ACTA ARITHMETICA
147.2 (2011)

On the parity of k-th powers modulo p. A generalization of a problem of Lehmer

by

Jean Bourgain (Princeton, NJ), Todd Cochrane (Manhattan, KS), Jennifer Paulhus (Manhattan, KS, and Villanova, PA) and Christopher Pinner (Manhattan, KS)

1. Introduction. Let p be an odd prime, $\mathbb{Z}_p = \mathbb{Z}/(p)$, $\mathbb{E}$ the set of even residues in $\mathbb{Z}_p$ and $\mathbb{O}$ the set of odd residues,

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

with characteristic functions $\chi_{\mathbb{E}}$, $\chi_{\mathbb{O}}$ respectively. Lehmer posed the problem of determining the number N_{-1} of even residues with an odd multiplicative inverse modulo p [17, Problem F12]. One expects $N_{-1} \sim p/4$ and this was proven by Zhang [30]. Here, we consider the more general problem of determining the number N_k of even residues such that Ax^k is odd,

$$N_k = N_k(A) = \#\{x \in \mathbb{E} : Ax^k \in \mathbb{O}\},$$

where k, A are any integers with $p \nmid A$ (with the convention that x^{-1} denotes the multiplicative inverse of x in $\mathbb{Z}_p$). Lehmer's original problem is just the case $k = -1$, $A = 1$. The Goresky–Klapper conjecture [14] on the decimation of ℓ-sequences amounts to proving that $N_k > 0$ for $p > 13$ and $(k, p-1) = 1$.

For the general case one does not always have N_k asymptotic to $p/4$. Two parameters play a key role in the determination of N_k,

$$d := (k, p-1) \quad \text{and} \quad d_1 := (k-1, p-1),$$

and their companion values,

$$s := \frac{p-1}{d} \quad \text{and} \quad t := \frac{p-1}{d_1}.$$

We find for instance (Example 9.1) that if t and $|A|$ are both small odd numbers then $N_k \sim \left(1 - \frac{1}{At}\right)\frac{p}{4}$. In other words, the probability that an even residue becomes odd under the mapping $x \mapsto Ax^{(p+t-1)/t}$ is asymptotic to

2010 *Mathematics Subject Classification*: 11K36, 11K38, 11L03, 11L07, 11N69.
Key words and phrases: exponential sums.

DOI: 10.4064/aa147-2-6

$\frac{1}{2}\big(1-\frac{1}{At}\big)$. On the other hand, if both s and k are even then we have exactly $N_k=(p-1)/4$ (Theorem 1.3). We also show that $N_k\sim p/4$ provided that k is even and the set of all k-th powers is uniformly distributed, or k is odd and $d_1=o(p)$ (Theorems 1.1 and 1.2).

Let $e_p(\cdot)=e^{2\pi i\cdot/p}$ denote the additive character on $\mathbb{Z}_p$, and set

$$\Phi(k)=\max_{\substack{a\in\mathbb{Z}_p\\ a\neq 0}}\Big|\sum_{x\neq 0}e_p(ax^k)\Big|, \tag{1.1}$$

$$\Phi(k,1)=\max_{\substack{a,b\in\mathbb{Z}_p\\ ab\neq 0}}\Big|\sum_{x\neq 0}e_p(ax^k+bx)\Big|, \tag{1.2}$$

$$\Phi'(k)=\max_{\substack{a\in\mathbb{Z}_p\\ a\neq 0}}\Big|\sum_{x=1}^{(p-1)/2}e_p(ax^k)\Big|. \tag{1.3}$$

Using the Erdős–Turán inequality we prove (Section 2)

Theorem 1.1. *For any integer k,*

$$\left|N_k-\frac{p}{4}\right|<\frac{1}{\pi}\Phi'(k)\min\left\{\log\left(\frac{356p}{\Phi'(k)}\right),\log(5p)\right\}. \tag{1.4}$$

If k is even then

$$\Phi'(k)=\frac{1}{2}\Phi(k).$$

If k is odd then

$$\Phi'(k)\le\frac{1}{2}\Phi(k)+\frac{1}{\pi}\log(5p)\Phi(k,1).$$

Since $x\log x\to 0$ as $x\to 0^+$, we see that if k is even then $N_k\sim p/4$ provided that $\Phi(k)=o(p)$, that is, the set of all k-th powers is uniformly distributed. This phenomenon fails when k and t are both odd. Indeed, one can have $(k,p-1)=1$, so that the set of k-th powers is all of $\mathbb{Z}_p^*$, but not have $N_k\sim p/4$; see Example 1.2. In the original Lehmer problem, where $k=-1$, we have $\Phi(-1)=1$, and $\Phi(-1,1)\le 2\sqrt{p}$, the Kloosterman sum bound, whence Theorem 1.1 gives the result of Zhang, $|N_{-1}-p/4|\ll\sqrt{p}\log^2 p$. Note that, since $\Phi'(k)\ge\frac{1}{2}\sqrt{p+1}$ (see (2.1)), the second option in (1.4) is only useful for small $p\le 20\,277$.

Open problem 1. How large must s be in order to have $\Phi(k)=o(p)$ (where s, as defined above, denotes the number of k-th powers in $\mathbb{Z}_p^*$)? It is known, by the work of Bourgain [4], that there exists a constant c such that $\Phi(k)=o(p)$ for $s>p^{c/\log\log p}$; see Section 5. It is also known that with $s\approx\log p$ one has $\Phi(k)\approx p$. The conjectured bound of Montgomery, Vaughan and Wooley [25], $\Phi(k)\ll\sqrt{dp\log p}$, gives $\Phi(k)=o(p)$ provided $(\log p)/s\to 0$ as $p\to\infty$.

For odd k we can bypass the concern of large $\Phi(k)$.

THEOREM 1.2.

(a) *If k is odd and t is even then*

$$\left|N_k - \frac{p}{4}\right| \le 0.35p^{89/92}\log^{3/2}(5p).$$

(b) *If k is odd and t is odd then*

$$\left|N_k - \frac{p}{4}\right| \ll d_1 + \frac{p}{\log p}.$$

Thus, if k is odd we have $N_k \sim p/4$ provided $d_1 = o(p)$. If d_1 is on the order of p in size, this can fail to happen; see Theorem 1.5. The proof of Theorem 1.2, given in Section 8, uses Theorem 1.1 as well as Theorems 1.3, 1.4, 1.5 and 5.1 below, and a small refinement given in Section 6.

There remain the cases where k is even and s is very small (so that $\Phi(k) \ne o(p)$), and when k is odd and t is very small (so that $d_1 \ne o(p)$). To get a feeling for what one should expect in these cases we consider a couple of examples.

EXAMPLE 1.1 (small s). If $k = p-1$, then $x^k = 1$ identically and so $N_k = 0$ or $(p-1)/2$, depending on whether A is even or odd. If $k = (p-1)/2$, then $x^k = \pm 1$. Since A and $-A$ have opposite parity and roughly half of the even residues are quadratic residues, one gets $N_k = (p-1)/4$ (k even) or $N_k \sim p/4$ (k odd). If $k = (p-1)/3$ and C_1, C_2, C_3 are the cube roots of unity then $Ax^k \equiv AC_1, AC_2$ or $AC_3 \pmod p$, and one obtains $N_k = 0, (p-1)/6, (p-1)/3$, or $(p-1)/2$ depending on the number of these values that are odd; see Theorem 1.3(a).

The following theorem treats the case of small s. When k is even we find that N_k is exactly $(p-1)/2$ times the proportion of k-th powers C_i with AC_i odd. If s is also even this proportion is $1/2$ since -1 is then a k-th power and so we get $N_k = (p-1)/4$. When k is odd we get $N_k \sim p/4$ for s sufficiently small.

THEOREM 1.3. *Let k, A be integers with $p \nmid A$ and $(\mathbb{Z}_p^*)^k = \{C_1, \dots, C_s\}$.*

(a) *If k is even then*

$$N_k = \frac{p-1}{2s}\sum_{i=1}^{s} \chi_{\mathbb{O}}(AC_i).$$

In particular, if k is even and s is even then $N_k = (p-1)/4$.

(b) *If k is odd then*

$$\left|N_k - \frac{p-1}{4}\right| < \frac{s-1}{2\pi}\sqrt{p}\log(5p).$$

Next, we deal with the case where t is small.

EXAMPLE 1.2 (small t). Suppose $k = (p+1)/2$, so that $t = 2$. Then $Ax^k \equiv Ax$ or $-Ax \pmod p$ according as x is a quadratic residue or not. Thus one expects half of the even residues to remain even and half to become odd; indeed, Corollary 1.1 gives $|N_k - p/4| \ll \sqrt{p}\log^2 p$.

If $k = (p+2)/3$, so that $t = 3$, then $Ax^k \equiv AC_1x, AC_2x$ or $AC_3x \pmod p$, where again C_1, C_2, C_3 are the cube roots of unity. In effect, the problem becomes linearized, and as we see in Section 7, we need to examine the distribution of points on the lattices $y \equiv AC_ix \pmod p$. If none of the lattices have a small point ($0 < \max(|x|,|y|) \ll 1$) then we find (Theorem 1.5) that the even and odd values are equidistributed and so $N_k \sim p/4$, but if one of the lattices has a small point, bias may occur. For $k = (p+2)/3$, we find that N_k is asymptotically somewhere between $p/4 - p/12$ and $p/4 + p/12$, depending on the size of the minimal point.

Let

$$(\mathbb{Z}_p^*)^{k-1} = \{C_1, \dots, C_t\},$$

and for any $C \in \mathbb{Z}$, $p \nmid C$, let $F(C)$ denote the number of even residues x such that Cx is odd,

$$F(C) = \sum_x \chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx). \tag{1.5}$$

In Section 4 we prove

THEOREM 1.4. *For any k and A with $p \nmid A$,*

$$\left| N_k - \frac{1}{t}\sum_{i=1}^{t} F(AC_i) \right| \le \frac{1}{\pi^2}(t-1)\sqrt{p}\log^2(5p).$$

COROLLARY 1.1. *For any k and A with $p \nmid A$,*

$$\left| N_k - \frac{p-1}{4} \right| \le \begin{cases} \dfrac{1}{\pi^2}(t-1)\sqrt{p}\log^2(5p) & \text{if } t \text{ is even,} \\ \dfrac{1}{\pi^2}(t-1)\sqrt{p}\log^2(5p) + \dfrac{p}{\pi^2 t}\log^2(5p) + \dfrac{1}{4} & \text{if } t \text{ is odd.} \end{cases} \tag{1.6}$$

Thus $N_k \sim p/4$ in the range $\log^{2+\epsilon} p < t < \sqrt{p}/\log^{2+\epsilon} p$. For very small odd t more work is required. On average $F(C)$ is $p/4$ and our interest is in estimating the discrepancy

$$\delta_C := F(C) - p/4. \tag{1.7}$$

Trivially $|\delta_C| \le p/4$. The value of δ_C depends on the distribution of points in the lattice

$$\mathcal{L}_C := \{(x,y) \in \mathbb{Z}^2 : y \equiv Cx \pmod p\}.$$

Let $|(x,y)|_0 = \max(|x|,|y|)$,

$$\lambda_C = \min\{|(x,y)|_0 : (x,y) \in \mathcal{L}_C,\ (x,y) \ne (0,0)\},$$

and (x_C, y_C) denote a point in $\mathcal{L}_C$ with $|(x_C,y_C)|_0 = \lambda_C$ (we call such a point a *minimal point* in $\mathcal{L}_C$). Put $\lambda_i = \lambda_{AC_i}$, $\delta_i = \delta_{AC_i}$, $1 \le i \le t$ and let (x_i, y_i) be a point in $\mathcal{L}_{AC_i}$ with $|(x_i,y_i)|_0 = \lambda_i$. Reorder the C_i so that

$$\lambda_1 \le \cdots \le \lambda_t.$$

In particular, $\lambda_1 = 1$ if and only if $AC_1 = \pm 1$, in which case we can take $(x_1, y_1) = (1, \pm 1)$. In Lemma 7.2 we give the estimate

$$|\delta_C| < \frac{\pi^2 p}{12|x_C y_C|} + \sqrt{2p}\log p + \frac{1}{2}.$$

Another estimate for the discrepancy is given in Lemma 9.1. If t is odd we show that only δ_1 can have any effect on the asymptotic value of N_k, establishing in Section 7 the following:

THEOREM 1.5.

