A GENERALIZATION OF THE GORESKY-KLAPPER CONJECTURE, PART I

BADRIA ALSULMI, TODD COCHRANE, MICHAEL J. MOSSINGHOFF, VINCENT PIGNO, CHRIS PINNER, C. J. RICHARDSON, AND IAN THOMPSON

Abstract. For a fixed integer \( n \geq 2 \), we show that a permutation of the least residues mod \( p \) of the form \( f(x) = Ax^k \mod p \) cannot map a residue class mod \( n \) to just one residue class mod \( n \) once \( p \) is sufficiently large, other than the maps \( f(x) = \pm x \mod p \) when \( n \) is even and \( f(x) = \pm x \) or \( \pm x^{(p+1)/2} \mod p \) when \( n \) is odd.

1. Introduction

For an odd prime \( p \) we let \( I \) denote the reduced residues mod \( p \),
\[
I = \{1, 2, \ldots, p-1\},
\]
and \( A \) and \( k \) integers with
\[
|A| < p/2, \quad p \nmid A, \quad 1 \leq k < p-1, \quad \gcd(k, p-1) = 1,
\]
so that the map \( f : I \to I \) given by
\[
f(x) = Ax^k \mod p,
\]
is a permutation of \( I \).

Goresky & Klapper [11] divided \( I \) into the even and odd residues
\[
E = \{2, 4, \ldots, p-1\}, \quad O = \{1, 3, \ldots, p-2\},
\]
and asked when \( f \) could also be a permutation of \( E \) (equivalently \( O \)). Originally the problem was phrased in terms of decimations of \( \ell \)-sequences and was restricted to cases where 2 is a primitive root mod \( p \), but this is the form that we are interested in here. Apart from the identity map \((p; A, k) = (p; 1, 1)\) they found six cases
\[
(p; A, k) = (5; -2, 3), (7; 1, 5), (11; -2, 3), (11; 3, 7), (11; 5, 9), (13; 1, 5),
\]
and conjectured that there were no more for \( p > 13 \). This was proved for sufficiently large \( p \) in [3] and in full in [6], with asymptotic counts on \( |f(E) \cap O| \) considered in [4]. Since \( x \mapsto p-x \) switches elements of \( E \) and \( O \), this is the same as asking when \( f(E) = O \) or \( f(O) = E \) on replacing \( A \) by \(-A\).

Somewhat related is a question of D. H. Lehmer [13, Problem F12, p. 381] concerning the number of \( x \mod p \) whose inverse, \( f(x) = x^{-1} \mod p \), has opposite
parity. Since $k$ is defined mod $(p - 1)$ it is sometimes useful to allow negative exponents, $|k| < (p - 1)/2$. This problem was solved by Zhang [26] using Kloosterman sums; see also the generalizations by Alkan, Stan and Zaharescu [1], Lu and Yi [17, 18], Shparlinski [20, 21], Xi and Yi [23], and Yi and Zhang [25].

Thinking of the evens and odds as a mod 2 restriction, we can ask a similar question for a general modulus $n$. Namely we can divide up $I$ into the $n$ congruence classes mod $n$

$$(1.2) \quad I_j = \{ x : 1 \leq x \leq p - 1, \ x \equiv j \mod n \}, \ j = 0, \ldots, n - 1,$$

and ask for examples of the following types.

**Type (i):** $f(I_j) = I_j$ for all $j = 0, \ldots, n - 1$.

**Type (iia):** $f(I_0), \ldots, f(I_{n-1})$ a permutation of $I_0, \ldots, I_{n-1}$.

**Type (iib):** $f(I_j) = I_j$ for some $j$.

**Type (iii):** There is a pair $i, j$ with $f(I_i) \subseteq I_j$.

**Type (iv):** There is a pair $i, j$ with $f(I_i) \cap I_j = \emptyset$.

In this paper we will be primarily be interested in the Type (i)-(iii) maps, though we will include some special cases of Type (iv), for example when

$$(1.3) \quad d := \gcd(k - 1, p - 1)$$

is small. We return to consider general Type (iv) in Part II.

Notice that for $n = 2$ determining Type (i) through Type (iv) are all the same problem, but for general $n$ they can be quite different (indeed the $I_j$ will not even have the same cardinality unless we restrict to $p \equiv 1 \mod n$). Note that these requirements become successively weaker (and the claim that there are no such examples for large enough $p$ a successively stronger statement) as we move from (i) to (iia) or (iib), to (iii), to (iv). To make sense here we should probably think of $p$ growing with $n$, for example we shall assume throughout that $p > n + 1$, otherwise all the residue classes have only 0 or 1 element and every permutation will be a Type (iia). Similarly if a permutation is not a Type (iii), or Type (iv), then we are demanding at least two, or at least $n$, values in each image of each residue class and so must have $p > 2n$, or $p > n^2$, for this to have any chance of being true.

If the map $f$ randomly distributes the values mod $n$ then we might expect to have $|f(I_i) \cap I_j| \sim p/n^2$ and so, for fixed $n$, no examples of Type (i) through (iv) once $p$ is sufficiently large. However, as shown in [4] for $n = 2$, if the parameter $d = \gcd(k - 1, p - 1)$ is large we can’t expect this equal distribution.

Indeed when $n$ is odd it is not hard to see that we will have infinitely many examples of Type (iib) in addition to the identity map.

**Example 1.1.** Suppose that $p \equiv 1 \mod 4$ and that

$$f(x) = \pm x^{(p+1)/2} \mod p.$$ 

If $n$ is odd and $i \equiv 2^{-1}p \mod n$ then

$$f(I_i) = I_i.$$

If $n$ is even, or $n$ is odd with $i \neq 2^{-1}p \mod n$, and $p > (n + 1)^2$, then $f(I_i)$ hits exactly two residue classes, namely $I_i$ and $I_{\bar{i}}$ where $\bar{i} \equiv p - i \mod n$.

The proof of Example 1.1 will be given in Section 7. At the expense of the explicit constant the condition $p > (n + 1)^2$ could be replaced with $p \gg (n \log n)^{4/3}$ using the Burgess [5] bound $O(p^{1/4} \log p)$ for gaps between quadratic residues or nonresidues.
A similar situation occurs for the map $f(x) = -x \mod p$; if $p > n$ and $n$ is even then the $f(I_j) = I_j$ will be a derangement (i.e., a permutation fixing no element) of the $I_j$, while if $n$ is odd this $f$ will fix the $I_i$ with $i \equiv 2^{-1}p \mod n$ and derange the remaining $I_j$.

Notice that in these examples the value of $d$ is unusually large, namely $d = p - 1$ or $(p - 1)/2$. If $d$ is not large then in fact each residue class does receive its fair share of values:

**Theorem 1.1.** For all $i,j$

$$|f(I_i) \cap I_j| = \frac{p}{n^2} + O(d \log^2 p) + O(p^{89/92} \log^2 p).$$

In particular, if $n$ is fixed and $d = o(p/ \log^2 p)$, then

$$|f(I_i) \cap I_j| \sim p/n^2.$$

This follows at once from the more numerically precise statement in Theorem 3.1 below, and relies on bounds for binomial exponential sums

$$\sum_{x=1}^{p-1} e_p(ax^k + bx).$$

As we show in Theorem 4.1 below, if we avoid those few cases in Example 1.1, then even for large $d$, for a given $n$ there are at most finitely many cases of Type (iii); that is for all other mappings the image of each residue class $f(I_i)$ hits at least two different residue classes mod $n$.

**Theorem 1.2.** If $n$ is even and $f(x) \neq \pm x \mod p$ or if $n$ is odd and $f(x) \neq \pm x \pm (p+1)/2 \mod p$, then there are no $i,j$ with $f(I_i) \subseteq I_j$ once

$$p \geq 9 \cdot 10^{34} n^{92/3}.$$

In the linear case we can be even more precise:

**Theorem 1.3.** Suppose that

$$f(x) = Ax \mod p, \quad A \neq \pm 1.$$

If $p > 2n$ then $f(x)$ is not a Type (iii) map.

Similarly for the maps with $k = (p+1)/2$, but not of the form considered in Example 1.1, we can refine the bound in Theorem 1.2.

**Theorem 1.4.** Suppose that

$$f(x) = Ax^{(p+1)/2} \mod p, \quad A \neq \pm 1.$$

If $p > (4n+1)^2$ then $f(x)$ is not a Type (iii) map.

In Lemma 6.2 we show that the $p > (4n+1)^2$ in this theorem can be reduced to $p > 18n$ when $A \neq 2, 2^{-1}$. The Burgess bound [5] can be used in the proof of Lemma 6.1 to replace it by $p \gg (n \log n)^{4/3}$ when $A = 2, 2^{-1}$.

Theorems 1.3, 1.4 and Example 1.1, are the cases where the integer

$$L := (p-1)/d$$

is 1 or 2. When $L \geq 3$ is small the argument in Theorem 4.1 similarly shows that there are no Type (iii) maps $f(x) = Ax^k \mod p$ once

$$p > 1214 n^2 (L-1)^2 \log^4 (n(L-1)).$$
At the other extreme, for the Lehmer type maps, \( k = -1 \), we have \( d = 2 \) and (1.4) certainly gives an asymptotic formula, but using the Kloosterman sum bound \( 2\sqrt{p} \) for (1.5) drastically improves the error term (see for example [1]). More generally for small \( |k|, k \neq 1 \), one can use the Weil [22] bound \( |k-1|\sqrt{p} \) to obtain (see also [21])

\[
|f(I_i) \cap I_j| = \frac{p}{n^2} + O(|k|p^{1/2} \log^2 p).
\]

Similarly when \( |k| \) is small we can obtain good bounds for both Type (iii) and (iv).

**Theorem 1.5.** Suppose that \( f(x) = Ax^k \mod p \) with \( k \neq 1 \) positive or negative.

(a) If \( p > 37|k-1|^2n^2 \) then \( f(x) \) is not a Type (iii) map.

(b) If \( p \geq 16.2|k-1|^2n^4 \) then \( f(x) \) is not a Type (iv) map.

If we want a stronger statement avoiding cases of Type (iv) even when \( d \) is large, that is, prove that the image of every residue class \( n \) hits every residue class mod \( n \), then we will need to exclude more examples for \( n > 2 \). We explore this problem in [7]. The proofs of Theorems 1.2, 1.3 and 1.5 are given in Section 5 and Theorem 1.4 in Section 6.

For a given \( n \) we know from Theorem 1.2 that there are at most finitely many occurrences of Type (i), (iia) and (iib), but of course the bounds in this paper are far too large to obtain a complete determination as was done for \( n = 2 \) in [6]. We hope to employ the methods of [6] to complete this determination in a subsequent work.

2. Computations and Conjectures

Computations looking for maps of Type (i)-(iv) were performed for the primes \( p < 20,000 \), exponents \( k < p - 1 \) and moduli \( n = 3 \) through 12. Of particular interest was obtaining Type (iii) examples with the ratio \( p/n \) as large as possible. This led to a more extensive investigation of the exponent \( k = (p+1)/2 \). We quickly discovered Example 1.1 where for any odd \( n \) and prime \( p \equiv 1 \mod 4 \), the mapping \( f(x) = \pm x^{(p+1)/2} \mod p \) is Type (iii). Further families with this exponent are given in Theorems 2.1 to 2.6. They were all discovered by looking at patterns in the data. Notice that a Type (iii) map of the form \( f(x) = \pm x^{(p+1)/2} \mod p \) must produce a Type (ii) map for \( f(x) \) or \(-f(x)\); of course we are only interested maps of this type for \( n \) even, or for \( n \) odd where the \( f(I_1) = I_1 \) has \( 2t \neq p \) mod \( n \).

2.1. **Type (iii) mappings:** In Theorem 1.2 we verified the existence of a constant \( K(n) \) such that for \( p > K(n) \) and \( f(x) \neq \pm x \) and when \( n \) is odd \( f(x) \neq \pm x^{(p+1)/2} \mod p \), every residue class is mapped to at least two different residue classes, that is, \( f(x) \) is not Type (iii). The constant \( K(n) = 9 \cdot 10^{34}n^{52/3} \) obtained there is undoubtedly far from the truth. Table 1 gives the five largest primes having an \( f(x) = Ax^k \mod p \) with \( f(I_i) \subseteq I_j \) for some \( i,j \), found for each \( 3 \leq n \leq 12 \) and \( 2n < p < 20,000 \). Since \( Ax^k \) has this property if and only if \(-Ax^k \) does, we just consider positive \( A \). From this data we make the following conjecture.

**Conjecture 2.1.** The optimal values for \( K(n) \) for \( n = 3 \) through 12 are

\[
K(3) = 17, \quad K(4) = 13, \quad K(5) = 43, \quad K(6) = 17, \quad K(7) = 37,
\]
\[
K(8) = 43, \quad K(9) = 43, \quad K(10) = 47, \quad K(11) = 67, \quad K(12) = 53.
\]

The data suggests that one can take \( K(n) = 2n^2 \), although the correct bound is likely of order somewhere between \( n \log n \log \log n \) and \( n^2 \).
Table 1. Type (iii): Five largest primes $2n < p < 20,000$ having \( f(x) = Ax^k \mod p \) with \( f(I_i) \subseteq I_j \) for some \( i, j \) if \( f(x) \neq x \) if \( n \) is even, and \( f(x) \neq x \) or \( x^{(p+1)/2} \) if \( n \) is odd). Type (iib): Cases of \( f(I_i) = I_i \), are marked with a *.

