ldots, \epsilon_r \in \{\pm 1\}$ has a size $N_p$, say, that satisfies the same estimate as in Theorem 2.1:

$$\left| N_p - \frac{p}{2^r} \right| < (r - 1)\sqrt{p} + \frac{r}{2}.$$
The only change needed in the proof of Theorem 2.1 is to replace the polynomial \( f_S(x) = \prod_{i \in S}(x + i - 1) \) with \( \prod_{i \in S}(x + c_i) \).

The Weil bound (2.3) extends to all finite fields, not just those of odd prime order \( p \), with the Legendre symbol on \( \mathbb{F}_p \) replaced by a nontrivial multiplicative character on \( \mathbb{F}_q \) and \( \sqrt{p} \) in the Weil bound replaced by \( \sqrt{q} \). In particular, for an odd prime power \( q \), if \( \chi \) is the quadratic character on \( \mathbb{F}_q^\times \) then for distinct \( c_1, \ldots, c_r \) in \( \mathbb{F}_q \) and any signs \( \varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\} \),

\[
N_q := \left| \left\{ a \in \mathbb{F}_q^\times : \chi(a + c_i) = \varepsilon_i \text{ for } i = 1, \ldots, r \right\} \right|
\]

satisfies

\[
\left| N_q - \frac{q}{2r} \right| < (r - 1)\sqrt{q} + \frac{r}{2}.
\]

3. Some history

The first work on counting quadratic residue patterns of two or more consecutive terms in \( \mathbb{F}_p^\times \) was by Aladov [1] in 1896. He counted each quadratic residue pattern of length 2 and, for \( p \equiv 3 \mod 4 \), the number of length 2 imply \( N(p)(\varepsilon_2) = p/4 + O(1) \). In 1898, Sterneck [8] counted patterns of length 3 and 4 with restrictions (each pattern was counted together with its opposite, e.g., \((+, +, -)\) and \((- - +, +)\) together, not separate). In 1906, Jacobsthal [6, Chap. III] in his dissertation found exact formulas for the number of quadratic residue patterns of length 2 and 3 in \( \mathbb{F}_p^\times \). The length 3 counts imply \( N_p(\varepsilon_1, \varepsilon_2, \varepsilon_3) = p/8 + O(\sqrt{p}) \).

Davenport considered this counting problem for \( r \geq 4 \) throughout the 1930s. In [2] he bounded the error \( |N_p(\varepsilon_1, \ldots, \varepsilon_r) - p/2^r| \) as \( O_r(p^{3/4}) \) for \( r = 4 \) and 5 by ad hoc methods that did not extend easily to \( r \geq 6 \). In [3] he used other tricks for \( 6 \leq r \leq 9 \) that led to error bounds \( O_r(p^7/8) \) for \( r = 6 \) and 7, and \( O_r(p^{19/20}) \) for \( r = 8 \) and 9, and he could reduce the error bound when \( r = 4 \) from \( O_r(p^{3/4}) \) to \( O_r(p^{2/3}) \). Reducing the exponent on \( p \) in the error bound is closely related to bounding the real parts of the zeros of the zeta-function of curves \( y^2 = f(x) \) over \( \mathbb{F}_p \). Davenport continued to refine his techniques throughout the 1930s, and in [4, Theorem 5] he got an error bound of the form \( O_r(p^{1-\theta_r}) \) for general \( r \) with an explicit formula for \( \theta_r \) that tends to 0 as \( r \to \infty \). A definitive error bound \( O_r(\sqrt{p}) \) for all \( r \), coming from the bound in (2.3), was given by Weil [9] (see also [5, Theorem 3.1]) after he proved the Riemann hypothesis for curves over finite fields.

An account of the work by Davenport, along with how it influenced Hasse and Mordell, is in [7, Sect. 3].

Appendix A. Extending Theorem 2.1 beyond the Legendre symbol

The Weil bound (2.3) for the Legendre symbol on \( \mathbb{F}_p \) has a generalization to other multiplicative characters on finite fields: if \( \chi \) is a nontrivial multiplicative character on \( \mathbb{F}_q \) with order \( n \geq 2 \) and \( f(x) \in \mathbb{F}_q[x] \) is monic and not an \( n \)-th power, then

\[
(A.1) \quad \left| \sum_{a \in \mathbb{F}_q} \chi(f(a)) \right| \leq (r - 1)\sqrt{q},
\]

where \( f(x) \) has \( r \) distinct roots (the roots need not be simple) in a splitting field over \( \mathbb{F}_q \).

