PROOF OF THE GORESKY KLAPPER CONJECTURE ON DECIMATIONS OF L-SEQUENCES

TODD COCHRANE AND SERGEI KONYAGIN

Abstract. Let $p$ be an odd prime and $E = \{2, 4, \ldots, p-1\}$ the set of nonzero even residues in $\mathbb{Z}_p = \mathbb{Z}/(p)$. We prove that for $p > 13$, if the mapping $x \rightarrow Ax^k$ is a permutation of $\mathbb{Z}_p$, but not the identity mapping, then the mapping is not a permutation of $E$. This establishes a conjecture of Goresky and Klapper stating that any two distinct decimations of a binary $\ell$-sequence are cyclically distinct.

1. Introduction

For any odd prime $p$, let $\mathbb{Z}_p = \mathbb{Z}/(p)$, $E$ be the set of nonzero even residues (mod $p$) and $O$ the set of odd residues,

$$E = \{2, 4, 6, \ldots, p-1\} \subset \mathbb{Z}_p, \quad O = \{1, 3, 5, \ldots, p-2\} \subset \mathbb{Z}_p.$$

For integers $A, k$ the mapping $x \rightarrow Ax^k$ is a permutation of $\mathbb{Z}_p$ if $p \nmid A$ and $(k, p-1) = 1$. Our interest is in determining when it is a permutation of $E$. It is known to be such a permutation in the following cases:

$$(1.1) \quad (p, A, k) = (5, 3, 3), (7, 1, 5), (11, 9, 3), (11, 3, 7), (11, 5, 9) \text{ and } (13, 1, 5).$$

Here we prove,

**Theorem 1.1.** For any odd prime $p$ and integers $A, k$ such that the mapping $x \rightarrow Ax^k$ is a permutation of $\mathbb{Z}_p$, but not the identity mapping or one of the exceptions in (1.1), the mapping is not a permutation of $E$.

The theorem establishes a conjecture of Goresky and Klapper [7] on decimations of $\ell$-sequences. For their conjecture we restrict our attention to primes $p$ for which $2$ is a primitive root. An $\ell$-sequence based on $p$ is a binary sequence $\{a_i\}$ of the form

$$a_i \equiv (A2^{-i} \pmod{p}) \pmod{2},$$

with $p \nmid A$, the notation meaning take the least positive residue (mod $p$) first, then reduce (mod 2) to 0 or 1. Such a sequence is strictly periodic with period $p-1$. A shift of $\{a_i\}$ means a sequence of the form $\{a_{i+t}\}$ while an allowable decimation of $\{a_i\}$ means a sequence of the form $\{a_{ki}\}$ with $k$ a positive integer, $(k, p-1) = 1$. Two binary sequences are said to be cyclically distinct if they are not shifts of one another. Goresky and Klapper conjectured that for $p > 13$, any two distinct
decimations of an \( \ell \)-sequence are cyclically distinct. To see why this follows from Theorem 1.1 set \( A \equiv 2^i \pmod{p} \), \( x \equiv 2^{-i} \pmod{p} \). Then the mapping \( x \rightarrow Ax^k \) on \( \Z_p \) is equivalent to \( 2^{-i} \rightarrow 2^{-ki+i} \) and so one sees that a permutation of the even residues corresponds to a shifted decimation of an \( \ell \)-sequence coinciding with itself.

Goresky, Klapper and Murty [8] proved the conjecture for \( k = -1 \) and for the case where \( p \equiv 1 \pmod{4} \) and \( k = (p+1)/2 \). Goresky, Klapper, Murty and Shparlinski [9, Theorem 2.2] sharpening the work of [8], proved it for all values of \( k \) with \(-2.98 \cdot 10^{-8}p < k < 5.96 \cdot 10^{-8}p\). They also gave an upper bound on the number of possible counterexamples to the conjecture for a given \( p \). Bourgain, Cochrane, Paulhus and Pinner [2] improved this range to \(-0.00274p < k < 0.00823p\). More importantly, they established the conjecture for all sufficiently large primes, specifically, \( p > 2.26 \cdot 10^{55} \). The latter bound was sharpened in the work of Cochrane and Pinner [5] to \( p > 4.92 \cdot 10^{44} \).

We note that Wen-Feng Qi and Hong Xu [10] proved the Goresky-Klapper conjecture for the case of all odd prime powers \( p^e \) with \( e \geq 2 \), \( p^e \neq 9 \). Thus the conjecture has now been proven for all moduli having 2 as a primitive root.

The proofs in [2] and [5] used methods of finite Fourier series together with estimates for binomial exponential sums. The proof here introduces a completely new technique, or perhaps one should call it a special trick. It only makes incidental use of additive and multiplicative character sums. The first key idea is the observation that a linear congruence \( y \equiv ax \pmod{p} \) has a signature number of solutions \( N_p(a) \) in even residues \((x,y)\) when \( a \) is a small enough odd prime. Specifically, we show in Lemma 3.2 that for any odd prime \( a \),

\[
\left| N_p(a) - \frac{p}{4} \left(1 + \frac{1}{a}\right) \right| \leq \frac{a}{8} + 3,
\]

from which we deduce that if \( a \) is an odd prime less than \( p^{1/3} \) (with \( p \) sufficiently large) then \( N_p(a) \neq N_p(b) \) for any integer \( b \neq a \) or \( a^{-1} \pmod{p} \). The second idea is that if \( x \rightarrow Ax^k \) is a permutation of the even residues then there is a one-to-one correspondence between the solutions of the linear congruence \( y \equiv ax \pmod{p} \) in even \((x,y)\) and the solutions of the congruence \( y \equiv a^kx \pmod{p} \) in even \((x,y)\).

Thus, if \( a \) is a prime less than \( p^{1/3} \) we must have \( a^k \equiv a \) or \( a^{-1} \pmod{p} \), that is, \( a \) is either a \((k-1)\)-th or \((k+1)\)-th root of unity! Of course, this cannot possibly happen for all primes \( a \) less than \( p^{1/3} \) for \( p \) sufficiently large, (for instance take \( a \) to be the minimal odd prime primitive root \( \pmod{p} \)), but there does not appear to be any existing numeric result at this time that one can appeal to directly. However, this observation provides an efficient algorithm for showing (on a computer) that small primes satisfy Theorem 1.1. For our purposes it suffices to test \( p \) up to \( 4 \times 10^8 \) in this manner.

To complete the proof for large \( p \) we proceed roughly as follows. First we establish the theorem for the cases where \( (k-1,p-1) > 9.1\sqrt{p} \) and where \( (k+1,p-1) > 18\sqrt{p} \) using character sums and results from [2]. This leaves the case where the total number of odd \((k-1)\)-th or \((k+1)\)-th roots of unity is no more than \( 14\sqrt{p} \). Now, since there are roughly \( 3p^{1/3}/\log p \) odd primes less than \( p^{1/3} \) and every one is either a \((k-1)\)-th or \((k+1)\)-th root of unity, it follows that one of the sets has at least \( \frac{3}{2}p^{1/3}/\log p \) elements. But then, by forming all products of three such primes, we lead to an over abundance of either \((k-1)\)-th or \((k+1)\)-th roots of unity.
The paper is organized as follows. We start by estimating the number of solutions of a linear congruence $Ax + By \equiv C \pmod{m}$ in a general box (Lemma 2.1) and then specialize in Lemma 2.2 to counting solutions with $m$ odd and $(x, y) \in [1, (m-1)/2]$, which is equivalent to counting solutions with $x, y$ both even. In Section 3 we sharpen the results of Section 2 for counting the number of even solutions of congruences of the form $y \equiv ax \pmod{m}$ by studying the dual congruence $y \equiv -mx \pmod{a}$. The method given provides a way of giving very precise estimates for this number in terms of the residue class of $m \pmod{a}$. The next few sections then proceed in the manner outlined above, culminating with the proof of Theorem 1.1 in the final section.

2. The number of solutions of $Ax + By \equiv C \pmod{m}$ in a box

**Lemma 2.1.** Let $A, B, C, m$ be integers with $A, B$ nonzero, $\gcd(A, B) = 1$, $m > 0$ and $\mathcal{L}$ be the set of integer points satisfying $Ax + By \equiv C \pmod{m}$. Let $\mathcal{R}$ be any rectangle $\mathcal{R} = [x_1, x_2] \times [y_1, y_2]$ in $\mathbb{R}^2$ and set $L = x_2 - x_1, M = y_2 - y_1$. Then we have

$$|\mathcal{L} \cap \mathcal{R}| - \frac{LM}{m} \leq \frac{m}{4|AB|} + \frac{|A|L + |B|M}{m} + 1.$$ 

The same estimate holds if any of the edges of $\mathcal{R}$ are removed from $\mathcal{R}$.

