

DECIMATIONS OF ℓ -SEQUENCES AND PERMUTATIONS OF EVEN RESIDUES $\bmod p^*$

JEAN BOURGAIN[†], TODD COCHRANE[‡], JENNIFER PAULHUS[‡], AND
CHRISTOPHER PINNER[‡]

Abstract. Goresky and Klapper conjectured that for any prime $p > 13$ and any ℓ -sequence \mathbf{a} based on p , every pair of allowable decimations of \mathbf{a} is cyclically distinct. The conjecture is essentially equivalent to the statement that the mapping $x \rightarrow Ax^d$, with $(d, p-1) = 1$, $p \nmid A$, is a permutation of the even residues $(\bmod p)$ if and only if $d = 1$ and $A \equiv 1 \pmod{p}$ for $p > 13$. We prove the conjecture for $p > 2.26 \cdot 10^{55}$ and establish it in a number of other special cases such as when $-.000274p < d < .000823p$.

Key words. ℓ -sequences, arithmetic correlation, exponential sums, permutations of residues

AMS subject classifications. 11A07, 11A15, 11B50, 11L07, 11T23, 94A55

DOI. 10.1137/080737678

1. Introduction. Let p be an odd prime, $\mathbb{Z}_p = \mathbb{Z}/(p)$, A, d integers with $(d, p-1) = 1$, $p \nmid A$, and let \mathbb{E}, \mathbb{O} be the set of even and odd residues $(\bmod p)$,

$$\mathbb{E} = \{2, 4, 6, 8, \dots, p-1\} \subset \mathbb{Z}_p, \quad \mathbb{O} = \{1, 3, 5, 7, \dots, p-2\} \subset \mathbb{Z}_p.$$

Let $A\mathbb{E}^d = \{Ax^d : x \in \mathbb{E}\} \subset \mathbb{Z}_p$. Since $(d, p-1) = 1$ the mapping $x \rightarrow Ax^d$ permutes the elements of \mathbb{Z}_p . Our interest is in determining when this mapping is a permutation of the elements of \mathbb{E} , that is, $A\mathbb{E}^d \cap \mathbb{O}$ is empty. It is trivially a permutation when $A = 1$ and $d = 1$. It is also known to be a permutation in the following cases:

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

Clearly, we may assume $|A| < p/2$ and $|d| < p/2$.

GK-conjecture (generalized Goresky–Klapper (GK) conjecture [9]). With the exception of the six cases listed above, if $(d, p-1) = 1$, $0 < |A| < p/2$, $|d| < p/2$, and $(A, d) \neq (1, 1)$, then $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty.

This conjecture is motivated by an (essentially) equivalent conjecture concerning binary ℓ -sequences based on p , sequences $\mathbf{a} = \{a_i\}_i$ of zeros and ones with $a_i \equiv (2^{-i} \bmod p) \pmod{2}$, (the parity of the least positive residue of $2^{-i} \pmod{p}$), or some shift $\mathbf{a}_t = \{a_{i+t}\}_i$ of \mathbf{a} . These sequences are strictly periodic with period $p-1$ when 2 is a primitive root.

If \mathbf{a} is an ℓ -sequence based on p , then an allowable decimation of \mathbf{a} is a sequence of the type $\mathbf{x} = \mathbf{a}^d$, where $x_i = a_{d \cdot i}$, and $(d, p-1) = 1$. Two periodic binary sequences \mathbf{a} and \mathbf{b} with the same period T are cyclically distinct if $\mathbf{a}_t \neq \mathbf{b}$ for all shifts \mathbf{a}_t , $0 < t < T$. The following conjecture implies that ℓ -sequences produce large families of cyclically distinct sequences with ideal arithmetic cross-correlation.

*Received by the editors October 9, 2008; accepted for publication (in revised form) January 29, 2009; published electronically DATE.

<http://www.siam.org/journals/sidma/x-x/73767.html>

[†]School of Mathematics, Institute of Advanced Study, Princeton, NJ 08540 (Bourgain@math.ias.edu).

[‡]Department of Mathematics, Kansas State University, Manhattan, KS 66506 (cochrane@math.ksu.edu, paulhus@math.ksu.edu, pinner@math.ksu.edu).

Original GK-conjecture (Goresky and Klapper [9]). If $p > 13$ is a prime, 2 a primitive root modulo p , and \mathbf{a} an ℓ -sequence based on p , then every pair of allowable decimations of \mathbf{a} is cyclically distinct.

To see how this conjecture is related to the first one, notice that the sequence \mathbf{a} is a cyclic permutation of \mathbf{a}^d if and only if there is some $A \in \mathbb{Z}_p^*$ such that $(A2^{-id} \bmod p) \equiv (2^{-i} \bmod p) \pmod{2}$ for all i . If 2 is a primitive root, then 2^{-i} runs through all nonzero residues $(\bmod p)$, and so the previous congruence is true if and only if $(Ax^d \bmod p) \equiv (x \bmod p) \pmod{2}$ for every x , that is, $A\mathbb{E}^d = \mathbb{E}$.

The assumption that 2 is a primitive root modulo p is essential for the connection with ℓ -sequences, but we believe this assumption to be unnecessary for the validity of the first conjecture.

The conjecture is elementary when $d = 1$; see the remark at the end of section 6. Klapper, using a computer, has verified the generalized conjecture for all primes less than two million. Goresky, Klapper, and Murty [10] proved the conjecture for $d = -1$ and for the case where $p \equiv 1 \pmod{4}$ and $d = (p+1)/2$. Goresky et al. [11, Theorem 2.2], sharpening the work of [10], proved it for all values of d with

$$(1) \quad 0 < d \leq \frac{(p^2 - 1)^4}{2^{24}p^7} \approx 5.96 \cdot 10^{-8}p, \quad \text{or} \quad 0 > d \geq -\frac{(p^2 - 1)^4}{2^{25}p^7} \approx -2.98 \cdot 10^{-8}p.$$

They also gave an upper bound on the number of possible counterexamples to the conjecture for a given p . The main result of this paper is to establish that the conjecture is valid for all sufficiently large p .

To state our first theorem let

$$(2) \quad M = \#\{(x_1, x_2, x_3, x_4) \in (\mathbb{Z}_p^*)^4 : x_1 + x_2 = x_3 + x_4, x_1^d + x_2^d = x_3^d + x_4^d\}.$$

Using the method of finite Fourier series and exponential sums we prove the following theorem.

THEOREM 1. *If $M < .000823p^3$, then the GK-conjecture holds true.*

It is elementary (see [8, Lemma 3.2]) that $M < d(p-1)^2$ for $d > 0$ and that $M < 3|d|(p-1)^2$ for $d < 0$, and thus we have the following improvement of (1).

COROLLARY 1. *If $-.000274p < d < .000823p$, then the GK-conjecture holds true.*

A result analogous to Theorem 1 can be stated with M replaced by a binomial exponential sum bound. Let $e_p(\cdot)$ denote the additive character on \mathbb{Z}_p , $e_p(x) = e^{2\pi ix/p}$, and set

$$(3) \quad \Phi_d = \max_{(u,v) \neq (0,0)} \left| \sum_{x=1}^{p-1} e_p(ux + vx^d) \right|,$$

where u, v run through \mathbb{Z}_p .

THEOREM 2. *If $\Phi_d \leq \frac{p-7}{9}$, then the GK-conjecture holds true.*

Unfortunately, the upper bound on M in Theorem 1 and the upper bound on Φ_d in Theorem 2 both fail if the quantity

$$d_1 := (d-1, p-1)$$

is large, as shown in [7]. For small d_1 we are able to establish the desired upper bound on M for p sufficiently large.