<table>
<thead>
<tr>
<th>( n = 3 )</th>
<th>( n = 4 )</th>
<th>( n = 5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p )</td>
<td>( A )</td>
<td>( k )</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>0,1,2*</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>9,0,1,2*</td>
</tr>
<tr>
<td>19</td>
<td>5</td>
<td>17,2*</td>
</tr>
<tr>
<td>23</td>
<td>10</td>
<td>21,4*</td>
</tr>
<tr>
<td>41</td>
<td>6</td>
<td>19,3,4*</td>
</tr>
<tr>
<td>43</td>
<td>6</td>
<td>41,5*</td>
</tr>
</tbody>
</table>

Looking for larger ratios of \( p \) to \( n \), we extended our computations to \( 13 \leq n \leq 86 \) and \( 5n \leq p \leq 15n \). The values found with \( p/n > 9 \) are recorded in Table 2.

A large number of the Type (iii) maps with \( p/n \) large have \( k = (p+1)/2 \). The bounds in Example 1.1 and Theorem 1.4 enable a complete determination when \( k = (p+1)/2 \) and \( p > 2n \) for small \( n \). There are no such Type (iii) mappings for \( n = 3, 4, 7 \) or 9, with a complete list of such maps for the remaining \( 5 \leq n \leq 13 \) shown in Table 3.
Table 2. Type (iii) with $3 \leq n \leq 86$ and $9 < p/n < 15$ ($f(x) = Ax^k \mod p$ with $A > 0$, and $f(x) \neq x^{(p+1)/2}$ if $n$ is odd).

<table>
<thead>
<tr>
<th>n</th>
<th>p</th>
<th>A</th>
<th>k</th>
<th>i</th>
<th>p/n</th>
</tr>
</thead>
<tbody>
<tr>
<td>70</td>
<td>641</td>
<td>1</td>
<td>321</td>
<td>27,54</td>
<td>9.157142...</td>
</tr>
<tr>
<td>84</td>
<td>773</td>
<td>1</td>
<td>387</td>
<td>27,36,64,74</td>
<td>9.202380...</td>
</tr>
<tr>
<td>30</td>
<td>277</td>
<td>1</td>
<td>139</td>
<td>10,27</td>
<td>9.233333...</td>
</tr>
<tr>
<td>39</td>
<td>367</td>
<td>1</td>
<td>245</td>
<td>8</td>
<td>9.410256...</td>
</tr>
<tr>
<td>62</td>
<td>593</td>
<td>1</td>
<td>297</td>
<td>16,19</td>
<td>9.564516...</td>
</tr>
<tr>
<td>82</td>
<td>809</td>
<td>1</td>
<td>405</td>
<td>20,51</td>
<td>9.865853...</td>
</tr>
<tr>
<td>60</td>
<td>593</td>
<td>1</td>
<td>297</td>
<td>21,32</td>
<td>9.883333...</td>
</tr>
<tr>
<td>37</td>
<td>367</td>
<td>1</td>
<td>245</td>
<td>17</td>
<td>9.918918...</td>
</tr>
<tr>
<td>85</td>
<td>853</td>
<td>221</td>
<td>143,569</td>
<td>10,202380...</td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>853</td>
<td>220</td>
<td>143,569</td>
<td>53</td>
<td>10.277108...</td>
</tr>
<tr>
<td>35</td>
<td>367</td>
<td>83</td>
<td>245</td>
<td>26</td>
<td>10.485714...</td>
</tr>
<tr>
<td>81</td>
<td>853</td>
<td>220</td>
<td>143,569</td>
<td>62</td>
<td>10.530864...</td>
</tr>
<tr>
<td>76</td>
<td>809</td>
<td>1</td>
<td>405</td>
<td>58,67</td>
<td>10.644730...</td>
</tr>
<tr>
<td>79</td>
<td>853</td>
<td>221</td>
<td>143,569</td>
<td>71</td>
<td>10.797468...</td>
</tr>
<tr>
<td>86</td>
<td>941</td>
<td>1</td>
<td>471</td>
<td>83,84</td>
<td>10.941860...</td>
</tr>
<tr>
<td>84</td>
<td>977</td>
<td>1</td>
<td>489</td>
<td>12,41</td>
<td>11.630952...</td>
</tr>
<tr>
<td>86</td>
<td>1013</td>
<td>1</td>
<td>507</td>
<td>2,65</td>
<td>11.779069...</td>
</tr>
</tbody>
</table>

Table 3. All Type (iii) of the form $f(x) = Ax^{(p+1)/2} \mod p$ for $3 \leq n \leq 13$ (for $p > 2n$ and $A > 0$ and excluding $f(x) = x^{(p+1)/2}$ if $n$ is odd).

<table>
<thead>
<tr>
<th>n</th>
<th>p</th>
<th>A</th>
<th>i</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>13</td>
<td>4.5</td>
<td>0.3</td>
</tr>
<tr>
<td>6</td>
<td>13</td>
<td>1</td>
<td>2,3,4,5</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>1</td>
<td>0.5</td>
</tr>
<tr>
<td>8</td>
<td>17</td>
<td>1</td>
<td>0,1,3,6</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>1</td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>41</td>
<td>1</td>
<td>3.6</td>
</tr>
<tr>
<td>10</td>
<td>29</td>
<td>2</td>
<td>2.7</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>9,10</td>
<td>0.9</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>14</td>
<td>4.5</td>
</tr>
<tr>
<td></td>
<td>41</td>
<td>2</td>
<td>3.8</td>
</tr>
<tr>
<td></td>
<td>41</td>
<td>20</td>
<td>5.6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n</th>
<th>p</th>
<th>A</th>
<th>i</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>29</td>
<td>1</td>
<td>0.7</td>
</tr>
<tr>
<td>12</td>
<td>29</td>
<td>1</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>12</td>
<td>8.9</td>
</tr>
<tr>
<td></td>
<td>37</td>
<td>1</td>
<td>4,5,8,9</td>
</tr>
<tr>
<td></td>
<td>41</td>
<td>1</td>
<td>8.9</td>
</tr>
<tr>
<td></td>
<td>53</td>
<td>1</td>
<td>1.4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n</th>
<th>p</th>
<th>A</th>
<th>i</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>29</td>
<td>4</td>
<td>6,10</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>7</td>
<td>5,11</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>9,10</td>
<td>0.3</td>
</tr>
<tr>
<td></td>
<td>37</td>
<td>12</td>
<td>0.11</td>
</tr>
</tbody>
</table>

In the proof of Theorem 1.4 for $k = (p+1)/2$ we had to deal separately with the case $A = 2$, so additional computations were performed for $f(x) = 2x^{(p+1)/2} \mod p$ looking for examples with large ratio $p/n$. These corresponded to primes with a certain pattern of quadratic residues. Examining the corresponding $n$ values led us to a family of Type (iii) mappings of the form $2x^{(p+1)/2}$, with arbitrarily large $p/n$, and requiring $K(n)$ to be as large as $n \log n$.

**Theorem 2.1.** Let 

$$f(x) = 2x^{(p+1)/2} \mod p.$$  

Suppose that $p \equiv 1 \mod 4$ has

$$\left(\frac{p}{q}\right) = \begin{cases} +1, & \text{if } q = 1 \mod 4, \\ -1, & \text{if } q = 3 \mod 4, \end{cases}$$  

(2.1)
for all primes $3 \leq q \leq 4t - 1$, and that $n \equiv 2 \mod 4$ with
\begin{equation}
\frac{2p}{4t + 1} \leq n < \frac{2p}{4t - 1}.
\end{equation}
Then for both
\begin{equation}
i := \frac{1}{4}(2p - (4t - 1)n), \quad j := \begin{cases} 2i \mod n, & \text{if } \left(\frac{n}{p}\right) = -1, \\ p - 2i \mod n, & \text{if } \left(\frac{n}{p}\right) = 1,
\end{cases}
\end{equation}
and
\begin{equation}
i := \frac{1}{4}(2p - (4t - 3)n), \quad j := \begin{cases} p - 2i \mod n, & \text{if } \left(\frac{n}{p}\right) = -1, \\ 2i \mod n, & \text{if } \left(\frac{n}{p}\right) = 1,
\end{cases}
\end{equation}
we have $f(I_i) \subseteq I_j$.

The primes $p < 100,000$ with property (2.1) with $t \geq 9$, and the smallest $n$ this gives in Theorem 2.1 are shown in Table 4.

Using the Chinese Remainder Theorem we can construct $p$ with this property for arbitrarily large $t$. For example we could take $p \equiv 1 \mod 4Q_1$ and $-1 \mod Q_2$ where $Q_1$ and $Q_2$ are the products of the primes $q \leq 4t - 1$ that are $1$ or $-1 \mod 4$ respectively (there are of course many other ways). Hence we can make Type (iii) examples with $p > (2t + \frac{1}{2} - \varepsilon)n$. In particular we can’t take $K(n) = Cn$ however large the $C$. Moreover, by the work of Heath-Brown [14] and Xylouris [24] on the smallest prime in an arithmetic progression, there exist such $p$ with $p \ll Q^{5.18}$, with $Q = 4Q_1Q_2$, and hence examples of Type (iii) with $p > \frac{1}{11}n \log n$. Assuming GRH guarantees such $p < 2(Q \log Q)^2$ (see Bach [2] or Lamzouri, Li and Soundararajan [16]) and thus $p > (\frac{1}{11} - \varepsilon)n \log n$. The proofs of the theorems in this section are given in Section 8.

In Lemma 6.2 we show that a Type (iii) map $f(x) = Ax^{(p+1)/2} \mod p$ with $A \neq \pm 1, \pm 2, \pm 2^{-1}$ must have $p < 18n$. For $n \leq 106$ the largest $p/n$ value found for such a map was $317/106 = 2.990566 \ldots$, so our computations do not rule out $p > 3n$ in place of $p > 18n$ in Lemma 6.2. This would be optimal, even for arbitrarily large $n$, the following examples showing that for any $p \equiv 5 \mod 8$ there will be a Type (iii) map with $p/n \to 3$ as $p \to \infty$.

**Theorem 2.2.** For $J = 0, 1, 2$ let $f_J(x) := \left(\frac{2}{p}\right)(n - J)x^{(p+1)/2} \mod p$.

If $p = 72k + 5$, $n = 24k + 2$ then $f_0(I_0), -f_0(I_{n-1}) \subseteq I_{8k}$.

If $p = 72k + 13$, $n = 24k + 5$ then $f_0(I_0), -f_0(I_{n-2}), f_1(I_0), -f_1(I_{n-2}) \subseteq I_{16k+2}$.

If $p = 72k + 29$, $n = 24k + 10$ then $f_0(I_0), -f_0(I_{n-1}), f_1(I_0), -f_1(I_{n-1}) \subseteq I_{8k+3}$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$t$</th>
<th>$n$</th>
<th>$p/n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>15461</td>
<td>9</td>
<td>838</td>
<td>18.449880. . .</td>
</tr>
<tr>
<td>23201</td>
<td>9</td>
<td>1258</td>
<td>18.442766. . .</td>
</tr>
<tr>
<td>Theorem 2.1</td>
<td>40169</td>
<td>9</td>
<td>2174</td>
</tr>
<tr>
<td>70769</td>
<td>10</td>
<td>3454</td>
<td>20.488998. . .</td>
</tr>
<tr>
<td>75869</td>
<td>9</td>
<td>4102</td>
<td>18.495611. . .</td>
</tr>
</tbody>
</table>

Table 4. Primes $p < 100,000$ with $p \equiv 1 \mod 4$ and $\left(\frac{p}{q}\right) = 1$ for all odd $q \leq 4t - 1$ for some $t \geq 9$. 
If \( p = 72k + 37, \) \( n = 24k + 13 \) then \( f_1(I_0), -f_1(I_{n-2}) \subseteq I_{10k+8}. \)
If \( p = 72k + 53, \) \( n = 24k + 19 \) then \( f_1(I_0), -f_1(I_{n-4}), f_2(I_0), -f_2(I_{n-4}) \subseteq I_{8k+5}. \)
If \( p = 72k + 61, \) \( n = 24k + 22 \) then \( f_2(I_0), -f_2(I_{n-5}) \subseteq I_{10k+13}. \)

2.2. Type (iib) Mappings. The Type (iib) maps, where \( f(I_i) = I_i \) for some \( i, \)
are marked with an asterisk in Table 1; of course for such cases the iterates will also
fix \( I_i \) and a number of these can be seen in the table. For example for \( n = 7, \) \( p = 19, \)
the map \( f(x) = 5x^5 \mod 19 \) fixes \( I_0, \) as does \( f^2(x) = 7x^7 \mod 19, \)
\( f^3(x) = -2x^{17} \mod 19, \) \( f^4(x) = -8x^{13} \mod 19, \) \( f^5(x) = -3x^{11} \mod 19 \) and \( f^6(x) = x \mod p; \)
in this case \( p - 6 \equiv 6 \mod n \) so that the maps with negative \( A \) recorded in their
positive guise also fix \( I_0. \)

Many examples of Type (iib) mappings in our data with large ratio \( p/n \) are of
the form \( f(x) = \pm x^{(p+1)/2} \equiv \pm \left( \frac{x}{p} \right) x \mod p. \) For \( n \) even, or \( n \) odd with \( i \neq 2^{-1}p \mod n, \) it is readily seen that this requires \( p \) to have a string of \( p/n \) consecutive quadratic residues or nonresidues. In Theorems 2.3 to 2.6 we explore how
conversely long blocks of consecutive residues or nonresidues can produce large \( p/n \) values. We distinguish several cases frequently encountered in the data. Theorem
2.3 deals with consecutive quadratic residues starting at 1, Theorem 2.4 with intervals
around \( p/n \) and a prime with \( p \equiv 1 \mod 8 \) and \( \left( \frac{p}{q} \right) = 1 \) for all odd primes \( q \leq t. \) Then for any \( n > (p - 1)/(t + 1) \) the map
\( f(x) = \left( \frac{x}{p} \right) x^{(p+1)/2} \mod p \) is the identity map on \( I_0. \)

Notice that \( i = 0 \) does not have \( 2i \equiv p \mod n, \) so these examples are of interest
for both odd and even \( n. \) Again, by the Chinese Remainder Theorem and Dirichlet’s
theorem, for any \( t, \) there exist infinitely many \( p \) satisfying the hypotheses of this
theorem and so we get examples with \( p \) as large as \( n \log n, \) but for certain \( p \) we
can push the size of \( K(n) \) a little bigger. By the work of Graham and Ringrose [12]
we know there exist infinitely many primes \( p \equiv 1 \mod 4 \) having a least quadratic
nonresidue of size at least \( c \log p \log \log \log p \) for some constant \( c \) (with improvement
to \( c \log p \log \log p \) under GRH by Montgomery [19]). Taking \( t = \left[ c \log p \log \log \log p \right], \)
the hypotheses of the theorem are satisfied by reciprocity, and thus with \( n = \left[ (p - 1)/t \right] \), we obtain a Type (iib) mapping with \( p \gg n \log n \log \log \log n \) (with
improvement under GRH).