(a) *If t is odd, then*

$$\left|N_k - \left(\frac{p}{4} + \frac{\delta_1}{t}\right)\right| \ll \frac{p}{\log p} + t\sqrt{p}\log^2 p.$$

(b) *If $t > 1$ is odd and $t \ll \log p$ then*

$$\left|N_k - \left(\frac{p}{4} + \frac{\delta_1}{t}\right)\right| \ll \frac{p^{1-\frac{1}{2(t-1)}}}{t}.$$

REMARKS. 1. In [5] the authors proved that if $d = 1$, then for p sufficiently large, $N_k > 0$, resolving a conjecture of Goresky and Klapper [14]; see also [15], [16]. The theorems above generalize this result to the following cases: (i) k is any odd integer, $t > 1$, and p is sufficiently large (Theorem 1.2 for t even, or t odd and $t \gg \log p$, Theorem 1.5 for t odd and $t \ll \log p$); (ii) k is even, p is arbitrary, and Ax^k is odd for some $x \in \mathbb{Z}_p$ (Theorem 1.3(a)); such is the case if s is even (Theorem 1.3(a)), or if s is odd and $\Phi(k) \le p/5.24$ (Theorem 1.1, for in this case $|N_k - p/4| < p/4$).

2. Yi and Zhang [29] studied the number of times $x^k \pmod q$ and $x^{-k} \pmod q$ have the same parity modulo q for general q and $(x,q) = 1$, obtaining the asymptotic value $\phi(q)/2 + O_k(q^{3/4}d(q)^{1/2}\log^2 q)$. We note that the constant in the big-O depends on k, although the dependence is not indicated. Shparlinski [27] generalized their result to systems of congruences.

3. Louboutin, Rivat and Sárközy [22] studied the related problem of determining when x and x^{-1} have the same parity over an interval, showing that for any $\epsilon > 0$ and any interval I of length $|I| > p^{1/2+\epsilon}$, as x runs through I, the probability that x and x^{-1} have the same parity tends to $1/2$ as $p \to \infty$. They also studied the pseudorandomness of the sequence $(-1)^{x+x^{-1}}$ (taking $x, x^{-1} \in \{1, \dots, p-1\}$).

Open problem 2. When does $N_k = 0$? More specifically, when is k even and x^k odd for all nonzero x? Example: If $p = (3^s - 1)/2$ and $k = (p-1)/s$ then the group of k-th powers G_k is just $\langle 3 \rangle = \{1, 3, 3^2, \dots, 3^{s-1}\}$, all odd, and $s \approx \log p$. More can be said if G_k contains a pair of multiplicatively independent integers a, b. In this case, by the work of Furstenberg [13] and more specifically Bourgain, Lindenstrauss, Michel and Venkatesh [8, Theorem 1.10] there exists a constant $c(a, b)$ such that if $p > c(a, b)$ then every coset of the subgroup $\langle a, b \rangle$ contains both even and odd residues, and therefore so does every coset of G_k. Indeed, for any integer x with $p \nmid x$ there will exist both even and odd residues of the type $xa^i b^j$ with $0 < i, j < 3 \log p$.

Open problem 3. How large can s be and still have a disproportionate number of even or odd values in the set of k-th powers? This has direct implications on a lower bound for $\Phi(k)$. Indeed, if (k_n, p_n) is a sequence of exponents k_n and prime moduli $p_n \to \infty$ such that $N_{k_n} \nrightarrow p_n/4$, then $\Phi(k_n)/p_n \nrightarrow 0$.

2. The Erdős–Turán inequality and proof of Theorem 1.1. In this section we employ a version of the Erdős–Turán inequality for estimating N_k. For any sequence of points $S = (x_1, \dots, x_N)$ in $\mathbb{Z}_p$ set

$$\Phi_S = \max_{p \nmid y} \Big| \sum_{n=1}^{N} e_p(y x_n) \Big|.$$

Since $\sum_{y=1}^{p-1} |\sum_{n=1}^{N} e_p(y x_n)|^2 \geq N(p-N)$, for $N < p$ we note the lower bound

$$\Phi_S \geq \sqrt{\frac{N(p-N)}{p-1}}. \tag{2.1}$$

Our goal is to estimate the number of points in S contained in a given interval $I = \{a+1, \dots, a+M\} \subset \mathbb{Z}_p$, with $M \leq p$. The simplest approach is to use the characteristic function χ_I of the interval, with Fourier expansion $\chi_I(x) = \sum_{y=1}^{p} a_I(y) e_p(yx)$, where

$$a_I(0) = M/p, \qquad a_I(y) = p^{-1} e_p\bigg(\Big(-a - \frac{M}{2} - \frac{1}{2}\Big) y\bigg) \frac{\sin(\pi M y/p)}{\sin(\pi y/p)}, \quad y \neq 0.$$

Now

$$\sum_{n=1}^{N}\chi_I(x_n)=\sum_{n=1}^{N}\sum_{y}a_I(y)e_p(yx_n)=a_I(0)N+\sum_{y\neq 0}a_I(y)\sum_{n=1}^{N}e_p(yx_n),$$

and so

$$\left|\sum_{n=1}^{N}\chi_I(x_n)-\frac{MN}{p}\right|\le \Phi_S\sum_{y=1}^{p-1}|a_I(y)|. \tag{2.2}$$

In Lemmas 11.1 and 11.2 we prove that for any interval I,

$$\sum_{y=1}^{p-1}|a_I(y)|\le\frac{4}{\pi^2}\log p+0.35\le\frac{4}{\pi^2}\log(3p), \tag{2.3}$$

and that for any interval of length $M=(p\pm 1)/2$,

$$\sum_{y=1}^{p-1}|a_I(y)|\le\frac{1}{\pi}\log p+0.482<\frac{1}{\pi}\log(5p). \tag{2.4}$$

From (2.2)–(2.4) we deduce that for any interval I,

$$\left|\sum_{n=1}^{N}\chi_I(x_n)-\frac{MN}{p}\right|\le\frac{4}{\pi^2}\log(3p)\Phi_S, \tag{2.5}$$

and when $M=\frac{1}{2}(p\pm 1)$,

$$\left|\sum_{n=1}^{N}\chi_I(x_n)-\frac{MN}{p}\right|\le\frac{1}{\pi}\log(5p)\Phi_S. \tag{2.6}$$

One can improve this estimate for large p by using a smooth approximation to the characteristic function, leading to an Erdős–Turán type inequality. At the end of Section 10 we prove

THEOREM 2.1. *For any sequence $S=(x_1,\dots,x_N)$ in $\mathbb{Z}_p$, interval $I=\{a+1,a+2,\dots,a+M\}\subset\mathbb{Z}_p$, and positive integer $H<p$,*

$$\left|\sum_{n=1}^{N}\chi_I(x_n)-\frac{MN}{p}\right|\le\frac{N}{H+1}-\frac{N}{p}+\frac{2}{\pi}(\log H+\gamma+\pi/2)\Phi_S,$$

where $\gamma=0.57721\dots$ is Euler's constant. If $M=(p\pm 1)/2$ we have the sharper bound

$$\left|\sum_{n=1}^{N}\chi_I(x_n)-\frac{N}{2}\right|\le\frac{N}{H+1}+\frac{1}{\pi}(\log H+\gamma+\pi+\log 2)\Phi_S.$$

COROLLARY 2.1. *For any sequence $S = (x_1, \dots, x_N)$ in $\mathbb{Z}_p$ and interval $I = \{a+1, \dots, a+M\} \subset \mathbb{Z}_p$,*

$$\left| \sum_{n=1}^{N} \chi_I(x_n) - \frac{MN}{p} \right| \le \frac{2}{\pi}(\log(N/\Phi_S) + 1 + \gamma + \pi/2 + \log(\pi/2))\Phi_S,$$

and if $M = \frac{1}{2}(p \pm 1)$ and $\pi N/\Phi_S < p$ then

$$\left| \sum_{n=1}^{N} \chi_I(x_n) - \frac{N}{2} \right| \le \frac{1}{\pi}(\log(N/\Phi_S) + 1 + \gamma + \pi + \log(2\pi))\Phi_S.$$

We note that the corollary improves on (2.5) and (2.6) when $p^{2/\pi}\Phi_S > 18.18N$ and $p\Phi_S > 140.79N$, respectively.

Proof of Corollary 2.1. Set $H = \left[\frac{\pi N}{2\Phi_S}\right]$. If $N < (2/\pi)p\Phi_S$, then $H < p$ and we can apply Theorem 2.1 to obtain the first upper bound

$$\frac{2\Phi_S}{\pi} + \frac{2}{\pi}\left(\log\left(\frac{\pi N}{2\Phi_S}\right) + \gamma + \pi/2\right)\Phi_S \le \frac{2}{\pi}\Phi_S(\log(N/\Phi_S) + 1 + \gamma + \pi/2 + \log(\pi/2)).$$

If $N \ge (2/\pi)p\Phi_S$ the corollary follows from (2.5). For the second inequality we similarly take $H = [\pi N/\Phi_S] < p$. ∎

Proof of Theorem 1.1. Let $x_n \equiv A2^{k-1}n^k \pmod p, 1 \le n \le (p-1)/2$, and

$$I' = \{-1, -2, \dots, -(p-1)/2\}.$$

Let $I = I'$ or $I' \cup \{0\}$. Note that for either choice of I, $x_n \in I$ is equivalent to $A(2n)^k \in \mathbb{O}$ and so $N_k = \sum_{n=1}^{(p-1)/2} \chi_I(x_n)$.

With $\Phi'(k)$ as in (1.3), from (2.1) we have the lower bound $\Phi'(k) \ge \frac{1}{2}\sqrt{p+1}$. We assume that $p \ge 7$ (otherwise the bounds are worse than the trivial bound $p/4$).

Taking $I = I' \cup \{0\}$, so that $M = (p+1)/2$, we obtain, in the manner of (2.6),

$$\left| N_k - \frac{p^2-1}{4p} \right| \le \sum_{y=1}^{p-1} |a_I(y)|\Phi'(k).$$

Hence, using Lemma 11.2,

$$\left| N_k - \frac{p}{4} \right| \le \left(\frac{1}{\pi}\log\left(\frac{8e^\gamma p}{\pi}\right) + E(p)\right)\Phi'(k) + \frac{1}{4p} < \frac{1}{\pi}\log\left(\frac{8e^\gamma p}{\pi}\right)\Phi'(k), \tag{2.7}$$

since

$$E(p) + \frac{1}{4p\Phi'(k)} < -\frac{0.192}{p} + \frac{1}{2p\sqrt{p+1}} < 0.$$

This gives the second inequality in (1.4).

On checking that $\pi N/\Phi_S < \pi\frac{1}{2}(p-1)/\frac{1}{2}\sqrt{p+1} < p$, Corollary 2.1 gives

$$\left|N_k - \frac{p-1}{4}\right| \le \frac{1}{\pi}\big(\log((p-1)/2\Phi'(k)) + 1 + \gamma + \pi + \log(2\pi)\big)\Phi'(k),$$

and so

$$\left|N_k - \frac{p}{4}\right| \le \frac{1}{\pi}\big(\log(p/\Phi'(k)) + 1 + \gamma + \pi + \log\pi\big)\Phi'(k) + \frac{1}{4}.$$

From the second inequality in (1.4) we can assume that $\Phi'(k) > 71.2$. The first inequality,

$$\left|N_k - \frac{p}{4}\right| \le \frac{1}{\pi}\log(356p/\Phi'(k))\Phi'(k),$$

now follows on observing that $1 + \gamma + \pi + \log\pi + \frac{\pi}{4}/71.2 < 5.8746$.