\( ^2 \)In [5] it is assumed for (A.1) that \( f(x) \) is not an \( n \)-th power but it is not explicitly stated that \( f(x) \) is not monic too. For non-monic \( f \) we get counterexamples to (A.1): if \( f(x) = cg(x)^n \) with \( c \in \mathbb{F}_q^\times \) not an
Using (A.1) we will prove the following generalization of Theorem 2.1.

**Theorem A.1.** Let $\chi_1, \ldots, \chi_r$ be nontrivial multiplicative characters on $\mathbf{F}_q$, where $\chi_i$ has order $n_i \geq 2$. For $r < q$, pick distinct $c_1, \ldots, c_r$ in $\mathbf{F}_q$ and an $n_i$-th root of unity $\varepsilon_i$ in $\mathbf{C}$ for $i = 1, \ldots, r$. Set

$$N_q = \{|a \in \mathbf{F}_q : \chi_i(a + c_i) = \varepsilon_i \text{ for } i = 1, \ldots, r\}|.$$

Then

$$|N_q - \frac{q}{n_1 \ldots n_r}| < (r - 1)\sqrt{q} + \frac{r}{2}.$$

When $q = p$ and all $\chi_i$ are quadratic ($n_i = 2$ for all $i$), Theorem A.1 becomes Theorem 2.1.

We take $r < q$ in Theorem A.1 because if $r \geq q$ then for each $a \in \mathbf{F}_q$ the numbers $a + c_1, \ldots, a + c_r$ fill up $\mathbf{F}_q$ so one of these is 0, and thus $N_q = 0$, which is uninteresting.

**Proof.** For $b \in \mathbf{F}_q^\times$, a nontrivial multiplicative character $\chi$ on $\mathbf{F}_q^\times$ of order $n$, and an $n$-th root of unity $\varepsilon$ in $\mathbf{C}$, the finite geometric series of $n$ terms with ratio $\varepsilon$ equals

$$1 + \frac{\chi(b)}{\varepsilon} + \left(\frac{\chi(b)}{\varepsilon}\right)^2 + \cdots + \left(\frac{\chi(b)}{\varepsilon}\right)^{n-1} = \begin{cases} n, & \text{if } \chi(b) = \varepsilon, \\ 0, & \text{if } \chi(b) \neq \varepsilon, \end{cases}$$

so

$$\frac{1}{n} \left(1 + \frac{\chi(b)}{\varepsilon} + \left(\frac{\chi(b)}{\varepsilon}\right)^2 + \cdots + \left(\frac{\chi(b)}{\varepsilon}\right)^{n-1}\right) = \begin{cases} 1, & \text{if } \chi(b) = \varepsilon, \\ 0, & \text{if } \chi(b) \neq \varepsilon, \end{cases}$$

which generalizes (2.1). Therefore

$$N_q = \sum_{a \in \mathbf{F}_q} \prod_{i=1}^r \frac{1}{n_i} \left(1 + \frac{\chi_i(a + c_i)}{\varepsilon_i} + \left(\frac{\chi_i(a + c_i)}{\varepsilon_i}\right)^2 + \cdots + \left(\frac{\chi_i(a + c_i)}{\varepsilon_i}\right)^{n_i-1}\right).$$

This sum over $\mathbf{F}_q$ is missing terms at those $a$ for which $a + c_j = 0$ for some $j$. For such an $a$, the product over $1 \leq i \leq r$ associated to it in the above formula would be 0 or $1/n_j$, so we can write $N_q$ as a sum over all of $\mathbf{F}_q$ by including an additional error term:

$$N_q = \sum_{a \in \mathbf{F}_q} \prod_{i=1}^r \frac{1}{n_i} \left(1 + \frac{\chi_i(a + c_i)}{\varepsilon_i} + \left(\frac{\chi_i(a + c_i)}{\varepsilon_i}\right)^2 + \cdots + \left(\frac{\chi_i(a + c_i)}{\varepsilon_i}\right)^{n_i-1}\right) + e$$

$$= \frac{1}{n_1 \cdots n_r} \sum_{a \in \mathbf{F}_q} \prod_{i=1}^r \left(1 + \frac{\chi_i(a + c_i)}{\varepsilon_i} + \left(\frac{\chi_i(a + c_i)}{\varepsilon_i}\right)^2 + \cdots + \left(\frac{\chi_i(a + c_i)}{\varepsilon_i}\right)^{n_i-1}\right) + e,$$

where $|e| \leq 1/n_1 + \cdots + 1/n_r \leq r/2$ (since $n_i \geq 2$). Multiplying out all the sums,