Since \( p \equiv 1 \mod 4, \) if our interval of consecutive quadratic residues or nonresidues
contains \( (p - 1)/2, \) then we have a symmetric interval around \( p/2 \) with \( \left( \frac{x}{p} \right) = \left( \frac{(p-1)/2}{p} \right) = \left( \frac{2}{p} \right). \) For odd \( n \) we obtain examples with \( p/n \) close to the interval
length \( t, \) but unfortunately (2.6) has \( 2i \equiv p \mod n \) which we know always gives a
Type (iii) by Example 1.1, though additionally here \( f(x) \) is the identity map on \( I_i. \)
If we restrict to even \( n \) then the ratio \( p/n \) is only close to \( t/2. \)
### Table 5. Type (iii): Primes \( p < 100,000 \) with \( t \geq 25 \) consecutive quadratic residues or consecutive nonresidues, \([a, a + t]\).

<table>
<thead>
<tr>
<th>( n \equiv 2 \mod 3 )</th>
<th>( p )</th>
<th>( t )</th>
<th>( a )</th>
<th>( T_1 )</th>
<th>( T_2 )</th>
<th>( n )</th>
<th>( i )</th>
<th>( p/n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>52361</td>
<td>29</td>
<td>17437</td>
<td>17</td>
<td>12</td>
<td>1976</td>
<td>1974</td>
<td>2648481...</td>
<td></td>
</tr>
<tr>
<td>65129</td>
<td>27</td>
<td>21693</td>
<td>17</td>
<td>10</td>
<td>2459</td>
<td>2436</td>
<td>26485969...</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( n \equiv 1 \mod 3 )</th>
<th>( p )</th>
<th>( t )</th>
<th>( a )</th>
<th>( T_1 )</th>
<th>( T_2 )</th>
<th>( n )</th>
<th>( i )</th>
<th>( p/n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>52361</td>
<td>29</td>
<td>17437</td>
<td>17</td>
<td>12</td>
<td>2833</td>
<td>2800</td>
<td>18577832...</td>
<td></td>
</tr>
<tr>
<td>65129</td>
<td>27</td>
<td>21693</td>
<td>17</td>
<td>10</td>
<td>4204</td>
<td>4182</td>
<td>15492150...</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( n \equiv 0 \mod 3 )</th>
<th>( p )</th>
<th>( t )</th>
<th>( a )</th>
<th>( T_1 )</th>
<th>( T_2 )</th>
<th>( n )</th>
<th>( i )</th>
<th>( p/n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>52361</td>
<td>29</td>
<td>17437</td>
<td>17</td>
<td>12</td>
<td>2964</td>
<td>2961</td>
<td>17665654...</td>
<td></td>
</tr>
<tr>
<td>65129</td>
<td>27</td>
<td>21693</td>
<td>17</td>
<td>10</td>
<td>3696</td>
<td>3529</td>
<td>17621482...</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( p )</th>
<th>( t )</th>
<th>( a )</th>
<th>( n )</th>
<th>( i )</th>
<th>( p/n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>90313</td>
<td>26</td>
<td>39556</td>
<td>38</td>
<td>3386</td>
<td>2437,3226</td>
</tr>
</tbody>
</table>

#### Theorem 2.4. Suppose that \( p \equiv 1 \mod 4 \) has \( t = 2T \) consecutive residues or nonresidues around \( p/2 \):

\[
\left( \frac{x}{p} \right) = \left( \frac{2}{p} \right), \quad a = \frac{p+1}{2} - T \leq x \leq \frac{p-1}{2} + T.
\]

Equivalently suppose that \( \left( \frac{q}{p} \right) = 1 \) for all odd primes \( q \leq 2T - 1 \).

Suppose \( n \) is even with

\[
\frac{2p}{t+1} < n < \frac{2p}{t-1}, \quad i := an - \left( \frac{n}{2} - 1 \right)p,
\]

or \( n \) is odd with

\[
\frac{p}{t+1} < n < \frac{p}{t-1}, \quad i := an - \left( \frac{n-1}{2} \right)p,
\]

then \( f(x) = \left( \frac{2n}{p} \right)x^{(p+1)/2} \mod p \) is the identity map on \( I_i \).

A large interval of consecutive quadratic residues or nonresidues around \( p/3 \) (and hence under \( x \mapsto p - x \) around \( 2p/3 \)) will also lead to large \( p/n \) values, the size depending on \( n \mod 3 \).
Theorem 2.5. Suppose that \( p \equiv 1 \mod 4 \) and set
\[
\delta := \begin{cases} 
1 & \text{if } p \equiv 1 \mod 3, \\
2 & \text{if } p \equiv 2 \mod 3. 
\end{cases}
\]
Suppose that
\[
\left( \frac{x}{p} \right) = \left( \frac{3}{p} \right),
\]
for
\[
a_1 := \frac{1}{3} (p - \delta) - (T_1 - 1) \leq x \leq \frac{1}{3} (p - \delta) + T_2,
\]
\[
a_2 := \frac{1}{3} (2p + \delta) - T_2 \leq x \leq \frac{1}{3} (2p + \delta) + (T_1 - 1).
\]
Equivalently
\[
(2.7) \quad \left( \frac{3m - \delta}{p} \right) = 1, \quad 1 \leq m \leq T_2, \quad \left( \frac{3m + \delta}{p} \right) = 1, \quad 0 \leq m < T_1.
\]
Suppose that \( n \equiv 0 \mod 3 \) has
\[
\frac{3p}{3T_1 + \delta} < n < \frac{3p}{3T_1 + \delta - 3}, \quad i := a_1 n - \left( \frac{n}{3} - 1 \right) p,
\]
or
\[
\frac{3p}{3T_2 + 3 - \delta} < n < \frac{3p}{3T_2 - \delta}, \quad i := a_2 n - \left( \frac{2n}{3} - 1 \right) p,
\]
or \( n \equiv 2 \mod 3 \), when \( T_1 \leq 2T_2 + 2 - \delta \) and
\[
\frac{2p}{3T_1 + \delta} < n < \frac{2p}{3T_1 + \delta - 3}, \quad i := a_1 n - \left( \frac{n - 2}{3} \right) p,
\]
or \( n \equiv 2 \mod 3 \), when \( T_1 \geq 2T_2 + 2 - \delta \) and
\[
\frac{p}{3T_2 + 3 - \delta} < n < \frac{p}{3T_2 - \delta}, \quad i := a_2 n - \left( \frac{2n - 1}{3} \right) p,
\]
or \( n \equiv 1 \mod 3 \), when \( T_2 \geq 2T_1 - 1 + \delta \) and
\[
\frac{p}{3T_1 + \delta} < n < \frac{p}{3T_1 + \delta - 3}, \quad i := a_1 n - \left( \frac{n - 1}{3} \right) p,
\]
or \( n \equiv 1 \mod 3 \), when \( T_2 \leq 2T_1 - 1 + \delta \) and
\[
\frac{2p}{3T_2 + 3 - \delta} < n < \frac{2p}{3T_2 - \delta}, \quad i := a_2 n - \left( \frac{2n - 2}{3} \right) p.
\]
Then \( f(x) = \left( \frac{3n}{p} \right) x^{(p+1)/2} \mod p \) is the identity map on \( I_i \).

Note if \( p \equiv 1 \mod 3 \) then \( \left( \frac{3}{p} \right) = 1 \) and a large interval around \( p/3 \) leads to a long interval starting at \( a = 1 \) where one can use Theorem 2.2 to potentially produce a larger \( p/n \). Similar theorems could no doubt be obtained for intervals around \( p/5 \) etc. Three \( p/3 \) type examples occur in Table 2; namely \( p = 277, T_1 = 10, T_2 = 0, \) where the largest \( p/n \) in Theorem 2.5 will be for \( n \equiv 0 \mod 3 \), with the smallest \( n = 27 \) (smallest even \( n = 30 \)), \( p = 569, T_1 = 3, T_2 = 6 \) where the best choice is \( n \equiv 1 \mod 3 \), smallest \( n = 61 \) (smallest even \( n = 64 \)), and \( p = 641, T_1 = 5, T_2 = 6 \) where the smallest \( n \equiv 1 \mod 3 \) is \( n = 70 \).

For general intervals of consecutive quadratic residues or nonresidues we have:
Theorem 2.6. Suppose that we have \( t \) consecutive quadratic residues or nonresidues \( \mod p \) starting at \( a \geq 2 \)

\[
\left( \frac{x}{p} \right) = \left( \frac{a}{p} \right), \quad a \leq x \leq a + t - 1, \quad a = st + r, \quad 0 \leq r < t.
\]

If \( i = na - (s - u)p \) and \( n \) is an integer in

\[
(2.8) \quad \max \left\{ \frac{(s - u + 1)p}{a + t}, \frac{(s - u)p}{a} \right\} \leq n \leq \frac{(s - u)p}{a - 1},
\]

or \( i = (s - u + 1)p - n(a + t - 1) \) and

\[
(2.9) \quad \frac{(s - u + 1)p}{a + t} \leq n \leq \min \left\{ \frac{s - u - 1}{a - 1}, \frac{s - u + 1}{a + t - 1} \right\} p,
\]

for some integer \( \frac{(s+1-r)}{(t+1)} > u > s + 1 - \frac{1}{2}(a + t) \), then

\[
(2.10) \quad f(x) = \left( \frac{an}{p} \right) x^{(p+1)/2} \mod p,
\]

is the identity map on \( I_i \).

For very large \( a + t \) and a given \( u \) we are not guaranteed an \( n \) in the range (2.8), but for small \( a \), for example \( a + t < \sqrt{p} \), there will be at least one \( n \), leading to an example with \( p/n \) close to \( t \) for small \( u \). Computationally searching the primes \( p < 10,000 \) for Type (iii) mappings of the form \( f(x) = x^{(p+1)/2} \mod p \), with \( 2i \equiv p \mod n \) if \( n \) is odd, found 578 primes \( p \equiv 1 \mod 4 \) admitting an \( n \) with \( 7 < p/n < 20 \). In each case we checked the minimal \( n \) found against Theorem 2.6.

Of these 545 corresponded to taking the longest string of consecutive quadratic residues or nonresidues in Theorem 2.6 (for \( a, t \) and a suitable \( u \)), with 16 to taking the second longest, and the remaining 17 cases found with shorter intervals.

Notice that if we have an interval \( [b-T, b+T] \) of consecutive quadratic residues or nonresidues \( \mod p \), then for any \( n > p/T \), taking \( J \) to be the least residue of \( nb \mod p \) and \( I_i \) to be the residue class \( \mod n \) containing \( J \), we have \( \left( \frac{j + fn}{p} \right) = \left( \frac{n}{p} \right) \) for all \( -p/n < \ell < p/n \) and \( f(x) = \left( \frac{nb}{p} \right) x^{(p+1)/2} \mod p \) will be the identity map on \( I_i \).

From well known estimates on character sums, see for example Gelfond and Linnik [10, Theorem 9.4.4], for any prime \( p \) there exist \( 2T + 1 \geq \left( 1-o(1) \right) \frac{\log p}{\log 4} \) consecutive quadratic residues and consecutive quadratic nonresidues \( \mod p \). Similar arguments work for \( f(x) = x^{\frac{(p-1)}{2}+1} \mod p \).

Theorems 2.3 to 2.6 used runs of \( x \) where \( x^{(p-1)/2} \mod p \) is constant. One could similarly consider intervals where \( x^{(p-1)/3} \mod p \) is constant. We state the counterpart of Theorem 2.4, since several examples of an interval around \( p/2 \) appear in Table 2 (namely \( p = 853 \) and 367 with \( t = 10 \) and \( a = 422 \) or 179 respectively).

