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 \( a \in \mathbb{F}_{19}^\times \).

| \( a \) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|-------|---|---|---|---|---|---|---|---|---|-----|-----|-----|-----|-----|-----|-----|-----|
| \( a \) is QR? | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| \( a + 1 \) is QR? | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |

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 \((a = 2, 12, 13, 14, \text{noting 18 doesn’t count since } 18 + 1 = 0)\). 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>(+, +, +)</th>
<th>(+, +, -)</th>
<th>(+, -, +)</th>
<th>(-, +, +)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( (a, a + 1, a + 2) )</th>
<th>(+, -, -)</th>
<th>(-, -, -)</th>
<th>(−, −, +)</th>
<th>(−, +, −)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>13</td>
<td>12</td>
<td>13</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.
\[
\begin{array}{c|cccc}
(a, a + 1) & (+, +) & (+, -) & (-, +) & (-, -) \\
\text{Count} & 251 & 252 & 252 & 252 \\
\hline
(a, a + 1, a + 2) & (+, +, +) & (+, +, -) & (+, -, +) & (-, +, +) \\
\text{Count} & 128 & 122 & 122 & 122 \\
(a, a + 1, a + 2) & (+, -, -) & (-, +, -) & (-, -, +) & (-, -, -) \\
\text{Count} & 130 & 130 & 130 & 122 \\
\end{array}
\]

These examples suggest that the possible quadratic residue patterns of a fixed length in \( \mathbb{F}_p^\times \) are approximately equally likely. For a set of \( r \) consecutive numbers in \( \mathbb{F}_p^\times \), 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 \( \mathbb{F}_p \) 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 \( \mathbb{F}_p^\times \) have predetermined quadratic residue or nonresidue behavior. (We need \( p > r \) so that \( \mathbb{F}_p^\times \) 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

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

\[
= \left\{ a \in \mathbb{F}_p^\times : \left( \frac{a + i - 1}{p} \right) = \varepsilon_i \text{ for } i = 1, \ldots, r \right\}.
\]

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 \( b \in \mathbb{F}_p^\times \) 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 \( b_1, \ldots, b_r \in \mathbb{F}_p^\times \) and \( \varepsilon_1, \ldots, \varepsilon_r \in \mathbb{F}_p^\times \),

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

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

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 $\prod_{i \in S} \varepsilon_i$ is $\pm 1$, so by the triangle inequality

\[(2.2) \quad \left| N_p(\varepsilon_1, \ldots, \varepsilon_r) - \frac{p}{2^r} \right| \leq \frac{1}{2^r} \sum_{S \subset \{1, \ldots, r\}} \left| \sum_{a \in F_p} \left( \frac{f_S(a)}{p} \right) \right| + \frac{r}{2}.\]

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

\[(2.3) \quad \left| \sum_{a \in F_p} \left( \frac{f(a)}{p} \right) \right| \leq (\deg f - 1)\sqrt{p}.\]

(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

\[\left| \sum_{a \in F_p} \left( \frac{f_S(a)}{p} \right) \right| \leq (\deg f_S - 1)\sqrt{p} = (|S| - 1)\sqrt{p} \leq (r - 1)\sqrt{p}.\]

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

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

\[= \frac{1}{2^r} (2^r - 1)(r - 1)\sqrt{p} + \frac{r}{2} \]

\[< (r - 1)\sqrt{p} + \frac{r}{2}. \quad \Box\]

For each $r$, the count $N_p(\varepsilon_1, \ldots, \varepsilon_r) = p/2^r + O_r(\sqrt{p})$ tends to $\infty$ as $p \to \infty$, so in particular $N_p(\varepsilon_1, \ldots, \varepsilon_r) \geq 1$ 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.** We will show for all odd primes $p$ that $N_p(1, -1) \geq 1$. By Theorem 2.1,

\[\left| N_p(1, -1) - \frac{p}{4} \right| < \sqrt{p} + 1.\]

If $N_p(1, -1) = 0$ then we have $p < 4(\sqrt{p} + 1)$. The only positive solution to $t = 4(\sqrt{t} + 1)$ is around 23.313, so $p < 4(\sqrt{p} + 1)$ for $p \leq 23$ and not for $p \geq 29$. Thus $N_p(1, -1) \geq 1$ when $p \geq 29$. For the primes $p = 3, 5, \ldots, 23$ we can do a direct search: for $p \leq 19$, the sign pattern $(\frac{a}{p}) = 1$ and $(\frac{a+1}{p}) = -1$ holds for $a = 1$ or $a = 2$, and for $p = 23$ we get that pattern for $a = 4$.