The upper bound is sharp in certain cases, as the following example shows, but can be greatly improved in other cases; see for example Lemma 2.2.

**Example 2.1.** Consider the congruence $Ax + By \equiv \frac{m}{2} \pmod{m}$ where $A, B, m$ are positive integers with $m$ even $\gcd(A, B) = 1$, $2B|m$, $2A|m$. Let $\mathcal{R} = [0, m/(2A)] \times [0, m/(2B)]$. Any solution in $\mathcal{R}$ must satisfy $Ax + By = m/2$, a line passing through the corner points $(0, m/(2B)), (m/(2A), 0)$. Altogether there are $m/(2AB) + 1$ solutions in $\mathcal{R}$. Also, $LM/m = m/(4AB)$. Thus

$$|\mathcal{L} \cap \mathcal{R}| - \frac{LM}{m} = \frac{m}{4AB} + \frac{AL + BM}{m}.$$ 

**Proof.** By a translation of the box we may assume $C = 0$. Also, we may assume $A > 0$. Replacing $B$ with $-B$ and $y_1, y_2$ with $-y_2, -y_1$ if necessary, we may also assume that $B > 0$. We must count the number of $(x, y) \in \mathcal{R}$ satisfying $Ax + By = mk$ for some integer $k$. Set

$$Ax_1 + By_1 = q_1m + r_1, \quad 0 \leq r_1 < m,$$

$$Ax_2 + By_1 = q_2m + r_2, \quad 0 \leq r_2 < m,$$

$$Ax_1 + By_2 = q_3m + r_3, \quad 0 \leq r_3 < m,$$

$$Ax_2 + By_2 = q_4m + r_4, \quad 0 \leq r_4 < m.$$ 

The family of lines $Ax + By = mk, k \in \mathbb{Z}$, partitions the rectangle $\mathcal{R}$ into a collection of polygonal regions. We call the line with the minimal $k$ meeting $\mathcal{R}$ in more than one point the “bottom line” and the line with the maximal $k$ meeting $\mathcal{R}$ the “top line”. The top line is allowed to meet $\mathcal{R}$ in just the corner $(x_2, y_2)$. Let $n = q_4 - q_1$ denote the total number of lines meeting $\mathcal{R}$ as such. There are several cases to consider. We start with cases with $n \geq 2$. In such cases the top line must meet $\mathcal{R}$ in either the top or right edge, while the bottom line must meet $\mathcal{R}$ in either the bottom or left edge.
Case i: Suppose that $n \geq 2$, the bottom line meets the left edge and bottom edge of $\mathcal{R}$ while the top line meets the top edge and right edge of $\mathcal{R}$. In this case $\mathcal{R}$ is partitioned into a collection of trapezoids and parallelograms of height $h = \frac{m}{\sqrt{A^2 + B^2}}$ (the distance between the parallel lines), and having parallel edges of lengths $\ell_1, \ldots, \ell_n$, say, together with four triangles $T_{11}, T_{12}, T_{21}, T_{22}$ in the lower left corner, upper left corner, lower right corner and upper right corner respectively. (Triangles $T_{12}, T_{21}$ and $T_{22}$ may be empty.) Note that $\ell_1$ is the hypotenuse of $T_{11}$ and $\ell_n$ the hypotenuse of $T_{22}$.

The vertices of the triangles are given as follows,

$T_{11} : (x_1, y_1), (x_1 + \frac{m - r_1}{A}, y_1), (x_1, y_1 + \frac{m - r_1}{B})$

$T_{12} : (x_1, y_2), (x_1 + \frac{m - r_3}{A}, y_2), (x_1, y_2 - \frac{r_3}{B})$

$T_{21} : (x_2, y_1), (x_2 - \frac{r_2}{A}, y_1), (x_2, y_1 + \frac{m - r_2}{B})$

$T_{22} : (x_2, y_2), (x_2 - \frac{r_4}{A}, y_2), (x_2, y_2 - \frac{r_4}{B})$,

and their corresponding areas are

$A_{11} = \frac{(m - r_1)^2}{2AB}$, $A_{12} = \frac{r_3(m - r_3)}{2AB}$, $A_{21} = \frac{r_2(m - r_2)}{2AB}$, $A_{22} = \frac{r_4^2}{2AB}$.

Since the area of a trapezoid with bases of lengths $\ell_i, \ell_{i+1}$ is $h(\ell_i + \ell_{i+1})/2$, the area of rectangle $\mathcal{R}$ is given by

$$LM = h \sum_{i=1}^{n} \ell_i - \frac{1}{2}h(\ell_1 + \ell_n) + A_{11} + A_{12} + A_{21} + A_{22}. \tag{2.2}$$

Using $h\ell_1 = m(m - r_1)/(AB)$, $h\ell_n = mr_4/(AB)$, we have

$$A_{11} - \frac{1}{2}h\ell_1 = -\frac{r_1(m - r_1)}{2AB}, \quad A_{22} - \frac{1}{2}h\ell_n = -\frac{r_4(m - r_4)}{2AB}.$$

Thus,

$$LM - h \sum_{i=1}^{n} \ell_i = \frac{1}{2AB} \left( r_3(m - r_3) + r_2(m - r_2) - r_1(m - r_1) - r_4(m - r_4) \right). \tag{2.3}$$
Since $0 \leq r(m - r) \leq m^2/4$ for any $r \geq 0$, we see that

\begin{equation}
|LM - h \sum_{i=1}^{n} \ell_i| \leq \frac{m^2}{4AB}.
\end{equation}

(2.4)

Now the integer points on a given line $Ax + By = km$ are spaced apart by a distance of $\sqrt{A^2 + B^2}$ since $\gcd(A, B) = 1$. Thus the number of integer points on a line segment of length $\ell_i$ is within 1 of $\frac{\ell_i}{\sqrt{A^2 + B^2}}$. Moreover, this estimate still holds if any of the edges of the rectangle are removed. The total number of line segments in our partition is

$$n = q_4 - q_1 = (AL + BM)/m + (r_1 - r_4)/m.$$  

Thus

$$|L \cap R| - \frac{1}{\sqrt{A^2 + B^2}} \sum_{i=1}^{n} \ell_i \leq \frac{AL + BM}{m} + \frac{r_1 - r_4}{m} + \theta,$$

where $\theta = 0$ unless $(x_1, y_1) \in R \cap L$, in which case $\theta = 1$ (since this point is not on any of the lines). Combining this with (2.4), and noting $h\sqrt{A^2 + B^2} = m$, we obtain

$$|L \cap R| - \frac{LM}{m} \leq \frac{m}{4AB} + \frac{AL + BM}{m} + \frac{r_1 - r_4}{m} + \theta.$$  

Noting that $|r_1 - r_4|/m < 1$ and that if $\theta = 1$ then $r_1 = 0$ and so $(r_1 - r_4)/m + \theta \leq 1$ we obtain the inequality of the lemma.

Case ii: Suppose that $n \geq 2$, the bottom line meets the left and right edges of $R$ and the top line meets the top and right edges of $R$.

In this case $q_1 = q_2$, $A(x_2 - x_1) = r_2 - r_1$ and the area $A_{\text{bot}}$ of the bottom trapezoid is given by

$$A_{\text{bot}} = \frac{1}{2}(r_2 - x_1) \left( \frac{m - r_1}{B} + \frac{m - r_2}{B} \right) = \frac{r_2 - r_1}{2AB}(2m - r_1 - r_2).$$

Furthermore, $h\ell_1 = m(r_2 - r_1)/(AB)$, $h\ell_n = m r_4/(AB)$, and we have

\begin{equation}
A_{\text{bot}} = \frac{1}{2} h\ell_1 = \frac{r_2 - r_1}{2AB}(m - r_1 + r_2),
\end{equation}

(2.5)

$$A_{22} = \frac{1}{2} h\ell_n = \frac{r_4 (m - r_4)}{2AB}, \quad A_{12} = \frac{r_3 (m - r_3)}{2AB}.$$  

Now for $0 \leq x, y \leq m$ the extremal values of the function $f(x, y) = (y - x)(m - (y + x))$ occur on the boundaries, where $f(0, y) = y(m - y), f(x, 0) = -x(m - x), f(x, y) = (y - x)(m - (y + x))$.
\[ f(m, y) = (y - m)(-y), \quad f(x, m) = (m - x)(-x). \] Thus \(|f(x, y)| \leq m^2/4\) uniformly on this square, and so
\[
|A_{\text{bot}} - \frac{1}{2}h\ell| \leq \frac{m^2}{8AB}.
\]
Since \(0 \leq A_{12} \leq \frac{m^2}{8AB}\) while \(-\frac{m^2}{8AB} \leq A_{22} - \frac{1}{2}h\ell_n \leq 0\) we obtain
\[
LM - h \sum_{i=1}^{n} \ell_i = (A_{\text{bot}} - \frac{1}{2}h\ell_1) + A_{12} + (A_{22} - \frac{1}{2}h\ell_n) \leq \frac{m^2}{8AB} + \frac{m^2}{8AB} + 0 = \frac{m^2}{4AB}.
\]

