RESIDUE RACES

Andrew Granville, Daniel Shiu and Peter Shiu

1. Introduction

Given a prime p and distinct non-zero integers $a_1, a_2, \dots, a_k \pmod p$, we investigate the number $N = N(a_1, a_2, \dots, a_k; p)$ of residues $n \pmod p$ for which

$$(na_1)_p < (na_2)_p < \cdots < (na_k)_p, \tag{1.1}$$

where $(b)_p$ is the least non-negative residue of $b \pmod p$. If $k = 2$ then $N = (p-1)/2$, since $(na_1)_p < (na_2)_p$ if and only if $(-na_1)_p > (-na_2)_p$.

The first non-trivial case is when $k = 3$. Since there are $3! = 6$ ways to order the residues $(na_1)_p, (na_2)_p, (na_3)_p$, one may expect that $N \approx p/6$ for most choices of a_1, a_2, a_3; this is indeed the case, as we will see later. However the value for N can differ from $p/6$ quite significantly, and we have the following rather simple lemma.

Lemma 1.1. *If $a_2 \equiv a_1 + a_3 \pmod p$ then $N(a_1, a_2, a_3; p) = 0$.*

Proof. First note that $(na_1)_p + (na_3)_p \equiv (na_2)_p \pmod p$. Since $0 < (na_i)_p < p$ for each i, we have $-p < (na_1)_p + (na_3)_p - (na_2)_p < 2p$. Therefore either $(na_1)_p + (na_3)_p = (na_2)_p$ in which case $(na_1)_p, (na_3)_p < (na_2)_p$; or $(na_1)_p + (na_3)_p = (na_2)_p + p$ in which case $(na_1)_p, (na_3)_p > (na_2)_p$ since each $(na_i)_p < p$. In neither case do we have $(na_1)_p < (na_2)_p < (na_3)_p$ so $N(a_1, a_2, a_3; p) = 0$.

It turns out that, for $k = 3$, we have $N > 0$ whenever $a_2 \not\equiv a_1 + a_3 \pmod p$ (see [3]), but we have no proof which is both simple and elementary. Our proof here is based on the use of Dedekind sums, which also shows that

$$\left[\frac{p+1}{12}\right] \le N(a_1, a_2, a_3; p) \le \left[\frac{p}{3}\right] \tag{1.2}$$

if $a_2 \not\equiv a_1 + a_3 \pmod p$. When $k = 4$, there are other conditions under which $N = 0$, and we find that if $N(a_1, a_2, a_3, a_4; p) > 0$ then

$$\left[\frac{p}{21}\right] - \left[\frac{p}{22}\right] \le N(a_1, a_2, a_3, a_4; p) \le \left[\frac{p}{4}\right]. \tag{1.3}$$

The first author is a Presidential Faculty Fellow. He is also supported, in part, by the National Science Foundation.

Typeset by $\mathcal{AMS}$-TEX

The bounds in (1.2) and (1.3) are sharp, and we also give asymptotic formulae for N (in terms of the a_i). Explicitly evaluating these formulae appears to be rather complicated in general: we conjecture that

$$N(a_1, \dots, a_k; p) \le \left[\frac{p}{k}\right], \qquad k = 3, 4, \dots \tag{1.4}$$

noting that the upper bound is attained when each $a_i = i$; we have proved $N \le [2p/(k+1)]$ for all p and k, and also that for all $k \ge 42$ we have $N \le [p/k]$ if p is sufficiently large. One can easily show that $N \sim p/k!$ as $p \to \infty$ for "almost all" choices of $a_1, a_2, \dots, a_k$. Our main concern here is to understand the *spectrum* of possible values of N when $k = 3$ and 4; our methods give little for $k \ge 5$.