If k is even then trivially $\Phi'(k) = \frac{1}{2}\Phi(k)$. For odd k we have, with $I = \{1, \dots, (p-1)/2\}$,

$$\begin{aligned}\sum_{x=1}^{(p-1)/2} e_p(yx^k) &= \sum_{x=1}^{p-1}\chi_I(x)e_p(yx^k) = \sum_{x=1}^{p-1} e_p(yx^k)\sum_z a_I(z)e_p(zx)\\ &= a_I(0)\sum_{x=1}^{p-1} e_p(yx^k) + \sum_{z\ne 0} a_I(z)\sum_{x=1}^{p-1} e_p(yx^k + zx),\end{aligned}$$

and so by (2.4),

$$\Phi'(k) \le \frac{1}{2}\Phi(k) + \frac{1}{\pi}\log(5p)\Phi(k,1). \ \blacksquare$$

3. Proof of Theorem 1.3. When s is small, that is, the number of k-th powers is small, then we have no nontrivial estimates available for $\Phi(k)$, and so an alternate method is required to estimate N_k. Let $d = (k, p-1)$, $s = (p-1)/d$, and

$$(\mathbb{Z}_p^*)^k = \{C_1, \dots, C_s\}$$

be the set of nonzero k-th powers. Let c_i be a value such that $c_i^k \equiv C_i \pmod p$, so that

$$\mathbb{Z}_p^* = c_1(\mathbb{Z}_p^*)^s \cup \cdots \cup c_s(\mathbb{Z}_p^*)^s.$$

Noting that $\chi_{\mathbb{O}}(x) = \chi_{\mathbb{E}}(-x)$, and that $x^k = C_i$ for $x \in c_i(\mathbb{Z}_p^*)^s$, we have

$$\begin{aligned}N_k &= \sum_x \chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Ax^k) = \sum_{i=1}^{s}\chi_{\mathbb{O}}(AC_i)\sum_{x\in c_i(\mathbb{Z}_p^*)^s}\chi_{\mathbb{E}}(x)\\ &= \frac{1}{s}\sum_{i=1}^{s}\chi_{\mathbb{O}}(AC_i)\sum_{x\ne 0}\Big(\sum_{\psi^s=\psi_0}\psi(\overline{c_i}x)\Big)\chi_{\mathbb{E}}(x) = \mathit{Main} + \mathit{Error},\end{aligned}$$

where ψ denotes a multiplicative character mod p and

$$Main = \frac{p-1}{2s}\sum_{i=1}^{s}\chi_{\mathbb{O}}(AC_i),$$

$$Error = \frac{1}{s}\sum_{\substack{\psi^s=\psi_0\\ \psi\neq\psi_0}}\sum_{i=1}^{s}\chi_{\mathbb{O}}(AC_i)\psi(\overline{c_i})\sum_{x\neq 0}\psi(x)\chi_{\mathbb{E}}(x).$$

Note that $Main = (p-1)/4$ if -1 is a k-th power, that is, s is even, for then the even and odd values can be paired, AC_i, $-AC_i$. For the error term, the sum over x is zero if $\psi(-1) = 1$ since in this case $\sum_{x=1}^{(p-1)/2}\psi(x) = \frac{1}{2}\sum_x \psi(x) = 0$. When $\psi(-1) = -1$ we appeal to the bound of Pólya, Landau, Schur and Vinogradov for incomplete character sums.

LEMMA 3.1. *Let I be any interval in $\mathbb{Z}_p$ and ψ any nonprincipal character modulo p. Then*

$$\Big|\sum_{x=a+1}^{a+M}\psi(x)\Big| \le \sqrt{p}\sum_y |a_I(y)| \le \frac{4}{\pi^2}\sqrt{p}\log(3p),$$

and for intervals of length $M = (p\pm 1)/2$,

$$\Big|\sum_{x=a+1}^{a+M}\psi(x)\Big| \le \sqrt{p}\sum_{y\neq 0}|a_I(y)| \le \frac{1}{\pi}\sqrt{p}\log(5p).$$

Slightly better bounds are available with greater effort; see Hildebrand [19] and Bachman and Rachakonda [1].

Proof. Letting χ_I be the characteristic function of I, we have

$$\begin{aligned}\sum_{x=a+1}^{a+M}\psi(x) &= \sum_x \psi(x)\chi_I(x) = \sum_x \psi(x)\sum_y a_I(y)e_p(yx)\\ &= a_I(0)\sum_x\psi(x) + \sum_{y\neq 0}a_I(y)\sum_x\psi(x)e_p(yx)\\ &= \sum_{y\neq 0}a_I(y)\sum_x\psi(x)e_p(yx).\end{aligned}$$

The sum over x is just a Gauss sum of modulus $\sqrt{p}$. The lemma is now immediate from (2.3) and (2.4). ∎

Thus for any nonprincipal ψ,

$$\Big|\sum_x \psi(x)\chi_{\mathbb{E}}(x)\Big| = \Big|\sum_{x=1}^{(p-1)/2}\psi(x)\Big| \le \frac{1}{\pi}\sqrt{p}\log(5p). \tag{3.1}$$

If k is even then $\psi(-1)=1$ for all ψ satisfying $\psi^s=\psi_0$, while if k is odd then $\psi(-1)=1$ for exactly half of the ψ satisfying $\psi^s=\psi_0$. Thus $Error=0$ if k is even, and if k is odd,

$$|Error| < \frac{s-1}{2\pi}\sqrt{p}\log(5p),$$

completing the proof of Theorem 1.3. ∎

4. Proofs of Theorem 1.4 and Corollary 1.1. In this section we proceed as in the previous section, but using the set of $(k-1)$-th powers rather than the set of k-th powers.

Proof of Theorem 1.4. Let $d_1=(k-1,p-1)$, $t=(p-1)/d_1$, and

$$(\mathbb{Z}_p^*)^{k-1}=\{C_1,\dots,C_t\} \tag{4.1}$$

be the set of nonzero $(k-1)$-th powers. Let c_i be a value such that $c_i^{k-1}\equiv C_i \pmod p$, so that

$$\mathbb{Z}_p^* = c_1(\mathbb{Z}_p^*)^t \cup \cdots \cup c_t(\mathbb{Z}_p^*)^t.$$

Noting that $\chi_{\mathbb{O}}(x)=\chi_{\mathbb{E}}(-x)$, and that $x^k=C_ix$ for $x\in c_i(\mathbb{Z}_p^*)^t$, we have

$$\begin{aligned}
N_k &= \sum_x \chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Ax^k) = \sum_{i=1}^{t}\sum_{x\in c_i(\mathbb{Z}_p^*)^t}\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(AC_ix)\\
&= \frac{1}{t}\sum_{i=1}^{t}\sum_x\Big(\sum_{\psi^t=\psi_0}\psi(\overline{c_i}x)\Big)\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(AC_ix)\\
&= \frac{1}{t}\sum_{i=1}^{t}\sum_x\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(AC_ix) + \frac{1}{t}\sum_{\substack{\psi^t=\psi_0\\ \psi\neq\psi_0}}\sum_{i=1}^{t}\sum_x\psi(\overline{c_i}x)\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(AC_ix)\\
&= \frac{1}{t}\sum_{i=1}^{t}F(AC_i)+Error,
\end{aligned}$$

where $F(AC_i)$ is as defined in (1.5) and

$$Error=\frac{1}{t}\sum_{\substack{\psi^t=\psi_0\\ \psi\neq\psi_0}}\sum_{i=1}^{t}\sum_x\psi(\overline{c_i}x)\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(AC_ix). \tag{4.2}$$

Now for any nonzero b, C,

$$\begin{aligned}
\sum_x\psi(bx)\chi_{\mathbb{E}}(x)\chi_{\mathbb{E}}(Cx) &= \sum_x\Big(\sum_y a_{\mathbb{E}}(y)e_p(yx)\Big)\Big(\sum_z a_{\mathbb{E}}(z)e_p(zCx)\Big)\psi(bx)\\
&= \sum_y\sum_z a_{\mathbb{E}}(y)a_{\mathbb{E}}(z)G(y+Cz,b),
\end{aligned}$$

where $G(y+Cz,b)$ is the Gauss sum $G(y+Cz,b)=\sum_x e_p((y+Cz)x)\psi(bx)$, of modulus $\sqrt{p}$, unless $y+Cz=0$ in which case it vanishes. Thus we deduce from (2.4) that

$$\Big|\sum_x \psi(bx)\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx)\Big| \le \sqrt{p}\sum_y |a_{\mathbb{E}}(y)|\sum_z |a_{\mathbb{E}}(z)| \le \frac{1}{\pi^2}\log^2(5p)\sqrt{p},$$

$$|Error| \le (t-1)\frac{1}{\pi^2}\log^2(5p)\sqrt{p},$$

completing the proof of Theorem 1.4. ∎

Proof of Corollary 1.1. If t is even, so that -1 is a $(k-1)$-th power, then by pairing AC_i with $-AC_i$ and observing that $F(AC_i)+F(-AC_i)=(p-1)/2$ one gets $\frac{1}{t}\sum_{i=1}^t F(AC_i)=(p-1)/4$ and so

$$\left|N_k - \frac{p-1}{4}\right| \le \frac{1}{\pi^2}(t-1)\sqrt{p}\log^2(5p).$$

Suppose now that t is any positive integer. Using the Fourier expansion for $\chi_{\mathbb{E}}$ we have

$$F(C)=\sum_x \chi_{\mathbb{E}}(x)\chi_{\mathbb{E}}(-Cx)=\sum_y\sum_z a_{\mathbb{E}}(y)a_{\mathbb{E}}(z)\sum_x e_p(yx-Czx) \tag{4.3}$$

$$= pa_{\mathbb{E}}(0)^2 + p\sum_{z\neq 0} a_{\mathbb{E}}(z)a_{\mathbb{E}}(Cz) = \frac{(p-1)^2}{4p} + pG(C),$$

where

$$G(C) := \sum_{z\neq 0} a_{\mathbb{E}}(z)a_{\mathbb{E}}(Cz). \tag{4.4}$$

Thus

$$\frac{1}{t}\sum_{i=1}^t F(AC_i) = \frac{(p-1)^2}{4p} + \frac{p}{t}\sum_{i=1}^t G(AC_i), \tag{4.5}$$

and

$$\Big|\sum_{i=1}^t G(AC_i)\Big| \le \sum_{i=1}^t\sum_{z\neq 0}|a_{\mathbb{E}}(z)a_{\mathbb{E}}(AC_iz)| \le \sum_{z\neq 0}\sum_{u\neq 0}|a_{\mathbb{E}}(z)a_{\mathbb{E}}(u)|$$

$$\le \frac{1}{\pi^2}\log^2(5p).$$

By (4.5) and Theorem 1.4 we get

$$\left|N_k - \frac{(p-1)^2}{4p}\right| \le \frac{p}{\pi^2 t}\log^2(5p) + \frac{t-1}{\pi^2}\sqrt{p}\log^2(5p). \ ∎$$

5. Estimates for monomial and binomial exponential sums. In order to apply Theorem 1.1 we need estimates for monomial and binomial exponential sums. Several are available. In [12, Theorem 2.2] Cochrane and Pinner proved the following explicit monomial bounds:

LEMMA 5.1. *Suppose* $k \mid (p-1)$. *Put* $\lambda = 2/\sqrt[4]{3} = 1.51967\ldots$. *Then*

$$\Phi(k) \le \begin{cases} kp^{1/2}, & k < 3p^{1/3}, \\ \lambda k^{5/8}p^{5/8}, & 3p^{1/3} \le k < p^{1/2}, \\ \lambda k^{3/8}p^{3/4}, & p^{1/2} \le k < \frac{1}{3}p^{2/3}. \end{cases}$$

The first bound is just the classical bound for a Gauss sum, while the second two are due to Heath-Brown and Konyagin [18] (with a big-O). Next to each bound we have indicated the interval where the estimate is optimal. Konyagin [20] established further bounds of this type, nontrivial for k as large as $p^{3/4}$. There is also the recent ϵ-δ bound of Bourgain and Konyagin [7] and Bourgain, Glibichuk and Konyagin [6]: For any $\epsilon > 0$ there exists a $\delta > 0$ such that $\Phi(k) < p^{1-\delta}$ provided $d < p^{1-\epsilon}$. More recently Bourgain [4] has proved that

$$\Phi(k) < p^{1-\exp(-C\frac{\log p}{\log((p-1)/d)})}$$

for some absolute (undetermined) constant $C > 1$.