Case iii: Suppose that \(n \geq 2\), the top line meets the left and right edges of \(R\) and the bottom line is arbitrary. Then \(q_3 = q_4, A(x_2 - x_1) = r_4 - r_3\) and the area \(A_{\text{top}}\) of the top trapezoid is given by
\[
A_{\text{top}} = \frac{1}{2}(x_2 - x_1)(r_4 + r_3) = \frac{1}{2} \left( r_4 - r_3 \right) A \left( \frac{r_4 + r_3}{B} \right).
\]
We also have \(h\ell_n = m(r_4 - r_3)/(AB)\) and so
\[
A_{\text{top}} - \frac{1}{2}h\ell_n = \frac{(r_4 - r_3)}{2AB}(r_4 + r_3 - m).
\]
Therefore, as in case (ii),
\[
|A_{\text{top}} - \frac{1}{2}h\ell| \leq \frac{m^2}{8AB}.
\]

Thus,
\[
LM - h \sum_{i=1}^{n} \ell_i = \left\{ \begin{array}{ll}
(A_{\text{bot}} - \frac{1}{2}h\ell_1) + (A_{\text{top}} - \frac{1}{2}h\ell_n), & \text{or} \\
(A_{11} - \frac{1}{2}h\ell_1) + A_{12} + (A_{\text{top}} - \frac{1}{2}h\ell_n), & \text{or}
\end{array} \right.
\]
and inequality (2.4) follows as before.

Case iv: Suppose that \(n \geq 2\) and that the bottom line meets the top and bottom edges of \(R\), and that the top line meets the top and right edges. This case is symmetric to case (ii) by interchanging the variables \(x, y\) and counting the number of solutions of the congruence \(Bx + Ay \equiv C \pmod{m}\) with \(x \in [y_1, y_2], y \in [x_1, x_2]\).

Case v: Suppose that \(n \geq 2\) and that the top line meets the top and bottom edges of \(R\). This case is symmetric to case (iii).

Case vi: Suppose that \(n = 1\), that is, exactly one line meets \(R\) at a point other than \((x_1, y_1)\). Then \(q_4 = q_1 + 1\) and so \(A(x_2 - x_1) + B(y_2 - y_1) = m + r_4 - r_1\), that is
\[
AL + BM = m + r_4 - r_1.
\]
Note that in order for \((x_1, y_1)\) to be in \(L\) we must have \(r_1 = 0\) and so \(AL + BM \geq m\). Thus the term \(AL + BM\) in the statement of the lemma can be used to account for this extra point in what follows. We consider several subcases.

(i) Suppose that the line meets the left edge and bottom edge of \(R\). In this case, the points of intersection are \((x_1, y_1 + (m - r_1)/B)\) and \((x_1 + (m - r_1)/A, y_1)\), \(\ell_1 = (m - r_1)\sqrt{A^2 + B^2}/AB\), and the number of integer points on the line is within 1 of \((m - r_1)/AB\). Say, without loss of generality that \(BM \leq AL\). Now,
\[
(m - r_1)/B \leq M \quad \text{since the line meets the left edge}, \quad \text{and so}
\]
\[
\frac{m - r_1}{AB} - \frac{LM}{m} \leq \frac{M}{A} - \frac{LM}{m} \leq \frac{m}{4AB}.
\]
the latter inequality following from $4BM(m - AL) \leq 4AL(m - AL) \leq m^2$. For a lower bound we claim that

$$\frac{m - r_1}{AB} - \frac{LM}{m} \geq -\frac{m}{4AB}.$$ 

Indeed, this bound is equivalent to

$$4ABLM \leq 5m^2 - 4mr_1.$$ 

By (2.8), we have

$$4ABLM \leq (AL + BM)^2 < (2m - r_1)^2 < 5m^2 - 4mr_1,$$

completing the claim. Thus,

$$\left|L \cap \mathcal{R}\right| - \frac{LM}{m} \leq \frac{m}{4AB} + 1.$$

(Note, in this case $(x_1, y_1)$ is not in $\mathcal{L}$.)

(ii) Suppose next that the line meets the left and right edges of $\mathcal{R}$. In this case the line divides the rectangle into a bottom trapezoid and top trapezoid with $LM = A_{bot} + A_{top}$. Thus by (2.6), (2.5) and $\ell_1 = \ell_n$,

$$LM - h\ell_1 = \frac{r_2 - r_1}{2AB}(m - r_1 - r_2) + \frac{r_4 - r_3}{2AB}(r_4 + r_3 - m)$$

and, as above, $|LM - h\ell_1| \leq \frac{m^2}{4AB}$. Dividing by $m$ yields the inequality of the lemma. (Again, in this case $(x_1, y_1)$ is not in $\mathcal{L}$.)

(iii) Suppose that the line meets the top and right edges of $\mathcal{R}$. The intersection points are $(x_2 - r_4/A, y_2)$, $(x_2, y_2 - r_4/B)$ and we must have $r_4/A \leq L$, $r_4/B \leq M$. The number of integer points on the line is within 1 of $r_4/(AB)$. We claim that

$$\left|\frac{r_4}{AB} - \frac{LM}{m}\right| \leq \frac{m}{4AB}.$$

Indeed,

$$\frac{r_4}{AB} \leq \frac{M}{A} \leq \frac{LM}{m} + \frac{m}{4AB},$$

as in subcase (i). Also

$$\frac{r_4}{AB} - \frac{LM}{m} \geq -\frac{m}{4AB},$$

by (2.8).

(iv) Suppose that the line meets the top and bottom edges of $\mathcal{R}$. In this case $\mathcal{R}$ is divided into a left and right trapezoid and the argument follows as in subcase (ii).

Case vii: Suppose that no line meets $\mathcal{R}$. Then $q_4 = q_1$ and so $AL + BM < m$. The lemma is established if we can show that $|LM/m| \leq m/(4AB)$, that is, $4ABLM \leq m^2$, but this is immediate since $4ABLM \leq (AL + BM)^2 \leq m^2$.

\[\square\]

**Lemma 2.2.** Let $A, B, m$ be integers with $A, B$ nonzero, $\gcd(A, B) = 1$, $m$ positive and odd. Let $\mathcal{N}_m(A, B)$ be the number of solutions of $Ax + By \equiv 0 \pmod{m}$ with $x, y \in [1, (m - 1)/2]$.

i) If $AB$ is even then

$$\left|\mathcal{N}_m(A, B) - \frac{m}{4}\right| \leq \frac{|A| + |B|}{2} + 1.$$
ii) If $AB$ is odd then

$$\left| N_m(A, B) - \frac{m}{4} \left( 1 - \frac{1}{AB} \right) \right| \leq |A| + |B| + 1.$$  

Proof. Suppose first that $A, B$ have the same sign, say both positive. We apply the method of the previous lemma to the box $(0, m/2) \times (0, m/2)$. The relations (2.1) are $r_1 = 0, r_2 \equiv Am/2 \pmod{m}, r_3 \equiv Bm/2 \pmod{m}, r_4 \equiv r_2 + r_3 \pmod{m}$.

(i) Suppose that $AB$ is even, say $A$ is even and $B$ is odd. Then $r_1 = r_2 = 0$, $r_3 = r_4 = \frac{m}{2}$. We claim that in cases (i)-(v) (in the proof of Lemma 2.1) we have $LM - \sum_{n=1}^{n} \ell_n = 0$, and thus $m - \frac{1}{\sqrt{AB}} \sum_{n=1}^{n} \ell_n = 0$. This follows readily from the following relations,

$$A_{11} - \frac{1}{2} h\ell_1 = -\frac{r_1(m-r_1)}{2AB} = 0,$$

$$A_{22} - \frac{1}{2} h\ell_n = -\frac{r_4(m-r_4)}{2AB} = -\frac{m^2}{8AB},$$

$$A_{12} = \frac{m^2}{8AB},$$

$$A_{21} = 0,$$

$$A_{top} - \frac{1}{2} h\ell_n = 0,$$

$$A_{bot} - \frac{1}{2} h\ell_1 = 0,$$

$$A_{right} - \frac{1}{2} h\ell_n = -\frac{m^2}{8AB},$$

$$A_{left} - \frac{1}{2} h\ell_1 = \frac{m^2}{8AB}.$$

For case (vi) we must have $AL + BM < 2m$, that is $A + B < 4$ and therefore $A = 2, B = 1$. One can easily check that $N_m(2, 1) = \frac{m+1}{4}$ or $\frac{m-1}{4}$ according as $m \equiv 3$ or 1 (mod 4), and the lemma follows. Case (vii) cannot occur for we would need $A + B \leq 2$. 
(ii) Suppose that $AB$ is odd. Then $r_1 = r_4 = 0$ and $r_2 = r_3 = \frac{m}{2}$. We claim that in cases (i)-(v) we have $LM - h \sum_{i=1}^{n} \ell_i = \frac{m^2}{4AB}$. The relations this time are,

$$
A_{11} - \frac{1}{2} h \ell_1 = 0,
A_{22} - \frac{1}{2} h \ell_n = 0,
A_{12} = \frac{m^2}{8AB},
A_{21} = \frac{m^2}{8AB},
A_{top} - \frac{1}{2} h \ell_n = \frac{m^2}{8AB},
A_{bot} - \frac{1}{2} h \ell_1 = \frac{m^2}{8AB},
A_{right} - \frac{1}{2} h \ell_n = \frac{m^2}{8AB},
A_{left} - \frac{1}{2} h \ell_1 = \frac{m^2}{8AB}.
$$

In cases (vi) and (vii) we must have $A = B = 1$, but in this case it is trivial that $N_m(A, B) = 0$, and the lemma follows.