THEOREM 3. *For any integer d with $(d, p-1) = 1$, $d_1 < .18(p-1)^{16/23}$, we have $M \leq 13658p^{66/23}$.*

In section 6, we use a different method involving multiplicative characters to handle the case of large d_1 . As it turns out, we are able to prove the GK-conjecture for d_1 sufficiently large.

THEOREM 4. (a) *If $d_1 > 8(\frac{4}{\pi^2} \log p + 1)^2 \sqrt{p}$, then the GK-conjecture holds true.*

(b) *If $p > 2.1 \cdot 10^7$ and $d_1 > 10\sqrt{p}$, then the GK-conjecture holds true.*

It is a simple matter to deduce from Theorems 1, 3, and 4 that the GK-conjecture is true for p sufficiently large.

THEOREM 5. *For any prime $p > 2.26 \cdot 10^{55}$ the GK-conjecture holds true.*

Proof. If $d_1 \leq .18(p-1)^{16/23}$, then by Theorem 3, $M \leq 13658p^{66/23} < .000823p^3$ for $p \geq 2.26 \cdot 10^{55}$. The result then follows from Theorem 1. Otherwise $d_1 > .18(p-1)^{16/23} > 10\sqrt{p}$ for $p > 8.3 \cdot 10^8$, and so Theorem 4(b) yields the result. \square

Remarks. 1. There are several available estimates for Φ_d , such as the Weil bound ($\Phi_d \leq (d-1)\sqrt{p}$) or the Mordell bound ($\Phi_d \leq p^{1/4}M^{1/4}$) but they (together with Theorem 2) lead to weaker results than Corollary 1 and Theorem 5. The first author recently established a new type of bound for a general exponential sum [2, Theorem 1]. For the binomial of interest here (where $(d, p-1) = 1$) it states that given $\epsilon > 0$ there is a $\delta > 0$ such that if $d_1 < p^{1-\epsilon}$, then

$$(4) \quad \Phi_d < p^{1-\delta}.$$

The proof of (4) uses additive combinatorics and harmonic analysis, and appeals to the Balog–Szemerédi–Gowers theorem; see [12]. It may not be easy to make the result numeric.

2. Xu and Qi [19] have proven the GK-conjecture for the case of odd prime powers p^e with $e \geq 2$, $p^e \neq 9$.

3. The methods developed in this paper can be applied in the same manner to q -ary ℓ -sequences, $a_i \equiv (q^{-i} \pmod{p}) \pmod{q}$, where q is a primitive root \pmod{p} .

4. The methods can also be applied to the following generalization of a problem of D.H. Lehmer. Given d relatively prime to $p-1$, obtain an asymptotic formula for the number N_d of even residues $x \pmod{p}$ such that $x^d \pmod{p}$ is an odd residue. Our interest in the current paper is just establishing that N_d is nonzero. In the classical Lehmer problem $d = -1$ it is well known (by the Kloosterman sum estimate) that $N_{-1} \sim p/4$; see Zhang [22], [23]. Many generalizations have appeared in recent years, Zhang [24], [25]; Alkan, Stan, and Zaharescu [1]; Cobeli and Zaharescu [4]; Shparlinski [18]; Liu and Zhang [14], [15], [16]; Louboutin, Rivat, and Sarkozy [17]; Yuan and Zhang [21]; Xu and Zhang [20], among others. For general d we see that $N_d \sim p/4$ for small d_1 , but for d_1 large there can be bias. For example when $d = \frac{p+2}{3}$, $N_d \sim p/6$. We will report on this problem and the problem of q -ary ℓ -sequences in what follows.

5. Canetti, Friedlander, and Shparlinski [3] have previously shown a bound slightly stronger than Theorem 3 for the average value of M (averaged over all values of d):

$$\frac{1}{p-1} \sum_{d=1}^{p-1} M \leq 72(p-1)^{11/4} \tau(p-1).$$

2. Finite Fourier series. This section provides a review of basic tools we shall need from the theory of finite Fourier series, and can be skipped by the experienced reader. Let p be an odd prime, $e_p(\cdot) = e^{2\pi i \cdot / p}$, and $\sum_x = \sum_{x=1}^p$. Any complex valued function α defined on \mathbb{Z}_p has a Fourier expansion

$$\alpha(x) = \sum_y a(y) e_p(xy),$$

where the coefficients $a(y)$ are given by

$$(5) \quad a(y) = \frac{1}{p} \sum_x \alpha(x) e_p(-xy).$$

The convolution of two functions α and β on \mathbb{Z}_p is defined by

$$\alpha * \beta(x) = \sum_u \sum_{\substack{v \\ u+v=x}} \alpha(u)\beta(v) = \sum_u \alpha(u)\beta(x-u).$$

If α and β have Fourier expansions with coefficients $a(y)$, $b(y)$, respectively, then $\alpha * \beta$ has coefficients $pa(y)b(y)$.

Let

$$I = \{a+1, a+2, \dots, a+B\} \subset \mathbb{Z}_p$$

be an interval in \mathbb{Z}_p with $B \leq p$, and χ_I be the characteristic function of I with Fourier expansion $\chi_I(x) = \sum_y a_I(y) e_p(yx)$. Then

$$a_I(0) = B/p, \quad a_I(y) = p^{-1} e_p \left(\left(-a - \frac{B}{2} - \frac{1}{2} \right) y \right) \frac{\sin(\pi B y / p)}{\sin(\pi y / p)}, \quad y \neq 0,$$

and

$$(6) \quad \sum_y |a_I(y)| = f(B, p) := \frac{1}{p} \sum_y \left| \frac{\sin(\pi B y / p)}{\sin(\pi y / p)} \right|,$$

where the summand is understood to be B when $y = 0$. In [5] the second author proved

$$f(B, p) \leq \frac{4}{\pi^2} \log p + 1.$$

The main term in this upper bound cannot be improved. Indeed, in [6, eq. 5] Cochrane and Peral showed

$$f(B, p) = \frac{4}{\pi^2} \log p + O(1).$$

Letting $I = \{1, 2, \dots, \frac{p-1}{2}\}$ we see that $\chi_{\mathbb{E}}(x) = \chi_I(2^{-1}x)$, and so $a_{\mathbb{E}}(y) = a_I(2y)$ and $\sum_y |a_{\mathbb{E}}(y)| = \sum_y |a_I(y)|$. Thus,

$$(7) \quad \sum_y |a_{\mathbb{E}}(y)| \leq \frac{4}{\pi^2} \log p + 1.$$

The same holds for $\sum_y |a_{\mathbb{O}}(y)|$.

Let

$$I = \{a_1+1, a_1+2, \dots, a_1+B_1\}, \quad J = \{b_1+1, \dots, b_1+B_2\}$$

be intervals of integers in \mathbb{Z}_p with $|I| = B_1$, $|J| = B_2$, and $1 \leq B_1, B_2 < p$, and let χ_I, χ_J have Fourier expansions

$$\chi_I(x) = \sum_y a_I(y) e_p(xy), \quad \chi_J(x) = \sum_y a_J(y) e_p(xy).$$

The convolution $\chi_I * \chi_J$, defined by $\chi_I * \chi_J(x) = \sum_u \chi_I(u)\chi_J(x-u)$, has Fourier coefficients $pa_I(y)a_J(y)$.