For binomials there is an abundance of bounds available; see [11] and [12] for a discussion. In particular, Cochrane and Pinner established [12, Theorem 3.1]:

LEMMA 5.2. *For any* $k \in \mathbb{Z}$,

$$\Phi(k, 1) \le (k-1, p-1) + 2.292p^{89/92}.$$

We readily deduce from Theorem 1.1:

THEOREM 5.1.

(a) *For any integer* k,

$$\left|N_k - \frac{p}{4}\right| \ll \begin{cases} d^{3/8}p^{3/4}\log p & \text{if } k \text{ is even}, \\ (d_1 + p^{89/92})\log^2 p & \text{if } k \text{ is odd}. \end{cases}$$

(b) *For any* $\epsilon > 0$ *there exists a* $\delta > 0$ *such that if* $d < p^{1-\epsilon}$ *then*

$$\left|N_k - \frac{p}{4}\right| < \begin{cases} p^{1-\delta} & \text{if } k \text{ is even}, \\ p^{1-\delta} + d_1\log^2 p & \text{if } k \text{ is odd}. \end{cases}$$

Proof. Inserting the third estimate of Lemma 5.1 and the estimate of Lemma 5.2 into Theorem 1.1 proves part (a) for k even, and for k odd yields

$$\left|N_k - \frac{p}{4}\right| \ll d^{3/8}p^{3/4}\log p + (d_1 + p^{89/92})\log^2 p.$$

If $d < p^{40/69}$ then the first term is $\le p^{89/92}\log p$ and we are done. If $d \ge p^{40/69}$ then $s < p^{29/69}$ and so by Theorem 1.3, for k odd,

$$\left|N_k - \frac{p}{4}\right| \ll s\sqrt{p}\log p < p^{127/138}\log p \ll p^{89/92}\log^2 p.$$

The ϵ-δ bound of Bourgain [3] for $\Phi(k)$ and Lemma 5.2 give part (b) in the same manner. ∎

6. Refinement of Theorem 5.1 for small d, d_1. In this section we obtain a slight improvement in the upper bound of Theorem 5.1. Let $\chi_{\mathbb{E}}$ be the characteristic function of $\mathbb{E}$ with Fourier expansion $\chi_{\mathbb{E}}(x) = \sum_{y=0}^{p-1} a_{\mathbb{E}}(y)e_p(yx)$. Noting that $\chi_{\mathbb{O}}(x) = \chi_{\mathbb{E}}(-x)$ we have

$$\begin{aligned}
N_k &= \sum_{x\neq 0}\chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Ax^k) = \sum_{x\neq 0}\chi_{\mathbb{E}}(x)\chi_{\mathbb{E}}(-Ax^k)\\
&= \sum_{x\neq 0}\sum_{u} a_{\mathbb{E}}(u)e_p(ux)\sum_{v} a_{\mathbb{E}}(v)e_p(-Avx^k)\\
&= \sum_{u}\sum_{v} a_{\mathbb{E}}(u)a_{\mathbb{E}}(v)\sum_{x\neq 0} e_p(ux - Avx^k)\\
&= (p-1)a_{\mathbb{E}}(0)^2 + a_{\mathbb{E}}(0)\sum_{u\neq 0} a_{\mathbb{E}}(u)\sum_{x\neq 0} e_p(ux)\\
&\quad + a_{\mathbb{E}}(0)\sum_{v\neq 0} a_{\mathbb{E}}(v)\sum_{x\neq 0} e_p(-Avx^k)\\
&\quad + \sum_{u\neq 0}\sum_{v\neq 0} a_{\mathbb{E}}(u)a_{\mathbb{E}}(v)\sum_{x\neq 0} e_p(ux - Avx^k)\\
&= (p-1)a_{\mathbb{E}}(0)^2 + a_{\mathbb{E}}(0)^2 + E_1 + E_2,
\end{aligned}$$

where

$$E_1 = a_{\mathbb{E}}(0)\sum_{v\neq 0} a_{\mathbb{E}}(v)\sum_{x\neq 0} e_p(-Avx^k),$$

$$E_2 = \sum_{u\neq 0}\sum_{v\neq 0} a_{\mathbb{E}}(u)a_{\mathbb{E}}(v)\sum_{x\neq 0} e_p(ux - Avx^k).$$

Now $a_{\mathbb{E}}(0) = |\mathbb{E}|/p = (p-1)/2p$, and so

$$pa_{\mathbb{E}}(0)^2 = \frac{(p-1)^2}{4p}.$$

If we proceed by using the bounds

$$|E_1| \le \frac{1}{2\pi}\log(5p)\Phi(k), \tag{6.1}$$

$$|E_2| \le \frac{1}{\pi^2}\log^2(5p)\Phi(k,1), \tag{6.2}$$

available by (2.4), then we just obtain

$$\left|N_k - \frac{p}{4}\right| \le \frac{1}{2} + \frac{1}{2\pi}\log(5p)\Phi(k) + \frac{1}{\pi^2}\log^2(5p)\Phi(k,1),$$

a bound already seen in Theorem 1.1.

We can save an extra $\sqrt{\log p}$ by using an alternate bound for E_2 that we shall derive below:

$$|E_2| \le \frac{1}{2^{1/4}\pi^{3/2}} p^{1/4}\mathbf{M}^{1/4}\log^{3/2}(5p), \tag{6.3}$$

where

$$\mathbf{M} = \#\{(x_1,x_2,x_3,x_4) \in (\mathbb{Z}_p^*)^4 : x_1+x_2 = x_3+x_4,\ x_1^k+x_2^k = x_3^k+x_4^k\}, \tag{6.4}$$

yielding

Proposition 6.1.

$$\left|N_k - \frac{p}{4}\right| \le \frac{1}{2} + \frac{1}{2\pi}\log(5p)\Phi(k) + \frac{1}{2^{1/4}\pi^{3/2}} p^{1/4}\mathbf{M}^{1/4}\log^{3/2}(5p). \tag{6.5}$$

Corollary 6.1. *Let $d = (k, p-1)$ and $d_1 = (k-1, p-1)$. If $d, d_1 < 1.68(p-1)^{16/23}$ then*

$$\left|N_k - \frac{p}{4}\right| \le \frac{1}{2} + \frac{1}{2\pi}\log(5p)\Phi(k) + 0.346041 p^{89/92}\log^{3/2}(5p).$$

Proof. Theorem 7.1 of [12] gives the estimate $\mathbf{M} \le 27.57(p-1)^{66/23}$ provided that $d, d_1 < 1.68(p-1)^{16/23}$. The corollary is now immediate from the proposition. ∎

Proof of Proposition 6.1. It suffices to establish (6.3). To do this we follow the method of [5]. Let $a(y) = a_{\mathbb{E}}(y)$. Then

$$\begin{aligned} |E_2| &\le \sum_{u\ne 0}\sum_{v\ne 0} |a(u)a(v)| \Big|\sum_{x\ne 0} e_p(ux - Avx^k)\Big| \\ &= \sum_{u'\ne 0}\sum_{v'\ne 0} \beta(u',v')\Big|\sum_{x\ne 0} e_p(u'x + v'x^k)\Big|, \end{aligned}$$

where $\beta(u',v') = \frac{1}{p-1}\sum_{x\ne 0}|a(xu')a(A_1x^kv')|$ and $A_1A \equiv -1 \pmod p$. Next, from Hölder's inequality,

$$\begin{aligned} |E_2| &\le \Big(\sum_{u'}\sum_{v'}\Big|\sum_{x\ne 0} e_p(u'x+v'x^k)\Big|^4\Big)^{1/4} \\ &\quad\times \Big(\sum_{u'\ne 0}\sum_{v'\ne 0}\beta(u',v')\Big)^{1/2}\Big(\sum_{u'\ne 0}\sum_{v'\ne 0}\beta(u',v')^2\Big)^{1/4} \\ &= E_3^{1/4}E_4^{1/2}E_5^{1/4}, \end{aligned} \tag{6.6}$$

say. Clearly, $E_3 = p^2\mathbf{M}$, with $\mathbf{M}$ as in (6.4). Next, using (2.4),

$$\begin{aligned} E_4 &= \sum_{u'\neq 0}\sum_{v'\neq 0}\beta(u',v') = \frac{1}{p-1}\sum_{x\neq 0}\sum_{u'\neq 0}\sum_{v'\neq 0}|a(xu')a(A_1x^kv')| \\ &= \sum_{u\neq 0}\sum_{v\neq 0}|a(u)a(v)| \le \frac{1}{\pi^2}\log^2(5p). \end{aligned}$$

Finally, for E_5 we have

$$\begin{aligned} E_5 &= \sum_{u'\neq 0}\sum_{v'\neq 0}\beta(u',v')^2 \\ &= \frac{1}{(p-1)^2}\sum_{x\neq 0}\sum_{y\neq 0}\sum_{u'\neq 0}\sum_{v'\neq 0}|a(xu')a(A_1x^kv')|\,|a(yu')a(A_1y^kv')| \\ &= \frac{1}{p-1}\sum_{\substack{1\le u_1,u_2,v_1,v_2<p\\ (v_1/v_2)\equiv(u_1/u_2)^k \,(\mathrm{mod}\, p)}}|a(u_1)a(v_1)|\,|a(u_2)a(v_2)| \\ &= \frac{1}{p-1}\sum_{1\le u_1,u_2,j<p}|a(u_1)a(ju_1^k)|\,|a(u_2)a(ju_2^k)| \\ &= \frac{1}{p-1}\sum_{1\le u_1,u_2<p}|a(u_1)a(u_2)|\sum_j|a(ju_1^k)a(ju_2^k)|. \end{aligned}$$

Using the Cauchy–Schwarz inequality, the Parseval identity

$$\sum_y |a(y)|^2 = \frac{1}{p}\sum_x \chi_{\mathbb{E}}^2(x) = \frac{p-1}{2p}$$

and (2.4) we obtain

$$\begin{aligned} E_5 &\le \frac{1}{p-1}\sum_{1\le u_1,u_2<p}|a(u_1)a(u_2)|\sum_j|a(j)|^2 = \frac{1}{2p}\sum_{1\le u_1,u_2<p}|a(u_1)a(u_2)| \\ &\le \frac{1}{2\pi^2 p}\log^2(5p). \end{aligned}$$

Thus, by (6.6) and the estimates for E_3, E_4 and E_5,

$$\begin{aligned} |E_2| &\le (p^2\mathbf{M})^{1/4}\left(\frac{1}{\pi^2}\log^2(5p)\right)^{1/2}\left(\frac{1}{2\pi^2 p}\log^2(5p)\right)^{1/4} \\ &\le \frac{1}{2^{1/4}\pi^{3/2}}p^{1/4}\mathbf{M}^{1/4}\log^{3/2}(5p). \ \blacksquare \end{aligned}$$

7. Proof of Theorem 1.5. For any integer C with $p \nmid C$, let $\mathcal{L}_C$ denote the lattice of integer points satisfying $y \equiv Cx \pmod p$, so that

$$G(C) = \sum_{\substack{(x,y)\in\mathcal{L}_C \\ 0<\max(|x|,|y|)<p/2}} a_{\mathbb{E}}(x)a_{\mathbb{E}}(y),$$

where $G(C)$ is as defined in (4.4). Let $|(x,y)|_0 = \max(|x|,|y|)$,

$$\lambda_C = \min\{|(x,y)|_0 : (x,y) \in \mathcal{L}_C,\ (x,y) \neq (0,0)\},$$

and let (x_C, y_C) denote a minimal point in $\mathcal{L}_C$ with $|(x_C,y_C)|_0 = \lambda_C$. Put $\lambda_i = \lambda_{AC_i}$, $1 \le i \le t$, where the C_i are as in (4.1), and let (x_i,y_i) be a primitive point in $\mathcal{L}_{AC_i}$ with $|(x_i,y_i)|_0 = \lambda_i$. By a *primitive point* in a lattice we mean a point with $\gcd(x_i,y_i) = 1$. Reorder the C_i so that $\lambda_1 \le \cdots \le \lambda_t$. In particular, $\lambda_1 = 1$ if and only if $AC_1 = \pm 1$, in which case we can take $(x_1,y_1) = (1,\pm 1)$. Let δ_C denote the discrepancy as in (1.7).