Theorem 2.7. Suppose that \( p \equiv 1 \mod 3 \) and that

\[
(2.11) \quad x^{(p-1)/3} \equiv a^{(p-1)/3} \mod p, \quad a = \frac{p + 1}{2} - T \leq x \leq \frac{p - 1}{2} + T.
\]

Then, with \( t = 2T \) and \( n \) and \( i \) as in (2.5) and (2.6), any map

\[
(2.12) \quad f(x) = (an)^{2(k-1)} x^k \mod p, \quad k = j(p-1)/3+1, \quad j = 1, 2, \quad \gcd(k, p-1) = 1,
\]
Table 6. Type (iia): \( f(x) = Ax^n \mod p \) with \( f(I_i) = I_{\sigma(i)} \) for some permutation \( \sigma \), for \( 3 \leq n \leq 12, n+1 < p < 20,000 \) (with \( A > 0 \) and \( f(x) \neq x \)).

\[
\begin{array}{ccc|c}
  p & A & k & \sigma \\
  \hline
  n = 3 & 5 & 1 & 3 & (02) \\
  & 7 & 3 & 5 & (13) \\
  n = 4 & 7 & 2 & 5 & (12) \\
  & 11 & 1 & 9 & (03) \\
  & 13 & 2 & 5 & (0312) \\
  n = 5 & 7 & 1 & 5 & (03)(24) \\
  n = 8 & 11 & 2 & 9 & (03)(12)(46) \\
  & 13 & 4 & 5 & (06)(14)(23)(57) \\
  n = 9 & 11 & 1 & 3 & (0354)(2867) \\
  & 11 & 1 & 7 & (0453)(2768) \\
  & 11 & 1 & 9 & (05)(26)(34)(78) \\
  & 13 & 1 & 7 & (58)(67) \\
  n = 10 & 13 & 2 & 11 & (08)(12)(35)(47)(69) \\
  n = 11 & 13 & 1 & 5 & (07)(26)(39)(410) \\
  & 13 & 1 & 7 & (02)(58)(67) \\
  & 13 & 1 & 11 & (06)(27)(39)(410)(58) \\
\end{array}
\]

2.3. Type (i) and (iia) Mappings. Only a few cases were found where \( Ax^n \mod p \) permutes every residue class:

Example 2.1. The only cases of Type (i), that is \( f(I_j) = I_j \) for all \( j \), found for \( 3 \leq n \leq 12 \) and \( p < 20,000 \), were \( n = 3, (p; A, k) = (5; -1, 3) \) and \( (7; -3, 5) \).

The examples of Type (iia) found, that is where \( f(I_1), \ldots, f(I_n) \) is a permutation of \( I_1, \ldots, I_n \), are shown in Table 6. By symmetry we include only \( A > 0 \) and of course exclude \( f(x) = x \).

This could be further generalized to intervals where \( x^{(p-1)/q} \mod p \) is constant.

\[ f(x) = (an)^{2(k-1)} x^k \mod p, \quad k = j(p-1)/6+1, \quad j = 1, 5, \quad \text{gcd}(k, p-1) = 1, \]

will be the identity map on \( I_i \), and when \( n \) is odd any map

\[ f(x) = x^{(p-1)/2} \mod p \]

produces a Type (iia) permutation.

Theorem 2.8. If \( p = n + w \) with \( 2 \leq w < n, p \equiv 1 \mod 4 \) and

\[
\left(\frac{y}{p}\right) = \left(\frac{w-y}{p}\right), \quad \text{for all} \quad 1 \leq y < w/2,
\]

then \( f(x) = x^{(p+1)/2} \mod p \) produces a Type (iia) permutation.
A GENERALIZATION OF THE GORESKY-KLAPPER CONJECTURE, PART I

<table>
<thead>
<tr>
<th>n</th>
<th>p</th>
<th>A</th>
<th>k</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>29</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>33</td>
<td>37</td>
<td>1</td>
<td>19</td>
</tr>
<tr>
<td>35</td>
<td>41</td>
<td>1</td>
<td>21</td>
</tr>
<tr>
<td>48</td>
<td>53</td>
<td>1</td>
<td>27</td>
</tr>
<tr>
<td>57</td>
<td>61</td>
<td>1</td>
<td>31</td>
</tr>
<tr>
<td>68</td>
<td>73</td>
<td>1</td>
<td>37</td>
</tr>
<tr>
<td>69</td>
<td>73</td>
<td>1</td>
<td>37</td>
</tr>
<tr>
<td>83</td>
<td>89</td>
<td>1</td>
<td>45</td>
</tr>
<tr>
<td>91</td>
<td>101</td>
<td>1</td>
<td>51</td>
</tr>
<tr>
<td>92</td>
<td>97</td>
<td>1</td>
<td>25, 49, 73</td>
</tr>
<tr>
<td>93</td>
<td>97</td>
<td>1</td>
<td>49</td>
</tr>
<tr>
<td>96</td>
<td>101</td>
<td>1</td>
<td>51</td>
</tr>
</tbody>
</table>

Table 7. Type (iia): \( f(x) \neq x \) for \( 13 \leq n \leq 100 \) and \( n + 4 \leq p < 5n \).

The additional \( f(x) = x^{(p+3)/4} \) and \( x^{(3p+1)/4} \mod p \) for \( p = 97 \) are also predictable; for example for \( p \equiv 1 \mod 24 \) all three \( f(x) \) will occur for \( p = n + 4 \) or \( p = n + 5 \) when \( 3^{(p-1)/4} \equiv 1 \mod p \) or \( 3^{(p-1)/4} \equiv 3^{(p-1)/4} \mod p \) respectively (where one might expect either of these to occur roughly half the time, 193 and 97 respectively being the first cases of these), with similar conditions for \( p = n + 6, n + 7 \) etc that should hold for a positive proportion of the time. The sparsity of Type (i) and (iia) examples suggests the following conjecture.

**Conjecture 2.2.** Suppose that \( p > 2n \).

Excluding \( f(x) = x \mod p \), there are only finitely many examples of Type (i), that is \( f(I_i) = I_i \) for all \( i \).

Excluding \( f(x) = \pm x \mod p \) there are only finitely many examples of Type (iia), that is \( f(I_i) = I_{\sigma(i)} \) for some permutation \( \sigma \) of \( \{0, 1, \ldots, n-1\} \).

Indeed there may be no Type (i) or (iia) maps with \( p > 2n \) other than the few cases found above for \( n = 3 \) or 4. From the Graham & Ringrose [12] bound \( g(p) \gg \log p \log \log \log p \) on the least quadratic nonresidue we see that we cannot replace the \( p > 2n \) in this conjecture by \( p > n + C \log n \), however large the \( C \).

3. Type (iii) and type (iv) intersections for small \( d \)

For \( j = 0, 1, \ldots, n-1 \), let \( I_j \) be the set of values in (1.2). Put

\[
N_j := |I_j| = \begin{cases} \lfloor \frac{p-1+n-j}{n} \rfloor, & \text{if } j \neq 0; \\ \lfloor \frac{p}{n} \rfloor, & \text{if } j = 0. \end{cases}
\]

**Theorem 3.1.** Suppose that \( p > 607 \). Then for any \( A \) and \( k \) satisfying (1.1), \( 2 \leq n < p \), and \( 0 \leq i,j \leq n - 1 \), we have

\[
|f(I_i) \cap I_j| = p^{-1} |I_i||I_j| + E,
\]

with

\[
|E| \leq \left( d + 1 + 2.293 p^{89/92} \right) \left( \frac{4}{\pi} \log p + 0.381 \right)^2,
\]

where \( d = \gcd(k-1, p-1) \), and

\[
\frac{p}{n^2} - 1 < p^{-1} |I_i||I_j| < \frac{p}{n^2} + 1.
\]
For $7 \leq p \leq 607$, the same result holds with .381 replaced by 1/2.

Proof. For any $i, j \in \{0, 1, \ldots, n - 1\}$ write

$$N_{ij} = |f(I_i) \cap I_j|.$$ 

We use $\mathbb{Z}_p$ to denote the integers mod $p$, and view $I_i, I_j$ as subsets of $\mathbb{Z}_p$. We write $I(x), J(x)$ for the characteristic functions for $I_i, I_j$ so that

$$N_{ij} = \sum_{x \mod p} I(x)J(Ax^k).$$

Since $I(x)$ is a periodic function mod $p$ we have a finite Fourier expansion

$$I(x) = \sum_{u \mod p} a_j(u)e_p(ux)$$

where $e_p(x) = e^{2\pi ix/p}$, and for $u = 0, \ldots, p - 1$,

$$a_j(u) = \frac{1}{p} \sum_{y \mod p} I(y)e_p(-yu) = \begin{cases} p^{-1}N_j, & \text{if } u = 0; \\ p^{-1}e_p(\xi_j u)^{\sin(\pi nuN_j/p)} \frac{\sin(\pi nu/p)}{\sin(\pi nu/p)}, & \text{if } u \neq 0, \end{cases}$$

for some $\xi_j$ in $\mathbb{Z}_p$. Hence, separating into zero and nonzero values of $u$ and $v$, and observing that $Ax^k$ is a permutation of $\mathbb{Z}_n$, we have

$$N_{ij} = \sum_{x=0}^{p-1} \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} a_j(u)e_p(ux)a_j(v)e_p(vAx^k) = M + T_1 + T_2 + E,$$

where

$$M = p^{-1}a_j(0)a_j(0) = p^{-1}N_iN_j,$$

$$T_1 = a_j(0)\sum_{u=1}^{p-1} a_j(u)\sum_{x=0}^{p-1} e_p(ux) = 0,$$

$$T_2 = a_j(0)\sum_{v=1}^{p-1} \sum_{x=0}^{p-1} e_p(vAx^k) = a_j(0)\sum_{v=1}^{p-1} a_j(v)\sum_{x=0}^{p-1} e_p(vx) = 0,$$

and

$$E = \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} a_j(u)a_j(v)\sum_{x=0}^{p-1} e_p(ux + vAx^k).$$

Now from [8, Theorem 1.3] we have, with $d = (k - 1, p - 1)$,

$$\sum_{x=0}^{p-1} e_p(ux + vAx^k) \leq 1 + d + 2.292\ p^{89/92},$$

and from [9, Theorem 1], observing that $nx$ is a permutation of the $x \mod p$,

$$\sum_{u=1}^{p-1} |a_j(u)| \leq \frac{1}{p} \sum_{x=1}^{p-1} \left| \frac{\sin(\pi xN_j/p)}{\sin(\pi x/p)} \right|$$

$$\leq \frac{4}{\pi^2} \log p + .38 + \frac{.608}{p} + \frac{.116}{p^3}$$

$$\leq \begin{cases} \frac{4}{\pi^2} \log p + .381, & \text{if } p > 607; \\ \frac{4}{\pi^2} \log p + \frac{1}{2}, & \text{if } p > 5. \end{cases}$$
Hence for $p > 607$,
\[
|E| \leq (d + 1 + 2.292 p^{89/92}) \left( \sum_{a=1}^{p-1} |a_i(u)| \right) \left( \sum_{v=1}^{p-1} |a_j(v)| \right)
\leq (d + 1 + 2.292 p^{89/92}) \left( \frac{4}{\pi^2} \log p + .381 \right)^2.
\]

Since $p/n - 1 < N_i, N_j < p/n + 1 - 1/n$ we have $p/n^2 - 1 < M < p/n^2 + 1$. \(\square\)

Notice that if $d < 0.006 p^{89/92}$ and $p \geq e^{333} (n \log n)^{184/3}$ then the main term in Theorem 3.1 exceeds the error term and we can say that $f(I_i) \cap I_j \neq \emptyset$ for all $i,j$. If our interest is just in proving that $f(I_i) \cap I_j$ is nonempty, rather than obtaining an asymptotic estimate of its cardinality, then as shown in the next theorem we do not need the log $n$ term.