For similar reasons, $N_p(\varepsilon_1, \varepsilon_2) \geq 1$ when $p \geq 7$ no matter what the signs $\varepsilon_1$ and $\varepsilon_2$ are: it holds for $p \geq 29$ as above and a direct search for $p = 7, 11, \ldots, 23$ shows each consecutive quadratic residue pattern $(1, 1), (-1, 1), \text{ and } (-1, -1)$ occurs at least once. These three patterns don’t occur for $p = 3$ and $(1, 1)$ also doesn’t occur for $p = 5$.

That $N_p(1, 1) \geq 1$ for $p \geq 7$ can be proved using an argument by contradiction instead of a formula for $N_p(1, 1)$. We’ll show $(1, 2), (4, 5), \text{ or } (9, 10)$ is a pair of consecutive squares mod $p$. Since $(\frac{1}{p}) = 1$ and $(\frac{4}{p}) = 1$, if $2$ and $5$ are not squares mod $p$ then $(\frac{9}{p}) = -1$ and
\((\frac{5}{p}) = -1\) since \(p > 5\). Therefore \((\frac{2}{p}) = 1\) and \((\frac{-10}{p}) = (\frac{2}{p})(\frac{5}{p}) = (-1)(-1) = 1\). This kind of reasoning can’t be used to prove \(N_p(1, -1), N_p(1, 1), \) or \(N_p(-1, -1)\) since each initial interval of integers \(\{1, 2, \ldots, n\}\) is entirely quadratic residues mod \(p\) for some prime \(p\). For example, \((\frac{3}{p}) = 1\) for \(a \leq 20\) when \(p\) is the prime number 193993801.

**Example 2.3.** What is the largest prime \(p\) for which there are not 3 consecutive quadratic residues mod \(p\)? This is asking for the largest \(p\) such that \(N_p(1, 1, 1) = 0\). 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 \(F_p\), the set

\[
\left\{ a \in F_p^\times : \left(\frac{a+c_i}{p}\right) = \varepsilon_i \text{ for } i = 1, \ldots, r \right\}
\]

for each choice of signs \(\varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}\) has a size \(N_p\), say, that satisfies the same estimate as in Theorem 2.1:

\[
|N_p - \frac{p}{2^r}| < (r - 1)\sqrt{p} + \frac{r}{2}.
\]

The only change needed in the proof of Theorem 2.1 is to replace the polynomial \(f_S(x) = \prod_{i \in S}(x + c_i)\).

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

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

satisfies

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

### 3. Some history

The first work on counting quadratic residue patterns of two or more consecutive terms in \(F_p^\times\) was by Aladov [1] in 1896. He counted each quadratic residue pattern of length 2, and some (but not all) quadratic residue patterns of length 3. The counts of length 2 were computed explicitly as in the table below, depending on \(p\) mod 4. The formulas are consistent with the determination of when \(N_p(\varepsilon_1, \varepsilon_2) > 0\) in Example 2.3.

<table>
<thead>
<tr>
<th>(p \mod 4)</th>
<th>(N_p(1, 1))</th>
<th>(N_p(1, -1))</th>
<th>(N_p(-1, 1))</th>
<th>(N_p(-1, -1))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>((p - 5)/4)</td>
<td>((p - 1)/4)</td>
<td>((p - 1)/4)</td>
<td>((p - 1)/4)</td>
</tr>
<tr>
<td>3</td>
<td>((p - 3)/4)</td>
<td>((p + 1)/4)</td>
<td>((p - 3)/4)</td>
<td>((p - 3)/4)</td>
</tr>
</tbody>
</table>

We can write these formulas for \(N_p(\varepsilon_1, \varepsilon_2)\) as \(p/4 + O(1)\). In 1898, von Sterneck [8] counted patterns of length 3 and 4 with restrictions (each pattern was counted along with its opposite, e.g., \((+,-,-)\) and \((-,-,+\) together, not separately). 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 \(F_p^\times\). The length 3 counts imply \(N_p(\varepsilon_1, \varepsilon_2, \varepsilon_3) = p/8 + O(\sqrt{p})\) in all cases (and it is \(p/8 + O(1)\) for \(p \equiv 3 \mod 4\)).
Davenport considered this counting problem for \( r \geq 4 \) throughout the 1930s. In [2] he showed \(|N_p(\varepsilon_1, \ldots, \varepsilon_r) - p/2^r| = O_r(p^{3/4})\) 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 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 bound when \( r = 4 \) from \( O_r(p^{3/4}) \) to \( O_r(p^{2/3}) \). Reducing the exponent on \( p \) in the \( O \)-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 a 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 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]) as a consequence of his proof of the Riemann hypothesis for curves over finite fields.