LEMMA 7.1. *If $\mathcal{L}_C$ has a primitive point (x_0,y_0) with $|(x_0,y_0)|_0 < \sqrt{p/2}$ then any other point in $\mathcal{L}_C$ with $|(x,y)|_0 < \sqrt{p/2}$ is a multiple of (x_0,y_0). In particular, $(x_0,y_0) = \pm(x_C,y_C)$.*

Proof. We have $y_0 \equiv Cx_0 \pmod p$ and $y \equiv Cx \pmod p$ and so $y_0x \equiv x_0y \pmod p$. But $|y_0x - x_0y| < p$ and so $y_0x - x_0y = 0$. The result follows from the assumption that (x_0,y_0) is primitive. ∎

Using the formula [5, Section 2] $a_{\mathbb{E}}(x) = -\frac{1}{p}e^{-\pi xi/p}\frac{\sin(\pi x/p)}{\sin(2\pi x/p)}$, one has

$$|a_{\mathbb{E}}(x)| = \frac{1}{p}\left|\frac{\sin(\pi x/p)}{\sin(2\pi x/p)}\right| \le \frac{1}{p}\,\frac{1}{|\sin(2\pi x/p)|}.$$

Then from the inequality $|\sin(\pi x)| \ge 2|x|$ for $|x| < 1/2$, we get

$$|a_{\mathbb{E}}(\overline{2}x)| \le \frac{1}{2|x|} \quad \text{for } 0 < |x| < p/2,$$

where $\overline{2}$ denotes the multiplicative inverse of 2 (mod p). We break $\mathcal{L}_C$ into two sets: the multiples of (x_C,y_C), and the remaining points (x,y) all of which satisfy $|x| \ge \sqrt{p/2}$ or $|y| \ge \sqrt{p/2}$ by Lemma 7.1. Thus

$$(7.1)\quad |G(C)| \le \sum_{\substack{(x,y)\in\mathcal{L}_C \\ 0<\max(|x|,|y|)<p/2}} |a_{\mathbb{E}}(\overline{2}x)|\,|a_{\mathbb{E}}(\overline{2}y)| \le \frac{1}{4} \sum_{\substack{(x,y)\in\mathcal{L}_C \\ 0<\max(|x|,|y|)<p/2}} \frac{1}{|xy|}$$

$$\le \frac{1}{2|x_Cy_C|}\sum_{l=1}^{\infty}\frac{1}{l^2} + \frac{1}{4}\sum_{\substack{(x,y)\in\mathcal{L}_C \\ \sqrt{p/2}\le|y|<p/2}} \frac{1}{\sqrt{p/2}\,|x|} + \frac{1}{4}\sum_{\substack{(x,y)\in\mathcal{L}_C \\ \sqrt{p/2}\le|x|<p/2}} \frac{1}{\sqrt{p/2}\,|y|}$$

$$\le \frac{\pi^2}{12|x_Cy_C|} + \frac{\sqrt{2}\log p}{\sqrt{p}}.$$

We immediately deduce from (4.3):

LEMMA 7.2. *For any integer C with $p \nmid C$ we have*

$$\left|F(C) - \frac{p}{4}\right| \le \frac{\pi^2 p}{12|x_C y_C|} + \sqrt{2p}\log p + \frac{1}{2},$$

where, as above, (x_C, y_C) is the minimal nonzero point of the lattice $\mathcal{L}_C$.

LEMMA 7.3. *Let $\delta_1 = \delta_{AC_1} = F(AC_1) - p/4$. Then*

$$\left|\frac{1}{t}\sum_{i=1}^{t} F(AC_i) - \left(\frac{p}{4} + \frac{\delta_1}{t}\right)\right| < \frac{\pi^2}{12}\,\frac{p}{t}\sum_{i=2}^{t}\frac{1}{|x_i y_i|} + \sqrt{2p}\log p + \frac{1}{2}.$$

Proof. By Lemma 7.2 we have

$$\begin{aligned}(7.2)\qquad \frac{1}{t}\sum_{i=1}^{t} F(AC_i) &= \frac{1}{t}F(AC_1) + \frac{1}{t}\sum_{i=2}^{t} F(AC_i)\\ &= \left(\frac{p}{4} + \frac{\delta_1}{t}\right) + \theta_1\frac{\pi^2 p}{12t}\sum_{i=2}^{t}\frac{1}{|x_i y_i|} + \theta_2\sqrt{2p}\log p + \frac{\theta_3}{2}\end{aligned}$$

for some $|\theta_i| \le 1$. ∎

As a consequence of Theorem 1.4 and Lemma 7.3 we have

$$(7.3)\qquad \left|N_k - \left(\frac{p}{4} + \frac{\delta_1}{t}\right)\right| \ll \frac{p}{t}\sum_{i=2}^{t}\frac{1}{|x_i y_i|} + t\sqrt{p}\log^2 p.$$

We are left with considering the distribution of the values $|x_i y_i|$. The following lemma is motivated by the ideas in Section 6 of Bombieri, Bourgain and Konyagin [2].

LEMMA 7.4. *Suppose that t is odd.*

(a) *Let $2 \le b < (p/2)^{1/4}$. The number of t-th roots of unity C with $1 \le |x_C y_C| \le b$ is at most $(t-1)\,[\log(p/2)/2\log b]^{-1} + 1$.*
(b) *Let $2 \le b < (p/2)^{1/8}$. The number of values i with $1 \le |x_i y_i| \le b$ is at most $(t-1)\,[\log(p/2)/4\log b]^{-1} + 1$.*

If t is even the same results hold with $+2$ in place of the $+1$.

Proof. (a) Suppose that C is such a value with $2 \le |x_C y_C| \le b$. We assume here that $x_C > 0$. Then for any positive integer n such that $|(x_C^n, y_C^n)|_0 \le |x_C y_C|^n < \sqrt{p/2}$, the point (x_C^n, y_C^n) is a primitive point in the lattice $\mathcal{L}_{C^n}$ satisfying the condition of Lemma 7.1, and so $(x_C^n, y_C^n) = (x_{C^n}, y_{C^n})$. Note that the values C^n are distinct t-th roots of unity by Lemma 7.1. Now if powers from two different C_1, C_2 coincide, $(x_{C_1}^r, y_{C_1}^r) = (x_{C_2}^s, y_{C_2}^s)$ say, then $(x_{C_1}, y_{C_1}) = (x^{s/\gcd(r,s)}, \pm y^{s/\gcd(r,s)})$, $(x_{C_2}, y_{C_2}) = (x^{r/\gcd(r,s)}, \pm y^{r/\gcd(r,s)})$ for some $x, y \in \mathbb{N}$ (and appropriate $\pm$ signs). Writing $\gcd(r,s) = as + br$

gives $(x, \pm y) = (x_{C_3}, y_{C_3})$ where $C_3 = C_1^a C_2^b$ (for an appropriate $\pm$ sign). Thus both (x_{C_1}, y_{C_1}) and (x_{C_2}, y_{C_2}) are powers of (x_{C_3}, y_{C_3}) (since t is odd the $\pm$ sign is decided by the power) with plainly $|x_{C_3} y_{C_3}| \le b$.

We may suppose then that the (x_C, y_C) with $2 \le |x_C y_C| \le b$ consist of powers (g_i^j, h_i^j), $j = 1, \dots, u_i$, of a basic set of (g_i, h_i), $i = 1, \dots, v$, all of whose powers are distinct. Hence if there are N values of C with $2 \le |x_C y_C| \le b$ then

$$N = \sum_{i=1}^{v} u_i = \sum_{i=1}^{v} \left[\frac{\log b}{\log |g_i h_i|} \right],$$

while the number of (x_C, y_C) with $|x_C y_C| < \sqrt{p/2}$ arising from taking powers of the (g_i, h_i) is $\sum_{i=1}^{v} \left[\frac{\log \sqrt{p/2}}{\log |g_i h_i|} \right]$. Hence

$$\begin{aligned} t - 1 &\ge \sum_{i=1}^{v} \left[\frac{\log \sqrt{p/2}}{\log |g_i h_i|} \right] = \sum_{i=1}^{v} \left[\frac{\log \sqrt{p/2}}{\log b} \frac{\log b}{\log |g_i h_i|} \right] \\ &\ge \sum_{i=1}^{v} \left[\frac{\log \sqrt{p/2}}{\log b} \right] \left[\frac{\log b}{\log |g_i h_i|} \right] = N \left[\frac{\log \sqrt{p/2}}{\log b} \right]. \end{aligned}$$

The result follows on including $C = 1$.

For even t the argument is similar except that the values occur in pairs $(x_C^n, \pm y_C^n)$.

(b) Suppose that (x_i, y_i), $i = 1, \dots, N$, are the minimal points satisfying $1 \le |x_i y_i| \le b$. By definition, $y_i \equiv A C_i x_i \pmod p$. Then $x_1 y_i \equiv (C_i/C_1) x_i y_1 \pmod p$ where C_i/C_1 is a t-th root of unity. After removing any common factor from $(x_1 y_i, x_i y_1)$, plainly $1 \le |x_{C_i/C_1} y_{C_i/C_1}| \le b^2$. The result now follows from part (a). ∎

Lemma 7.5.

(a) *If $t > 1$ is odd and $C \ne 1$ is a t-th root of unity modulo p, then $\lambda_C > (p/t)^{1/(t-1)}$.*

(b) *If $t > 1$ is odd then $\lambda_2 \ge (p/t)^{1/2(t-1)}$.*

Proof. (a) Any point $(x, y) \in \mathcal{L}_C$ must satisfy $x^t \equiv y^t \pmod p$ with $x \not\equiv y \pmod p$ and so

$$x^{t-1} + x^{t-2} y + \cdots + x y^{t-2} + y^{t-1} \equiv 0 \pmod p.$$

Since the form on the left-hand side is positive definite (for odd t) the sum is at least p and the result follows.