We make frequent appeal to Parseval's identity which states that if α is any complex valued function on \mathbb{Z}_p with expansion $\alpha(x) = \sum_y a(y)e_p(xy)$, then

$$p \sum_y |a(y)|^2 = \sum_x |\alpha(x)|^2.$$

The theory extends naturally to functions of two (or more) variables. If $\alpha(x, y)$ is a complex valued function defined on \mathbb{Z}_p^2 , then it has a finite Fourier expansion

$$\alpha(x, y) = \sum_u \sum_v a(u, v)e_p(ux + vy).$$

In particular, if $\alpha(x, y) = f(x)g(y)$, then the Fourier coefficients of $\alpha(x, y)$ are just the products of the coefficients of f and g .

3. Proof of Theorem 1. To show there exists an $x \in \mathbb{E}$ such that $Ax^d \in \mathbb{O}$, we must show there exists a solution (x, y) to the equation $A(2x)^d = 2y - 1$, over \mathbb{Z}_p , with $(x, y) \in I_1 \times I_2$, where

$$I_1 = \left\{0, 1, 2, \dots, \frac{p-1}{2}\right\} \subset \mathbb{Z}_p, \quad I_2 = I_1 - \{0\} \subset \mathbb{Z}_p.$$

Put

$$I = \{0, 1, 2, 3, \dots, [(p-1)/4]\} \subset \mathbb{Z}_p, \quad J = \{1, 2, 3, \dots, [(p+1)/4]\} \subset \mathbb{Z}_p,$$

and let χ_I, χ_J be the characteristic functions of I, J with Fourier expansions

$$\chi_I(x) = \sum_u a_I(u)e_p(ux), \quad \chi_J(x) = \sum_v a_J(v)e_p(vx).$$

Let α be the convolution

$$\alpha(x, y) = \chi_I * \chi_I(x) \cdot \chi_I * \chi_J(y),$$

with Fourier expansion $\alpha(x, y) = \sum_{u,v} a(u, v)e_p(ux + vy)$, where

$$(8) \quad a(u, v) = p^2 a_I(u)^2 a_I(v) a_J(v).$$

In particular,

$$(9) \quad a(0, 0) = \frac{|I|^3 |J|}{p^2}.$$

Since $I + I \subset I_1$ and $I + J \subset I_2$, α is supported on $I_1 \times I_2$, and so it suffices to show that $\sum_{A(2x)^d=2y-1} \alpha(x, y) > 0$. We have

$$\begin{aligned} \sum_{\substack{A(2x)^d=2y-1 \\ x \neq 0}} \alpha(x, y) &= \sum_{\substack{A(2x)^d=2y-1 \\ x \neq 0}} \sum_{u,v} a(u, v)e_p(ux + vy) \\ &= a(0, 0)(p-1) + \sum_{(u,v) \neq (0,0)} a(u, v)e_p(2^{-1}v) \sum_{x=1}^{p-1} e_p(ux + v(A2^{d-1}x^d)) \\ &= \text{Main} + \text{Error}, \end{aligned}$$

say. Now, by (9),

$$(10) \quad \text{Main} = a(0,0)(p-1) = \frac{p-1}{p^2} |I|^3 |J|.$$

To estimate the error term we break it up as

$$\text{Error} = E_1 + E_2 + E_3,$$

where E_1 is the sum over $u = 0, v \neq 0$; E_2 the sum over $u \neq 0, v = 0$; and E_3 the sum over $u \neq 0, v \neq 0$. For E_1 and E_2 the sum over x is -1 since $(d, p-1) = 1$. Thus

$$(11) \quad |E_1| \leq \sum_v |a(0, v)| = p^2 \sum_v |a_I(0)|^2 |a_I(v) a_J(v)| \leq p^2 \frac{|I|^2}{p^2} \frac{|I|^{1/2} |J|^{1/2}}{p} = \frac{|I|^{5/2} |J|^{1/2}}{p}$$

by the Cauchy–Schwarz inequality and Parseval’s identity, and

$$(12) \quad |E_2| \leq \sum_u |a(u, 0)| = p^2 \sum_u |a_I(u)|^2 |a_I(0) a_J(0)| = \frac{|I|^2 |J|}{p}.$$

For E_3 we use a variant from the argument of Konyagin and Shparlinski [13, section 7]. By invariance under the group action we have

$$(13) \quad |E_3| \leq \sum_{u \neq 0} \sum_{v \neq 0} |a(u, v)| \left| \sum_{x \neq 0} e_p(ux + vA_2^{d-1}x^d) \right| \\ = \sum_{u' \neq 0} \sum_{v' \neq 0} \beta(u', v') \left| \sum_{x \neq 0} e_p(u'x + v'x^d) \right|,$$

where

$$(14) \quad \beta(u', v') = \frac{1}{p-1} \sum_{x \neq 0} |a(xu', A_1 x^d v')|,$$

and $A_1 A_2^{d-1} \equiv 1 \pmod{p}$. Next, from Hölder’s inequality

$$(15) \quad |E_3| \leq \left(\sum_{u'} \sum_{v'} \left| \sum_x e_p(u'x + v'x^d) \right|^4 \right)^{\frac{1}{4}} \left(\sum_{u' \neq 0} \sum_{v' \neq 0} \beta(u', v') \right)^{\frac{1}{2}} \left[\sum_{u' \neq 0} \sum_{v' \neq 0} \beta(u', v')^2 \right]^{\frac{1}{4}} \\ = E_4^{1/4} E_5^{1/2} E_6^{1/4},$$

say.

Clearly,

$$(16) \quad E_4 = p^2 M,$$

with M as in (2). Next, using (8)

$$\begin{aligned}
E_5 &= \sum_{u' \neq 0} \sum_{v' \neq 0} \beta(u', v') = \frac{1}{p-1} \sum_{x \neq 0} \sum_{u' \neq 0} \sum_{v' \neq 0} |a(xu', A_1 x^d v')| = \sum_{u \neq 0} \sum_{v \neq 0} |a(u, v)| \\
&= p^2 \left(\sum_{u \neq 0} |a_I(u)|^2 \right) \left(\sum_{v \neq 0} |a_I(v)| |a_J(v)| \right) \\
&\leq p^2 \left(\sum_{u \neq 0} |a_I(u)|^2 \right) \left(\sum_{v \neq 0} |a_I(v)|^2 \right)^{\frac{1}{2}} \left(\sum_{v \neq 0} |a_J(v)|^2 \right)^{\frac{1}{2}},
\end{aligned}$$

and so by Parseval's identity

$$(17) \quad E_5 \leq p^{-2} (p - |I|)^{3/2} |I|^{3/2} (p - |J|)^{1/2} |J|^{1/2} \leq p^{-2} (p - |I|)^2 |I|^2.$$

Finally, for E_6 we have

$$\begin{aligned}
E_6 &= \sum_{u' \neq 0} \sum_{v' \neq 0} \beta(u', v')^2 = \frac{1}{(p-1)^2} \sum_{x \neq 0} \sum_{y \neq 0} \sum_{u' \neq 0} \sum_{v' \neq 0} |a(xu', A_1 x^d v')| |a(yu', A_1 y^d v')| \\
&= \frac{1}{p-1} \sum_{\substack{1 \leq u_1, u_2, v_1, v_2 < p \\ (v_1/v_2) \equiv (u_1/u_2)^d \pmod{p}}} |a(u_1, v_1)| |a(u_2, v_2)| \\
&= \frac{1}{p-1} \sum_{1 \leq u_1, u_2, j < p} |a(u_1, ju_1^d)| |a(u_2, ju_2^d)| \\
&= \frac{p^4}{p-1} \sum_{1 \leq u_1, u_2 < p} |a_I(u_1)|^2 |a_I(u_2)|^2 \sum_{1 \leq j < p} |a_I(ju_1^d) a_J(ju_1^d)| |a_I(ju_2^d) a_J(ju_2^d)| \\
&\leq \frac{p^4}{p-1} \left(\sum_{u \neq 0} |a_I(u)|^2 \right)^2 \left[\sum_{j \neq 0} |a_I(j) a_J(j)|^2 \right] \\
&= \frac{1}{p-1} |I|^2 (p - |I|)^2 \left[\sum_{j \neq 0} |a_I(j) a_J(j)|^2 \right].
\end{aligned}$$