Next, suppose that $A, B$ have opposite signs, say $A$ is positive, $B$ negative. We replace $B$ with $-B$ and count the number of solutions with $x \in (0, m/2)$, $y \in (-m/2, 0)$.

(i) Suppose that $A$ is even and $B$ is odd. Then $r_1 = r_2 = m/2$, $r_3 = r_4 = 0$.

$$
A_{11} - \frac{1}{2} h \ell_1 = -\frac{r_1(m - r_1)}{2AB} = -\frac{m^2}{8AB},
A_{22} - \frac{1}{2} h \ell_n = -\frac{r_4(m - r_4)}{2AB} = 0,
A_{12} = 0,
A_{21} = \frac{m^2}{8AB},
A_{top} - \frac{1}{2} h \ell_n = 0,
A_{bot} - \frac{1}{2} h \ell_1 = 0,
A_{right} - \frac{1}{2} h \ell_n = \frac{m^2}{8AB},
A_{left} - \frac{1}{2} h \ell_1 = \frac{m^2}{8AB}.
$$

Thus in cases (i) to (v), $LM - h \sum_{i=1}^{n} \ell_i = 0$. In case (vi) we must have $A = 2$, $B = -1$. One can check that $N_m(2, -1) = \frac{m-1}{4}$ or $\frac{m-3}{4}$ according as $m \equiv 1$ or $3 \pmod{4}$, and the lemma follows. Case (vii) doesn’t occur.

Finally, if $A$ and $B$ are both odd, then $r_1 = r_4 = m/2$, $r_2 = r_3 = 0$. 


Lemma 2.3. Let \( p \) be an odd prime, \( A, B \) be integers with \( p \nmid AB \) and \( A \neq B \mod p \). Then the number \( N_p(A, B) \) of solutions of the congruence \( Ax + By \equiv 0 \mod p \) with \( x, y \in [1, (p - 1)/2] \) satisfies

\[
N_p(A, B) \geq (p - 1)/6.
\]

If \( A \equiv B \mod p \) then plainly \( N_p(A, B) = 0 \). Also, the lower bound in the lemma is sharp since \( N_p(3, 1) = N_p(1, 3) = (p - 1)/6 \) if \( p \equiv 1 \mod 6 \) (as seen in the proof below).

Proof. Consider first the case where \( AB = 3 \), say without loss of generality, \( A = 3, B = 1 \). We must count the number of solutions of the congruence \( y \equiv -3x \mod p \) with \( x, y \in [1, (p - 1)/2] \). This is just the number of \( x \in [1, (p - 1)/2] \) with \(-p + 1 \leq -3x \leq -p + \frac{p - 1}{2} \), that is, \( \frac{p + 1}{6} \leq x \leq \frac{p - 1}{3} \). Setting \( p = 6k + \ell \) with \( \ell \in \{1, 5\} \), we obtain \( N_p(3, 1) = \frac{p - 1}{6} \) if \( \ell = 1 \) and \( N_p(3, 1) = \frac{p + 1}{6} \) if \( \ell = 5 \).

Consider now a general \( A, B \) with \( p \nmid AB, A \neq B \mod p \). The lattice \( Ax + By \equiv 0 \mod p \) contains a nonzero point \((x_0, y_0)\) with \( x_0 > 0, |x_0|, |y_0| < \sqrt{p} \). Moreover, by dividing out any common factor we may assume \( \gcd(x_0, y_0) = 1 \). We replace \((A, B)\) with \((-y_0, x_0)\) and note that since \( A \neq B \mod p \), \( x_0y_0 \neq -1 \).

If \( x_0y_0 \) is even, or \( x_0y_0 \) is odd and positive then by Lemma 2.2,

\[
N_p(A, B) \geq \frac{p}{4} - \frac{|x_0| + |y_0|}{2} - 1 \geq \frac{p}{4} - \sqrt{p} - 1.
\]

If \( x_0y_0 \) is odd and negative then by Lemma 2.2,

\[
N_p(A, B) \geq \frac{p}{4} \left( 1 - \frac{1}{|x_0y_0|} \right) - \frac{|x_0| + |y_0|}{2} - 1.
\]

We know \( x_0y_0 \neq -1 \) and we’ve accounted for the case \( x_0y_0 = -3 \) above. Thus we may assume \( x_0y_0 \leq -5 \). If \( |x_0y_0| \geq \sqrt{p} \) then since \( |x_0|, |y_0| < \sqrt{p} \) we have

\[
N_p(A, B) \geq \frac{p}{4} - \frac{5}{4}\sqrt{p} - 1 \geq \frac{p - 1}{6}, \quad \text{for } p > 245.
\]
Suppose \( |x_0y_0| < \sqrt{p} \). For fixed \( |x_0y_0| \) the value \( |x_0| + |y_0| \) is maximized when \( |x_0| = 1 \) or \( |y_0| = 1 \). Thus we seek the minimum value of \( \frac{p}{4}(1 - \frac{1}{t}) - \frac{p+3}{2} \) with \( 5 \leq t < \sqrt{p} \) and get

\[
N_p(A, B) \geq \min \left\{ \frac{p}{5} - 4, \frac{p}{3} - \frac{3}{4}\sqrt{p} - \frac{3}{2} \right\}.
\]

Now \( \frac{p}{4} - 4 \geq \frac{p-1}{n} \) for \( p \geq 115 \), and \( \frac{p}{4} - \frac{3}{4}\sqrt{p} - \frac{3}{2} \geq \frac{p-1}{n} \) for \( p \geq 110 \). For \( p < 245 \) one can check on a computer that the inequality holds true. \( \square \)

3. Congruences of the type \( y \equiv ax \pmod{m} \) and their duals

Let \( a, m \) be positive integers with \( m \) odd. Suppose that we wish to count the number of solutions of a linear congruence \( y \equiv ax \pmod{m} \) with \( x, y \in \mathbb{Z} \). This is equivalent to counting the number of solutions of the congruence

\[
y \equiv ax \pmod{m}
\]

with \( x, y \in I := [1, (m-1)/2] \). Any such solution satisfies

\[y = ax - mz,\]

for some integer \( z \in [0, a/2) \). (Check: \( z = \frac{1}{m}(ax - y) < ax/m < a/2 \) and \( z > \frac{a}{m} - \frac{1}{2} > -1 \).) Moreover, given any integer solution of \( y = ax - mz \) with \( z \in [0, a/2) \) and \( y \in I \), it follows that \( x \in I \). (Check: \( x = \frac{1}{2}(y + mz) < \frac{1}{2}(\frac{m}{2} + \frac{m(a-1)}{2}) = m/2 \), and \( x \geq y/a > 0 \).) Thus the number of solutions of (3.1) in \( I \times I \) is the same as the number of solutions of the dual congruence

\[
y \equiv -mz \pmod{a},
\]

with \( (y, z) \in I \times [0, a/2) \). Using this idea we obtain

Lemma 3.1. Let \( a, m \) be positive integers with \( m \) odd, and \( N_m(a) \) be the number of solutions of \( y \equiv ax \pmod{m} \) with \( x, y \in [1, (m-1)/2] \). Suppose that \( A, B \) are any integers with \( \gcd(B, aA) = 1 \), such that \( m \equiv AB^{-1} \pmod{a} \).

