DECIMATIONS OF L-SEQUENCES AND PERMUTATIONS OF EVEN RESIDUES MOD 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 $x \to Ax^d$, with $(d, p-1) = 1$, $p \nmid A$, is a permutation of the even residues $\pmod p$ 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 $0 < d < .000823p$ or $0 > d > -.000274p$.

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 $\pmod p$,

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

Let $A\mathbb{E}^d = \{Ax^d : x \in \mathbb{E}\} \subset \mathbb{Z}_p$. Since $(d, p-1) = 1$ the mapping $x \to Ax^d$ 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 conjecture [6]) 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 $\mathbf{x} = \mathbf{a}^{\mathbf{d}}$ 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.

Date: October 9, 2008.

Original GK-Conjecture. (Goresky and Klapper [6]) 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 $\mathbf{a}^{\mathbf{d}}$ 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 $\pmod p$ 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 four. Klapper, using a computer, has verified the generalized conjecture for all primes less than two million. Goresky, Klapper and Murty [7] proved the conjecture for $d = -1$ and for the case where $p \equiv 1 \pmod 4$ and $d = (p+1)/2$. Goresky, Klapper, Murty and Shparlinski [8, Theorem 2.2] sharpening the work of [7], 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

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

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

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

It is elementary (see [5, 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 $0 < d < .000823p$ or $0 > d > -.000274p$ then the GK-conjecture holds true.*

Unfortunately, the upper bound on M in Theorem 1 fails if the quantity

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

is large, as shown in [4]. For small d_1 we are able to establish the upper bound on M for p sufficiently large.

Theorem 2. *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 four, 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 Goresky-Klapper conjecture for d_1 sufficiently large.

Theorem 3. *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, 2 and 3 that the Goresky-Klapper conjecture is true for p sufficiently large.

Theorem 4. *For any prime $p > 2.26 \cdot 10^{55}$ 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 $\mathbb{Z}_p$, $e_p(x) = e^{2\pi i x/p}$, and set

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

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

Theorem 5. *If $\Phi_d \le \frac{p-7}{9}$ then the GK-conjecture holds true.*

There are several available estimates for Φ_d, such as the Weil bound ($\Phi_d \le (d-1)\sqrt{p}$) or the Mordell bound ($\Phi_d \le p^{1/4} M^{1/4}$) but they lead to weaker results than those above. The first author recently established a new type of bound for a general exponential sum [1, 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

$$\Phi_d < p^{1-\delta}. \tag{4}$$

The proof of (4) uses additive combinatorics and harmonic analysis, and appeals to the Balog-Szemeredi-Gowers theorem; see [9]. It may not be easy to make the result numeric.

Finally, we note that Hong Xu and Wen-Feng Qi [11] have proven the Goresky-Klapper conjecture for the case of odd prime powers p^e with $e \ge 2$, $p^e \ne 9$.

2. Proof of Theorem 1

We use the method of finite Fourier series. A summary of basic facts we call upon is provided in section seven. 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

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

Put

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

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

$$a(u, v) = p^2 a_I(u)^2 a_I(v) a_J(v). \tag{5}$$

In particular,

$$a(0, 0) = \frac{|I|^3 |J|}{p^2}. \tag{6}$$

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

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

say. Now, by (6),

$$Main = a(0,0)(p-1) = \frac{p-1}{p^2}|I|^3|J|. \tag{7}$$

To estimate the error term we break it up as

$$Error = E_1 + E_2 + E_3,$$

where E_1 is he 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

$$|E_1| \le \sum_v |a(0,v)| = p^2\sum_v |a_I(0)|^2|a_I(v)a_J(v)| \le p^2\frac{|I|^2}{p^2}\frac{|I|^{1/2}|J|^{1/2}}{p} = \frac{|I|^{5/2}|J|^{1/2}}{p}, \tag{8}$$

by the Cauchy-Schwarz inequality and Parseval's identity, and

$$|E_2| \le \sum_u |a(u,0)| = p^2\sum_u |a_I(u)|^2|a_I(0)a_J(0)| = \frac{|I|^2|J|}{p}. \tag{9}$$