2. Asymptotic formulae for $N(\mathbf{a}, p)$, and a reciprocity rule.

It will be convenient to let $\mathbf{a}$ represent the vector with components $a_1, \dots, a_k$. For a given vector $\mathbf{a} = (a_1, \dots, a_k)$, we let $\mathbf{b} = (b_0, \dots, b_k)$ be given by $b_0 \equiv -a_k \pmod p$ and $b_j \equiv a_j - a_{j-1} \pmod p$ for $j = 1, 2, \dots, k$, with $a_0 = 0$. Thus

$$b_0 + b_1 + \cdots + b_k \equiv 0 \pmod p, \tag{2.1}$$

and we let $M(\mathbf{b}; p)$ be the number of residues $n \pmod p$ for which

$$(b_0 n)_p + (b_1 n)_p + \cdots + (b_k n)_p = p. \tag{2.2}$$

The next result simplifies our calculations since it is easier to deal with the equation (2.2) than with the inequalities (1.1).

Lemma 2.1. *We have $N(\mathbf{a}; p) = M(\mathbf{b}; p)$.*

Proof. If we have a solution to (1.1) then $p > (a_j n)_p > (a_{j-1} n)_p > 0$ so that $p > (a_j n)_p - (a_{j-1} n)_p > 0$, and $(a_j n)_p - (a_{j-1} n)_p \equiv (b_j n)_p \pmod p$, and hence $(a_j n)_p - (a_{j-1} n)_p = (b_j n)_p$. Thus $(b_1 n)_p + \cdots + (b_k n)_p = (a_k n)_p$ and so (2.2) is satisfied.
In the other direction, we define $a_j = b_j + b_{j-1} + \cdots + b_1$ for each $j, 1 \le j \le k$. Then $(a_j n)_p \equiv (b_j n)_p + \cdots + (b_1 n)_p \pmod p$ and, by (2.2), $0 < (a_j n)_p, (b_j n)_p + \cdots + (b_1 n)_p < p$, so they are equal. Thus $(a_j n)_p = (a_{j-1} n)_p + (b_j n)_p > (a_{j-1} n)_p$, so we have (1.1).

In order to state our results concerning $N(\mathbf{a}; p)$, we define a function $\theta = \theta_p$ as follows. Given integers $u, v \pmod p$, select $a, b \pmod p$ with $|a| + |b|$ minimal such that $a/b \equiv u/v \pmod p$, and then let $\theta_p(u, v) = 1/ab$. We remark that if $|u|, |v| < \sqrt{p/2}$ then $\theta_p(u, v) = (u, v)^2/uv$. The following is our main result.

Theorem A. *Let $k = 3$ and let $\mathbf{b} = (b_0, b_1, b_2, b_3)$ be associated with $\mathbf{a}$. Then*

$$N(\mathbf{a}; p) = \frac{p}{6} + \frac{p}{12} \sum_{0 \le i < j \le 3} \theta_p(b_i, b_j) + O(\sqrt{p}). \tag{2.3}$$

Similarly, for $k = 4$, we have

$$N(\mathbf{a}; p) = \frac{p}{24} + \frac{p}{24} \sum_{0 \le i < j \le 4} \theta_p(b_i, b_j) + O(\sqrt{p}). \tag{2.4}$$

The error term "$O(\sqrt{p})$" may be replaced by "$O(\max_i |a_i|)$". In section 5b these error terms are given explicitly in terms of Dedekind sums when the b_i are all prime. This inspired a certain *Reciprocity Rule for Residue Races*:
Let $b_0, \ldots, b_k$ be pairwise coprime, nonzero integers which sum to 0, and then define $M_\ell(b_0, \ldots, b_k; b) = \#\{n : \ 1 \le n \le b-1, \ \text{ for which } (b_0 n)_b + \cdots + (b_k n)_b = \ell b\}$ for positive integers ℓ and b; and $M_\ell(\mathbf{b}; -b) = -M_\ell(\mathbf{b}; b)$. Then

$$\sum_{i=0}^{k} M_\ell(\mathbf{b}; b_i) = \begin{cases} 1 & \text{if } \#\{i : \ b_i > 0\} \le \ell < \#\{i : \ b_i < 0\} \\ -1 & \text{if } \#\{i : \ b_i < 0\} \le \ell < \#\{i : \ b_i > 0\} \\ 0 & \text{otherwise.} \end{cases} . \tag{2.5}$$