(i) If \( a \) is even then,

\[
\left| N_m(a) - \frac{m}{4} \right| \leq \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + \frac{5}{4}.
\]

(ii) If \( a \) is odd then,

\[
\left| N_m(a) - \frac{m}{4} \left(1 + \frac{1}{a}\right)\right| \leq \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + \frac{3}{2}.
\]

Proof. Put \( \mathcal{N} = N_m(a) \). By assumption, congruence (3.2) is equivalent to

\[
By \equiv -Az \pmod{a},
\]

and so \( \mathcal{N} \) is the number of solutions \( (y, z) \) of (3.3) in \( [1, \frac{m-1}{2}] \times [0, a/2) \). Say

\[
m - \frac{1}{2} = qa + r, \quad 0 \leq r < a.
\]

Case i: Suppose \( r \leq a/2 \). The number of solutions \( (y, z) \) of (3.3) in \([1, qa] \times [0, a/2)\) is \( q[a/2] \), because for each choice of \( z \) there are exactly \( q \) choices for \( y \). We must add to these the solutions in \([1, r] \times [0, a/2) \) (in case \( r > 0 \).) Applying Lemma
2.1 to the rectangle \((0, r) \times [0, a/2]\) gives this number to be \(r/2\) with error no more than
\[
\frac{a}{4|AB|} + \frac{|B|r + |A|a/2}{a} + 1 \leq \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + 1.
\]
Thus the total number of solutions with \(a\) odd is (up to error)
\[
\frac{q(a + 1)}{2} + \frac{r}{2} = \frac{qa + r}{2} + \frac{q}{2} + \frac{1}{2} = \frac{m - 1}{4} + \frac{m - 1}{4a} - \frac{r}{2a} + \frac{1}{2} = \frac{m}{4} \left(1 + \frac{1}{a}\right) + \frac{1}{4} - \frac{1}{2} - \frac{r}{2a},
\]
and so
\[
\left|N - \frac{m}{4} \left(1 + \frac{1}{a}\right) \right| \leq \frac{1}{4} + \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + 1.
\]

With \(a\) even we omit the term \(q/2\) and just get \(\frac{m-1}{4}\) up to error. Thus
\[
\left|N - \frac{m}{4} \left(1 + \frac{1}{a}\right) \right| \leq \frac{1}{4} + \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + 1.
\]

Case ii: Suppose that \(r > a/2\) and that \(a\) is odd. The number of solutions of (3.3) in \([1, (q + 1)a] \times [0, a/2]\) is \((q + 1)(a + 1)/2\). We must subtract from these the solutions \((y, z) \in [r + 1, a] \times [0, a/2]\). Applying Lemma 2.1 to the rectangle \((r, a) \times [0, a/2]\) gives this number to be \((a - r)/2\) with error no more than
\[
\frac{a}{4|AB|} + \frac{|B|(a - r) + |A|a/2}{a} + 1 \leq \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + 1.
\]
Thus the total number of solutions is (up to error)
\[
\frac{(q+1)(a+1)}{2} - \frac{a-r}{2} = \frac{qa + r}{2} + \frac{q}{2} + \frac{1}{2} = \frac{m - 1}{4} + \frac{m - 1}{4a} - \frac{r}{2a} + \frac{1}{2} = \frac{m}{4} \left(1 + \frac{1}{a}\right) + \frac{1}{4} - \frac{r}{2a} - \frac{1}{4a},
\]
and so
\[
\left|N - \frac{m}{4} \left(1 + \frac{1}{a}\right) \right| \leq \frac{r}{2a} + \frac{1}{4} + \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + 1 \leq \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + \frac{5}{4},
\]
since \(r \leq a - 1\).

Finally, suppose that \(r > a/2\) and that \(a\) is even. In this case we get \((q + 1)\frac{a}{2} - \frac{a-r}{2} = \frac{m-1}{4}\) solutions (up to error) and so
\[
\left|N - \frac{m}{4} \right| \leq \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + 1.
\]
\[\Box\]

**Example 3.1.** 1) Suppose that \(A = 1, B = 1\), that is \(m \equiv 1 \pmod{a}\). By (3.4), we have \(r \equiv \frac{m-1}{2} \pmod{a}\). Thus, if \(a\) is odd then \(r = 0, N_m(a) = qa + 1/2 = m - 1 \left(1 + \frac{1}{a}\right)\). If \(a\) is even then we have either \(r = 0\), in which case \(N_m(a) = qa/2 = \frac{m-1}{4}\) or \(r = a/2\), in which case \(N_m(a) = qa/2 + N'\) where \(N'\) is the number of
solutions of the congruence \( y \equiv -z \pmod{a} \) in \([1, \frac{a}{2}] \times [0, \frac{a}{2} - 1]\). Plainly \( N' = 0 \) and so \( N_m(a) = \frac{m-1}{4} - \frac{a}{4} \). In summary, if \( m \equiv 1 \pmod{a} \) then

\[
N_m(a) = \begin{cases} 
\frac{m-1}{4}(1 + \frac{1}{a}), & \text{a odd,} \\
\frac{m-1}{4}, & \text{a even and } r = 0, \\
\frac{m-1}{4} - \frac{a}{4}, & \text{a even and } r = a/2.
\end{cases}
\]

2) Suppose that \( A = 1, B = -1 \), that is \( m \equiv -1 \pmod{a} \). If a is odd then \( r \equiv 1 \pmod{a} \), that is \( r = a - 1 \), and so \( N_m(a) = (q + 1)(a + 1)/2 - N' \) where \( N' \) is the number of solutions of the congruence \( y \equiv z \pmod{a} \) in \([0] \times [0, a/2]\).

Plainly \( N' = 1 \) so we get \( N_m(a) = \frac{m+1}{4}(a+1)/2 - 1 = \frac{q}{2}(1 + \frac{1}{a}) + \frac{1}{2}a - \frac{3}{4} \). If \( a \) is even then either \( r = a - 1 \) and \( N_m(a) = (q + 1)a/2 - 1 \), or \( r = \frac{a}{2} - 1 \) and \( N_m(a) = qa/2 + N' \) where \( N' \) is the number of solutions of \( y \equiv z \pmod{a} \) in \([1, \frac{a}{2} - 1] \times [0, \frac{a}{2} - 1]\). Plainly, \( N' = \frac{a}{2} - 1 \) and so we obtain in summary, if \( m \equiv -1 \pmod{a} \) then

\[
N_m(a) = \begin{cases} 
\frac{m+1}{4}(1 + \frac{1}{a}) - 1, & \text{a odd,} \\
\frac{m-3}{4}, & \text{a even and } r = a - 1, \\
\frac{m}{4} + \frac{a}{4} - \frac{3}{4}, & \text{a even and } r = \frac{a}{2} - 1.
\end{cases}
\]

**Lemma 3.2.**

1) Suppose that \( p, a \) are distinct odd primes. Then the number \( N_p(a) \) of solutions of the congruence \( y \equiv ax \pmod{p} \) with \( x, y \in [1, (p - 1)/2] \) satisfies

\[
\left| N_p(a) - \frac{p}{4} \left(1 + \frac{1}{a}\right) \right| \leq \frac{a}{8} + 3.
\]

If \( a < 43 \) the constant 3 on the right-hand side may be replaced by 1.

2) Suppose that \( p \) is an odd prime and that \( a \) is any positive odd integer. Then with \( N_p(a) \) as above

\[
\left| N_p(a) - \frac{p}{4} \left(1 + \frac{1}{a}\right) \right| \leq \frac{a}{6} + \frac{11}{4}.
\]

**Proof.** Put \( N = N_p(a) \). a) Suppose that \( a \) is an odd prime. By the pigeonhole principle we know that there exist nonzero integers \( A, B \) with \( |A| \leq \sqrt{a}, |B| \leq \sqrt{a} \) and \( Bp \equiv A \pmod{a} \), that is, \( p \equiv AB^{-1} \pmod{a} \). Moreover, by dividing out any common factor we may assume \( \gcd(A, B) = 1 \). Then by Lemma 3.1,

\[
\left| N - \frac{p}{4} \left(1 + \frac{1}{a}\right) \right| \leq \frac{a}{4|AB|} + \frac{|A| + |B|}{2} + 3/2.
\]

If \(|AB| = 1\) then Example 3.1 gives a much sharper estimate for \( N \). For \(|AB| \geq 2\) the error is maximized when \(|AB| = 2\) for \( a \geq 43 \) (since \(|A|, |B| < \sqrt{a}\), where the error equals \( \frac{a}{2} + 3 \). (Note, at the other extreme \(|A|, |B| = \sqrt{a}\), the error is \( 7/4 + \sqrt{a} \) which is smaller for \( a \geq 43 \).)