For E_3 we use a variant from the argument of Konyagin and Shparlinski [10, Section 7]. By invariance under the group action we have

$$|E_3| \le \sum_{u\neq 0}\sum_{v\neq 0}|a(u,v)|\left|\sum_{x\neq 0} e_p(ux+vA2^{d-1}x^d)\right| = \sum_{u'\neq 0}\sum_{v'\neq 0}\beta(u',v')\left|\sum_{x\neq 0} e_p(u'x+v'x^d)\right|, \tag{10}$$

where

$$\beta(u',v') = \frac{1}{p-1}\sum_{x\neq 0}|a(xu',A_1x^dv')|, \tag{11}$$

and $A_1A2^{d-1} \equiv 1 \pmod p$. Next, from Hölder's inequality

$$\begin{aligned}|E_3| &\le \left(\sum_{u'}\sum_{v'}\left|\sum_x e_p(u'x+v'x^d)\right|^4\right)^{\frac14}\left(\sum_{u'\neq 0}\sum_{v'\neq 0}\beta(u',v')\right)^{\frac12}\left[\sum_{u'\neq 0}\sum_{v'\neq 0}\beta(u',v')^2\right]^{\frac14}\\ &= E_4^{1/4}E_5^{1/2}E_6^{1/4},\end{aligned} \tag{12}$$

say.

Clearly,

$$E_4 = p^2M, \tag{13}$$

with M as in (2). Next,

$$
\begin{aligned}
E_5 &= \sum_{u'\neq 0}\sum_{v'\neq 0}\beta(u',v') = \frac{1}{p-1}\sum_{x\neq 0}\sum_{u'\neq 0}\sum_{v'\neq 0}|a(xu',A_1x^dv')| = \sum_{u\neq 0}\sum_{v\neq 0}|a(u,v)| \\
&= p^2\left(\sum_{u\neq 0}|a_I(u)|^2\right)\left(\sum_{v\neq 0}|a_I(v)||a_J(v)|\right) \\
&\le p^2\left(\sum_{u\neq 0}|a_I(u)|^2\right)\left(\sum_{v\neq 0}|a_I(v)|^2\right)^{\frac{1}{2}}\left(\sum_{v\neq 0}|a_J(v)|^2\right)^{\frac{1}{2}},
\end{aligned}
$$

and so by Parseval's identity

$$E_5 \le p^{-2}(p-|I|)^{3/2}|I|^{3/2}(p-|J|)^{1/2}|J|^{1/2} \le p^{-2}(p-|I|)^2|I|^2. \tag{14}$$

Finally, for E_6 we have

$$
\begin{aligned}
E_6 &= \sum_{u'\neq 0}\sum_{v'\neq 0}\beta(u',v')^2 = \frac{1}{(p-1)^2}\sum_{x\neq 0}\sum_{y\neq 0}\sum_{u'\neq 0}\sum_{v'\neq 0}|a(xu',A_1x^dv')||a(yu',A_1y^dv')| \\
&= \frac{1}{p-1}\sum_{\substack{1\le u_1,u_2,v_1,v_2<p \\ (v_1/v_2)\equiv(u_1/u_2)^d \pmod p}}|a(u_1,v_1)||a(u_2,v_2)| \\
&= \frac{1}{p-1}\sum_{1\le u_1,u_2,j<p}|a(u_1,ju_1^d)||a(u_2,ju_2^d)| \\
&= \frac{p^4}{p-1}\sum_{1\le u_1,u_2,j<p}|a_I(u_1)|^2|a_I(u_2)|^2||a_I(ju_1^d)a_J(ju_1^d)||a_I(ju_2^d)a_J(ju_2^d)| \\
&= \frac{p^4}{p-1}\left(\sum_{u\neq 0}|a_I(u|^2\right)^2\left[\sum_{j\neq 0}|a_I(j)a_J(j)|^2\right] \\
&= \frac{1}{p-1}|I|^2(p-|I|)^2\left[\sum_{j\neq 0}|a_I(j)a_J(j)|^2\right].
\end{aligned}
$$

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

$$\sum_x\alpha^2(x) = 2\left[1^2+2^2+\cdots+((p-1)/4)^2\right] = \frac{1}{96}(p^2-1)(p+3),$$

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

$$\sum_x\alpha^2(x) = 2\left[1^2+2^2+\cdots+((p-3)/4)^2\right]+((p+1)/4)^2 = \frac{1}{96}(p-3)(p^2-1)+\frac{(p+1)^2}{16}.$$

Thus
(15)
$$\sum_{j\neq 0}|a_I(j)a_J(j)|^2=\begin{cases}\frac{5}{3\cdot 2^8}\left(1+\frac{12}{5p}-\frac{2}{5p^2}+\frac{12}{5p^3}-\frac{27}{5p^4}\right), & \text{if } p\equiv 1 \pmod 4,\\ \frac{5}{3\cdot 2^8}\left(1+\frac{12}{5p}+\frac{14}{p^2}+\frac{12}{p^3}-\frac{3}{5p^4}\right), & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