In our case we have $\ell = 1$ so the above gives:

$$\sum_{i=0}^{k} M(\mathbf{b}; b_i) = \begin{cases} 1 & \text{if } \#\{i : \ b_i > 0\} = 1 \\ -1 & \text{if } \#\{i : \ b_i < 0\} = 1 \\ 0 & \text{otherwise.} \end{cases} .$$

From Theorem A (and a weak generalization) we deduce

Corollary 1. *Fix integer $k \ge 3$. Let $\eta(p) \to \infty$ as $p \to \infty$. We have*

$$N(\mathbf{a}; p) \sim p/k!$$

for all but at most $O(p^{k-1}\eta(p))$ of the $\sim p^k$ choices of residues $\mathbf{a} \mod p$. On the other hand $N(\mathbf{a}; p) = 0$ for $\gtrsim (k-2)p^{k-1}$ choices of distinct non-zero residues $\mathbf{a} \pmod p$.

Two challenges arise: Determine all $\mathbf{a} \mod p$ for which $N(\mathbf{a}; p) = 0$; and, since $N(\mathbf{a}; p)$ can take values other than 0 and $\sim p/k!$, determine the spectrum of possible values, and the accumulation points of this spectrum. We met both challenges for $k = 3$ and 4, but not for larger k.

3. Spectra for $k = 3$, $k = 4$ and beyond

$N(\mathbf{a};p)$ can take values other than 0 and $\sim p/k!$. Our main interest in this paper is to investigate the spectrum of possible values, and the accumulation points of the spectrum, for $k = 3$ and 4. (Our methods do not yield much for larger k).
Since $(an)_p = p\{\frac{an}{p}\}$, (1.1), and equivalently (2.2), can be rewritten as

$$\{a_1 t\} < \{a_2 t\} < \cdots < \{a_k t\} \tag{3.1}$$

$$\{b_0 t\} + \{b_1 t\} + \ldots + \{b_k t\} = 1 \tag{3.2}$$

where $t = n/p$. Let $\nu(a_1, a_2, \dots, a_k)$ be the measure of the set T of $t \in [0, 1)$ for which (3.1), or equivalently (3.2), holds. A simple argument (see section 3c) gives that

$$N(a_1, \dots, a_k; p) = \nu(a_1, \dots a_k)p + O\left(\sum_{i=1}^{k} |a_i|\right). \tag{3.3}$$

Without loss of generality one can assume that the a_i are not too large (by Lemma 4.2 below), and so the "spectrum" of values of $N(\mathbf{a}; p)/p$ is more-or-less given by the "spectrum" of values of $\nu(\mathbf{a})$, when p is large. This is what we will study in section 10 below.

In section 3c we show that $N(\mathbf{a}; p) = 0$ whenever $\nu(\mathbf{a}) = 0$. Moreover, if $\nu(\mathbf{a}) \neq 0$ and $p \geq L := LCM[b_0, b_1, \dots, b_k]$ then $N(\mathbf{a}; p) > 0$. This suggests that to study when $N(\mathbf{a}; p) = 0$ we need to classify when $\nu(\mathbf{a}) = 0$. One can interpret this geometrically as asking which vectors $\mathbf{t} \in \mathbb{T}^k$ (where $\mathbb{T}$ is the torus $\mathbb{R}/\mathbb{Z}$) of the form $t(a_1, a_2, \dots, a_k)$, $t \in [0, 1)$, never intersect the region $t_1 < t_2 < \cdots < t_k$? We have been unable to find elementary criteria describing the a_i that satisfy this.

The results that we do have can be summarized as follows:

3a. The spectrum for $k = 3$.

$M(b_0, b_1, b_2, b_3; p) = 0$ if and only if some proper subset of the b_is sums to zero.