For \( a < 43 \) we use a computer to verify that

\[
(3.5) \quad \left| N - \frac{p}{4} \left(1 + \frac{1}{a}\right) \right| \leq \frac{a}{8} + 1,
\]

by following the proof of Lemma 3.1. Write

\[
p - \frac{1}{2} = qa + r, \quad 0 \leq r < a.
\]
Lemma 4.1. Suppose that \( \text{permutes the even residues of } \mathbb{Z} \) \( \text{of these approximations, numerical evidence indicates that they are remarkably} \)

\[ N = N' + \frac{p}{4} \left( 1 + \frac{1}{a} \right) - \frac{1}{4} (1 + 2r) \left( 1 + \frac{1}{a} \right) \]

where \( N' \) is the number of solutions of \( y \equiv -pz \pmod{a} \) (that is, \( y \equiv -(2r+1)z \pmod{a} \)) with \( (y, z) \in [1, r] \times [0, (a-1)/2] \). A program then calculates \( N' \) and \( N \) for each pair \((r, a)\) with \(0 \leq r < a < 43\).

b) Let \( a \) be any odd positive number. Say \( p = A \pmod{a} \) where \( A \) is an integer with \( |A| \leq \frac{a-1}{2} \). Suppose first that \( |A| \leq \frac{a}{2} \). Then we take \( B = 1 \) in Lemma 3.1 and get

\[ \left| N - \frac{p}{4} \left( 1 + \frac{1}{a} \right) \right| \leq \frac{a}{4|A|} + \frac{|A|}{2} + 2. \]

If \( |A| = 1 \) the result follows as before. For \( |A| \geq 2 \) the upper bound is maximized when \( |A| = a/3 \), where we obtain the stated bound.

Next, suppose that \( \frac{a}{3} < |A| < \frac{a}{2} \), say without loss of generality \( \frac{a}{3} < A < \frac{a}{2} \). Then \( \frac{2A}{a} < 2A < a \). We take \( B = -2 \) and replace \( A \) with \( a - 2A \) in Lemma 3.1, so that \( 0 < A < a/3 \). Then for \( 1 \leq A < a/3 \) the upper bound

\[ \left| N - \frac{p}{4} \left( 1 + \frac{1}{a} \right) \right| \leq \frac{a}{8|A|} + \frac{|A|}{2} + \frac{5}{2}, \]

is maximized at \( A = (a-1)/3 \) where it is at most \( \frac{3}{8} \frac{a}{a-1} + \frac{a}{6} - \frac{1}{6} + \frac{5}{2} = \frac{a}{6} + \frac{11}{4}, \) for \( a > 10 \). For odd \( a < 10 \) we can use (3.5).

Remark: The upper bound \( a/8 \) in Lemma 3.2 cannot be improved for arbitrary \( p, a \). Indeed, better approximations can be obtained by extending the analysis done in Example 3.1 to other small values of \( A \) and \( B \). Let \( A, B \) be integers with \( \text{AP} \equiv B \pmod{a} \), \( |A|, |B| < \sqrt{a} \), \( \text{gcd}(A, B) = 1 \). If \( A \) is even then \( N' \approx \frac{p}{4} (1 + \frac{1}{a}) - \frac{a}{a^2} \), while if \( A \) is odd, then \( N' \approx \frac{p}{4} (1 + \frac{1}{a}) \). Although we have not worked out the details of these approximations, numerical evidence indicates that they are remarkably accurate. For instance, it appears that if \( 2p \equiv \pm 1 \pmod{a} \) then \( |N - \frac{p}{4} (1 + \frac{1}{a})| < \frac{a}{8} \); for \( 2p \equiv \pm 3 \pmod{a} \), \( |N - \frac{p}{4} (1 + \frac{1}{a})| < \frac{a}{24} \); and \( 4p \equiv \pm 1 \pmod{a} \), \( |N - \frac{p}{4} (1 + \frac{1}{a})| < \frac{a}{10} \). For all pairs with \( |AB| < 10 \) and \( A \) odd, \( |N - \frac{p}{4} (1 + \frac{1}{a})| < 2 \). In particular, one can most likely improve the upper bound \( \frac{a}{8} + 3 \) in the lemma to \( \frac{a}{16} + 3 \) unless \( 2p \equiv \pm 1 \pmod{a} \).

4. Implications of a counterexample to Theorem 1.1

Lemma 4.1. Suppose that \( k, C \) are integers such that the mapping \( x \rightarrow Cx^k \) permutes the even residues of \( \mathbb{Z}/p \). Then for any odd prime \( a \) with \( a^3 + 23a^2 + 42a < \frac{12}{p} \) we have \( a^{k-1} \equiv 1 \pmod{p} \) or \( a^{k+1} \equiv 1 \pmod{p} \).

Proof. Let \( a \) be an odd prime with \( a^3 + 23a^2 + 42a < \frac{12}{p} \). Put \( I = [1, (p-1)/2] \cap \mathbb{Z} \). Let \( N_0(a) \) denote the number of \( x, y \in I \) with \( y \equiv ax \pmod{p} \). Thus \( N_0(a) \) is also the number of \( x, y \in \mathbb{E} \) with \( y \equiv ax \pmod{p} \). Now, since \( x \rightarrow Cx^k \pmod{p} \) is a permutation of the even residues, \( (x, y) \in \mathbb{E}^2 \) and satisfies \( y \equiv ax \pmod{p} \), if and only if \( (Cx^k, Cy^k) \in \mathbb{E}^2 \) and satisfies \( Cy^k \equiv a^k(Cx^k) \pmod{p} \). Therefore
\( N_p(a) = N_p(a^k) \). Now, by Lemma 3.2

\[ \left| N_p(a) - \frac{p}{4} \left( 1 + \frac{1}{a} \right) \right| \leq \frac{a}{8} + 3, \]

where 3 may be replaced by 1 for \( a < 43 \). To estimate \( N_p(a^k) \), set \( d = a^k \). The congruence \( y \equiv dx \pmod{p} \) is equivalent to a congruence of the form \( Ax - By \equiv 0 \pmod{p} \) with \( A > 0, |A|, |B| < \sqrt{p} \) and \( \gcd(A, B) = 1 \). We claim the following:

(i) \( AB \neq 1 \).
(ii) \( AB \) is odd.
(iii) \( B \) is positive.
(iv) \( AB \leq 4\sqrt{p} \).

Indeed, if \( AB = 1 \) then \( A = B = 1, a^k \equiv 1 \pmod{p} \), \( a \equiv 1 \pmod{p} \) (since \( k, p - 1 = 1 \)) and so \( a = 1 \), a contradiction. If \( AB \) is even then by Lemma 2.2

\[ N_p(d) < \frac{p}{4} + \sqrt{p} + 1. \]

Since \( N_p(d) = N_p(a) \) we conclude that

\[ \left| \frac{p}{4} \left( 1 + \frac{1}{a} \right) - \frac{a}{8} - 3 \leq \frac{p}{4} + \sqrt{p} + 1, \]

that is,

\[ \frac{p}{4a} \leq \frac{a}{8} + \sqrt{p} + 4, \]

but, as one sees after some calculations, this contradicts \( a^3 + 23a^2 + 42a < (12/7)p \) unless \( a \leq 7 \). In the latter case, replacing the 3 with 1 in (4.1) leads to a contradiction. If \( AB \) is odd and \( B \) is negative then again by Lemma 2.2, \( N_p(d) < \frac{p}{4} + \sqrt{p} + 1 \) and the same contradiction follows.

Since \( AB \) is odd and positive we have by Lemma 2.2 that

\[ \left| N_p(d) - \frac{p}{4} \left( 1 + \frac{1}{AB} \right) \right| \leq \frac{|A| + |B|}{2} + 1, \]

and obtain, using \( N_p(a) = N_p(d) \),

\[ \frac{p}{4} \left| \frac{1}{a} - \frac{1}{AB} \right| \leq \frac{a}{8} + 1 + \frac{|A| + |B|}{2} + 1, \]

for \( a < 43 \). Suppose that \( AB > 4\sqrt{p} \). Then for \( a < 43 \), we have using \( A, B \leq \sqrt{p} \),

\[ \frac{p}{4} \left| \frac{1}{a} - \frac{1}{4\sqrt{p}} \right| \leq \frac{a}{8} + \sqrt{p} + 2, \]

implying that \( p < \frac{1}{4^2} a^2 + 8a + 4.25a\sqrt{p} \). But this contradicts \( p > \frac{7}{12} (a^3 + 23a^2 + 42a) \) unless \( a = 3 \) and \( 210 < p < 216 \), \( a = 5 \) and \( 530 < p < 551 \) or \( a = 7 \) and \( 1029 < p < 1039 \), ranges where it is known that no such permutation of the even residues exists. If \( a \geq 43 \) we obtain in a similar manner \( p < \frac{1}{4} a^2 + 16a + 4.25a\sqrt{p} \) which also contradicts \( p > \frac{7}{12} (a^3 + 23a^2 + 42a) \) on this range.