To evaluate the latter sum we apply Parseval's identity to $\alpha(x) = \chi_I * \chi_J$ to obtain

$$\begin{aligned}
\sum_{j \neq 0} |a_I(j) a_J(j)|^2 &= \sum_j |a_I(j) a_J(j)|^2 - |a_I(0) a_J(0)|^2 \\
&= \frac{1}{p^3} \sum_x \alpha^2(x) - \frac{1}{p^4} |I|^2 |J|^2.
\end{aligned}$$

If $p \equiv 1 \pmod{4}$, then $|I| = \frac{p+3}{4}$, $|J| = \frac{p-1}{4}$, and the function α is given by

$$\alpha(x) = \begin{cases} x & \text{for } 1 \leq x \leq \frac{p-1}{4}, \\ \frac{p-1}{2} - x + 1 & \text{for } \frac{p-1}{4} < x \leq \frac{p-1}{2}, \\ 0 & \text{otherwise,} \end{cases}$$

since the solutions to $u + v = x$ with $(u, v) \in I \times J$ are $(0, x)$, $(1, x - 1)$, $(2, x - 2), \dots, (x - 1, 1)$ in the first case and $(u, v) = (x - \frac{p-1}{4}, \frac{p-1}{4}), (x - \frac{p-1}{4} + 1, \frac{p-1}{4} - 1), \dots, (\frac{p-1}{4}, x - \frac{p-1}{4})$ in the second case. Thus

$$\sum_x \alpha^2(x) = 2 [1^2 + 2^2 + \dots + ((p-1)/4)^2] = \frac{1}{96}(p^2 - 1)(p + 3).$$

If $p \equiv 3 \pmod{4}$, then $|I| = |J| = \frac{p+1}{4}$ and

$$\alpha(x) = \begin{cases} x & \text{for } 1 \leq x \leq \frac{p+1}{4}, \\ \frac{p-1}{2} - x + 1 & \text{for } \frac{p+1}{4} < x \leq \frac{p-1}{2}, \\ 0 & \text{otherwise,} \end{cases}$$

and so

$$\begin{aligned} \sum_x \alpha^2(x) &= 2 [1^2 + 2^2 + \dots + ((p-3)/4)^2] + ((p+1)/4)^2 \\ &= \frac{1}{96}(p-3)(p^2 - 1) + \frac{(p+1)^2}{16}. \end{aligned}$$

Hence

$$(18) \quad \sum_{j \neq 0} |a_I(j)a_J(j)|^2 = \begin{cases} \frac{5}{3 \cdot 2^8} \left(1 + \frac{12}{5p} - \frac{2}{5p^2} + \frac{12}{5p^3} - \frac{27}{5p^4}\right) & \text{if } p \equiv 1 \pmod{4}, \\ \frac{5}{3 \cdot 2^8} \left(1 + \frac{12}{5p} + \frac{14}{p^2} + \frac{12}{p^3} - \frac{3}{5p^4}\right) & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Let γ_p denote the value on the right-hand side of (18), and note that for $p > 10^6$, $\gamma_p \leq .0065105$. Then

$$(19) \quad E_6 \leq \frac{\gamma_p}{p-1} |I|^2 (p - |I|)^2.$$

By (15), (16), (17), and (19) we have

$$(20) \quad |E_3| \leq \gamma_p^{1/4} \frac{M^{1/4}}{p^{1/2}(p-1)^{1/4}} |I|^{3/2} (p - |I|)^{3/2},$$

and then by (11) and (12),

$$(21) \quad |Error| \leq \frac{|I|^{5/2}|J|^{1/2}}{p} + \frac{|I|^2|J|}{p} + \gamma_p^{1/4} \frac{M^{1/4}}{p^{1/2}(p-1)^{1/4}} |I|^{3/2} (p - |I|)^{3/2}.$$

If $p \equiv 3 \pmod{4}$, so that $|I| = |J| = \frac{p+1}{4}$, then

$$|Error| \leq \frac{1}{32} \frac{(p+1)^3}{p} + \frac{\gamma_p^{1/4}}{64} \frac{M^{1/4}}{p^{1/2}(p-1)^{1/4}} (p+1)^{3/2} (3p-1)^{3/2}$$

while

$$Main = \frac{1}{256} \frac{(p+1)^4(p-1)}{p^2}.$$

If $p > 10^6$ and $M < .000823p^3$, one can check with a calculator that $|Error| < Main$. A similar calculation can be made for the case $p \equiv 1 \pmod{4}$.

4. Proof of Theorem 2. The proof is almost identical to the proof of Theorem 1, the only change being in the estimate of E_3 . We have by (13)

$$\begin{aligned} |E_3| &\leq \sum_{u \neq 0} \sum_{v \neq 0} |a(u, v)| \left| \sum_{x \neq 0} e_p(ux + vA2^{d-1}x^d) \right| \leq \Phi_d \sum_{u \neq 0} \sum_{v \neq 0} |a(u, v)| \\ &\leq p^2 \Phi_d \left(\sum_u |a_I(u)|^2 - |a_I(0)|^2 \right) \left(\sum_v |a_I(v)a_J(v)| - |a_I(0)a_J(0)| \right) \\ &\leq p^2 \Phi_d \left(\frac{|I|}{p} - \frac{|I|^2}{p^2} \right) \left(\frac{|I|^{1/2}|J|^{1/2}}{p} - \frac{|I||J|}{p^2} \right), \end{aligned}$$

and so

$$(22) \quad |Error| \leq |E_1| + |E_2| + |E_3| \\ \leq \frac{|I|^{5/2}|J|^{1/2}}{p} + \frac{|I|^2|J|}{p} + p^{-2}\Phi_d |I|^{3/2}|J|^{1/2}(p - |I|)(p - |I|^{1/2}|J|^{1/2}).$$

The main term is again $Main = \frac{p-1}{p^2}|I|^3|J|$. With a calculator one can check that $|Error| < Main$ provided that $\Phi_d \leq \frac{p-7}{9}$ and $p > 2 \cdot 10^6$.

5. Proof of Theorem 3. For any integers k, l let $M(k, l)$ denote the number of solutions in $(\mathbb{Z}_p^*)^4$ of the system

$$\begin{aligned} x_1^k + x_2^k &= x_3^k + x_4^k, \\ x_1^l + x_2^l &= x_3^l + x_4^l. \end{aligned}$$

We have the elementary bounds [8, Lemma 3.2]

$$(23) \quad M(k, l) \leq \begin{cases} kl(p-1)^2 & \text{for } 1 \leq l < k < p-1, \\ 3k|l|(p-1)^2 & \text{for } l < 0, |l| \leq k, k + |l| < p-1. \end{cases}$$

Also, since $x^{p-1} \equiv 1 \pmod{p}$ for $x \in \mathbb{Z}_p^*$, we have $M(k, l) = M(k', l')$ for $k \equiv k'$ and $l \equiv l' \pmod{p-1}$.