An account of Davenport’s work and its influence on 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

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

where \( f(x) \) has \( r \) distinct roots (the roots need not be simple) in a splitting field over \( \mathbb{F}_q \). This is [5, Theorem 3.1].

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 \( \mathbb{F}_q \), where \( \chi_i \) has order \( n_i \geq 2 \). For \( r < q \), pick distinct \( c_1, \ldots, c_r \) in \( \mathbb{F}_q \) and an \( n_i \)-th root of unity \( \varepsilon_i \) in \( \mathbb{C} \) for \( i = 1, \ldots, r \). Set

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

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 \( a \in \mathbb{F}_q \) the numbers \( a + c_1, \ldots, a + c_r \) fill up \( \mathbb{F}_q \) so one of these is 0, and thus \( N_q = 0 \), which is uninteresting.

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

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

\[\text{In [5] it is assumed for (A.1) that } f(x) \text{ is not an } n \text{-th power but it is not explicitly stated that } f(x) \text{ is not monic too. For non-monic } f \text{ we get counterexamples to (A.1): if } f(x) = cg(x)^n \text{ with } c \in \mathbb{F}_q^\times \text{ not an } n \text{-th power, then } \sum_{a \in \mathbb{F}_q} \chi(f(a)) = \sum_{a \in \mathbb{F}_q} \chi(cg(a)^n) = \chi(c)(q - \{a \in \mathbb{F}_q : g(a) \neq 0\}), \text{ so } |\sum_{a \in \mathbb{F}_q} \chi(f(a))| = q - |\{a \in \mathbb{F}_q : g(a) \neq 0\}| \geq q - r, \text{ which contradicts (A.1) if } r \text{ is small, such as } r = 1 (f(x) = cx^n) \text{ for any } q \text{ or } r = 2 (f(x) = cx^n(x - 1)^n) \text{ for } q > 4.\]
where we will use (A.1) to show each inner sum over $\mathbb{F}_q$ so we can write

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

which generalizes (2.1). Therefore

$$N_q = \sum_{a \in \mathbb{F}_q \text{ all } a+c_j \neq 0} \prod_{i=1}^r \frac{1}{n_i} \left( 1 + \frac{\chi_i(a+c_i)}{\varepsilon_i} + \left( \frac{\chi_i(a+c_i)}{\varepsilon_i} \right)^2 + \ldots + \left( \frac{\chi_i(a+c_i)}{\varepsilon_i} \right)^{n_i-1} \right).$$

This sum over $\mathbb{F}_q$ 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 $\mathbb{F}_q$ by including an additional error term:

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

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

$$N_q = \frac{1}{n_1 \cdots n_r} \sum_{a \in \mathbb{F}_q} \sum_{0 \leq t_i \leq n_i-1 \text{ for all } i} \chi_1(a+c_1)^{t_1} \cdots \chi_r(a+c_r)^{t_r} + \epsilon$$

$$= \frac{1}{n_1 \cdots n_r} \sum_{0 \leq t_i \leq n_i-1 \text{ for all } i} \sum_{\epsilon_1^{t_1} \cdots \epsilon_r^{t_r}} \chi_1(a+c_1)^{t_1} \cdots \chi_r(a+c_r)^{t_r} + \epsilon.$$

The inner term when all $t_i$ are 0 is $\sum_{a \in \mathbb{F}_q} 1 = q$, so

$$\left| N_q - \frac{q}{n_1 \cdots n_r} \right| \leq \frac{1}{n_1 \cdots n_r} \sum_{0 \leq t_i \leq n_i-1 \text{ for all } i} \left| \sum_{a \in \mathbb{F}_q} \chi_1(a+c_1)^{t_1} \cdots \chi_r(a+c_r)^{t_r} \right| + \frac{r}{2}.$$
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

\[
\sum_{a \in \mathbb{F}_q} \chi_1(a + c_1)^{t_1} \cdots \chi_r(a + c_r)^{t_r} = \sum_{a \in \mathbb{F}_q} \chi((a + c_1)^{t_1} \cdots (a + c_r)^{t_r}) = \sum_{a \in \mathbb{F}_q} \chi(f(a)),
\]

where \(f(x) = (x + c_1)^{t_1} \cdots (x + c_r)^{t_r}\). This polynomial is monic with \(r\) distinct roots. In order to apply (A.1) to bound \(\left| \sum_{a \in \mathbb{F}_q} \chi(f(a)) \right|\), 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 \((q - 1) \mid t_i m_i\) is the same as having \((q - 1)/(q - 1, m_i) \mid t_i\) 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 \((q - 1) \mid t_i m_i\) is equivalent to \(n_i \mid t_i\). Recalling that \(0 \leq t_i \leq n_i - 1\), we can have \(n_i \mid t_i\) 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.

**References**