Thus we may assume that \( A, B \) are positive odd integers with \( AB \leq 4\sqrt{p} \). We claim that

\[ \left| N_p(d) - \frac{p}{4} \left( 1 + \frac{1}{AB} \right) \right| \leq \frac{AB}{6} + \frac{11}{4}. \]

Indeed, if \( A = 1 \) or \( B = 1 \) then this is just the statement of Lemma 3.2 (b). Otherwise \( A \geq 3 \) and \( B \geq 3 \), whence \( \frac{|A| + |B|}{2} \leq \frac{AB/3 + 3}{2} = \frac{AB}{6} + \frac{3}{2} \), and the claimed
bound follows from (4.2). Thus, using $N_p(a) = N_p(d)$ and (4.1), 

$$
\frac{\phi(\frac{1}{4} a - \frac{1}{AB})}{\phi(\frac{1}{a - 2})} \leq \frac{a}{8} + 3 + \frac{AB}{6} + \frac{11}{4} = \frac{a + AB + 23}{8} + \frac{AB}{6} + \frac{23}{4}.
$$

Suppose that $AB \neq a$. Then the left-hand side is minimized when $AB = a + 2$, where we obtain

$$
\frac{\phi(\frac{1}{4} a - \frac{1}{a + 2})}{\phi(\frac{1}{a})} \leq \frac{a}{8} + \frac{a + 2}{6} + \frac{23}{4} = \frac{7}{24} a + \frac{73}{12}.
$$

We claim that the same inequality holds for any allowable value of $AB \neq a$. Indeed, if $AB < a$, then

$$
\frac{\phi(\frac{1}{4} a - \frac{1}{a + 2})}{\phi(\frac{1}{a})} \leq \frac{a}{8} + \frac{AB}{6} + \frac{23}{4} \leq \frac{a}{8} - \frac{a - 2}{6} + \frac{23}{4}.
$$

For $AB > a$, set $b = AB$ and observe that the function $f(b) = \frac{b}{4} (\frac{1}{a} - \frac{1}{b}) - \frac{a}{8} - \frac{b}{6} - \frac{23}{4}$ satisfies $f(b) \geq f(a + 2)$ for $a + 2 \leq b \leq \frac{3p}{\phi(p) + 1}$. Then since $4\sqrt{p} \leq \frac{3p}{\phi(p) + 1}$, that is, $p \geq (8/3)^2(a + 2)^2$ for any $a$ satisfying $a^3 + 23a^2 + 42a < (12/7)p$, we obtain the claim.

The bound in (4.3) implies that

$$12p < 7(a + 2)(a + 21) = 7(a^3 + 23a^2 + 42a),$$

contradicting our assumption on $a$. Therefore $AB = a$, and since $a$ is a prime this means $(A, B) = (a, 1)$ or $(1, a)$. In the former case, $d \equiv a \pmod{p}$, that is $a^{k-1} \equiv 1 \pmod{p}$, while in the latter case $d \equiv a^{-1} \pmod{p}$, that is, $a^{k+1} \equiv 1 \pmod{p}$.

\[\Box\]

5. Computer Generated Information

Lemma 4.1 provides a very efficient algorithm for showing that small primes satisfy Theorem 1.1. We need only produce an odd prime $a$ satisfying

$$a^3 + 23a^2 + 42a < (12/7)p,$$

whose order $(\pmod{p})$ exceeds $k + 1$.

Using a modified version of the UBASIC program GENSHP, which calculates the minimal odd primitive root of a given prime, we calculated the minimal odd primitive roots of primes up to $4 \cdot 10^8$ on a desktop computer. Let $a = a_p$ denote the minimal such odd prime primitive root. We found that $a_p$ satisfies (5.1) for all primes $p$ on the interval $10^6 < p < 4 \cdot 10^8$ with the exceptions of $p = 2080597$ where $a_p = 151$, $p = 2697301$ where $a_p = 191$, and $p = 4022911$ where $a_p = 211$. By Lemma 4.1, for all primes in this interval except for the three exceptional primes, we must have $p - 1/k = 1$, that is $k \equiv \pm 1 \pmod{p - 1}$. These two cases were dealt with by Goresky and Klapper [7], but they also follow easily from results in this paper, the case $k \equiv 1 \pmod{p - 1}$ from Lemma 2.3, and the case $k \equiv -1 \pmod{p - 1}$ from Lemma 6.3 and the Kloosterman sum bound $\Phi_{-1} \leq 2\sqrt{p}$, for $p > 337$.

For any prime $p$ with $a_p$ failing (5.1) we calculated the maximal order $(\pmod{p})$ of all odd primes $a$ satisfying (5.1). We found that for primes $p$ in the interval $10^5 < p < 4 \cdot 10^8$, the maximal order of such $a$ is always $(p - 1)/2$, with the exception of $p = 267901$ where the maximal order is $(p - 1)/3$ at $a = 31$. If $ord_p(a) = (p - 1)/2$ then $a^{k+1} \equiv 1 \pmod{p}$ implies that $p^{\frac{1}{2}} | (k + 1)$. The case
\((p - 1, k \pm 1) = p - 1\) has already been dealt with. If \((p - 1, k \pm 1) = \frac{p - 1}{2}\) then by Lemma 6.2 and Lemma 7.1, for \(p > 7770\), \(N_k(A) > 0\), with \(N_k(A)\) as defined in (6.1). (Note, these two lemmas are proven without any assumption on the size of \(p\), unlike Lemma 6.1.) Smaller \(p\) with \((p - 1, k \pm 1) = \frac{p - 1}{2}\) were tested directly.

For the remaining \(p\) with \(p > 2500\) we found that there is always some odd prime \(a\) satisfying (5.1) such that \(\text{ord}_p(a) = \frac{p - 1}{3}\) or \(\frac{p - 1}{4}\). For these primes, the handful of permissible values of \(k\) \((k \equiv \pm 1 \pmod{\frac{p - 1}{3}})\) or \((\text{mod}\ \frac{p - 1}{4})\) were tested directly to show \(N_k(A) > 0\). Finally, values of \(p < 2500\) were tested directly. Thus, with an hour or two of running time on a PC, we established

**Lemma 5.1.** For all primes \(p\) with \(p < 4 \cdot 10^8\), Theorem 1.1 is true.

6. The case of large \((k - 1, p - 1)\)

For any integers \(A, k\), let \(N_k(A)\) denote the number of even residues such that \(Ax^k\) is odd,

\[
N_k(A) = |AB^k \cap \mathbb{O}|
\]

The first lemma is a slight sharpening of Theorem 4 of [2].

**Lemma 6.1.** Suppose that the mapping \(x \rightarrow Ax^k\) is a permutation of \(\mathbb{Z}_p\) but not the identity mapping and that \((k - 1, p - 1) > 9.06\ \sqrt{p}\). Then \(N_k(A) > 0\).

We begin by proving a weaker bound,

**Lemma 6.2.** Suppose that the mapping \(x \rightarrow Ax^k\) is not the identity mapping on \(\mathbb{Z}_p\). Set \(t = (p - 1)/(k - 1, p - 1)\). Then \(N_k(A) > 0\) provided that

\[
(k - 1, p - 1) > 6 \left(1 - \frac{1}{t}\right) \left(\frac{1}{\pi} \log p + 0.98126\right)^2 \sqrt{p}.
\]

**Proof.** Let \(B\) be an integer with \(AB^k \not\equiv B \pmod{p}\), and \(C\) an integer with \(C \equiv AB^{k-1} \pmod{p}\), so that \(C \not\equiv 0, 1 \pmod{p}\). Put \(k_1 = (p - 1, k - 1)\) and \(t = (p - 1)/k_1\). Our strategy is to find an element of the form \(Bz^t \in \mathbb{E}\) with \(CBz^t \in \mathbb{O}\). For any such element we have \(A(Bl^t) \equiv CBz^t \pmod{\mathbb{O}}\), implying that \(N_k(A) > 0\). To do this, we count the number \(N\) of solutions of the congruence \(y \equiv Cx \pmod{p}\) such that \(x \in \mathbb{E}\), \(B^{-1}x\) is a \(t\)-th power, and \(y \in \mathbb{O}\). Let \(\chi_{\mathbb{E}} = \sum_{y=1}^p a_{\mathbb{E}}(y)e_p(yx)\) and \(\chi_{\mathbb{O}} = \sum_{y=1}^p a_{\mathbb{O}}(y)e_p(yx)\) be the characteristic functions of the sets \(\mathbb{E}\) and \(\mathbb{O}\) respectively.