**Theorem 3.2.** Let $p$ be an odd prime and $A,k,n$ integers satisfying (1.1) with $2 \leq n < p$, and
\[
d = \gcd(k-1, p-1) \leq 0.006 p^{89/92}.
\]
(a) For any $i,j$, $0 \leq i, j < n$, we have $f(I_i) \cap I_j \neq \emptyset$ provided that
\[
p > 4 \cdot 10^{29} n^{44/3}.
\]
(b) For any $i,j$, $0 \leq i, j < n$, we have $f(I_i) \subseteq I_j$ provided that
\[
p > 9 \cdot 10^{34} n^{92/3}.
\]

**Proof.** (a) Recall, for $0 \leq j \leq n-1$, $I_j = \{ x : x \equiv j \mod n, x \neq 0 \} \subseteq \mathbb{Z}_p$, $N_j = |I_j|$. Let
\[
J_j := \{ j, j+n, \ldots, j+(\lceil N_j/2 \rceil - 1)n \} \subseteq \mathbb{Z}_p, \quad j \neq 0,
\]
\[
K_j := \{ 0, n, 2n, \ldots, \lfloor N_j/2 \rfloor n \} \subseteq \mathbb{Z}_p,
\]
with $J_0 = \{ n, 2n, \ldots, \lceil N_0/2 \rceil n \}$, so that $J_j + K_j \subseteq I_j$, and let $\alpha_j = \mathcal{F}_{J_j} * \mathcal{F}_{K_j}$, the convolution of the characteristic functions of $J_j$ and $K_j$,
\[
\alpha_j(x) := \sum_{u \in J_j} \sum_{v \in K_j} 1,
\]
with Fourier coefficients $b_j(y)$ say. Then $\alpha_j$ is supported on $I_j$, and so our goal is to show that for any $i,j$,
\[
\sum_{x \mod p} \alpha_i(x)\alpha_j(Ax^k) > 0.
\]
Expanding the sum as before we obtain
\[
\sum_{x \mod p} \alpha_i(x)\alpha_j(Ax^k) = b_i(0)b_j(0)p + \sum_{u \not\equiv 0} \sum_{v \not\equiv 0} b_i(u)b_j(v) \sum_{x \mod p} e_p(ux + vAx^k)
= M' + E',
\]
say, where $M'$ is the main term and $E'$ the error term. Plainly, we have
\[
M' = |J_i||K_i||J_j||K_j|p^{-1}.
\]
Next, using the fact that $b_j(v) = pa'_j(v)a''_j(v)$ where $a'_j(v)$, $a''_j(v)$ are the Fourier coefficients of $I_{K_j}$, we obtain from the Cauchy-Schwarz inequality and Parseval identity that for any $j$,

$$\sum_{v \mod p} |b_j(v)| = p \sum_{v \mod p} |a'_j(v)||a''_j(v)| \leq p \left( \sum_{v \mod p} |a'_j(v)|^2 \right)^{\frac{1}{2}} \left( \sum_{v \mod p} |a''_j(v)|^2 \right)^{\frac{1}{2}} = |J_j|^\frac{1}{2} |K_j|^\frac{1}{2}.$$ 

Thus, since $d \leq 0.006 p^{89/92}$ and $p > 10^{20}$, $|E'| \leq (d+1+2.292 p^{89/92})|J_j|^\frac{1}{2} |K_j|^\frac{1}{2} |J_i|^\frac{1}{2} |K_i|^\frac{1}{2} < 2.299 p^{89/92} |J_j|^\frac{1}{2} |K_j|^\frac{1}{2} |J_i|^\frac{1}{2} |K_i|^\frac{1}{2},$ and we see that $M' > |E'|$ provided that

$$|J_j||K_j||J_i||K_i| > p^2 \left( 2.299 p^{89/92} \right)^2.$$ 

Since $|J_j| \geq N_j/2$, $|K_j| \geq N_j/2$ and $N_j \geq \frac{p}{n} - 1$ for all $j$, it suffices to have

$$(p - n)^4 > 2^4 n^4 p^2 \left( 2.299 p^{89/92} \right)^2,$$

and for this it suffices to have $p > 4 \cdot 10^{20} n^{4.44}$.

(b) We may assume that $n \geq 3$. For type (iii) intersections, we let $I_j^c = \mathbb{Z}_p \setminus I_j$, a set of cardinality $N_j^c = p - |I_j| \geq p(1 - \frac{1}{n}) - 1 \geq 2p/3 - 1$. For $j \neq 0$ we shall think of $I_j^c$ as the arithmetic progression

$$I_j^c = \{ j + nt : t = N_j, N_j + 1, \ldots, p-1 \},$$

on observing that the values corresponding to $t = 0, 1, \ldots, p-1$ are distinct mod $p$, giving $\mathbb{Z}_p$, and that we have removed the $t = 0, 1, \ldots, N_j - 1$ constituting $I_j$. Similarly $I_j^c = \{ nt : t = N_0 + 1, \ldots, p \}$. We define $\alpha_j$ as above with sets

$$J_j^c = \{ j + N_j n, j + (N_j + 1)n, \ldots, j + (N_j + [N_j^c/2] - 1)n \}, \quad K_j' = \{ 0, n, 2n, \ldots, [N_j^c/2]n \},$$

with $J_j^c = \{ (N_j + 1)n, \ldots, (N_j + [N_j^c/2])n \}$, so that $J_j^c, K_j'$ have cardinalities at least $N_j^c/2$, and $\alpha_j$ is supported on $I_j^c$. Once again we succeed in obtaining $f(I_i) \cap I_j \neq \emptyset$, provided that

$$|J_j^c||K_j'||J_i||K_i| > p^2 (2.299 p^{89/92})^2,$$

and for this it suffices to have

$$p > 9 \cdot 10^{34} n^{9.2}. \quad \square$$

4. Type (iii) intersections for large $d$

In this section we show that for large $d$ we cannot have $f(I_i) \subseteq I_j$ for any $i, j$ provided $p$ is sufficiently large. Recall

$$I = \{1, 2, \ldots, p-1\}, \quad I_j = \{x \in I : x \equiv j \mod n\}.$$

Theorem 4.1. Suppose that $f(x) \neq \pm x \mod p$ when $n$ is even, and $f(x) \neq \pm x$ or $\pm x^{(n+1)/2} \mod p$ when $n$ is odd. If $p > 10^6$ and $d \geq 0.66np^{1/2} \log^2 p$, then $f(I_i) \cap (I \setminus I_j) \neq \emptyset$ for all $i, j$.

The same conclusion holds if $p \geq 7$ and $d > 3n\sqrt{p} \log^2 p$. 


Plainly \( f(x) = \pm x \mod p \) maps \( I_i \) to \( I_i \) or to \( I_j \) where \( i \equiv p - i \mod n \) so must be excluded. The \( f(x) = \pm x^{(p+1)/2} \) are dealt with in Example 1.1, where for \( p > 4n^2 \) and \( n \) even we always have \( f(I_i) \cap (I \setminus I_j) \neq \emptyset \), but for odd \( n \) must be excluded.

**Proof.** Suppose that \((A, k) \neq (\pm 1, 1)\) or \((\pm 1, (p + 1)/2)\). Observe that the set of absolute least residues

\[ C = \{ C = Ax^{k-1} \mod p : 1 \leq x \leq p - 1, \quad |C| < p/2 \}, \]

must contain at least one element \( C \neq \pm 1 \). To see this observe that \( C \) contains \((p - 1)/d\) elements and hence more than two unless \( d = (p - 1) \) or \((p - 1)/2\) and \( k = 1 \) or \((p + 1)/2\). In these cases \( C \) contains only \( A \) or \( \pm A \) and we just need to avoid \( A = \pm 1 \). We need to prove that \( f(I_i) \cap (I \setminus I_j) \neq \emptyset \). We shall suppose that our \( C = AB^{k-1} \mod p \) satisfies \( 1 < C < p/2 \); if all the potential \( C \)'s are negative we replace \( A \) by \(-A\) and \( j \) by the least residue of \( p - j \mod n \). We let

\[ L := (p - 1)/d \]

and

\[ \mathcal{U} = \{ x \in I_i : Cx \mod p \in I \setminus I_j, \quad x \equiv Bz^{L} \mod p \text{ for some } z \}. \]

Notice that if \( x \) is in \( \mathcal{U} \) we have

\[ Ax^{k} \equiv Cx(B^{-1}x)^{k-1} \equiv Cxz^{L(k-1)} = Cx(z^{p-1}(p-1)/d) \equiv Cx \mod p \]

and we have an \( f(x) \) in \( f(I_i) \cap (I \setminus I_j) \). So it is enough to show that \(|\mathcal{U}| > 0\).

Let \( \hat{G} \) denote the set of Dirichlet (multiplicative) characters on \( \mathbb{Z}_p^* \) with principal character \( \chi_0 \) and recall that

\[ \sum_{\chi \in \hat{G} \chi^L = \chi_0} \chi(y) = \begin{cases} L, & \text{if } y \text{ is an } L \text{th power mod } p, \\ 0, & \text{if } y \text{ is not an } L \text{th power mod } p. \end{cases} \]

Hence, writing \( \mathcal{F}^c_j(x) \) for the characteristic function of \( I \setminus I_j \), the complement of \( I_j \), we have

\[ L|\mathcal{U}| = \sum_{x \in \mathbb{Z}_p^*} \mathcal{F}_i(x) \mathcal{F}^c_j(Cx) \sum_{\chi \in \hat{G} \chi^L = \chi_0} \chi(B^{-1}x). \]

Separating the principal character from the remaining \( L - 1 \) characters with \( \chi^L = \chi_0 \)

\[ L|\mathcal{U}| = M + E, \]

where \( M \) is our ‘main term’

\[ M = \sum_{x \in \mathbb{Z}_p^*} \mathcal{F}_i(x) \mathcal{F}^c_j(Cx), \]

and \( E \) the ‘error’

\[ E = \sum_{\chi^L = \chi_0, \chi \neq \chi_0} \chi(B^{-1}) S(\chi), \]

with \( E = 0 \) when \( k = 1 \), where

\[ S(\chi) = \sum_{x \in \mathbb{Z}_p} \chi(x) \mathcal{F}_i(x) \mathcal{F}^c_j(Cx). \]
Error Term. Taking the finite Fourier expansion for the intervals as in the proof of Theorem 3.1 we have as before

$$J_i(x) = \sum_{y \in \mathbb{Z}_p} a_i(y)e_p(yx), \quad |a_i(y)| = \frac{1}{p} \left\{ \begin{array}{ll} N_i, & \text{if } y = 0; \\ |\sin(\pi N_i ny/p)|, & \text{if } y \neq 0, \end{array} \right.$$ 

with $N_i = |I_i|$, and

$$J_j^c(x) = \sum_{y \in \mathbb{Z}_p} a_j^c(y)e_p(yx), \quad a_j^c(y) = \begin{cases} 1 - a_j(0), & \text{if } y = 0; \\ -a_j(y), & \text{if } y \neq 0. \end{cases}$$

Again, separating the terms with $u$ or $v$ zero, we have

$$S(\chi) = \sum_{x \in \mathbb{Z}_p} \chi(x) \sum_{u=0}^{p-1} a_i(u)e_p(ux) \sum_{v=0}^{p-1} a_j^c(v)e_p(vCx) = T_1 + E_1 + E_2 + E_3$$

where

$$T_1 = a_i(0)a_j^c(0) \sum_{x \in \mathbb{Z}_p} \chi(x) = 0,$$

$$E_1 = a_i(0) \sum_{v=1}^{p-1} a_j^c(v) \sum_{x=0}^{p-1} \chi(x)e_p(Cvx),$$

$$E_2 = a_j^c(0) \sum_{u=1}^{p-1} a_i(u) \sum_{x=0}^{p-1} \chi(x)e_p(ux),$$

and

$$E_3 = \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} a_i(u)a_j^c(v) \sum_{x \in \mathbb{Z}_p} \chi(x)e_p((u + Cv)x).$$

Recalling that, for a non-principal character $\chi$, the classic Gauss sums $G(\chi, A) = \sum_{x=0}^{p-1} \chi(x)e_p(Ax)$ satisfy $|G(\chi, A)| = p^{1/2}$ if $p \nmid A$ and trivially $G(\chi, A) = 0$ if $p \mid A$, and again invoking [9, Theorem 1], we have for $p > 607$

$$|E_1| \leq \frac{N_i}{p} \sum_{v=1}^{p-1} |a_j^c(v)|p^{1/2} \leq \frac{N_i}{p} \left( \frac{4}{\pi^2} \log p + 0.381 \right) p^{1/2},$$

$$|E_2| \leq \frac{(p - 1 - N_j)}{p} \sum_{u=1}^{p-1} |a_i(u)|p^{1/2} \leq \frac{(p - 1 - N_j)}{p} \left( \frac{4}{\pi^2} \log p + 0.381 \right) p^{1/2},$$

$$|E_3| \leq \left( \sum_{u=1}^{p-1} |a_i(u)| \right) \left( \sum_{v=1}^{p-1} |a_j^c(v)| \right) \leq \left( \frac{4}{\pi^2} \log p + 0.381 \right)^2 p^{1/2},$$

with $N_i + (p - 1 - N_j) \leq p$. Hence, for $p > 10^6$,

$$|S(\chi)| \leq \left( \frac{4}{\pi^2} \log p + 0.381 \right) p^{1/2} + \left( \frac{4}{\pi^2} \log p + 0.381 \right)^2 p^{1/2} < 0.22 p^{1/2} \log^2 p,$$

and

$$|E| < 0.22(L - 1)p^{1/2} \log^2 p.$$
Main Term. We have

$$M = |I_i| - \sum_{x \in \mathbb{Z}_p} \mathcal{J}_i(x) \mathcal{J}_j(Cx) = N_i - M_{ij},$$

where $N_i$ is as given in (3.1), and

$$M_{ij} = |\{x \in I_i : Cx \mod p \in I_j\}|.$$

So for a lower bound on $M$ we need an upper bound on $M_{ij}$. Since for $1 \leq x < p$ we have $0 < Cx < Cp$ we have

$$M_{ij} = \sum_{u=0}^{C-1} |\{x \in I_i : up \leq Cx < (u+1)p, \ Cx - up \in I_j\}|.$$

Note, if $x \equiv i \mod n$ then $Cx - up \equiv j \mod n$ requires $u \equiv K := (Ci - j)p^{-1} \mod n$. Observing that the number of elements in a particular residue class mod $n$ in an interval of cardinality $B$ is at most $\left\lfloor \frac{(B - 1)n}{C} \right\rfloor + 1$ we have

$$M_{ij} = \sum_{u=0}^{C-1} \left|\{x \in I_i : up \leq Cx < (u+1)p, \ Cx - up \in I_j\}\right| \leq \left(\left\lfloor \frac{C-1}{n} \right\rfloor + 1\right) \left(\left\lfloor \frac{p/C}{n} \right\rfloor + 1\right).$$