LEMMA 1. *For any integers k, l, m we have $M(k, l) \leq M(mk, ml)$.*

Proof. For any nonzero $A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4 \in \mathbb{Z}_p$ let $M(k, l, A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4)$ be the number of solutions in $(\mathbb{Z}_p^*)^4$ of the system

$$\begin{aligned} A_1x_1^k + A_2x_2^k &= A_3x_3^k + A_4x_4^k, \\ B_1x_1^l + B_2x_2^l &= B_3x_3^l + B_4x_4^l. \end{aligned}$$

We first note that for any choice of A_i, B_j ,

$$M(k, l, A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4) \leq M(k, l).$$

Indeed, $p^2 M(k, l, A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4)$ is just

$$\begin{aligned}
& \sum_{x_1 \neq 0} \cdots \sum_{x_4 \neq 0} \sum_{\alpha, \beta} e_p(\alpha(A_1 x_1^k + A_2 x_2^k - A_3 x_3^k - A_4 x_4^k) \\
& \quad + \beta(B_1 x_1^l + B_2 x_2^l - B_3 x_3^l - B_4 x_4^l)) \\
& \leq \sum_{\alpha, \beta} \prod_{i=1}^2 \left| \sum_{x_i \neq 0} e_p(\alpha A_i x_i^k + \beta B_i x_i^l) \right| \prod_{i=3}^4 \left| \sum_{x_i \neq 0} e_p(-\alpha A_i x_i^k - \beta B_i x_i^l) \right| \\
& \leq \prod_{i=1}^2 \left(\sum_{\alpha, \beta} \left| \sum_{x_i \neq 0} e_p(\alpha A_i x_i^k + \beta B_i x_i^l) \right|^4 \right)^{1/4} \\
& \quad \cdot \prod_{i=3}^4 \left(\sum_{\alpha, \beta} \left| \sum_{x_i \neq 0} e_p(-\alpha A_i x_i^k - \beta B_i x_i^l) \right|^4 \right)^{1/4} \\
& = p^2 M(k, l).
\end{aligned}$$

Next, set $m_1 = (m, p-1)$ and let $\{w_1, \dots, w_{m_1}\}$ be a set of representatives for $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^m$. Then decomposing \mathbb{Z}_p^* as a union over the different cosets of \mathbb{Z}_p^{*m} , we see that

$$\begin{aligned}
M(k, l) &= \frac{1}{m_1^4} \sum_{i_1=1}^{m_1} \sum_{i_2=1}^{m_1} \sum_{i_3=1}^{m_1} \sum_{i_4=1}^{m_1} M(mk, ml, w_{i_1}^k, w_{i_2}^k, w_{i_3}^k, w_{i_4}^k, w_{i_1}^l, w_{i_2}^l, w_{i_3}^l, w_{i_4}^l) \\
&\leq \frac{1}{m_1^4} \sum_{i_1=1}^{m_1} \sum_{i_2=1}^{m_1} \sum_{i_3=1}^{m_1} \sum_{i_4=1}^{m_1} M(mk, ml) = M(mk, ml). \quad \square
\end{aligned}$$

LEMMA 2. *If $k \not\equiv l \pmod{p-1}$ and either k or l is coprime to $p-1$, then*

$$M(k, l) \leq p^3.$$

Proof. Suppose without loss of generality that $(l, p-1) = 1$. Let m satisfy $ml \equiv 1 \pmod{p-1}$ and put $d \equiv km \pmod{p-1}$ with $1 < d < p$. Then $M(k, l) = M(km, lm) = M(d, 1) \leq dp^2 \leq p^3$. \square

Let

$$(24) \quad \lambda_1 = (l, k), \quad \lambda = (l, k, p-1), \quad l_+ = l, \quad l_- = 2l,$$

$$(25) \quad \delta_+ = \frac{(k-l)}{\lambda_1}, \quad \delta_- = \frac{(k+l)}{\lambda_1},$$

and

$$M_+(k, l) = M(k, l) \quad \text{for } 1 \leq l < k < p-1,$$

$$M_-(k, l) = M(k, -l) \quad \text{for } 1 \leq l < k, \quad l+k < p-1.$$

The next lemma is essentially Corollary 3.1 of [7] with the implied constants made explicit.

LEMMA 3. For $1 \leq l \leq k < p - 1$ then for $k < \frac{1}{32}(p-1)^{\frac{2}{3}}\lambda_1^{\frac{1}{6}}l^{\frac{1}{6}}$,

$$M_{\pm}(k, l) \leq \lambda^2(p-1)^2 + 2k^2l_{\pm}(p-1) + (p-1)^2\mu,$$

where

$$\mu = \max\{768 \cdot 5^{2/3}kl_{\pm}\delta_{\pm}^{-\frac{1}{3}}\lambda/\lambda_1, 557\delta_{\pm}\lambda\}.$$

Proof. We follow the proof of Corollary 3.1 of [7]. For $\mathbf{u} = (u_1, u_2) \in \mathbb{Z}_p^{*2}$ define

$$C_{\pm}(\mathbf{u}) = \#\{x \in \mathbb{Z}_p^* : x^k - 1 = u_1y^k, x^{\pm l} - 1 = u_2y^{\pm l} \text{ for some } y \in \mathbb{Z}_p^*\}.$$

From (2.1) of [7] we have

$$M_{\pm}(k, l) \leq \lambda^2(p-1)^2 + 2k^2l_{\pm}(p-1) + \lambda(p-1) \sum_{i=1}^N C_{\pm}^2(\mathbf{u}_i),$$

where $\mathbf{u}_1, \dots, \mathbf{u}_N$ represent the N distinct nonempty sets of x being counted as \mathbf{u} varies, ordered so that $C_{\pm}(\mathbf{u}_1) \geq C_{\pm}(\mathbf{u}_2) \geq \dots \geq C_{\pm}(\mathbf{u}_N) > 0$. Thus, it suffices to show that $\lambda \sum_{i=1}^N C_{\pm}^2(\mathbf{u}_i) \leq (p-1)\mu$. Let

$$T = \begin{cases} \left\lfloor 2^{-\frac{9}{2}}(p-1) \left(\frac{\delta_{\pm}^2}{kl_{\pm}/\lambda_1} \right)^{-\frac{3}{2}} \right\rfloor & \text{if } kl_{\pm}/\lambda_1 < \frac{1}{2}\delta_{\pm}^2, \\ \left\lfloor 2^{-7}(p-1) \left(\frac{\delta_{\pm}^2}{kl_{\pm}/\lambda_1} \right) \right\rfloor & \text{if } kl_{\pm}/\lambda_1 \geq \frac{1}{2}\delta_{\pm}^2. \end{cases}$$

When $k < \frac{1}{32}(p-1)^{\frac{2}{3}}\lambda_1^{\frac{1}{6}}l^{\frac{1}{6}}$ it was shown in Lemma 3.1 of [7] that

$$(26) \quad C_{\pm}(\mathbf{u}_t) \leq 2^{\frac{26}{5}}(p-1)^{\frac{2}{5}}(kl_{\pm}/\lambda_1)^{\frac{3}{5}}t^{-\frac{2}{5}}\delta_{\pm}^{-\frac{1}{5}}, \quad 1 \leq t \leq T;$$

in particular $C_{\pm}(\mathbf{u}_T) \leq 2^{\frac{37}{5}}\delta_{\pm}$ when $kl_{\pm}/\lambda_1 < \frac{1}{2}\delta_{\pm}^2$.