If $M(\mathbf{b}; p) > 0$ then $M(\mathbf{b}; p) \geq [(p + 1)/12]$. Equality holds for the races

$$\{1 \leq n \leq p-1 :\ n < (-n)_p < (3n)_p\} = \left(\frac{p}{4}, \frac{p}{3}\right), \quad \text{when } p \equiv \pm 1, \pm 5 \pmod{12};$$

$$\{1 \leq n \leq p-1 :\ n < (-2n)_p < (4n)_p\} = \left(\frac{p}{6}, \frac{p}{4}\right), \quad \text{when } p \equiv \pm 1, \pm 7 \pmod{12}.$$

Also, $M(\mathbf{b}; p) \leq [p/3]$ and equality holds for the race

$$\{1 \leq n \leq p-1 :\ n < (2n)_p < (3n)_p\} = \left(0, \frac{p}{3}\right).$$

Notice the surprising fact that if $M(\mathbf{b}; p)$ is non-zero then it is quite large. This can be reinterpreted as stating that $1/3 \geq \nu(\mathbf{a}) \geq 1/12$, so long as $\nu(\mathbf{a}) \neq 0$; and that these bounds are sharp since $\nu(1, 2, 3) = 1/3$ and $\nu(1, -2, 4) = 1/12$. Moreover, Corollary 1 implies that $\nu(\mathbf{a}) = 1/6$ "almost always". In section 10a we show that the spectrum of values taken by $\nu(\mathbf{a})$ is discrete, though there are accumulation points at 0, 1/6 and all numbers of the form $1/6 + 1/12d$ with d an integer other than 0 or -1, and nowhere else. The largest accumulation point is 1/4 and the only numbers in the spectrum $\geq 1/4$ are 1/4 itself and the numbers of the form $(1/4)(1 + 1/d)$ with $d \geq 3$ odd. The smallest accumulation point, other than 0, is 1/8 and the only numbers in the spectrum $\leq 1/8$ are 1/8 itself and the numbers of the form $(1/8)(1 - 1/d)$ with $d \geq 1$ odd.

3b. The spectrum for $k = 4$.

$M(\mathbf{b}; p) = 0$ if and only if the b_is satisfy the hypothesis of Lemmas 6.1 or 6.2, or belong to the list in section 10b. If $M(\mathbf{b}; p) > 0$ then $M(\mathbf{b}; p) \geq [p/21] - [p/22] = p/462 + O(1)$. Equality holds for the race

$$\{1 \leq n \leq p-1 :\ (3n)_p < (10n)_p < (-n)_p < (21n)_p\} = \left(\frac{p}{22}, \frac{p}{21}\right).$$

Also, $M(\mathbf{b};p) \leq [p/4]$ and equality holds for the race

$$\{1 \leq n \leq p-1 : \; n < (2n)_p < (3n)_p < (4n)_p\} = \Big(0, \frac{p}{4}\Big).$$

We can re-interpret this as $1/4 \geq \nu(\mathbf{a}) \geq 1/462$, so long as $\nu(\mathbf{a}) \neq 0$. Moreover, we know that $\nu(\mathbf{a})= 1/24$ "almost always". The spectrum of values is again discrete, and the accumulation points are described in section 10b. The smallest elements of the spectrum are, in ascending order,

$$\frac{1}{462}, \frac{1}{420}, \frac{1}{390}, \frac{1}{336}, \frac{1}{330}, \frac{1}{312}, \frac{1}{308}, \frac{1}{288}, \frac{1}{286}, \frac{1}{273}, \frac{1}{270}, \frac{1}{266}, \frac{1}{264}, \frac{1}{260}, \frac{1}{255}, \frac{1}{252}.$$

3c. Calculating the spectrum.

Define $\beta(t) := [b_0 t] + [b_1 t] + \cdots + [b_k t]$, so that (3.2) is equivalent to $\beta(t) = -1$, since each $\{b_i t\} = b_i t - [b_i t]$. Thus $\nu(\mathbf{a})$ is the measure of the set $t \in [0,1)$ for which $\beta(t) = -1$. Now $\beta(t)$ is fixed on intervals for which each $[b_i t]$ is fixed; and $[b_i t]$ only changes value at rationals of the form k/b_i. Therefore T is a collection of subintervals of $[0,1)$, where each subinterval is of the form $[r/L, s/L]$ with $L := LCM[b_0, b_1, \ldots, b_k]$, and so $L\nu(\mathbf{a})$ is an integer. The number of values of $n/p \in [r/L, s/L]$ is $p(s-r)/L + O(1)$. Moreover if $p(s-r)/L \geq 1$ we are guaranteed such an n, so if $\nu(\mathbf{a}) > 0$ and $p \geq L$ then $N(\mathbf{a}) \geq 1$ as claimed above.