(b) Suppose that $\lambda_1 \le \lambda_2 \le (p/t)^{1/2(t-1)}$. Then as we observed above $\lambda_{C_1/C_2} \le (p/t)^{1/(t-1)}$, contradicting part (a). ∎

LEMMA 7.6. *If $t > 1$ is odd, then*

$$\sum_{i=2}^{t} \frac{1}{|x_i y_i|} \le \frac{8(t-1)}{\log(p/2)} \frac{\log(\lambda_2^2 e)}{\lambda_2} \ll \begin{cases} \dfrac{t}{\log p} & \text{always,} \\ \dfrac{1}{p^{1/2(t-1)}} & \text{if } t \ll \log p. \end{cases}$$

Proof. Writing

$$m_j = |\{i \ge 2 : |x_i y_i| = j\}|$$

we first note that for $x \ge \lambda_2$,

$$C(x) := \sum_{j \le x} m_j \le \frac{8(t-1)}{\log(p/2)} \log(\lambda_2 x).$$

For $\lambda_2 x \ge (p/2)^{1/8}$ this follows from the trivial bound $C(x) \le t-1$. For $\lambda_2 x < (p/2)^{1/8}$ we use the fact that $[z] \ge z/2$ for $z \ge 1$ to get $[\log(p/2)/4\log(\lambda_2 x)] \ge \frac{1}{2}\log(p/2)/4\log(\lambda_2 x)$ and so by Lemma 7.4(b),

$$C(x) \le C(\lambda_2 x) \le \frac{t-1}{\left[\frac{\log(p/2)}{4\log(\lambda_2 x)}\right]} \le \frac{8(t-1)}{\log(p/2)} \log(\lambda_2 x).$$

(The +1 in Lemma 7.4(b) can be omitted since, on this interval, $|x_1 y_1| \le \lambda_2 x$ but $C(\lambda_2 x)$ does not count $|x_1 y_1|$.) Applying partial summation we have

$$\begin{aligned} \sum_{i=2}^{t} \frac{1}{|x_i y_i|} &= \sum_{j=\lambda_2}^{\infty} \frac{m_j}{j} = \int_{\lambda_2}^{\infty} \frac{C(u)}{u^2}\, du \\ &\le \frac{8(t-1)}{\log(p/2)} \int_{\lambda_2}^{\infty} \frac{\log(\lambda_2 u)}{u^2}\, du = \frac{8(t-1)}{\log(p/2)} \frac{\log(\lambda_2^2 e)}{\lambda_2}. \end{aligned}$$

The first upper bound in the lemma is immediate since $\log(\lambda_2^2 e)/\lambda_2 < 1.2$. For the second inequality we use the lower bound for λ_2 in Lemma 7.5(b) to get $\lambda_2 \ge 3^{-1/4} p^{1/2(t-1)}$ (for $t \ge 3$), with this value at least 3 for $t-1 < 0.36 \log p$, and hence $\log(\lambda_2^2 e)/\lambda_2 \ll \log(p^{1/2(t-1)})/p^{1/2(t-1)}$ for $t - 1 \le 0.36 \log p$.

Finally, we note that the two bounds are the same for $t \approx \log p$. ∎

We immediately deduce Theorem 1.5 from (7.3) and Lemma 7.6.

8. Proof of Theorem 1.2. (a) Suppose k is odd and t is even. If $p < 10^{27}$ then we have trivially

$$\left| N_k - \frac{p}{4} \right| \le \frac{p}{4} < 0.35 p^{89/92} \log^{3/2}(5p). \tag{8.1}$$

If $s < (0.35)(2\pi) p^{43/92} \log^{1/2}(5p)$ then by Theorem 1.3(b),

$$\left| N_k - \frac{p}{4} \right| \le \frac{s-1}{2\pi} \sqrt{p} \log(5p) < 0.35 p^{89/92} \log^{3/2}(5p),$$

while if $t < (0.35)\pi^2 p^{43/92}\log^{-1/2}(5p)$, then by Corollary 1.1,

$$\left|N_k - \frac{p}{4}\right| \le \frac{t-1}{\pi^2}\sqrt{p}\log^2(5p) < 0.35p^{89/92}\log^{3/2}(5p).$$

Thus we may assume that $p \ge 10^{27}$, $d < 0.454729p^{49/92}/\log^{1/2}(5p)$ and $d_1 < 0.28949p^{49/92}\log^{1/2}(5p)$. Using the upper bound $\Phi(k) \le \lambda d^{3/8}p^{3/4}$ (Lemma 5.1) we obtain, from Corollary 6.1,

$$\begin{aligned}\left|N_k - \frac{p}{4}\right| &< 0.5 + 0.18p^{699/736}\log^{13/16}(5p) + 0.346041p^{89/92}\log^{3/2}(5p)\\ &< 0.35p^{89/92}\log^{3/2}(5p)\end{aligned}$$

for $p \ge 10^{27}$.

(b) Suppose next that k is odd and t is odd. By Theorem 1.3,

$$\left|N_k - \frac{p}{4}\right| \ll s\sqrt{p}\log p.$$

By Theorem 1.1 and the bounds $\Phi(k) \ll d^{3/8}p^{3/4}$, $\Phi(k,1) \ll d_1 + p^{89/92}$,

$$\left|N_k - \frac{p}{4}\right| \ll d^{3/8}p^{3/4}\log p + (d_1 + p^{89/92})\log^2 p.$$

Using the first inequality if $d > p^{6/11}$ and the second if $d \le p^{6/11}$ we obtain

$$\left|N_k - \frac{p}{4}\right| \ll (d_1 + p^{89/92})\log^2 p$$

uniformly for odd k. If $d_1 < p^{89/92}$ we keep this inequality. If $d_1 \ge p^{89/92}$ we apply Theorem 1.5(a), and the trivial bound $|\delta_1| \le p/4$, to get

$$\left|N_k - \frac{p}{4}\right| \ll \frac{|\delta_1|}{t} + \frac{p}{\log p} + p^{3/92}\sqrt{p}\log^2 p \ll d_1 + \frac{p}{\log p}. \ \blacksquare$$

9. Estimates for $F(C)$ and the discrepancy δ_C. Recall that $F(C)$ is the number of even residues x such that Cx is odd,

$$F(C) = \sum_x \chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Cx),$$

and the discrepancy δ_C equals $F(C) - p/4$. We can also talk about the complementary function $H(C) = F(-C)$, the number of even residues x such that Cx is even. The following statements are evident:

$$\begin{aligned}F(-C) &= \frac{p-1}{2} - F(C),\\ F(-1) &= \frac{p-1}{2}, \quad F(1) = 0,\\ F(\overline{C}) &= F(C),\end{aligned} \tag{9.1}$$

where $\overline{C}$ denotes the multiplicative inverse of $C \pmod p$.

LEMMA 9.1.

(a) *For any nonzero integer C with $|C|$ even,*

$$\left|F(C) - \frac{p}{4}\right| < \frac{|C|+1}{2}. \tag{9.2}$$

(b) *For any integer C with $|C|$ odd,*

$$\left|F(C) - \left(1 - \frac{1}{C}\right)\frac{p}{4}\right| < \frac{|C|}{2} + \frac{3}{4}. \tag{9.3}$$

Proof. We shall prove the corresponding statements for $H(C)$. The statements are trivial if $|C| \geq p/2$ so we may assume that $|C| < p/2$. Moreover, from the identity $H(-C) = (p-1)/2 - H(C)$, it suffices to consider the case where $1 \leq C < p/2$. Then $H(C)$ is the number of values of $n \in \{1, \dots, (p-1)/2\}$ such that $2jp \leq 2nC < (2j+1)p$, that is, $jp/C \leq n < jp/C + p/2C$ for some j with $0 \leq j \leq [(C-1)/2]$. Thus

$$H(C) = \sum_{j=0}^{[(C-1)/2]} \left[\frac{jp}{C} + \frac{p}{2C}\right] - \left[\frac{jp}{C}\right]. \tag{9.4}$$

Using $[y] \leq [x] - [x-y] \leq [y] + 1$, we have

$$\left[\frac{p}{2C}\right]\left[\frac{C+1}{2}\right] \leq H(C) \leq \left(\left[\frac{p}{2C}\right] + 1\right)\left[\frac{C+1}{2}\right], \tag{9.5}$$

and so

$$\left|H(C) - \frac{p}{4}\right| < \frac{C}{2}, \qquad 1 < C < \frac{p}{2},\ C \text{ even}, \tag{9.6}$$

$$\left|H(C) - \left(1 + \frac{1}{C}\right)\frac{p}{4}\right| < \frac{C}{2} + \frac{1}{4}, \quad 1 < C < \frac{p}{2},\ C \text{ odd}. \tag{9.7}$$ ∎

COROLLARY 9.1. *Suppose that $t > 1$ is odd, $t \ll \log p$, and that for some t-th root of unity C_i, $AC_i \equiv m \pmod p$, where m is an odd number satisfying $|m| < (p/t)^{1/2(t-1)}$. Then $\left|\delta_1 + \frac{p}{4m}\right| < \frac{|m|}{2} + \frac{3}{4}$ and*

$$\left|N_k - \left(1 - \frac{1}{mt}\right)\frac{p}{4}\right| \ll \frac{p^{1-\frac{1}{2(t-1)}}}{t}.$$

In particular $N_k \sim \left(1 - \frac{1}{mt}\right)\frac{p}{4}$, with $N_k - \frac{p}{4} \sim -\frac{p}{4mt}$ provided that $m = o(p^{1/2(t-1)})$.

Proof. Suppose that $AC_i \equiv m \pmod p$ where m is an odd number satisfying $|m| < (p/t)^{1/2(t-1)}$. Since $(1, m) \in \mathcal{L}_m$ we have $\lambda_{AC_i} = \lambda_m = |m| < (p/t)^{1/2(t-1)}$. But then by Lemma 7.5, $\lambda_2 > \lambda_{AC_i}$. Therefore $\lambda_1 = \lambda_{AC_i}$

and so by (9.3) we obtain

$$\left|\delta_1 + \frac{p}{4m}\right| = \left|F(m) - \left(1 - \frac{1}{m}\right)\frac{p}{4}\right| \le \frac{|m|}{2} + \frac{3}{4}.$$

The result then follows from Theorem 1.5(b). ∎

EXAMPLE 9.1. Suppose A is an odd number with $|A| < (p/t)^{1/2(t-1)}$ and $t \ll \log p$. Then the hypotheses of the corollary hold with $C_i = 1$, $m = A$ and so we get $N_k \sim \left(1 - \frac{1}{At}\right)\frac{p}{4}$.

EXAMPLE 9.2. Let t be a positive odd integer such that $3^t - 1$ has a prime factor p with $p > \sqrt{3^t - 1}$. Then p is such that $\operatorname{ord}_p(3) = t$, where t is an odd value with $t := l \log_3 p$ for some l with $1 < l < 2$. Set $A = -1$. The t-th roots of unity modulo p are just $\{1, 3, 3^2, \dots, 3^{t-1}\}$. For $0 \le i < t/2$ we have, by (9.3),

$$\left|F(-3^i) - \left(1 + \frac{1}{3^i}\right)\frac{p}{4}\right| < \frac{3^i}{2} + \frac{3}{4},$$

while for $i > t/2$ we have, by (9.1) and the fact that $3^t \equiv 1 \pmod p$,

$$F(-3^i) = F(-\overline{3}^i) = F(-3^{t-i}).$$

Thus

$$\begin{aligned}\frac{1}{t}\sum_{i=1}^{t} F(AC_i) &= \frac{1}{t}\sum_{i=0}^{t-1} F(-3^i) = \frac{1}{t}\left[F(-1) + 2\sum_{i=1}^{(t-1)/2} F(-3^i)\right] \\ &= \frac{1}{t}\left[\frac{p-1}{2} + 2\sum_{i=1}^{(t-1)/2}\left\{\left(1 + \frac{1}{3^i}\right)\frac{p}{4} + \theta_i\left(\frac{3^i}{2} + \frac{3}{4}\right)\right\}\right] \\ &= \frac{1}{t}\left[\frac{p}{2} - \frac{1}{2} + \frac{p}{4}(t-1) + \frac{p}{6}\left(\frac{3}{2} - \epsilon\right) + \theta 3^{(t-1)/2}\left(\frac{3}{2} - \epsilon\right) + \frac{3}{4}\theta t\right],\end{aligned}$$

where $\epsilon := \frac{1}{2}\frac{1}{3^{(t-3)/2}} < \frac{3^{3/2}}{2\sqrt{p}}$ and $|\theta|, |\theta_i| < 1$. Thus,

$$\left|\frac{1}{t}\sum_{i=1}^{t} F(AC_i) - \left(1 + \frac{2}{t}\right)\frac{p}{4}\right| \le \frac{1}{t}\frac{3}{2}\cdot 3^{(t-1)/2} + \frac{3}{4} + \frac{\sqrt{3}}{4}\frac{\sqrt{p}}{t} < \frac{2p^{l/2}}{t},$$

and by Theorem 1.4,

$$\left|N_k - \left(1 + \frac{2}{t}\right)\frac{p}{4}\right| \ll \frac{p^{l/2}}{t} + \sqrt{p}\log^3 p.$$

On the other hand, $\delta_1 = p/4 - 1/2$, and so Theorem 1.5(a) shows that $|N_k - (1 + 1/t)p/4| \ll p/\log p$. This apparent discrepancy in the asymptotic estimate is explained by the fact that in this example $p/t \approx p/l\log_3 p$, the same order of magnitude as the error term in Theorem 1.5(a). In particular we see that the error estimate in Theorem 1.5(a) cannot be improved.