If $T = 0$, then, as shown at the end of the proof of [7, Lemma 3.1], we must have $(kl_{\pm}/\lambda_1) \geq \frac{1}{2}\delta_{\pm}^2$, and thus from the definition of T , $\delta_{\pm} < 2^{\frac{7}{2}}(kl_{\pm}/\lambda_1)^{\frac{1}{2}}/(p-1)^{\frac{1}{2}}$. We can then use the trivial bounds

$$C_{\pm}(\mathbf{u}_i) \leq \min\{p-1, kl_{\pm}/\lambda_1\} \leq (kl_{\pm}/\lambda_1)^{\frac{5}{6}}(p-1)^{\frac{1}{6}},$$

and $\sum_{i=1}^N C_{\pm}(\mathbf{u}_i) \leq p-1$, to get

$$\begin{aligned} \lambda \sum_{i=1}^N C_{\pm}^2(\mathbf{u}_i) &\leq \lambda(kl_{\pm}/\lambda_1)^{\frac{5}{6}}(p-1)^{\frac{1}{6}} \sum_{i=1}^N C_{\pm}(\mathbf{u}_i) \\ &\leq \lambda(kl_{\pm}/\lambda_1)^{\frac{5}{6}}(p-1)^{\frac{7}{6}} \leq \frac{\mu}{1000}(p-1). \end{aligned}$$

Suppose now that $T > 0$. Set

$$L = \left\lfloor 5^{-5/3}2^{-7}(p-1) \frac{\delta_{\pm}^{\frac{1}{3}}}{(kl_{\pm}/\lambda_1)} \right\rfloor.$$

When $L < T$ we have by (26)

$$\begin{aligned} \sum_{i \leq L} C_{\pm}^2(\mathbf{u}_i) &\leq 2^{52/5} (p-1)^{4/5} (kl_{\pm}/\lambda_1)^{6/5} \delta_{\pm}^{-2/5} \sum_{i \leq L} i^{-4/5} \\ &\leq 2^{52/5} (p-1)^{4/5} (kl_{\pm}/\lambda_1)^{6/5} \delta_{\pm}^{-2/5} 5L^{1/5} \\ &\leq 2^9 5^{2/3} (kl_{\pm}/\lambda_1) \delta_{\pm}^{-1/3} (p-1), \end{aligned}$$

and

$$\begin{aligned} \sum_{L < i \leq N} C_{\pm}^2(\mathbf{u}_i) &\leq 2^{26/5} (p-1)^{2/5} (kl_{\pm}/\lambda_1)^{3/5} \delta_{\pm}^{-1/5} (L+1)^{-2/5} \sum_{L < i \leq N} C_{\pm}(\mathbf{u}_i) \\ &\leq 2^{26/5} (p-1)^{2/5} (kl_{\pm}/\lambda_1)^{3/5} \delta_{\pm}^{-1/5} (L+1)^{-2/5} (p-1) \\ &\leq 2^8 5^{2/3} (kl_{\pm}/\lambda_1) \delta_{\pm}^{-1/3} (p-1), \end{aligned}$$

giving $\lambda \sum_{i=1}^N C_{\pm}^2(\mathbf{u}_i) \leq 768 \cdot 5^{2/3} (\lambda/\lambda_1) kl_{\pm} \delta_{\pm}^{-1/3} (p-1)$. Plainly $5^{-5/3} 2^{-7} (p-1) \frac{\delta_{\pm}^{1/3}}{(kl_{\pm}/\lambda_1)}$ is less than $\frac{1}{2} 2^{-7} (p-1) \frac{\delta_{\pm}^2}{(kl_{\pm}/\lambda_1)}$ and less than $\frac{1}{2} 2^{-9/2} (p-1) \frac{(kl_{\pm}/\lambda_1)^{3/2}}{\delta_{\pm}^3}$ when $(kl_{\pm}/\lambda_1) \geq 5^{-2/3} 2^{-3/5} \delta_{\pm}^{4/3}$. Thus $L < T$ unless $(kl_{\pm}/\lambda_1) < 5^{-2/3} 2^{-3/5} \delta_{\pm}^{4/3} < \frac{1}{2} \delta_{\pm}^2$ in which case

$$\begin{aligned} \sum_{i \leq T} C_{\pm}^2(\mathbf{u}_i) &\leq 2^{52/5} (p-1)^{4/5} (kl_{\pm}/\lambda_1)^{6/5} \delta_{\pm}^{-2/5} 5T^{1/5} \\ &\leq 2^{19/2} \cdot 5 (p-1) (kl_{\pm}/\lambda_1)^{3/2} \delta_{\pm}^{-1} \\ &\leq 2^{43/5} \delta_{\pm} (p-1), \end{aligned}$$

and

$$\sum_{T < i \leq N} C_{\pm}^2(\mathbf{u}_i) \leq 2^{37/5} \delta_{\pm} \sum_{T < i \leq N} C_{\pm}(\mathbf{u}_i) \leq 2^{37/5} \delta_{\pm} (p-1),$$

giving $\lambda \sum_{i \leq N} C_{\pm}^2(\mathbf{u}_i) \leq (2^{43/5} + 2^{37/5}) \delta_{\pm} \lambda (p-1) \leq 557 \delta_{\pm} \lambda (p-1)$. \square

Theorem 3 is just a special case of the following theorem with $k = d$, $l = 1$.

THEOREM 6. *Let $1 \leq l < k < p-1$ be positive integers with $(kl, p-1) = 1$, and for $M_-(k, l)$, $k+l < p-1$. Let $d^* = (k \mp l, p-1)$, $-$ for $M_+(k, l)$, $+$ for $M_-(k, l)$. If $d^* < .18(p-1)^{16/23}$, then*

$$M_{\pm}(k, l) \leq 13658 p^{66/23}.$$

Proof. Let k, l be integers with $l < k < p-1$ and $(kl, p-1) = 1$. By Lemma 2 the bound on $M_{\pm}(k, l)$ is trivial if $p^3 \leq 13658 p^{66/23}$, and so we may assume that $p > 10^{31}$. The idea is to make a transformation of the type $x \rightarrow x^m$ so that Lemma 3 can be effectively applied. Choose m so that

$$(27) \quad mk \equiv \alpha \pmod{p-1}, \quad \pm ml \equiv \beta \pmod{p-1}$$

(plus sign for S_+ and minus for S_-), with

$$(28) \quad 0 \leq \alpha \leq \frac{1}{c} (p-1)^{\frac{16}{23}}, \quad |\beta| \leq c (p-1)^{\frac{7}{23}}, \quad c = 2^{60/23} 5^{-2/23} = 5.3029 \dots,$$

$(\alpha, \beta) \neq (0, 0)$. Such a pair (α, β) exists since the set of all (α, β) satisfying (27) is a lattice of volume $p - 1$ (or one can apply Dirichlet's box principle). Now, $(p - 1) \nmid m$ (since $(\alpha, \beta) \neq (0, 0)$) and so, since $(lk, p - 1) = 1$ we have $\alpha \neq 0$ and $\beta \neq 0$. If $\alpha = \beta$, then $p - 1 \mid m(k \mp l)$, $\frac{p-1}{d^*} \mid m$, and $|\beta| \geq (p - 1)/d^*$, contradicting our assumption on the size of d^* . Thus $\alpha \neq \beta$. Set

$$\beta' = \begin{cases} |\beta| & \text{if } \beta > 0, \\ 2|\beta| & \text{if } \beta < 0. \end{cases}$$

Case 1. Suppose that $\alpha \leq 100|\beta|$. Then by Lemma 1 and (23) we have

$$M_{\pm}(k, l) \leq M(\alpha, \beta) \leq 3\alpha|\beta|p^2 \leq 300|\beta|^2p^2 \leq 8437p^{60/23}.$$