The number of intervals in T is no more than half the number of values of t for which $\{b_i t\} = 0$ for some i, which is $\leqq \sum |b_i| \leqq 2 \sum |a_i|$; this gives (3.3).

Now if $\nu(\mathbf{a}) = 0$ then $T = \emptyset$ so that (3.1), and thus (1.1), is never satisfied, and so $N(\mathbf{a}) = 0$ as claimed above.

This description of ν lends itself to an easy way to compute the value of $\nu(\mathbf{a})$: Let $t_0 = 0 < t_1 < \cdots < t_r = 1$, be the sequence of fractions of the form $j/|b_i|$ with $0 \leq j \leq |b_i|$ and $0 \leq i \leq k$, put in ascending order. Then $\nu(\mathbf{a})$ is the sum of the measure of those intervals $(t_\ell, t_{\ell+1})$ for which $\beta(t) = -1$. Since $\beta(t)$ remains constant on each such interval, we need only evaluate it at one point in the interval. Therefore

$$\nu(a_1, \ldots, a_k) = \sum_{\substack{0 \leq \ell \leq r-1 \\ \beta((t_\ell + t_{\ell+1})/2) = -1}} (t_{\ell+1} - t_\ell). \tag{3.4}$$

3d. The spectrum for $k = 5$.

The methods used to determine the spectra of $\nu(\mathbf{a})$ for $k = 3$ and 4, do not work for $k \geq 5$ (because we would need to be able to simply evaluate higher order Dedekind sums as in (5.2) below which are, for now, somewhat mysterious). However we can, via direct computation of values of $\nu(\mathbf{a})$ using (3.4), see what seems likely for $k = 5$. The largest element of the spectrum we found was 1/5 as predicted. The smallest nonzero element found was $\nu(211, 199, 203, 210, 225) = 1/47475$.

3e. The spectrum for arbitrary k.
We have shown that the largest element of the spectrum is $1/k$ for $k = 2, 3, 4$ and ≥ 42 (in section 9), justifying our conjecture that the answer is always 1/k. This should surely have a straightforward geometric proof: As at the beginning of section 3, one can interpret this geometrically as the question: Show that the total length of the segments of the line $t(a_1, a_2, \dots, a_k)$, $t \in [0, 1)$ inside the region $t_1 < t_2 < \cdots < t_k$ is always $\leq 1/k$. This puts one in mind of an old open problem of Poincaré (see e.g. [1]): Find the maximal intersection in $\mathbb{R}^k$ of a degree d curve with the unit sphere. Even the $k = d = 2$ problem is non-trivial (see the 2001 Putnam exam, question A6).
We have shown that the smallest non-zero elements of the spectra are $1/2, 1/12, 1/462, \leq 1/47475$ for $k = 2, 3, 4, 5$, respectively. We have no idea what to predict should happen in general!

4. Dedekind sums and exponential sums

We need a characteristic function on the set of residues n satisfying (1.1), and we find the use of Dedekind sums the most suitable for this purpose. Let

$$S(u_1, u_2, \dots, u_k; p) = \sum_{n=1}^{p-1} \psi\left(\frac{u_1 n}{p}\right) \psi\left(\frac{u_2 n}{p}\right) \cdots \psi\left(\frac{u_k n}{p}\right),$$

where $\psi(t) = \{t\} - \frac{1}{2}$ for $t \notin \mathbb{Z}$, and $\psi(n) = 0$ for $n \in \mathbb{Z}$. Note that the value of the sum is 0 if k is odd, since the n and $-n$ terms cancel, as ψ is an odd function. Another observation is that, by considering residue systems, $S(gu_1, gu_2, \dots, gu_k; p) = S(u_1, \dots, u_k; p)$ if $(g, p) = 1$. Lying much deeper is Rademacher's remarkable 'reciprocity law' [4]: If a, b and c are pairwise coprime positive integers then

$$S(a, b; c) + S(c, a; b) + S(b, c; a) = \frac{-1}{4} + \frac{1}{12}\left(\frac{a}{bc} + \frac{b}{ac} + \frac{c}{ab}\right). \tag{4.1}$$