10. The Erdős–Turán inequality and proof of Theorem 2.1. The discrepancy of a finite sequence $S = (x_1, \dots, x_N)$ of real numbers is given by

$$D_N(x_1, \dots, x_N) := \sup_{I=[\alpha,\beta)\subset[0,1)} \Big| \frac{1}{N} \sum_{i=1}^{N} \chi_I(\{x_i\}) - (\beta - \alpha) \Big|.$$

The Erdős–Turán inequality states that there exist absolute constants c_1, c_2 such that for any positive integer H,

$$ND_N(x_1, \dots, x_N) \le \frac{c_1 N}{H+1} + c_2 \sum_{h=1}^{H} \frac{1}{h} \Big| \sum_{n=1}^{N} e(hx_n) \Big|.$$

Kuipers and Niederreiter [21] obtained the admissible pair $(c_1, c_2) = (6, 4/\pi)$, Montgomery [24] the pair $(c_1, c_2) = (1, 3)$, Mauduit, Rivat and Sárközy [23] the pair $(c_1, c_2) = (1, 1)$ and Rivat and Tenenbaum [26] the pairs $(c_1, c_2) = (1, 0.6528)$, $(c_1, c_2) = (1.1435, 2/\pi)$, among others. The latter authors also proved that any such pair must satisfy $c_1 \ge 1$ and $c_2 \ge 2/\pi$. Here we obtain these optimal constants, but in a slightly weaker form of the inequality. If we restrict to intervals I of length $1/2$, as in our applications, the constants can be reduced further.

THEOREM 10.1. *Let $(x_1, \dots, x_N)$ be a sequence of real numbers and H a positive integer. Put $\Phi = \max_{1\le h\le H} |\sum_{n=1}^{N} e(hx_n)|$.*

(a) *If $I = [\alpha, \beta]$ is an interval in $[0, 1]$ then*

$$\Big| \sum_{n=1}^{N} \chi_I(\{x_n\}) - N|I| \Big| \le \frac{N}{H+1} + \frac{2}{\pi}(\log H + \gamma + \pi/2)\Phi,$$

where $\gamma = 0.57721\dots$ is Euler's constant.

(b) *If $|I| = 1/2$ then*

$$\Big| \sum_{n=1}^{N} \chi_I(\{x_n\}) - \frac{N}{2} \Big| \le \frac{N}{H+1} + \frac{1}{\pi}(\log H + \gamma + \pi + \log 2)\Phi.$$

Proof. The results follow readily from an inequality of Vaaler [28, Theorem 20, (8.3)], which reads

$$\Big| \sum_{n=1}^{N} \chi_I(\{x_n\}) - N|I| \Big|$$
$$\le \frac{N}{H+1} + 2 \sum_{h=1}^{H} \Big(|\sin \pi h|I|| \frac{\hat{J}(h/(H+1))}{\pi h} + \frac{\hat{K}(h/(H+1))}{H+1} \Big) \Big| \sum_{n=1}^{N} e(hx_n) \Big|,$$

where by [28, (2.28),(2,29)],

$$\hat{J}(t) = \pi t(1 - |t|)\cot(\pi t) + |t|, \qquad \hat{K}(t) = (1 - |t|) \tag{10.1}$$

for $0 < |t| < 1$. Setting $m = H + 1$, and observing that $0 < \hat{J}(t) < 1$ for $0 < t < 1$, we obtain

$$\begin{aligned}
&\Big|\sum_{n=1}^{N} \chi_I(\{x_n\}) - N|I|\Big| \\
&\qquad \le \frac{N}{m} + 2\sum_{h=1}^{m-1}\left(\frac{1}{\pi h} + \frac{1-h/m}{m}\right)\Phi \\
&\qquad = \frac{N}{m} + 2\Phi\left(\frac{1}{\pi}\left(\log(m-1) + \gamma + \int_{m-1}^{\infty} \frac{\{u\}}{u^2}\,du\right) + \frac{1}{2}\,\frac{m-1}{m}\right) \\
&\qquad = \frac{N}{m} + \frac{2\Phi}{\pi}\left(\log(m-1) + \gamma + \frac{\pi}{2} + E_1\right),
\end{aligned}$$

with

$$E_1 \le \frac{1}{m-1} - \frac{\pi}{2m} < 0$$

for $m \ge 3$ (and $E_1 = 1 - \gamma - \pi/4 < 0$ for $m = 2$), giving (a).

If $|I| = 1/2$ then using the fact that $\sin(\pi h|I|) = 0$ for even h, the sum $\sum_{h=1}^{m-1} 1/h$ can be replaced by

$$\begin{aligned}
\sum_{\substack{h=1\\ h\text{ odd}}}^{m-1} \frac{1}{h} &= \sum_{h=1}^{m-1} \frac{1}{h} - \sum_{h=1}^{[(m-1)/2]} \frac{1}{2h} \\
&= \frac{1}{2}\log\left(\frac{(m-1)^2}{[(m-1)/2]}\right) + \frac{1}{2}\gamma + \int_{m-1}^{\infty} \frac{\{u\}}{u^2}\,du - \frac{1}{2}\int_{[(m-1)/2]}^{\infty} \frac{\{u\}}{u^2}\,du \\
&\le \frac{1}{2}\left(\log(m-1) + \gamma + \log 2\right) + \frac{1}{2(m-1)} + \frac{1}{2}\log\left(\frac{\frac{1}{2}(m-1)}{\left[\frac{1}{2}(m-1)\right]}\right)
\end{aligned}$$

and thus

$$\left|\sum_{n=1}^{N} \chi_I(\{x_n\}) - \frac{N}{2}\right| \le \frac{N}{m} + \frac{\Phi}{\pi}\left(\log(m-1) + \gamma + \log 2 + \pi + E_2\right),$$

with

$$E_2 = \frac{1}{m-1} + \log\left(\frac{\frac{1}{2}(m-1)}{\left[\frac{1}{2}(m-1)\right]}\right) - \frac{\pi}{m}.$$

The bound (b) follows since $E_2 < 0$ for $m \ge 3$ (and the bound is worse than the trivial bound $N/2$ for $m = 2$, i.e. $H = 1$). ∎

Proof of Theorem 2.1. Let $(x_1 + (p), \dots, x_N + (p))$ be a sequence in $\mathbb{Z}_p$ with $x_i \in \mathbb{Z}$. We simply apply Theorem 10.1 to the sequence of reals $(x_1/p, \dots, x_N/p)$. For any interval $I = \{a+1, \dots, a+M\}$ in $\mathbb{Z}_p$ and $0 < \delta < 1$

there is a corresponding interval $I' = [(a+\delta)/p, (a+M+1-\delta)/p]$ in $\mathbb{R}/\mathbb{Z}$ of length $|I'| = (M+1-2\delta)/p$. So we have

$$\Big|\sum_{n=1}^{N} \chi_I(x_n) - N|I'|\Big| = \Big|\sum_{n=1}^{N} \chi_{I'}(\{x_n/p\}) - N|I'|\Big|.$$

For the first inequality we take $\delta \to 1$, $|I'| \to (M-1)/p$ and $\delta \to 0$, $|I'| \to (M+1)/p$ to obtain the stated upper and lower bounds respectively for $\sum_{n=1}^{N} \chi_I(x_n)$. When $M = \frac{1}{2}(p-1)$ or $\frac{1}{2}(p+1)$ we can take $\delta = 1/4$ or $3/4$ giving $|I'| = 1/2$ and the second inequality. The results are now immediate, upon observing that the value Φ in Theorem 10.1 satisfies $\Phi \le \Phi_S$. ∎

11. A trigonometric sum of Vinogradov. In this section we discuss the estimation of the Vinogradov sum

$$\sum_{y=1}^{p-1} |a_I(y)| = \frac{1}{p} \sum_{y=1}^{p-1} \Big| \frac{\sin(\pi M y/p)}{\sin(\pi y/p)} \Big|,$$

which was needed in Sections 2, 4 and 6. As before, the $a_I(y)$ are the Fourier coefficients of the characteristic function of an interval $I \subset \mathbb{Z}_p$ with $|I| = M$.

LEMMA 11.1. *For any prime p and interval I we have*

$$\sum_{y=1}^{p-1} |a_I(y)| \le \frac{4}{\pi^2} \log p + 0.35 \le \frac{4}{\pi^2} \log(3p). \tag{11.1}$$

The estimate is a slight improvement on the upper bound given in [9, Theorem 1].

Proof. The bound is trivial for $M = p$ so we may assume $1 \le M < p$. Cochrane and Peral [10, Proposition] obtained the asymptotic formula

$$\begin{aligned} \frac{1}{p} \sum_{y=1}^{p-1} \Big| \frac{\sin(\pi M y/p)}{\sin(\pi y/p)} \Big| \\ = \frac{4}{\pi^2} \left(\log(4p/\pi) + \gamma\right) + \frac{8}{\pi^2} \sum_{\substack{j=1 \\ p \nmid j}}^{\infty} \frac{\log|\sin(\pi j M/p)|}{4j^2 - 1} + E'(p, M), \end{aligned} \tag{11.2}$$

where γ is Euler's constant and

$$E'(p, M) = E(p, M) - \frac{8}{\pi^2} (\log(4p/\pi) + \gamma) \sum_{p \mid j} \frac{1}{4j^2 - 1},$$

with

$$\frac{-4}{\pi^2 p} \le E(p, M) \le \frac{1}{3\pi^2} \sum_{p \nmid j} \frac{1}{R(jM)^2 (4j^2 - 1)} + \frac{4}{\pi^2 p}.$$

Here $R(jM) = \min_{l\in\mathbb{Z}} |jM - lp|$. Using the trivial bound $R(jM) \geq 1$ we have

$$E'(p,M) \leq E(p,M) \leq \frac{1}{6\pi^2} + \frac{4}{\pi^2 p} \leq .018$$

for $p > 364$. Since the sum over j in the asymptotic formula is plainly negative, one obtains the result of the lemma (checking small p on a computer). ∎

For certain length intervals, the contribution from the sum over j in (11.2) gives an extra savings on the main term. For instance, when $M = (p \pm 1)/2$ we get

LEMMA 11.2. *For* $M = \frac{1}{2}(p \pm 1)$,

$$\sum_{y=1}^{p-1} |a_I(y)| = \frac{1}{p}\sum_{y=1}^{p-1} \left|\frac{\sin(\pi My/p)}{\sin(\pi y/p)}\right| = \frac{1}{\pi}\log p + C + E,$$

with

$$C = \frac{1}{\pi}\log\left(\frac{8e^\gamma}{\pi}\right) = 0.481261\ldots, \qquad -\frac{0.822}{p} < E < -\frac{0.192}{p}.$$

Numerical checking shows that the minimum value of $E = E(p)$ occurs at $p = 3$, and so we have uniformly $E \geq E(3) = -\pi^{-1}\log(24e^{\gamma-2\pi/3}/\pi) = -0.1642\ldots$.