Case 2. Suppose that $\alpha > 100|\beta|$ and $\alpha \geq 2^{-5}(p - 1)^{2/3}\lambda_1^{1/6}(\beta')^{1/6}$. Then $(\beta')^{1/6} \leq (32/c)p^{2/69}$, $\beta' \leq (32/c)^6p^{4/23}$. By Lemma 1 and (23) we get

$$M_{\pm}(k, l) \leq M(\alpha, \beta) \leq \frac{3}{2}\alpha\beta'p^2 \leq \frac{3}{2c}p^{16/23} \left(\frac{32}{c}\right)^6 p^{4/23}p^2 \leq 13658p^{66/23}.$$

Case 3. Suppose that $\alpha > 100|\beta|$ and that $\alpha < 2^{-5}(p - 1)^{2/3}\lambda_1^{1/6}(\beta')^{1/6}$, so that Lemma 3 applies. In particular, since $\delta_{\pm} = |\alpha - \beta|/\lambda_1$ we have

$$.99\frac{\alpha}{\lambda_1} \leq \delta_+ \leq \frac{\alpha}{\lambda_1}, \quad \frac{\alpha}{\lambda_1} \leq \delta_- \leq 1.01\frac{\alpha}{\lambda_1},$$

and $\beta'\delta_{\pm}^{-1/3} \leq 2|\beta|\alpha^{-1/3}\lambda_1^{1/3}$. The value μ in Lemma 3 is bounded by

$$\begin{aligned} & \max\{768 \cdot 5^{2/3}(\lambda/\lambda_1)\alpha 2|\beta|\alpha^{-1/3}\lambda_1^{1/3}, 557(1.01\alpha)\} \\ & \leq \max\{1536 \cdot 5^{2/3}\alpha^{2/3}|\beta|^{4/3}, 563\alpha\} \\ & \leq \max\{1536 \cdot 5^{2/3}c^{2/3}(p - 1)^{20/23}, 563c^{-1}(p - 1)^{16/23}\} \\ & \leq \max\{13657.9(p - 1)^{20/23}, 107(p - 1)^{16/23}\} = 13657.9(p - 1)^{20/23}. \end{aligned}$$

Thus we get

$$\begin{aligned} M_{\pm}(k, l) & \leq M(\alpha, \beta) \leq (cp^{7/23})^2p^2 + 4(1/c)p^{39/23}p + 13657.9p^2p^{20/23} \\ & \leq 29p^{60/23} + .76p^{62/23} + 13657.9p^{66/23} \leq 13658p^{66/23}. \quad \square \end{aligned}$$

6. Proof of Theorem 4. Let A, d be integers such that $0 < |A| < p/2$, $|d| < p/2$, $(A, d) \neq (1, 1)$. Put $d_1 = (p - 1, d - 1)$ and $k = (p - 1)/d_1$. Let B be chosen so that $p \nmid B$ and $AB^{d-1} \not\equiv 1 \pmod{p}$; such a B exists since either $d = 1$, $A \neq 1$, or $d \neq 1$ and B^{d-1} takes on at least two distinct nonzero values \pmod{p} . Put $C \equiv AB^{d-1} \pmod{p}$ with $-p/2 < C < p/2$, $C \neq 0, 1$. Suppose that we can find an element of the form $Bz^k \in \mathbb{E}$ such that $BCz^k \in \mathbb{O}$. Then $A(Bz^k)^d \equiv BCz^k \in \mathbb{O}$; that is, $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty. Let $x \equiv Bz^k \pmod{p}$, $y \equiv BCz^k \pmod{p}$. 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 k th power,

and $y \in \mathbb{O}$. Then letting $\sum_{\psi^k=\psi_0}$ denote a sum over all multiplicative characters $\psi \pmod{p}$ satisfying $\psi^k = \psi_0$, where ψ_0 is the principal character, we have

$$\begin{aligned} N &= \frac{1}{k} \sum_x \left(\sum_{\psi^k=\psi_0} \psi(B^{-1}x) \right) \chi_{\mathbb{E}}(x) \chi_{\mathbb{O}}(Cx) \\ &= \frac{1}{k} \sum_x \chi_{\mathbb{E}}(x) \chi_{\mathbb{O}}(Cx) + \frac{1}{k} \sum_{\psi \neq \psi_0} \sum_x \psi(B^{-1}x) \chi_{\mathbb{E}}(x) \chi_{\mathbb{O}}(Cx) \end{aligned}$$

$$(29) \quad = \text{Main} + \text{Error}.$$

Main term. Suppose first that $1 < C < p/2$. The main term is just the number of values of $n \in \{1, 2, \dots, \frac{p-1}{2}\}$ such that $(2j-1)p < 2nC < 2jp$ for some j , that is,

$$\frac{(2j-1)p}{2C} < n < \frac{jp}{C}$$

with $1 \leq j \leq [C/2]$. Thus, using $[x] - [x-y] \geq [y]$, we have

$$(30) \quad \text{Main} = \frac{1}{k} \sum_{j=1}^{[C/2]} \left[\frac{jp}{C} \right] - \left[\frac{(2j-1)p}{2C} \right] \geq \frac{1}{k} \sum_{j=1}^{[C/2]} \left[\frac{p}{2C} \right] = \frac{1}{k} \left[\frac{C}{2} \right] \left[\frac{p}{2C} \right].$$

We consider first a few small values of C . Let S denote the sum appearing in the main term, $S = k(\text{Main})$. If $C = 2$, then $S = [p/2] - [p/4] \geq \frac{p-1}{4}$. If $C = 3$, then $S = [p/3] - [p/6] \geq \frac{p-1}{6}$. For $C = 4$ we have $S = ([p/4] - [p/8]) + ([p/2] - [3p/8]) \geq \frac{p-3}{4}$. For $\frac{p}{4} < C < \frac{p}{2}$ we have

$$[C/2] [p/2C] = [C/2] \geq \frac{C-1}{2} \geq \frac{p-3}{8}.$$

For $5 \leq C < p/4$ we have

$$\begin{aligned} [C/2] [p/2C] &\geq \frac{C-1}{2} \left(\frac{p}{2C} - \frac{2C-1}{2C} \right) \\ &= \frac{p}{4} + \frac{3}{4} - \left(\frac{p+1}{4C} + \frac{C}{2} \right). \end{aligned}$$

The quantity being subtracted takes on its maximum value when $C = \frac{p-1}{4}$, and so we obtain

$$\left[\frac{C}{2} \right] \left[\frac{p}{2C} \right] \geq \frac{p-1}{8} - \frac{2}{p-1} > \frac{p-3}{8}.$$

Thus in all cases $S \geq (p-3)/8$.