Plainly

$$M_{ij} \leq \left(\frac{C}{n} + 1\right) \left(\frac{p}{Cn} + 1\right) = \frac{p}{n^2} + \frac{C}{n} + \frac{p}{Cn} + 1,$$

and so for $p/2n \geq C \geq 2n$,

$$M_{ij} \leq \frac{2p}{n^2} + 1.$$

For $2n > C \geq n$, $\left\lfloor (C - 1)/n \right\rfloor = 1$ and so by (4.2),

$$M_{ij} \leq 2 \left(\frac{p}{Cn} + 1\right) \leq 2 \left(\frac{p}{n^2} + 1\right) = \frac{2p}{n^2} + 2,$$

while for $p/n \geq C > p/2n$, $\left\lfloor p/(Cn) \right\rfloor = 1$, and so

$$M_{ij} \leq 2 \left(\frac{C}{n} + 1\right) \leq 2 \left(\frac{p}{n^2} + 1\right) = \frac{2p}{n^2} + 2.$$

For $C < n$, since $2 \leq C < p/2$, we have by (4.2),

$$M_{ij} \leq \left(\left\lfloor \frac{C}{n} \right\rfloor + 1\right) \left(\left\lfloor \frac{p/C}{n} \right\rfloor + 1\right) \leq \left(\frac{C}{n} + 1\right) \cdot \left(\frac{p}{Cn} + 1\right) \leq \frac{p}{2n} + 1,$$

and when $C > p/n$

$$M_{ij} \leq \left(\left\lfloor \frac{C}{n} \right\rfloor + 1\right) \left(\left\lfloor \frac{p/C}{n} \right\rfloor + 1\right) \leq \left(\frac{C}{n} + 1\right) \cdot \frac{C}{n} + 1 < \frac{p}{2n} + 1.$$

Hence, in all cases we have

$$M_{ij} \leq \max\left\{\frac{2p}{n^2} + 2, \ \frac{p}{2n} + 1\right\},$$

and see that for $n \geq 3$,

$$M_{ij} \leq \frac{2p}{3n} + 2,$$
and

\begin{equation}
M \geq \left| \frac{p}{n} \right| - M_{ij} > \frac{p}{n} - 1 - M_{ij} \geq \frac{p}{3n} - 3.
\end{equation}

From (4.1), when \( p > 10^6 \) we certainly have \( |E| < 0.22Lp^{1/2} \log^2 p - 3 \) with \( L < p/d \). Thus if \( p/3n \geq (0.22)p^{3/2} \log^2 p/d \) we have \( |E| < M \) and \( |\mathcal{Y}| > 0 \).

If instead, we use the bound \( \sum |a_i(u)| \leq \frac{1}{n} \log p + \frac{1}{2} \), valid for \( p \geq 7 \), we obtain \( |E| < L\sqrt{p} \log^2 p - 4 \), and conclude that \( M > |E| \) for \( d \geq 3n\sqrt{p} \log^2 p \). \( \square \)

5. Proofs of Theorems 1.2, 1.3, 1.5

Proof of Theorems 1.2. Suppose that \( p > 9 \cdot 10^{34} n^{92/3} \). Then certainly \( p > 6.7 \times 10^8 \). If \( d \leq 0.006 p^{89/92} \) then Theorem 1.2 follows from Theorem 3.2, while if \( d > 0.66 np^{1/2} \log^2 p \) it follows from Theorem 4.1. If neither of these occurs then \( 0.66 np^{1/2} \log^2 p > d > 0.006 p^{89/92} \) and so \( p^{43/92} / \log^2 p < 110n \). But this does not occur for \( p > 9 \cdot 10^{34} n^{92/3} \). \( \square \)

Proof of Theorem 1.3. We revisit the proof of Theorem 4.1. For \( k = 1 \) there is no error term \( E \), and so we need only show that \( M > 0 \). This follows from (4.5) for \( p > 9n \). Our computations, see Table 1, have checked \( 2n < p < 9n \) for \( 3 \leq n \leq 12 \) so we can assume that \( n > 12 \). For \( 4n < p < 9n \) we plainly have \( 2p/n^2 + 2 < 18/n + 2 < 4 \leq |p/n| \) and \( p/2n + 1 < p/n - 1 \) and thus by (4.4) \( N_i > M_{ij} \). Finally for \( 2n < p < 4n \) by (4.4) we have \( M_{ij} < 3 \) and, since \( M_{ij} \) is a count, \( M_{ij} \leq 2 \).

Hence the result when \( p > 3n \) and \( |p/n| \geq 3 \), or when \( 2n < p < 3n \) and \( |I_i| = 3 \).

It remains to check the case \( 2n < p < 3n \) when \( |I_i| = 2 \). Writing \( p = 2n + e \) with \( 1 \leq e < n \), and \( I_n \) for \( I_0 \), we have \( I_j = \{ j, j + n, j + 2n \} \) for \( 1 \leq j \leq e \), and \( I_j = \{ j, j + n \} \) for \( e < j \leq n \). Suppose \( f(I_i) \subseteq I_j \) with \( e < i \leq n, 1 \leq j \leq n \). We assume that \( A \neq \pm 1 \) and that \( A > 0 \) (else replace \( A \) by \( -A \) and \( j \) by \( j = p - j \) mod \( n \)). Then

\[ f(i) \equiv A_i \equiv j + un \mod p, \quad f(i + n) \equiv A_i + An \equiv j + vn \mod p, \]

for some \( u, v \in \{0, 1, 2\}, u \neq v \). Subtracting, we get \( A \equiv v - u \mod p \), and since \( A \geq 2 \), get \( A = 2, v = 2, u = 0 \). This yields \( 2i \equiv j \mod p \), meaning \( j = 2i > i \) since \( p > 2n \). But, \( v = 2 \) implies that \( |I_j| = 3 \) and hence \( j < i \). \( \square \)

Proof of Theorem 1.5. In the proof of Theorem 3.2 we use the Weil bound [22] \( |k - 1|/\sqrt{p} \) in place of (3.3) and for (a) and (b) we just need

\[ |J_j||K_j||I_i||K_i| > |k - 1|p^3 \quad \text{and} \quad |J_j||K_j||I_i||K_i| > |k - 1|p^3, \]

in place of (3.5) and (3.4).

\( \square \)

6. Proof of Theorem 1.4

Notice that \( f(x) = Ax^{(p+1)/2} \mod p \) is related to two linear maps:

\begin{equation}
f(x) \equiv A \left( \frac{x}{p} \right) x \equiv \pm Ax \mod p,
\end{equation}

and that the inverse mapping \( f^{-1}(x) \) is given by

\begin{equation}
f^{-1}(x) = \left( \frac{A}{p} \right) A^{-1}x^{(p+1)/2} \mod p.
\end{equation}
In order to prove \( f(x) \) is not a Type (iii) mapping we can replace \( f(x) \) with \( \pm f(x) \) or \( \pm f^{-1}(x) \) (with one exception), which amounts to changing \( A \) to \( \pm A \) or \( \pm A^{-1} \).

Thus we define the quantity
\[
C := \min\{|A|, |A^{-1}|\},
\]
where \( A, A^{-1} \) are taken to be integers with \( |A|, |A^{-1}| < p/2 \). Note that if \( |I_i| = |I_j| \) then \( f(I_i) \subseteq I_j \) is the same as \( f(I_i) = I_j \) or \( f^{-1}(I_j) = I_i \). The one exception that needs special attention is if for some \( i, j \), \( f(I_i) \) is a proper subset \( I_j \), that is, \( |I_j| = |I_i| + 1 \). Then \( f(I_i) = I_j \setminus \{a\} \) for some \( a \), with \( f^{-1}(I_j \setminus \{a\}) = I_i \), and so in replacing \( f \) with \( f^{-1} \) we must remove one element from each of the larger \( I_i \) and still show that \( f(I_i) \) hits at least two different residue classes.

To prove Theorem 1.4 we must show that for \( p > (4n + 1)^2 \), and \( C \geq 2 \), the mapping (6.1) is not a Type (iii) mapping. The theorem is an immediate consequence of the following two lemmas, the first dealing with the case \( C = 2 \), and the second all larger \( C \).

**Lemma 6.1.** Suppose that \( n \geq 2 \), \( f(x) = Ax^{(p+1)/2} \mod p \) with \( A \neq \pm 1 \), and let \( C \) be as given in (6.3). If \( p > (2Cn + 1)^2 \) then \( f(x) \) is not a Type (iii) mapping.

**Proof.** Suppose first that \( A = C \) and \( 0 \leq i < n \). Consider the sets
\[
U_1 = \{u \in \mathbb{Z} : 0 \leq u < (p/C - i)/n\},
\]
\[
U_2 = \{u \in \mathbb{Z} : (p/C - i)/n \leq u \leq (2p/C - i)/n\},
\]
with \( u = 0 \) excluded from \( U_1 \) when \( i = 0 \). Since \( p > (2Cn + 1)^2 \) we have
\[
|U_i| \geq \frac{p}{Cn} - 1 > 2\sqrt{p},
\]
and thus by the result of Hummel [15], any translate of these intervals must contain at least two quadratic residues and two nonresidues. Hence there will be \( u_1, u_2 \) in \( U_1 \) and \( u_3, u_4 \) in \( U_2 \) with
\[
\left(\frac{in^{-1} + u_l}{p}\right) = \left(\frac{n}{p}\right), \quad l = 1, 2, 3, 4,
\]
and therefore
\[
\left(\frac{i + u_l n}{p}\right) = 1, \quad l = 1, 2, 3, 4.
\]
Note that
\[
0 < i + u_1 n < p/A, \quad l = 1, 2,
\]
\[
p/A < i + u_4 n < 2p/A \leq p, \quad l = 3, 4,
\]
and thus \( i + u_l n \in I_l, 1 \leq l \leq 4 \) with by (6.1),
\[
f(i + u_l n) = C(i + u_l n) \equiv C_l \mod n, \quad l = 1, 2
\]
\[
f(i + u_l n) = C(i + u_l n) - p \equiv C_l - p \mod n, \quad l = 3, 4.
\]
These two values must be distinct mod \( n \).

Finally, if \( A \neq C \) then we replace \( f(x) \) with \( -f(x) \), \( f^{-1}(x) \) or \( -f^{-1}(x) \) to make \( A = C \), and note that passing to \( f^{-1}(x) \) presents no new difficulties because each \( I_i \) had at least two quadratic residues and two quadratic nonresidues. \( \square \)

**Lemma 6.2.** Suppose that \( f(x) = Ax^{(p+1)/2} \mod p \), with \( A \neq \pm 1, \pm 2, \pm (p-1)/2, \)
\[ n \geq 2 \text{ and } p > 18n. \] Then \( f(x) \) is not a Type (iii) map.
Indeed, in this case either $C(6.4)$ or $M(6.7) \leq \frac{p}{n}$.

Proof. Suppose first that $n \geq 4$ and that $C$ is as given in (6.3). By assumption $3 \leq C < \frac{p}{2}$.

Writing $j = p - j$ mod $n$, and

$$M_{ij} = | \{ x \in I_i : Ax \mod p \in I_j \} |,$$

if $f(I_i) \subseteq I_j$ then by (6.1) the image of $I_i$ under the linear map $Ax \mod p$ must lie in $I_j$ or $I_7$ and we must have $|I_i| \leq M_{ij} + M_{7j}$. Hence to rule out a Type (iii) it will be enough to check that for all $i, j$

$$2M_{ij} < \frac{p}{n} - 1. \tag{6.4}$$

We proceed as in the proof of Theorem 4.1 considering various ranges for the size of $C$. In the cases where we need to replace $f$ with $f^{-1}$ and delete one element from the larger $I_i$, we have for some $j$, $|I_i| - 1 = |I_j| > p/n - 1$ and so it is still enough to show (6.4) for $f^{-1}$.

High $C$'s. For $n \geq 5$ we claim that we cannot have $C$ in the range

$$\frac{p}{2} - \frac{1}{2}\sqrt{p - 4} < C \leq \frac{p}{2}. \tag{6.5}$$

Indeed, in this case either $C^{-1}$ or $-C^{-1}$ is also in this range, say $C' := \pm C^{-1}$. Then

$$\pm 4 \equiv (p - 2C)(p - 2C') \mod p,$$

but $|(p - 2C)(p - 2C')| \leq 4 + \sqrt{p - 4} = p$ and parity rules out equality. Similarly, for $n = 4$ we claim that we cannot have both $C$ and $C' = \pm C^{-1}$ in intervals

$$\frac{p}{s} - \frac{1}{4}\sqrt{p - 16} < C \leq \frac{p}{s}, \quad s \in \{2, 4\},$$

$$\frac{p}{s'} - \frac{1}{4}\sqrt{p - 16} < C' \leq \frac{p}{s'}, \quad s' \in \{2, 4\},$$

otherwise

$$\pm 16 \equiv \left(\frac{4}{s}p - 4C\right)\left(\frac{4}{s'}p - 4C'\right) \mod p,$$

$$0 < \left(\frac{4}{s}p - 4C\right)\left(\frac{4}{s'}p - 4C'\right) < p - 16, \tag{6.6}$$

implying equality in (6.6) which cannot occur since $4 \nmid \frac{4}{s}p - 4C$ or $\frac{4}{s'}p - 4C$. Hence when $n = 4$, replacing $C$ by $\pm C^{-1}$ as necessary, we can assume that $C$ does not satisfy (6.5).