Let γ_p denote the value on the right-hand side of (15) and note that for $p>10^6$, $\gamma_p\leq .0065105$. Then

$$E_6\leq\frac{\gamma_p}{p-1}|I|^2(p-|I|)^2. \tag{16}$$

By (12), (13), (14) and (16) we have

$$|E_3|\leq\gamma_p^{1/4}\frac{M^{1/4}}{p^{1/2}(p-1)^{1/4}}|I|^{3/2}(p-|I|)^{3/2}, \tag{17}$$

and then by (8) and (9),

$$|Error|\leq\frac{|I|^{5/2}|J|^{1/2}}{p}+\frac{|I|^2|J|}{p}+\gamma_p^{1/4}\frac{M^{1/4}}{p^{1/2}(p-1)^{1/4}}|I|^{3/2}(p-|I|)^{3/2}. \tag{18}$$

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 $p\equiv 1 \pmod 4$.

3. Proof of Theorem 2

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

$$x_1^k+x_2^k=x_3^k+x_4^k$$
$$x_1^l+x_2^l=x_3^l+x_4^l.$$

We have the elementary bounds ([5, Lemma 3.2])

$$M(k,l)\leq\begin{cases}kl(p-1)^2, & \text{for } 1\leq l<k<p-1,\\ 3k|l|(p-1)^2, & \text{for } l<0,\ |l|\leq k,\ k+|l|<p-1.\end{cases} \tag{19}$$

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

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

$$A_1x_1^k+A_2x_2^k=A_3x_3^k+A_4x_4^k$$
$$B_1x_1^l+B_2x_2^l=B_3x_3^l+B_4x_4^l.$$

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

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

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

$$\sum_{x_1\ne 0}\cdots\sum_{x_4\ne 0}\sum_{\alpha,\beta} e_p(\alpha(A_1x_1^k+A_2x_2^k-A_3x_3^k-A_4x_4^k)+\beta(B_1x_1^l+B_2x_2^l-B_3x_3^l-B_4x_4^l))$$

$$\le \sum_{\alpha,\beta}\prod_{i=1}^{2}\left|\sum_{x_i\ne 0} e_p(\alpha A_i x_i^k+\beta B_i x_i^l)\right|\prod_{i=3}^{4}\left|\sum_{x_i\ne 0} e_p(-\alpha A_i x_i^k-\beta B_i x_i^l)\right|$$

$$\le \prod_{i=1}^{2}\left(\sum_{\alpha,\beta}\left|\sum_{x_i\ne 0} e_p(\alpha A_i x_i^k+\beta B_i x_i^l)\right|^4\right)^{1/4}\prod_{i=3}^{4}\left(\sum_{\alpha,\beta}\left|\sum_{x_i\ne 0} e_p(-\alpha A_i x_i^k-\beta B_i x_i^l)\right|^4\right)^{1/4}$$

$$= p^2M(k,l).$$

Next, set $m_1=(m,p-1)$ and let $\{w_1,...,w_{m_1}\}$ 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

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

□

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

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

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 $M(k,l)=M(km,lm)=M(d,1)\le dp^2\le p^3$. □

Let

$$\lambda_1=(l,k),\quad \lambda=(l,k,p-1),\quad l_+=l,\quad l_-=2l, \tag{20}$$

$$\delta_+=\frac{(k-l)}{\lambda_1},\quad \delta_-=\frac{(k+l)}{\lambda_1}, \tag{21}$$

and

$$\begin{aligned} M_+(k,l)&=M(k,l)\quad \text{for } 1\le l<k<p-1,\\ M_-(k,l)&=M(k,-l)\quad \text{for } 1\le l<k,\quad l+k<p-1. \end{aligned}$$

The next lemma is essentially Corollary 3.1 of [4] with the implied constants made explicit.