This has subsequently been generalized in many different directions, and it implies the following: If $a + b + c \equiv 0 \pmod{p}$ and $p \not| abc$ then

$$S(a, b; p) + S(a, c; p) + S(b, c; p) = \frac{1}{4} - \frac{1}{4p}. \tag{4.2}$$

A byproduct of our work here leads to a new simple proof of (4.2), (see section 6b).
With the usual Fourier expansion for $\psi(t)$, namely

$$\psi(t) = -\frac{1}{2i\pi} \sum_{\substack{h \in \mathbb{Z} \\ h \neq 0}} \frac{e(ht)}{h},$$

where $e(t) = e^{2i\pi t}$, we have

$$\begin{aligned} S(u_1,\dots,u_k;p) &= \left(-\frac{1}{2i\pi}\right)^k \sum_{h_1,\dots,h_k\in\mathbb{Z}^*} \frac{1}{h_1\dots h_k} \sum_{n=0}^{p-1} e\left(\frac{n}{p}(h_1u_1+\cdots+h_ku_k)\right) \\ &= \frac{p}{(-2i\pi)^k} \sum_{\substack{h_1,\dots,h_k\in\mathbb{Z}^* \\ h_1u_1+\cdots+h_ku_k\equiv 0 \pmod p}} \frac{1}{h_1\dots h_k}. \end{aligned} \tag{4.3}$$

(Here we could include the '$n = 0$' term since the contributions for h and $-h$ cancel). We now define

$$\sigma(u_1,\dots,u_k) = \frac{1}{(-2i\pi)^k} \sum_{\substack{h_1,\dots,h_k\in\mathbb{Z}^* \\ h_1u_1+\cdots+h_ku_k=0}} \frac{1}{h_1h_2\dots h_k},$$

since we expect the dominant term in (4.3) to be $\sigma(u_1,\dots,u_k)p$. By the same argument, though replacing sums by integrals, we have

$$\sigma(u_1,\dots,u_k) = \int_0^1 \psi(u_1t)\psi(u_2t)\dots\psi(u_kt)dt;$$

so, for example, $\sigma(1,\dots,1) = 1/2^k(k+1)$ if k is even. As with Dedekind sums, we have

$$\sigma(gu_1,\dots,gu_k) = \sigma(u_1,\dots,u_k), \text{ and } \sigma(u_1,\dots,u_k) = 0 \text{ if } k \text{ is odd.}$$

Lemma 4.1. *Let $U = |u_1| + \cdots + |u_k|$, where $k \ge 2$. If $p \nmid u_1 \dots u_k$ then*

$$S(u_1,\dots,u_k;p) = p\sigma(u_1,\dots,u_k) + O(U/2^k), \qquad p \to \infty.$$

Proof. Since $|\psi(x)| \le 1/2$, we have

$$\begin{aligned} \left|\prod_{i=1}^k \psi\left(u_i\frac{n}{p}\right) - \prod_{i=1}^k \psi(u_it)\right| &= \sum_{j=1}^k \left|\left(\psi\left(u_j\frac{n}{p}\right) - \psi(u_jt)\right)\prod_{i=1}^{j-1}\psi\left(u_i\frac{n}{p}\right)\prod_{i=j+1}^k \psi(u_it)\right| \\ &\le \frac{1}{2^{k-1}}\sum_{j=1}^k \left|\psi\left(u_j\frac{n}{p}\right) - \psi(u_jt)\right|, \end{aligned}$$

and

$$|\psi(uw) - \psi(ut)| = |\{uw\} - \{ut\}| \le \begin{cases} 1 & \text{if } [uw] \ne [ut], \\ |u||w-t| & \text{if } [uw] = [ut]. \end{cases}$$