Letting \(\sum_{\psi^t = \psi_0}\) denote a sum over all multiplicative characters \(\psi \pmod{p}\) satisfying \(\psi^t = \psi_0\), where \(\psi_0\) is the principal character, we have

\[
N = \frac{1}{t} \sum_x \left( \sum_{\psi^t = \psi_0} \psi(B^{-1}x) \right) \chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx)
\]

\[
= \frac{1}{t} \sum_x \chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx) + \frac{1}{t} \sum_{\psi \neq \psi_0} \sum_x \psi(B^{-1}x)\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx)
\]

\[
= \text{Main + Error}.
\]

**Main Term:** Let \(I = [1, (p - 1)/2]\). The sum \(\sum_x \chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx)\) counts the number of \(x \in I\) such that \(2Cx \equiv -2y \pmod{p}\) for some \(y \in I\), that is, the number of
Proof of Lemma 6.1.

By Lemma 5.1, we may assume that $k > 9.06 \sqrt{p}$. By Lemmas 6.3 and 6.4, $N_k(A) > 0$ provided that $k_1 + \frac{p^{3/2}}{k_1} < \frac{p - 7}{9}$. Otherwise, either

$$k_1 < \frac{1}{2} \left( \frac{p - 7}{9} - \sqrt{\frac{(p - 7)^2}{81} - 4p^{3/2}} \right) \quad \text{or} \quad k_1 > \frac{1}{2} \left( \frac{p - 7}{9} + \sqrt{\frac{(p - 7)^2}{81} - 4p^{3/2}} \right).$$

The first inequality fails for $k_1 > 9.06 \sqrt{p}$ and $p > 4 \cdot 10^8$, while the second inequality implies that $k_1 > 6\left(\frac{1}{\pi} \log(p) + .981262\right)^2 \sqrt{p}$ for $p > 4 \cdot 10^8$. In this case Lemma 6.2 gives $N_k(A) > 0$.

$x, y \in I$ such that $y \equiv -Cx \pmod{p}$. By Lemma 2.3, since $C \not\equiv 1 \pmod{p}$ we get

$$\text{Main} = \frac{1}{t} \sum_{x} \chi_E(x) \chi_0(Cx) \geq \frac{p - 1}{6t} = \frac{k_1}{6}. \quad (6.5)$$

Error Term: Let $\psi$ be a nonprincipal character $\pmod{p}$. Then

$$\sum_{x} \psi(B^{-1}x) \chi_E(x) \chi_0(Cx) = \sum_{x} \left( \sum_{y} a_E(y) e_\psi(yx) \right) \left( \sum_{z} a_\psi(z) e_\psi(zCx) \right) \psi(B^{-1}x)$$

$$= \sum_{y} \sum_{z} a_E(y)a_\psi(z)G(y + Cz, B^{-1}),$$

where $G(y + Cz, B^{-1})$ is the Gauss sum $G(y + Cz, B^{-1}) = \sum_{x} e_p((y + Cz)x)\psi(B^{-1}x)$, of modulus $\sqrt{p}$, unless $y + Cz = 0$ in which case it vanishes. Thus,

$$\left| \sum_{x} \psi(B^{-1}x) \chi_E(x) \chi_0(Cx) \right| \leq \sqrt{p} \sum_{y} |a_E(y)| \sum_{z} |a_\psi(z)|. \quad (1 - 1/t)\left( \frac{1}{\pi} \log(p) + .981262 \right)^2 \sqrt{p}.$$
7. The Case of Large \( (k + 1, p - 1) \)

**Lemma 7.1.** If \( (k + 1, p - 1) > 18 \frac{p-1}{p} \sqrt{p} \) then \( N_k(A) > 0 \).

**Proof.** Let \( d = (p - 1)/(k + 1, p - 1) \), \( S = \sum_{x=1}^{p-1} e_p(Ax^k + Bx) \), where \( A, B \) are integers not divisible by \( p \). Now for any integer \( u \) with \( p \nmid u \), \( u^{2k} \equiv u^{-d} \pmod{p} \), and so we have
\[
(p - 1)S = \sum_{u=1}^{p-1} \sum_{x=1}^{p-1} e_p(A(xu^d)^k + Bxu^d) = \sum_{x=1}^{p-1} e_p(Ax^{k-1}u^{-d} + Bxu^d).
\]
By the Weil estimate, the sum over \( u \) is bounded by \( 2d\sqrt{p} \) and so we obtain
\[
\lvert S \rvert \leq 2d\sqrt{p}.
\]
We can apply Lemma 6.3 and conclude \( N_k(A) > 0 \) provided that \( 2d\sqrt{p} < (p - 7)/9 \), that is, \( (k + 1, p - 1) > 18 \frac{p-1}{p} \sqrt{p} \). \( \square \)

Remark: With extra effort, one can save a factor \( \sqrt{2} \) in the estimate of \( |S| \) in (7.1) by using the estimate of Adolphson and Sperber [1, Corollary 4.3], and Denef and Loeser [6, Theorem 1.3] for two variable exponential sums over tori.

8. Proof of Theorem 1.1

By Lemma 5.1 we may assume that \( p > 4 \cdot 10^8 \). Let
\[
(k - 1, p - 1) = \alpha\sqrt{p}, \quad (k + 1, p - 1) = \beta\sqrt{p}.
\]
By Lemma 6.1, Lemma 7.1 and the fact that \( (k - 1, k + 1) = 2 \), we may assume that
\[
\alpha < 9.06, \quad \beta < 18.001 \quad \text{and} \quad \alpha\beta \leq 2,
\]
the latter inequality following from
\[
\alpha\beta p = (k - 1, p - 1)(k + 1, p - 1) \leq ((k - 1)(k + 1), p - 1)(k - 1, k + 1) \leq (p - 1)^2.
\]
Suppose that there exists a nontrivial permutation of the even residues. Then, by Lemma 4.1, for any odd prime \( a \) such that \( a^3 + 23a^2 + 42a < \frac{12}{7}p \) we have \( a^{k-1} \equiv 1 \pmod{p} \) or \( a^{k+1} \equiv 1 \pmod{p} \). In particular, every odd prime up to \( p^{1/3} \) is either a \((k - 1)\)-th or \((k + 1)\)-th root of unity (for \( p > 4 \cdot 10^8 \)). Let
\[
\Lambda_- := \{ a : a \text{ is an odd prime, } a < p^{1/3}, \quad a^{k-1} \equiv 1 \pmod{p} \},
\]
\[
\Lambda_+ := \{ a : a \text{ is an odd prime, } a < p^{1/3}, \quad a^{k+1} \equiv 1 \pmod{p} \},
\]
and put \( \lambda_- = \lvert \Lambda_- \rvert, \lambda_+ = \lvert \Lambda_+ \rvert \). By Rosser and Schoenfeld [11, Theorem 1] the number of primes up to \( t \) satisfies
\[
\pi(t) > \frac{t}{\log t} \left( 1 + \frac{1}{2\log t} \right), \quad \text{for } t \geq 59,
\]
and so
\[
\lambda_- + \lambda_+ = \pi(p^{1/3}) - 1 > \frac{3p^{1/3}}{\log p} \left( 1 + \frac{3}{2\log p} \right) - 1.
\]
Now, the number of monomials of degree less than or equal to 3 in \(n\)-variables is \(\binom{n+3}{3}\), and thus by considering all products of one, two or three primes less than \(p^{1/3}\) we obtain at least \(\binom{\lambda_- + 3}{3}\) distinct odd \((k - 1)\)-th roots of unity, and \(\binom{\lambda_+ + 3}{3}\) distinct odd \((k + 1)\)-th roots of unity. Since there are exactly \(\frac{1}{2}(k - 1, p - 1)\) of the former and \(\frac{1}{2}(k + 1, p - 1)\) of the latter (the factor \(\frac{1}{2}\) coming from the observation that \(-1\) is a \((k \pm 1)\)-th root of unity), we must have

\[
\binom{\lambda_- + 3}{3} \leq \frac{\alpha}{2} \sqrt{p}, \quad \binom{\lambda_+ + 3}{3} \leq \frac{\beta}{2} \sqrt{p}.
\]

In particular, \((\lambda_- + 1.8)^3 < 3\alpha \sqrt{p}\), \((\lambda_+ + 1.8)^3 < 3\beta \sqrt{p}\), and thus

\[
\lambda_- + \lambda_+ + 3.6 \leq 3^{1/3} (\alpha^{1/3} + \beta^{1/3}) p^{1/6}.
\]

Subject to the constraints (8.1) the expression in \(\alpha, \beta\) is maximized when \(\beta = 18.001, \alpha = 2/\beta = .111...\). Thus, we get

\[
\lambda_- + \lambda_+ \leq 4.474 p^{1/6} - 3.6,
\]

and so by (8.2),

\[
\frac{3p^{1/3}}{\log p} \left(1 + \frac{3}{2 \log p}\right) < 4.474 p^{1/6} - 2.6.
\]

But this implies \(p < 3.65 \cdot 10^8\), a contradiction.

Acknowledgement: The authors wish to thank the referee for the many helpful comments on the preparation of this paper.

References