Lemma 3. *For $1\le l\le k<p-1$ then for $k<\frac{1}{32}(p-1)^{\frac{2}{3}}\lambda_1^{\frac{1}{6}}l_\pm^{\frac{1}{6}}$,*

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

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 [4]. From (2.1) of [4] it suffices to show that $\lambda\sum_{i=1}^{N} C_{\pm}^2(\mathbf{u}_i) \le (p-1)\mu$. Let T be as defined in [4, (3.1)]. If $T=0$ then as shown at the end of the proof of [4, Lemma 3.1], we must have $(kl_{\pm}/\lambda_1) \ge \frac{1}{2}\delta_{\pm}^2$ 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

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

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

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

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 Lemma 3.1 and (3.2) of [4]

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

and

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

giving $\lambda\sum_{i=1}^{N} C_{\pm}^2(\mathbf{u}_i) \le 768\cdot 5^{2/3}(\lambda/\lambda_1)kl_{\pm}\delta_{\pm}^{-1/3}(p-1)$. Plainly $5^{-5/3}2^{-7}(p-1)\frac{\delta_{\pm}^{\frac{1}{3}}}{(kl_{\pm}/\lambda_1)}$ 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 $(kl_{\pm}/\lambda_1) \ge 5^{-2/3}2^{-3/5}\delta_{\pm}^{4/3}$. Thus $L<T$ (we assume $T\ge 1$ else the claim is trivial) unless $(kl_{\pm}/\lambda_1) < 5^{-2/3}2^{-3/5}\delta_{\pm}^{4/3} < \frac{1}{2}\delta_{\pm}^2$ in which case

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

and

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

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

Theorem 2 is just a special case of the following theorem with $k=d$, $l=1$.

Theorem 6. *Let $1 \le l < k < p-1$ 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*

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

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 $p^3 \le 13658p^{66/23}$ and so we may assume that $p > 10^{31}$. The idea is to make a transformation of the type $x \to x^m$ so that Lemma 3 can be effectively applied. Choose m so that

$$mk \equiv \alpha \mod (p-1), \quad \pm ml \equiv \beta \mod (p-1), \tag{22}$$

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

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

$(\alpha, \beta) \ne (0,0)$. Such a pair (α, β) exists since the set of all (α, β) satisfying (22) is a lattice of volume $p-1$. Now, $(p-1) \nmid m$ (since $(\alpha, \beta) \ne (0,0)$) and so, since $(lk, p-1) = 1$ we have $\alpha \ne 0$ and $\beta \ne 0$. If $\alpha = \beta$ then $p-1 | m(k \mp l)$, $\frac{p-1}{d^*} | m$ and $|\beta| \ge (p-1)/d^*$ contradicting our assumption on the size of d^*. Thus $\alpha \ne \beta$. Set

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

Case i: Suppose that $\alpha \le 100|\beta|$. Then by Lemma 1 and (19) we have,

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

Case ii: Suppose that $\alpha > 100|\beta|$ and $\alpha \ge 2^{-5}(p-1)^{2/3}\lambda_1^{1/6}(\beta')^{1/6}$. Then $(\beta')^{1/6} \le (32/c)p^{2/69}$, $\beta' \le (32/c)^6p^{4/23}$. By Lemma 1 and (19) we get

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

Case iii: 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

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

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

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

Thus we get

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

□

4. Proof of Theorem 3

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

$$N = \frac{1}{k}\sum_x \left(\sum_{\psi^k=\psi_0} \psi(B^{-1}x)\right)\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx) \tag{24}$$

$$= \frac{1}{k}\sum_x \chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx) + \frac{1}{k}\sum_{\psi\neq\psi_0}\sum_x \psi(B^{-1}x)\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx) \tag{25}$$

$$= \mathrm{M}ain + \mathrm{E}rror. \tag{26}$$

Main Term: Suppose first that $1 < C < p/2$. The main term is just the number of values of $n \in \{1, 2, \ldots, \frac{p-1}{2}\}$ 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

$$Main = \frac{1}{k}\sum_{j=1}^{[C/2]} \left[\frac{jp}{C}\right] - \left[\frac{(2j-1)p}{2C}\right] \geq \frac{1}{k}\sum_{j=1}^{[C/2]} \left[\frac{p}{2C}\right] = \frac{1}{k}\left[\frac{C}{2}\right]\left[\frac{p}{2C}\right]. \tag{27}$$

We consider first a few small values of C. Let S denote the sum appearing in the main term, $S = k(Main)$. 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 $-p/2 < C \le -1$. 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 $0 \le j \le [(C-1)/2]$. Then,

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

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

$$\text{Main} \ge \frac{p-3}{8k}. \tag{28}$$

Error Term: Let ψ be a nonprincipal character $\pmod p$. Then

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

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 (32)

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

and

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

We conclude from (14) and (28) that N is positive provided that $\frac{p-3}{8} \ge (k-1)(\frac{4}{\pi^2}\log p+1)^2\sqrt{p}$. If $d_1 > 1$ then $k \le \frac{p-1}{2}$ and $\frac{p-3}{k-1} \ge \frac{p-1}{k} = d_1$. Thus N is positive provided that $d_1 > 8(\frac{4}{\pi^2}\log p+1)^2\sqrt{p}$.