For the remaining ranges we use the inequality in (4.2), (4.3),

$$M_{ij} \leq \left(\left\lfloor \frac{C - 1}{n} \right\rfloor + 1 \right)\left(\left\lfloor \frac{p/C}{n} \right\rfloor + 1 \right) < \frac{p}{n^2} + \frac{C}{n} + \frac{p}{Cn} + 1. \tag{6.7}$$

Middle $C$ values. Suppose that $2n \leq C \leq p/2n$. This case only occurs when $p \geq 4n^2$, so $2n \leq \sqrt{p} \leq p/2n$ and

$$M_{ij} < \frac{p}{n^2} + \frac{C}{n} + \frac{p}{Cn} + 1 \leq \frac{3p}{2n^2} + 3.$$

Hence,

$$2M_{ij} < 3n^{-1} \frac{p}{n} + 6 \leq \frac{p}{n} - 1,$$

for $p \geq 7/(1 - 3n^{-1})n$; in particular for $p > 112$ if $n = 4$ and $p \geq 17.5n$ if $n \geq 5$. 
Small $C$ values. Suppose that $n < C < 2n$. Then by (6.7),
\[
M_{ij} < 2 \left( \frac{p}{Cn} + 1 \right) \leq \frac{2p}{(n+1)n} + 2
\]
and $2M_{ij} < p/n - 1$ for $p > \frac{5}{1 - 4(n+1)^{-1}}$, for example $p > 100$ if $n = 4$ and $p > 15n$ if $n \geq 5$.

Very Small $C$ values. Suppose that $3 \leq C < n$. Then by (6.7),
\[
M_{ij} \leq \left( \frac{p}{Cn} + 1 \right) \leq \frac{p}{3n} + 1
\]
and $2M_{ij} < p/3n + 2 < p/n - 1$ as long as $p > 9n$.

Large $C$ values. Suppose that $n \geq 5$ and $p/n < C < p/2 - \frac{1}{2}\sqrt{p-4}$, or $n = 4$ and $p/n < C < p/2 - \frac{1}{4}\sqrt{p} - 16$. For $n \geq 5$ we get by (6.7),
\[
M_{ij} \leq \left( \frac{C-1}{n} + 1 \right) \leq \frac{p}{2n} - \frac{\sqrt{p}}{2n} + 1
\]
and $2M_{ij} < (p/n) - 1$ for $p > 9n^2$.

For $n = 4$ we have $2M_{ij} \leq \frac{p}{n} - \frac{\sqrt{p}}{2n} + 2 < \frac{p}{n} - 1$ for $p > 36n^2$, but there are no values giving Type (iii) with $k = (p+1)/2$ and $p < 576$; see Table 3.

For later use, observe also that if $\delta > 3$ and $p/n < C \leq \frac{1}{2}(1 - 3\delta^{-1})p$ and $p \geq \delta n$ then
\[
(6.8) \quad 2M_{ij} < 2 \left( \frac{C}{n} + 1 \right) < (1 - 3\delta^{-1})\frac{p}{n} + 2 \leq \frac{p}{n} - 1.
\]

Largish $C$ values. Suppose that $n \geq 5$ and $p/2n < C \leq p/n$, or $n = 4$ and $p/2n < C \leq p/4 - \frac{1}{4}\sqrt{p} - 16$. If $n \geq 5$ then by (6.7),
\[
M_{ij} \leq \left( \frac{C-1}{n} + 1 \right) \leq 2n^{-1} \frac{p}{n} + 2
\]
and $2M_{ij} < (p/n) - 1$ for $p > \frac{5}{1 - 4n^{-1}} n$; for example if $p > 125$ for $n = 5$ and $p > 15n$ for $n \geq 6$.

For $n = 4$ we get from (6.7),
\[
2M_{ij} \leq \frac{p}{4} - \frac{1}{4}\sqrt{p} + 4 < \frac{p}{4} - 1
\]
for $p > 20^2$. As seen in Table 3, there are no examples with $p < 400$.

Hence there are none of these Type (iii) maps when $n \geq 4$ and $p > 9n^2$. Computations show that there are none with $18n < p < 9n^2$ for $4 \leq n \leq 13$; see Table 3. Hence we can assume that $n \geq 14$ and $18n < p < 9n^2$. Suppose now that $p \geq \delta n$ with $28 \geq \delta > 17$, then from the above cases and (6.8) we are left only to consider the range
\[
\frac{1}{2}(1 - 3/\delta)p \leq C < \frac{p}{2} - \frac{1}{2}\sqrt{p-4}.
\]
Taking $C'' := p - 2C$ we have
\[
(6.9) \quad \sqrt{p-4} < C'' < \frac{3}{\delta} p.
\]
Observe that if \( Cx \mod p \) is in \( I_j \) for all \( x \) in \( I_i \) then \( 2Cx \mod p \) will be in \( I_i \) where \( \ell \equiv 2j, 2j - p, 2j \) or \( 2j - p \mod n \) and \( C''x \mod p \) can fall in at most four different \( I_i \). Hence with \( M'_{ij} = \{ x \in I_i : C''x \mod p \in I_j \} \) we will get a contradiction if \( 4M'_{ij} < \frac{p}{n} - 1 \). As before we have

\[
M'_{ij} < \frac{p}{n^2} + \frac{C''}{n} + \frac{p}{C''n} + 1.
\]

For \( C'' \) in the interval (6.9), the quantity \( C'' + p/C'' \) is maximized at \( \frac{3}{5}p \geq \frac{3}{28}p \) (since \( p > 91 \)) and so

\[
M'_{ij} < \frac{p}{n^2} + \frac{1}{n} \left( \frac{3}{5}p + \frac{\delta}{3} \right) + 1 \leq \frac{1}{4} \left( \frac{p}{n} - 1 \right),
\]

provided that

\[
\frac{p}{n} \left( \frac{1}{3} - \frac{3}{\delta} - \frac{1}{n} \right) \geq \frac{\delta}{3n} + \frac{5}{4},
\]

and for \( p \geq \delta n \) this holds for \( n \geq 16\delta/3(\delta - 17) \). Taking \( \delta = 28 \) this holds for \( n \geq 14 \) and we obtain the lemma for \( p > 28n \) and all \( n \geq 4 \). Taking \( \delta = 18 \) this holds for \( n \geq 96 \). It remains to computationally check the \( 14 \leq n \leq 95 \) and \( 20n < p < 28n \). Moreover, by successively decreasing \( \delta \), we can further reduce the range to be checked; so for example we just need to check \( p < 19n \) for the \( 51 \leq n \leq 95 \), check \( p < 20n \) for the \( 36 \leq n \leq 50 \), etc. Computations for \( n = 14 \) to \( 50 \) and \( 2n < p < cn \), with the appropriate \( c \) between 28 and 19, produced 2241 Type (iii) maps of the form \( Ax^{(p+1)/2} \mod p \) with \( 2 < A < (p-1)/2 \). None of these had \( p > 18n \), indeed none had \( p > 3n \).

**The Case** \( n = 3 \). It remains to deal with \( n = 3 \). From our computations we know that there are no Type (iii) mappings with \( 6 < p < 20,000 \). Replacing \( A \) by \( A^{-1} \) as necessary we may assume that our \( C \) does not lie in any of the intervals

\[
U_s = \left( \frac{s}{p}, 12\sqrt[3]{p-144}, \frac{s}{p} \right), \quad s = 2, 4 \text{ or } 6.
\]

To see this observe that if \( C = \pm A \) is in \( U_s \) and \( C' = \pm A^{-1} \) is in \( U_s' \) then

\[\pm 144 \equiv (12p/s-12C)(12p/s'-12C') \mod p, \quad 0 < (12p/s-12C)(12p/s'-12C') < p-144,\]

where \( 2^2 | 12p/s-12C \) or \( 12p/s'-12C' \) rules out equality.

For \( 2 \leq C \leq 9 \) from Lemma 6.1 there are no such Type (iii) with \( p > 3025 \).

For \( 9 \leq C \leq p/9 \) and \( p > 243 \) we have

\[
2M_{ij} \leq 2 \left( \frac{p}{9} + \frac{C}{3} + \frac{p}{3C} + 1 \right) \leq \frac{8p}{27} + 8 < \frac{p}{3} - 1.
\]

For \( p/9 < C < p/6 - \frac{1}{12}\sqrt[p-144]{} \) and \( p > 1764 \) we have

\[
2M_{ij} \leq 2 \left( \frac{C-1}{3} + 1 \right) \cdot 3 \leq \frac{p-\sqrt[p]{p}}{6} + 6 < \frac{p}{3} - 1.
\]

For \( p/6 < C < p/4 - \frac{1}{12}\sqrt[p-144]{} \) and \( p > 2025 \) we have

\[
2M_{ij} \leq 2 \left( \frac{C-1}{3} + 1 \right) \cdot 2 \leq \frac{p-\sqrt[p]{p}}{9} + 4 < \frac{p}{3} - 1.
\]
For $p/3 < C < p/2 - \frac{1}{12}\sqrt{p-144}$ and $p > 2916$ we have

$$2M_{ij} \leq 2 \left( \frac{C-1}{3} + 1 \right) \cdot 1 \leq \frac{p}{3} - \frac{\sqrt{p}}{18} + 2 < \frac{p}{3} - 1.$$

That just leaves the case where $p/4 < C < p/3$. We deal with the map

$$g(x) = Cx^{(p+1)/2} \equiv \left( \frac{x}{p} \right) Cx \mod p$$

directly on $I_0 = \{3, 6, 9, \ldots\}$, $I_1 = \{1, 4, 7, \ldots\}$ and $I_2 = \{2, 5, 8, \ldots\}$.

For $I_0$ observe that $g(6) = 6C - p$ or $2p - 6C \equiv 2p \mod 3$ while $g(9) = 9C - 2p \equiv p \mod 3$ giving us an element in $I_1$ and an element in $I_2$.

For $I_1$ we have $g(1) = C$ and $g(4) = 4C - p$ and these are distinct mod 3.

For $I_2$ we have

$$\left( \frac{2}{p} \right) = 1 \Rightarrow g(2) = 2C, \quad g(8) = 8C - 2p,$$

$$\left( \frac{2}{p} \right) = -1 \Rightarrow g(2) = p - 2C, \quad g(8) = 2p - 8C,$$

and in either case these are distinct mod 3.

This deals with the case $C = \pm A$ and $f(x) = \pm g(x)$ or if $C = A^{-1}$ in the case when $f(I_i) \subseteq I_j$ and the $|I_i| = |I_j|$ as must happen when $p \equiv 1 \mod 3$. This just leaves the case where $p \equiv 2 \mod 3$ and $f(I_0)$ or $f(I_2)$ equals $I_1 \setminus \{a\}$ when the missing $a = 1$ or 4. But notice that when $p \equiv 2 \mod 3$ we have $(p-1)$ and $(p-4)$ in $I_1$ where $g(p-x) \equiv -g(x) \mod p$. Hence $g(p-1) = p - C$ and $g(p-4) = 2p - 4C$ and these two values are again distinct mod 3.

\[\square\]

7. Proof of Example 1.1

**Proof of Example 1.1.** Suppose that $f(x) = \pm x^{(p+1)/2} \mod p$. We have

$$x^{(p+1)/2} = x \cdot x^{(p-1)/2} \equiv x \left( \frac{x}{p} \right) \equiv \pm x \mod p,$$

and $f(x) = x$ or $p - x$, where $(p-x) \equiv x \mod n$ exactly when $x \equiv 2^{-1}p \mod n$ if $n$ is odd and in no cases if $n$ is even, and the first claim is plain.

If $n$ is even, or $n$ is odd and $i \neq 2^{-1}p \mod n$, then $x \neq p - x \mod n$ for $x$ in $I_i$, and $f(I_i)$ will hit two different residue classes as long as $I_i$ contains both quadratic residues and nonresidues. Suppose that $\left( \frac{x}{p} \right)$ is constant on $I_i$, then $\left( \frac{n^{-1}+i}{p} \right)$ is constant for $y$ in an interval of length $|I_i|$. But by [15] there are less than $\sqrt{p}$ consecutive residues or nonresidues, and for $p > (n+1)^2$ we have $|I_i| > p/n - 1 > \sqrt{p}$. \[\square\]

8. Proofs of Theorems 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7 and 2.8

**Proof of Theorem 2.1.** Notice that

$$f(x) = 2x^{(p+1)/2} \mod p = 2 \left( \frac{x}{p} \right) x \mod p.$$

Since $p = 1 \mod 4$ the quadratic residue property gives us

\begin{equation}
\left( \frac{m}{p} \right) = \begin{cases} +1, & \text{if } m = 1 \mod 4, \\ -1, & \text{if } m = 3 \mod 4, \end{cases}
\end{equation}
for any integer \( m \) with \( 1 \leq m \leq 4t - 1 \).