Proof. Rather than appeal to the asymptotic formula above, we give a direct proof. Since

$$|\sin(\pi My/p)| = \begin{cases} |\cos(\pi y/2p)| & \text{if } y \text{ is odd,} \\ |\sin(\pi y/2p)| & \text{if } y \text{ is even,} \end{cases}$$

we have

$$\sum_{y=1}^{p-1} |a_I(y)| = \frac{2}{p}\sum_{y=1}^{(p-1)/2} \left|\frac{\sin(\pi My/p)}{\sin(\pi y/p)}\right| \tag{11.3}$$

$$= \frac{1}{p}\sum_{\substack{y=1 \\ y \text{ odd}}}^{(p-1)/2} \frac{1}{\sin(\pi y/2p)} + \frac{1}{p}\sum_{\substack{y=1 \\ y \text{ even}}}^{(p-1)/2} \frac{1}{\cos(\pi y/2p)}.$$

Writing $m_2 = \lfloor \frac{1}{4}(p+1) \rfloor$, we have, see [10, Lemma 1],

$$\frac{1}{p}\sum_{\substack{y=1 \\ y \text{ odd}}}^{(p-1)/2} \frac{1}{(\pi y/2p)} = \frac{2}{\pi}\sum_{k=1}^{m_2} \frac{1}{2k-1} = \frac{1}{\pi}\log p + \frac{\gamma}{\pi} + E_1,$$

with

$$\frac{1}{\pi}\log\left(\frac{m_2}{p/4}\right) \leq E_1 \leq \frac{1}{\pi}\log\left(\frac{m_2}{p/4}\right) + \frac{1}{24\pi m_2^2}.$$

In order to estimate the sums in (11.3) we first note the following. If $0 \le \delta \le 1$ and $f(x)$ is a positive and increasing function on $(1/2, m+\delta)$ then plainly

$$\int_{1/2}^{1} f(u)\,du \le f(1) \le \int_{1/2}^{2} f(u)\,du,$$
$$\int_{j-1}^{j} f(u)\,du \le f(j) \le \int_{j}^{j+1} f(u)\,du, \qquad j = 2, \dots, m-1,$$

and

$$\int_{m-1}^{m+\delta} f(u)\,du - \delta f(m+\delta) \le f(m) \le \int_{m}^{m+\delta} f(u)\,du + (1-\delta) f(m+\delta),$$

giving

$$-\delta f(m+\delta) \le \sum_{j=1}^{m} f(j) - \int_{1/2}^{m+\delta} f(u)\,du \le (1-\delta) f(m+\delta). \tag{11.4}$$

Similarly if $f(x)$ is positive and increasing on $(0, m+\delta)$ then

$$\int_{0}^{1} f(u)\,du \le f(1) \le \int_{0}^{2} f(u)\,du - f(0)$$

and

$$-\delta f(m+\delta) \le \sum_{j=1}^{m} f(j) - \int_{0}^{m+\delta} f(u)\,du \le -f(0) + (1-\delta) f(m+\delta). \tag{11.5}$$

Since $1/\sin u - 1/u$ is increasing on $(0, \pi)$, applying (11.4) with $f(x) = \frac{1}{\sin(\pi(2x-1)/2p)} - \frac{1}{\pi(2x-1)/2p}$ and $\delta = \frac{p}{4} + \frac{1}{2} - m_2$, we therefore have

$$\begin{aligned}
&\frac{1}{p} \sum_{\substack{y=1 \\ y \,\mathrm{odd}}}^{(p-1)/2} \left(\frac{1}{\sin(\pi y/2p)} - \frac{1}{\pi y/2p} \right) \\
&\qquad = \frac{1}{p} \sum_{k=1}^{m_2} \left(\frac{1}{\sin(\pi(2k-1)/2p)} - \frac{1}{\pi(2k-1)/2p} \right) \\
&\qquad = \frac{1}{p} \int_{1/2}^{p/4+1/2} \left(\frac{1}{\sin(\pi(2x-1)/2p)} - \frac{1}{\pi(2x-1)/2p} \right) dx + E_2 \\
&\qquad = \frac{1}{\pi} \log\left(\frac{8}{\pi}(\sqrt{2}-1) \right) + E_2,
\end{aligned}$$

with

$$-\frac{1}{p}\Big(\sqrt{2}-\frac{4}{\pi}\Big)\Big(\frac{1}{2}+\frac{p}{4}-m_2\Big) < E_2 < \frac{1}{p}\Big(\sqrt{2}-\frac{4}{\pi}\Big)\Big(m_2+1-\Big(\frac{1}{2}+\frac{p}{4}\Big)\Big).$$

Similarly, writing $m_1 = \lfloor \frac{1}{4}(p-1)\rfloor$, since $1/\cos x$ is increasing on $(0,\pi/2)$, applying (11.5) with $f(x) = \frac{1}{\cos(\pi x/p)}$ and $\delta = \frac{p}{4} - m_1$, we get

$$\frac{1}{p}\sum_{\substack{y=1\\ y\,\text{even}}}^{(p-1)/2}\frac{1}{\cos(\pi y/2p)} = \frac{1}{p}\sum_{l=1}^{m_1}\frac{1}{\cos(\pi l/p)} = \frac{1}{p}\int_0^{p/4}\frac{1}{\cos(\pi x/p)}\,dx + E_3$$
$$= \frac{1}{\pi}\log(\sqrt{2}+1) + E_3,$$

with

$$-\frac{\sqrt{2}}{p}\Big(\frac{p}{4}-m_1\Big) < E_3 < -\frac{1}{p}+\frac{\sqrt{2}}{p}\Big(m_1+1-\frac{p}{4}\Big).$$

Hence

$$\sum_{y=1}^{p-1}|a_I(y)| = \frac{1}{\pi}\log p + \frac{\gamma}{\pi} + \frac{1}{\pi}\log\Big(\frac{8}{\pi}(\sqrt{2}-1)\Big) + \frac{1}{\pi}\log(\sqrt{2}+1) + E,$$

where

$$\begin{aligned} E &= E_1 + E_2 + E_3 \\ &\le \frac{1}{\pi}\log\Big(\frac{m_2}{p/4}\Big) + \frac{1}{24\pi m_2^2} + \frac{1}{p}\Big(\sqrt{2}-\frac{4}{\pi}\Big)\Big(m_2+\frac{1}{2}-\frac{p}{4}\Big) \\ &\quad -\frac{1}{p}+\frac{\sqrt{2}}{p}\Big(m_1+1-\frac{p}{4}\Big) \\ &= -\Big(1+\frac{2}{\pi}-\sqrt{2}\Big)\frac{1}{p} \\ &\quad + \begin{cases} \frac{1}{\pi}(\log(1-1/p)+1/p) + \frac{2}{3\pi(p-1)^2} & \text{if } p\equiv 1 \pmod 4, \\ \frac{1}{\pi}(\log(1+1/p)-1/p) + \frac{2}{3\pi(p+1)^2} & \text{if } p\equiv 3 \pmod 4, \end{cases} \\ &< -\frac{0.192}{p}. \end{aligned}$$

Similarly

$$E \ge \frac{1}{\pi}\log\left(\frac{m_2}{p/4}\right) - \frac{1}{p}\left(\sqrt{2}-\frac{4}{\pi}\right)\left(\frac{p}{4}+\frac{1}{2}-m_2\right) - \frac{\sqrt{2}}{p}\left(\frac{p}{4}-m_1\right)$$
$$= -\left(\sqrt{2}-\frac{2}{\pi}\right)\frac{1}{p} + \begin{cases} \frac{1}{\pi}(\log(1-1/p)+1/p) & \text{if } p \equiv 1 \pmod 4, \\ \frac{1}{\pi}(\log(1+1/p)-1/p) & \text{if } p \equiv 3 \pmod 4, \end{cases}$$
$$> -\frac{0.822}{p}. \ \blacksquare$$

References

[1] G. Bachman and L. Rachakonda, *On a problem of Dobrowolski and Williams and the Pólya–Vinogradov inequality*, Ramanujan J. 5 (2001), 65–71.

[2] E. Bombieri, J. Bourgain and S. V. Konyagin, *Roots of polynomials in subgroups of $\mathbb{F}_p^*$ and applications to congruences*, Int. Math. Res. Notices 2009, 802–834.

[3] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc. 18 (2005), 477–499.

[4] —, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, Geom. Funct. Anal. 18 (2009), 1477–1502.

[5] J. Bourgain, T. Cochrane, J. Paulhus and C. Pinner, *Decimations of l-sequences and permutations of even residues mod p*, SIAM J. Discrete Math. 23 (2009), 842–857.

[6] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) 73 (2006), 380–398.

[7] J. Bourgain and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C. R. Math. Acad. Sci. Paris 337 (2003), 75–80.

[8] J. Bourgain, E. Lindenstrauss, P. Michel and A. Venkatesh, *Some effective results for $\times a \times b$*, Ergodic Theory Dynam. Systems 29 (2009), 1705–1722.

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

[10] T. Cochrane and J. C. Peral, *An asymptotic formula for a trigonometric sum of Vinogradov*, ibid. 91 (2001), 1–19.

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

[12] —, —, *Explicit bounds on monomial and binomial exponential sums*, preprint, 2009.

[13] H. Furstenberg, *Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation*, Math. Systems Theory 1 (1967), 1–49.

[14] M. Goresky and A. Klapper, *Arithmetic crosscorrelations of feedback with carry shift register sequences*, IEEE Trans. Inform. Theory 43 (1997), 1342–1345.

[15] M. Goresky, A. Klapper and R. Murty, *On the distinctness of decimations of ℓ-sequences*, in: Sequences and Their Applications (Bergen, 2001), T. Helleseth et al. (eds.), Discrete Math. Theor. Comput. Sci., Springer, London, 2002, 197–208.

[16] M. Goresky, A. Klapper, R. Murty and I. Shparlinski, *On decimations of ℓ-sequences*, SIAM J. Discrete Math. 18 (2004), 130–140.

[17] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Problem Books in Math., Springer, New York, 2004.

[18] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Quart. J. Math. 51 (2000), 221–235.

[19] A. Hildebrand, *On the constant in the Pólya–Vinogradov inequality*, Canad. Math. Bull. 31 (1988), 347–352.

[20] S. V. Konyagin, *Estimates for trigonometric sums over subgroups and for Gauss sums*, in: IV Internat. Conf. "Modern Problems of Number Theory and Its Applications": Current Problems, Part III (Tula, 2001), Mekh.-Mat. Fak. Mosk. Gos. Univ. im. Lomonosova, Moscow, 2002, 86–114 (in Russian).

[21] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Pure Appl. Math., Wiley-Interscience, New York, 1974.

[22] S. R. Louboutin, J. Rivat and A. Sárközy, *On a problem of D. H. Lehmer*, Proc. Amer. Math. Soc. 135 (2007), 969–975.

[23] C. Mauduit, J. Rivat and A. Sárközy, *On the pseudo-random properties of n^c*, Illinois J. Math. 46 (2002), 185–197.

[24] H. L. Montgomery, *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, CBMS Reg. Conf. Ser. Math. 84, Amer. Math. Soc., Providence, RI, 1994.

[25] H. L. Montgomery, R. C. Vaughan and T. D. Wooley, *Some remarks on Gauss sums associated with kth powers*, Math. Proc. Cambridge Philos. Soc. 118 (1995), 21–33.

[26] J. Rivat et G. Tenenbaum, *Constantes d'Erdős–Turán*, Ramanujan J. 9 (2005), 111–121.

[27] I. E. Shparlinski, *On a generalised Lehmer problem for arbitrary powers*, East-West J. Math. 2008, Special Vol., 197–204.

[28] J. D. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc. (N.S.) 12 (1985), 183–216.

[29] Y. Yi and W. P. Zhang, *On the generalization of a problem of D. H. Lehmer*, Kyushu J. Math. 56 (2002), 235–241.

[30] W. Zhang, *On a problem of D. H. Lehmer and its generalization*, Compos. Math. 86 (1993), 307–316.

Jean Bourgain
School of Mathematics
Institute of Advanced Study
Princeton, NJ 08540, U.S.A.
E-mail: Bourgain@math.ias.edu

Todd Cochrane
Jennifer Paulhus
Christopher Pinner
Department of Mathematics
Kansas State University
Manhattan, KS 66506, U.S.A.
E-mail: cochrane@math.ksu.edu
pinner@math.ksu.edu

Current address of Jennifer Paulhus:
Department of Mathematical Sciences
Villanova University
800 Lancaster Avenue, SAC305
Villanova, PA 19085-1699, U.S.A.
E-mail: jennifer.paulhus@villanova.edu

Received on 15.2.2010
and in revised form on 19.7.2010 (6307)