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

$$|\sum_{x\ne 0} e_p(ax^d + bx)| \le d_1 + \frac{p^{3/2}}{d_1},$$

for any nonzero a, b. Thus Theorem 5 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 $d_1 > 8(\frac{4}{\pi^2}\log(p)+1)^2\sqrt{p}$. Thus part (a) of the theorem applies.

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

5. Proof of Theorem 4

If $d_1 \le .18(p-1)^{16/23}$ then by Theorem 2, $M \le 13658p^{66/23} < .000823p^3$ for $p \ge 2.26 \cdot 10^{55}$. 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 3 (b) yields the result.

6. Proof of Theorem 5

The proof proceeds identically as the proof of Theorem 1 the only change being in the estimate of E_3. We have

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

and so
(29)

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

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

7. Finite Fourier Series

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

$$a(y) = \frac{1}{p}\sum_x \alpha(x)e_p(-xy). \tag{30}$$

Let

$$I = \{a+1, a+2, \ldots, a+M\} \subset \mathbb{Z}_p$$

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

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

and

$$\sum_y |a_I(y)| = f(M,p) := \frac{1}{p}\sum_y\left|\frac{\sin(\pi My/p)}{\sin(\pi y/p)}\right|, \tag{31}$$

where the summand is understood to be M when $y = 0$. In [2] the first author proved

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

The main term in this upper bound cannot be improved. Indeed, in [3, Equation 5] Cochrane and Peral showed

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

Letting $I = \{1, 2, \ldots, \frac{p-1}{2}\}$ 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,

$$\sum_y |a_{\mathbb{E}}(y)| \le \frac{4}{\pi^2}\log p + 1. \tag{32}$$

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

Let

$$I = \{a_1+1, a_1+2, \ldots, a_1+M\}, \qquad J = \{b_1+1, \ldots b_1+N\},$$

be intervals of integers in $\mathbb{Z}_p$ with $|I| = M$, $|J| = N$ and $1 \le M, N < p$, 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 $pa_I(y)a_J(y)$.

Parseval's identity 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

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

References

[1] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc. 18, (2005), no. 2, 477-499.

[2] T. Cochrane, *On a trigonometric inequality of Vinogradov*, J. Number Theory 27, (1987), 9-16.

[3] T. Cochrane and J.C. Peral, *An asymptotic formula for a trigonometric sum of Vinogradov*, J. Number Theory 91 (2001), 1-19.

[4] T. Cochrane and C. Pinner, *Stepanov's method applied to binomial exponential sums*, Quart. J. Math. 54 (2003), 243-255.

[5] ———, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. 133 (2005), no. 2, 313-320.

[6] M. Goresky, A. Klapper, *Arithmetic cross-correlations of FCSR sequences*, IEEE Trans. Inform. Theory, 43 (1997), 1342-1346.

[7] M. Goresky, A. Klapper and R. Murty, *On the distinctness of decimations of ℓ-sequences*, (Proceedings of SETA'01), T. Helleseth, ed., Discrete Mathematics and Computer Science, Springer Verlag, NY, 2002.

[8] M. Goresky, A. Klapper, R. Murty and I. Shparlinski, *On decimations of ℓ-sequences*, SIAM J. Discrete Math. 18 (2004), no. 1, 130-140 (electronic).

[9] T. Gowers, *A new proof of Szemerédis theorem for arithmetic progressions of length 4*, GAFA 8 (1998), no. 3, 529-551.

[10] S. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press 136, United Kingdom, 1999.

[11] H. Xu and W.F. Qi, *Further results on the distinctness of decimations of l-sequences,* IEEE Trans. on Info. Theory 52 (2006), no. 8, 3831-3836.

School of Mathematics, Institute of Advanced Study, Princeton, NJ 08540, USA
E-mail address: Bourgain@math.ias.edu

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: cochrane@math.ksu.edu

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: paulhus@math.ksu.edu

Department of Mathematics, Kansas State University, and Manhattan, KS 66506
E-mail address: pinner@math.ksu.edu