Next assume that $-p/2 < C \leq -1$. Then $2nC \in \mathbb{O}$ if and only if $-2nC$ is even, and so we replace C with $-C$ and count the number of values n with $2jp < 2nC < (2j+1)p$ for some j with $0 \leq j \leq [(C-1)/2]$. Then,

$$\sum_{j=0}^{[(C-1)/2]} \left[\frac{(2j+1)p}{2C} \right] - \left[\frac{jp}{C} \right] \geq \left[\frac{C+1}{2} \right] \left[\frac{p}{2C} \right],$$

and the lower bound follows as before. Thus we have uniformly

$$(31) \quad \text{Main} \geq \frac{p-3}{8k}.$$

Error term. Let ψ be a nonprincipal character (mod p). Then

$$\begin{aligned} \sum_x \psi(B^{-1}x) \chi_{\mathbb{E}}(x) \chi_{\mathbb{O}}(Cx) &= \sum_x \left(\sum_y a_{\mathbb{E}}(y) e_p(yx) \right) \left(\sum_z a_{\mathbb{O}}(z) e_p(zCx) \right) \psi(B^{-1}x) \\ &= \sum_y \sum_z a_{\mathbb{E}}(y) a_{\mathbb{O}}(z) G(y+Cz, B^{-1}), \end{aligned}$$

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 we obtain from (7)

$$\left| \sum_x \psi(B^{-1}x) \chi_{\mathbb{E}}(x) \chi_{\mathbb{O}}(Cx) \right| \leq \sqrt{p} \sum_y |a_{\mathbb{E}}(y)| \sum_z |a_{\mathbb{O}}(z)| \leq \left(\frac{4}{\pi^2} \log p + 1 \right)^2 \sqrt{p},$$

and

$$|\text{Error}| \leq (1 - 1/k) \left(\frac{4}{\pi^2} \log p + 1 \right)^2 \sqrt{p}.$$

We conclude from (29) and (31) that N is positive provided that $\frac{p-3}{8} \geq (k-1) \left(\frac{4}{\pi^2} \log p + 1 \right)^2 \sqrt{p}$. If $d_1 > 1$, then $k \leq \frac{p-1}{2}$ and $\frac{p-3}{k-1} \geq \frac{p-1}{k} = d_1$. Thus N is positive provided that $d_1 > 8 \left(\frac{4}{\pi^2} \log p + 1 \right)^2 \sqrt{p}$.

To prove part (b) of Theorem 4 suppose that $p > 2.1 \cdot 10^7$ and $d_1 > 10\sqrt{p}$. In [7, Proposition 1.1] we proved

$$\left| \sum_{x \neq 0} e_p(ax^d + bx) \right| \leq d_1 + \frac{p^{3/2}}{d_1}$$

for any nonzero a, b . Thus Theorem 2 can be applied if $d_1 + \frac{p^{3/2}}{d_1} < \frac{p-7}{9}$. Otherwise, either

$$d_1 < \frac{1}{2} \left(\frac{p-7}{9} - \sqrt{\frac{(p-7)^2}{81} - 4p^{3/2}} \right) \quad \text{or} \quad d_1 > \frac{1}{2} \left(\frac{p-7}{9} + \sqrt{\frac{(p-7)^2}{81} - 4p^{3/2}} \right).$$

The first inequality fails for $d_1 > 10\sqrt{p}$ and $p > 811000$. Thus the second inequality holds true. But for $p > 2.007 \cdot 10^7$, it implies that $d_1 > 8 \left(\frac{4}{\pi^2} \log(p) + 1 \right)^2 \sqrt{p}$. Thus part (a) of Theorem 4 applies.

Remark. When $d = 1$ there is no error term in the above calculation and we obtain that $|\mathbb{A}\mathbb{E} \cap \mathbb{O}| > \frac{p-3}{8}$. Thus $\mathbb{A}\mathbb{E} \cap \mathbb{O}$ is nonempty for any odd prime p and $A \neq 1$.

Acknowledgment. The authors express their thanks to the referee for his/her helpful suggestions in improving the organization of this paper and for pointing out valuable connections between this work and related problems.

REFERENCES

- [1] E. ALKAN, F. STAN, AND A. ZAHARESCU, *Lehmer k -tuples* (English summary), Proc. Amer. Math. Soc., 134 (2006), pp. 2807–2815.
- [2] J. BOURGAIN, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc., 18 (2005), pp. 477–499.
- [3] R. CANETTI, J. FRIEDLANDER, AND I. SHPARLINSKI, *On certain exponential sums and the distribution of Diffie-Helman triples*, J. London Math. Soc. (2), 59 (1999), pp. 799–812.
- [4] C. COBELI AND A. ZAHARESCU, *Generalization of a problem of Lehmer*, Manuscripta Math., 104 (2001), pp. 301–307.
- [5] T. COCHRANE, *On a trigonometric inequality of Vinogradov*, J. Number Theory, 27 (1987), pp. 9–16.
- [6] T. COCHRANE AND J. C. PERAL, *An asymptotic formula for a trigonometric sum of Vinogradov*, J. Number Theory, 91 (2001), pp. 1–19.
- [7] T. COCHRANE AND C. PINNER, *Stepanov's method applied to binomial exponential sums*, Q. J. Math., 54 (2003), pp. 243–255.
- [8] T. COCHRANE AND C. PINNER, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc., 133 (2005), pp. 313–320.
- [9] M. GORESKEY AND A. KLAPPER, *Arithmetic crosscorrelations of feedback with carry shift register sequences*, IEEE Trans. Inform. Theory, 43 (1997), pp. 1342–1346.
- [10] M. GORESKEY, A. KLAPPER, AND R. MURTY, *On the Distinctness of Decimations of ℓ -Sequences*, (Proceedings of SETA'01), T. Helleseth, ed., Discrete Math. Theor. Comput. Sci. (Lond.), Springer, London, 2002.
- [11] M. GORESKEY, A. KLAPPER, R. MURTY, AND I. SHPARLINSKI, *On decimations of ℓ -sequences*, SIAM J. Discrete Math., 18 (2004), pp. 130–140.
- [12] T. GOWERS, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal., 8 (1998), pp. 529–551.
- [13] S. V. KONYAGIN AND I. E. SHPARLINSKI, *Character Sums with Exponential Functions and Their Applications*, Cambridge Tracts in Math. 136, Cambridge University Press, Cambridge, UK, 1999.
- [14] H. LIU AND W. ZHANG, *On a problem of D. H. Lehmer*, Acta Math. Sin. (Engl. Ser.), 22 (2006), pp. 61–68.
- [15] H. LIU AND W. ZHANG, *Hybrid mean value results for a generalization on a problem of D. H. Lehmer and hyper-Kloosterman sums*, Osaka J. Math., 44 (2007), pp. 615–637.
- [16] H. LIU AND W. ZHANG, *Hybrid mean value for a generalization of a problem of D. H. Lehmer*, Acta Arith., 130 (2007), pp. 1–17.
- [17] S. LOUBOUTIN, J. RIVAT, AND A. SÁRKÖZY, *On a problem of D. H. Lehmer* (English summary), Proc. Amer. Math. Soc., 135 (2007), pp. 969–975.
- [18] I. SHPARLINSKI, *On a Generalisation of a Lehmer Problem*, Math. Z., to appear.
- [19] H. XU AND W. F. QI, *Further results on the distinctness of decimations of l -sequences*, IEEE Trans. Inform. Theory, 52 (2006), pp. 3831–3836.
- [20] Z. XU AND W. ZHANG, *A problem of D. H. Lehmer and its mean value*, Math. Nachr., 281 (2008), pp. 596–606.
- [21] Y. YUAN AND W. ZHANG, *On the generalization of a problem of D. H. Lehmer*, Kyushu J. Math., 56 (2002), pp. 235–241.
- [22] W. ZHANG, *On a problem of D. H. Lehmer and its generalization*, Compositio Math., 86 (1993), pp. 307–316.
- [23] W. ZHANG, *A problem of D. H. Lehmer and a generalization of it*, J. Northwest Univ., 23 (1993), pp. 103–108 (in Chinese).
- [24] W. ZHANG, *A problem of D. H. Lehmer and its generalization. II*, Compositio Math., 91 (1994), pp. 47–56.
- [25] W. ZHANG, *On a problem of D. H. Lehmer and Kloosterman sums*, Monatsh. Math., 139 (2003), pp. 247–257.