Suppose first that \( i = (2p - (4t - 1)n)/4 \). Since \( n \equiv 2 \mod 4 \) we are guaranteed that \( i = (2p - (4t - 1)n)/4 \) is an integer, with \( i > 0 \) from the upper bound in (2.2), and \( i < n \) for \( n > 2p/(4t + 3) \) which certainly follows from the lower bound. Plainly

\[
4i \equiv 2p \mod n.
\]

The lower bound in (2.2) is to ensure that \( i + 2tn \geq p \) so that the elements \( x \) of \( I_i \) can be written \( x = i + \ell n \) with \( 0 \leq \ell \leq 2t - 1 \), where \( n < 2p/(4t - 3) \) from the upper bound ensures that \( i + (2t - 1)n < p \). Writing \( x = i + \ell n \) we have

\[
\left( \frac{x}{p} \right) = \left( \frac{4x}{p} \right) = \left( \frac{-(4t - 1)n + 4\ell n}{p} \right) = \left( \frac{n}{p} \right) \left( \frac{4\ell - (4t - 1)}{p} \right).
\]

Since \( \left( \frac{-1}{p} \right) = 1 \) we get from (8.1) that

\[
\left( \frac{x}{p} \right) = \left( \frac{n}{p} \right) \left( \frac{4(t - \ell) - 1}{p} \right) = - \left( \frac{n}{p} \right), \quad \ell = 0, \ldots, t - 1,
\]

and

\[
\left( \frac{x}{p} \right) = \left( \frac{n}{p} \right) \left( \frac{4(\ell - t) + 1}{p} \right) = \left( \frac{n}{p} \right), \quad \ell = t, \ldots, 2t - 1.
\]

Notice that \( 2x < p \) iff \( 4\ell < 4t - 1 \), that is \( 0 < 2x < p \) for \( 0 \leq \ell \leq t - 1 \) and \( p < 2x < 2p \) for \( \ell = t, \ldots, 2t - 1 \). Hence

\[
\left( \frac{n}{p} \right) = -1 \Rightarrow f(x) = \begin{cases} 2x, & \text{if } \ell = 0, \ldots, t - 1, \\ 2p - 2x, & \text{if } \ell = t, \ldots, 2t - 1, \end{cases}
\]

while

\[
\left( \frac{n}{p} \right) = 1 \Rightarrow f(x) = \begin{cases} p - 2x, & \text{if } \ell = 0, \ldots, t - 1, \\ 2x - p, & \text{if } \ell = t, \ldots, 2t - 1. \end{cases}
\]

Condition (8.2) ensures that \( f(x) \) takes the value \( j \mod n \) in (2.3) for all \( x \) in \( I_i \).

Similarly for \( i = (2p - (4t - 3)n)/4 \) we have \( 0 < i < n \) and \( I_i = \{ x = i + \ell n : 0 \leq \ell \leq 2t - 1 \} \) for \( 2p/(4t + 1) < n < 2p/(4t - 3) \) with \( 2x < p \) iff \( \ell \leq t - 1 \). This time

\[
\left( \frac{x}{p} \right) = \left( \frac{n}{p} \right) \left( \frac{4t - 3 - 4\ell}{p} \right) = \left( \frac{n}{p} \right), \quad \ell = 0, \ldots, t - 1,
\]

and

\[
\left( \frac{x}{p} \right) = \left( \frac{n}{p} \right) \left( \frac{4\ell - 4t + 3}{p} \right) = - \left( \frac{n}{p} \right), \quad \ell = t, \ldots, 2t - 1,
\]

giving the same forms for \( f(x) \), but with the role of \( \left( \frac{n}{p} \right) = 1 \) or \(-1\) reversed. \( \square \)

**Proof of Theorem 2.2.** Since \( p < 3n \) we have \( I_0 = \{ n, 2n \} \). As \( p \equiv 5 \mod 8 \) we get \( \left( \frac{\pm 1}{p} \right) = -1 \) and

\[
f_{f_{j}}(n) \equiv n^2 - Jn \mod p, \quad f_{f_{j}}(2n) \equiv 2Jn - 2n^2 \mod p.
\]

Writing \( p = 3n - \delta \), \( 0 < \delta < n \), we have \( I_{n-\delta} = \{ n - \delta, 2n - \delta \} = \{ p - 2n, p - n \} \), with \( f_{f_{j}}(p - x) \equiv - f_{f_{j}}(x) \mod p \) and \(- f_{f_{j}}(I_{n-\delta}) = f_{f_{j}}(I_0) \). So it is enough to show the claims for \( I_0 \).

It remains to find the least residue mod \( p \) satisfying (8.3).

For \( p = 72k + 5 \) and \( n = 24k + 2 \), we have

\[
f_0(n) = n^2 - 8kp = 2n + 8k, \quad f_0(2n) = (16k + 2)p - 2n^2 = n + 8k.
\]
For $p = 72k + 13$ and $n = 24k + 5$ we have
\[ f_0(n) = n^2 - (8k + 1)p = 2n + (16k + 2), \quad f_0(2n) = (16k + 4)p - 2n^2 = 16k + 2, \]
and hence $f_1(n) = n + (16k + 2)$, $f_1(2n) = 2n + (16k + 2)$.

For $p = 72k + 29$ and $n = 24k + 10$, we have
\[ f_0(n) = n^2 - (8k + 3)p = n + (8k + 3), \quad f_0(2n) = (16k + 7)p - 2n^2 = 8k + 3, \]
and $f_1(n) = (8k + 3)$, $f_1(2n) = 2n + (8k + 3)$.

For $p = 72k + 37$ and $n = 24k + 13$ we have
\[ f_1(n) = n^2 - n - (8k + 4)p = 16k + 8, \quad f_1(2n) = 2n - 2n^2 + (16k + 9)p = n + (16k + 8). \]

For $p = 72k + 53$ and $n = 24k + 19$ we have
\[ f_1(n) = n^2 - n - (8k + 6)p = n + (8k + 5), \quad f_1(2n) = (16k + 13)p - 2n^2 = 8k + 5, \]
and $f_2(n) = (8k + 5)$, $f_2(2n) = 2n + (8k + 5)$.

For $p = 72k + 61$ and $n = 24k + 22$ we have
\[ f_2(n) = n^2 - 2n - (8k + 7)p = 16k + 13, \quad f_2(2n) = (16k + 15)p + 4n - 2n^2 = n + (16k + 13). \]

\[ \square \]

Proof of Theorem 2.3. Let $f(x) = \left(\frac{n}{p}\right) x^{(p+1)/2}$. Since $p \equiv 1 \pmod{8}$ the quadratic residue condition says that $\left(\frac{2}{p}\right) = 1$ for $1 \leq \ell \leq t$. We have $I_0 = \{\ell n : 1 \leq \ell \leq \lfloor (p - 1)/n \rfloor\}$, where $\lfloor (p - 1)/n \rfloor \leq t$. Hence for the $x = n\ell$ in $I_0$ we have $f(x) \equiv \left(\frac{n}{p}\right) \left(\frac{n\ell}{p}\right) x \pmod{p} = x$.

\[ \square \]

Proof of Theorem 2.4. Observe that $\left(\frac{2(p-1-i)}{p}\right) = \left(\frac{2}{p}\right), \left(\frac{2i+1}{p}\right)$, reducing the consecutive residues or nonresidues about $p/2$ condition to $\left(\frac{2i+1}{p}\right) = 1$ all $1 \leq i \leq T$.

For $i = an - (n/2 - 1 + \delta/2)p = p(1 - \delta/2) - n(t-1)/2$, where $\delta = 0$ for $n$ even and 1 for $n$ odd, we have $i > 0$ for $n < (2 - \delta)p/(t-1)$, and $i < n$ for $n > (2 - \delta)p/(t+1)$. We also have $i + nt = p(1 - \delta/2) + n(t+1)/2 > p$ (immediately for $n$ even and from $n > p/(t + 1)$ for $n$ odd).

Hence $x$ in $I_x$ can be written $i + \ell n$ with $0 \leq \ell < t$ and
\[ (\text{8.4}) \quad \left(\frac{x}{p}\right) = \left(\frac{an + \ell n}{p}\right) = \left(\frac{n}{p}\right) \left(\frac{a + \ell}{p}\right) = \left(\frac{n}{p}\right) \left(\frac{2}{p}\right). \]

\[ \square \]

Proof of Theorem 2.5. Since $p \equiv 1 \pmod{4}$ we have $\left(\frac{2(p-\delta)+i}{p}\right) = \left(\frac{3}{p}\right) \left(\frac{3\delta+3}{p}\right)$ and the equivalent form (2.7) is plain. Writing $\epsilon = 1, 2$ or 3 as $n \equiv \epsilon \pmod{3}$, suppose that $i = na_1 - (n - \epsilon)p/3 = \epsilon p/3 - n(3T_1 - 3 + \delta)/3$ and $i > 0$ for $n < \epsilon p/(3T_1 - 3 + \delta)$ and $i < n$ for $n > \epsilon p/(3T_1 + \delta)$. We also have $a_1 + (T_1 + T_2)n = \epsilon p/3 + (T_2 + 2 - 1 - \delta)/3$ naturally for $\epsilon = 3$, and for $\epsilon = 1$ or 2 if $n \geq (3 - \epsilon)p/(3T_2 - 3 + \delta)$ which follows from $n > \epsilon p/(3T_1 + \delta)$ for $\epsilon T_2 + \epsilon \geq \delta + (3 - \epsilon)T_1$. Hence $x$ in $I_x$ can be written $x = i + \ell n$ with $0 \leq \ell < T_1 + T_2$ and $\left(\frac{x}{p}\right) = \left(\frac{na_1 + \ell n}{p}\right) = \left(\frac{n}{p}\right) \left(\frac{a_1 + \ell}{p}\right) = \left(\frac{3n}{p}\right)$.

The remaining cases are similar with $i = \epsilon' p/3 - n(T_2 - \delta/3)$ where $\epsilon' = 3, 2, 1$ as $n \equiv 0, 1$ or 2 mod 3.

\[ \square \]
Proof of Theorem 2.6. For $i = na - (s - u)p$ the upper bound $n \leq (s - u)p/(a - 1)$ in (2.8) ensures that $i \equiv n$, and the lower bound $n > (s - u)p/a$ that $i > 0$. From $n \geq (s - u + 1)p/(a + t)$ we also have $i + tn \geq p$, so that the elements of $I_i$ can be written $x = i + \ell n$ with $0 \leq \ell < t$ and

$$\frac{x}{p} = \left(\frac{i + \ell n}{p}\right) = \left(\frac{na + \ell n}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{a + \ell}{p}\right) = \left(\frac{na}{p}\right).$$

Since the gap between our upper and lower bounds in (2.8) is

$$\min \left\{\frac{(s - 1 - r - u(t + 1)}{(a - 1)(a + t)}, \frac{an + \ell n}{a(a - 1)}\right\} p > \frac{p}{(a + t)^2},$$

we are guaranteed an $n$ if $(a + t) < \sqrt{p}$.

The proof for $i = (s - u + 1)p - n(a + t - 1)$ is similar. \(\square\)

Proof of Theorem 2.7. As in the proof of Theorem 2.4 we can write any $x$ in $I_i$ in the form $x = i + \ell n \equiv an + \ell n \mod p$ for $0 \leq \ell < t$, and so by (2.11),

$$x^{(p-1)/3} \equiv (an + \ell n)^{(p-1)/3} \equiv n^{(p-1)/3}(a + \ell)^{(p-1)/3} \equiv (an)^{(p-1)/3} \mod p.$$  

So for (2.12) we have $f(x) \equiv (an)^{(3k-1)/3} x \equiv x \mod p$ on $I_i$. Similarly, for $x$ in $I_i$,

$$x^{(p-1)/6} \equiv n^{(p-1)/6}(a + \ell)^{(p-1)/6} \equiv \pm(an)^{(p-1)/6} \mod p,$$

and for (2.13) we have $f(x) \equiv \pm(an)^{(3k-1)/3} x \equiv x \mod q$ on $I_i$, where $p - i \equiv i \mod n$ for $n$ odd. \(\square\)

Proof of Theorem 2.8. Suppose that $p \equiv 1 \mod 4$, $p = n + w$ with $2 \leq w < n$. The residue classes with two elements consist of the pairs $I_y = \{y, p - (w - y)\}$, $I_{w-y} = \{w - y, p - y\}$, $1 \leq y \leq w/2$, with the remaining classes containing one element. If $\left(\frac{w-y}{p}\right)$ both equal 1 then $f(x) = x^{(p+1)/2}$ fixes these sets; if both equal $-1$ it switches the pair. \(\square\)

9. Acknowledgement

The authors thank the reviewer for some insightful comments, in particular a significant improvement in Lemma 6.2.

References


DEPARTMENT OF MATHEMATICS, UMM AL-QUARA UNIVERSITY, MECCA 24382, SAUDI ARABIA  
E-mail address: bmsulmi@uqu.edu.sa

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506 USA  
E-mail address: cochrane@ksu.edu, pinner@ksu.edu, crichardson@ksu.edu, iamiat11@gmail.com

DEPARTMENT OF MATHEMATICS & COMPUTER SCIENCE, DAVIDSON COLLEGE, DAVIDSON, NC 28035, USA. E-mail address: mimossinghoff@davidson.edu

DEPARTMENT OF MATHEMATICS & STATISTICS, CALIFORNIA STATE UNIVERSITY, SACRAMENTO, SACRAMENTO, CA 95819, USA. E-mail address: vincent.pigno@csus.edu