$$N_q = \frac{1}{n_1 \cdots n_r} \sum_{a \in \mathbf{F}_q} \sum_{0 \leq t_i \leq n_i - 1} \frac{\chi_1(a + c_1)^{t_1} \cdots \chi_r(a + c_r)^{t_r}}{\varepsilon_1^{t_1} \cdots \varepsilon_r^{t_r}} + e$$

$$= \frac{1}{n_1 \cdots n_r} \sum_{0 \leq t_i \leq n_i - 1} \frac{1}{\varepsilon_1^{t_1} \cdots \varepsilon_r^{t_r}} \sum_{a \in \mathbf{F}_q} \chi_1(a + c_1)^{t_1} \cdots \chi_r(a + c_r)^{t_r} + e.$$
The inner term when all \( t_i \) are 0 is \( \sum_{a \in \mathbb{F}_q} 1 = q \), so
\[
\left| N_q - \frac{q}{n_1 \cdots n_r} \right| \leq \frac{1}{n_1 \cdots n_r} \sum_{0 \leq t_i \leq n_i - 1} \sum_{r \in \mathbb{F}_q} \chi_1(a + c_1)^{t_1} \cdots \chi_r(a + c_r)^{t_r} + \frac{r}{2}.
\]

We will use (A.1) to show each inner sum over \( \mathbb{F}_q \) on the right side has magnitude at most \((r - 1)\sqrt{q}\), which would give us what we want:
\[
\left| N_q - \frac{q}{n_1 \cdots n_r} \right| \leq \frac{1}{n_1 \cdots n_r} \sum_{0 \leq t_i \leq n_i - 1} \sum_{r \in \mathbb{F}_q} ((r - 1)\sqrt{q}) + \frac{r}{2}
\]
\[
= \frac{1}{n_1 \cdots n_r} (n_1 \cdots n_r - 1)(r - 1)\sqrt{q} + \frac{r}{2}
\]
\[
< (r - 1)\sqrt{q} + \frac{r}{2}.
\]

It remains to show
\[
\left| \sum_{a \in \mathbb{F}_q} \chi_1(a + c_1)^{t_1} \cdots \chi_r(a + c_r)^{t_r} \right| \leq (r - 1)\sqrt{q}
\]
when \( 0 \leq t_i \leq n_i - 1 \) with some \( t_i \) not 0. Since \( \mathbb{F}_q^\times \) is cyclic, its character group is cyclic: let \( \chi \) be a generator of the character group of \( \mathbb{F}_q^\times \) and write \( \chi_i = \chi^{m_i} \) for \( m_i \in \mathbb{Z}^+ \). Then
\[
\sum_{a \in \mathbb{F}_q} \chi_1(a + c_1)^{t_1} \cdots \chi_r(a + c_r)^{t_r} = \sum_{a \in \mathbb{F}_q} \chi(a + c_1)^{t_1 m_1} \cdots \chi(a + c_r)^{t_r m_r}
\]
\[
= \sum_{a \in \mathbb{F}_q} \chi((a + c_1)^{t_1 m_1} \cdots (a + c_r)^{t_r m_r})
\]
\[
= \sum_{a \in \mathbb{F}_q} \chi(f(a)),
\]
where \( f(x) = (x + c_1)^{t_1 m_1} \cdots (x + c_r)^{t_r m_r} \). This polynomial is monic with \( r \) distinct roots. In order to apply (A.1) to bound \( |\sum_{a \in \mathbb{F}_q} \chi(f(a))| \), all that remains to be checked is that \( f(x) \) is not a \((q - 1)\)-th power in \( \mathbb{F}_q[x] \) (since \( \chi \) has order \( q - 1 \)). That is equivalent, since \( f \) is monic, to the root multiplicities \( t_1 m_1, \ldots, t_r m_r \) not all being multiples of \( q - 1 \).

Having \( (q - 1) | t_i m_i \) is the same as having \( (q - 1)/(q - 1, m_i) | t_i \) since \( (q - 1)/(q - 1, m_i) \) and \( m_i/(q - 1, m_i) \) are relatively prime. The order of \( \chi \) is \( q - 1 \) and the order of \( \chi_i \) is \( n_i \), so from \( \chi_i = \chi^{m_i} \) we get \( n_i = (q - 1)/(q - 1, m_i) \). Therefore \( (q - 1) | t_i m_i \) is equivalent to \( n_i | t_i \). Recalling that \( 0 \leq t_i \leq n_i - 1 \), we can have \( n_i | t_i \) only if \( t_i = 0 \). Since some \( t_i \) is not 0 this completes the proof that \( f(x) \) is not an \( n \)-th power.

\[ \square \]

**References**