Therefore

$$\begin{aligned}\left|\frac{1}{p}S(\mathbf{u},p)-\sigma(\mathbf{u})\right| &= \left|\sum_{n=1}^{p}\int\limits_{\frac{n-1}{p}}^{n/p}\Big(\prod_{i=1}^{k}\psi\left(u_i\frac{n}{p}\right)-\prod_{i=1}^{k}\psi(u_it)\Big)dt\right| \\ &\le \frac{1}{2^{k-1}}\sum_{j=1}^{k}\sum_{n=1}^{p}\int\limits_{(n-1)/p}^{n/p}\left|\psi\left(u_j\frac{n}{p}\right)-\psi(u_it)\right|dt \\ &\le \frac{1}{2^{k-1}}\sum_{j=1}^{k}\left(|u_j|\sum_{n=1}^{p}\int\limits_{(n-1)/p}^{n/p}\left|\frac{n}{p}-t\right|dt+\sum_{n\in A}\int\limits_{(n-1)/p}^{n/p}1dt\right)\end{aligned}$$

where A is the set of positive integers $n\le p$ for which $[u_jn/p]\ne[u_j(n-1)/p]$. Since there are exactly $|u_j|$ such integers n, the above is $\le (U/2^{k-1})(1/2p+1/p)$, as required.

Lemma 4.2. *Suppose that $p\nmid u_1\dots u_k$. Then there exist $m\not\equiv 0 \pmod p$ and $v_1,\dots,v_k$ such that $v_j\equiv mu_j \pmod p$ and $|v_j|\le p^{1-1/k}$ for $1\le j\le k$.*

Remark. The number of non-zero vectors $(u_1,\dots,u_k) \pmod p$ up to scalar multiples is $(p^k-1)/(p-1)$. The number of non-zero vectors $(v_1,\dots,v_k)$ with each $|v_i|\le x$ is $(2x+1)^k-1$, and this is $<(p^k-1)/(p-1)$ for $x<(p^{1-1/k}-1)/2$. So Lemma 4.2 is 'best possible' up to a constant factor.

Proof. Draw a rectangular box around the point $Q_r=(\{ru_1/p\},\dots,\{ru_k/p\})$ on the k-dimensional torus $[0,1)^k$ with side lengths $p^{-1/k}$ and Q in the center. The total volume of all these boxes is $p(p^{-1/k})^k=1$, so two, say Q_r and Q_s, must touch, say at $(t_1,\dots,t_k)$. Taking $m=|r-s|$ we have

$$\begin{aligned}\left|\left\{\frac{v_i}{p}\right\}\right| &= \left|\left\{\frac{mu_i}{p}\right\}\right| \le \left|\left\{\frac{ru_i}{p}\right\}-\left\{\frac{su_i}{p}\right\}\right| \\ &\le \left|\left\{\frac{ru_i}{p}\right\}-t_i\right|+\left|t_i-\left\{\frac{su_i}{p}\right\}\right| \le \frac{1}{2p^{1/k}}+\frac{1}{2p^{1/k}}\le p^{-1/k},\end{aligned}$$

and the result follows.

Corollary 4.3. *Suppose that $p\nmid u_1\dots u_k$ and choose $v_1,\dots,v_k$ according to lemma 4.2. Then*

$$S(u_1,\dots,u_k;p)=p\sigma(v_1,\dots,v_k)+O_k(p^{1-1/k}).$$

This follows by noting that $S(\mathbf{u};p)=S(\mathbf{v};p)$ and then using Lemma 4.1.
If $(u_1,u_2)=1$ and $h_1u_1+h_2u_2=0$ then $h_1=u_2t, h_2=-u_1t$ for some $t\in\mathbb{Z}^*$. Therefore

$$\sigma(u_1,u_2)=-\frac{1}{4\pi^2}\sum_{t\in\mathbb{Z}^*}\frac{1}{(u_2t)(-u_1t)}=\frac{1}{4\pi^2u_1u_2}\sum_{t\in\mathbb{Z}^*}\frac{1}{t^2}=\frac{1}{12u_1u_2}, \tag{4.4}$$

and, in general, we have $\sigma(u_1,u_2)=(u_1,u_2)^2/12u_1u_2$.

Corollary 4.4. *If $p \not| u_1u_2$ then $S(u_1, u_2; p) = \frac{p}{12}\theta_p(u_1, u_2) + O(\sqrt{p})$.*

Proof. By the pigeonhole principle we know there exists w_1, w_2 with each $|w_i| < \sqrt{p}$ and $w_1/w_2 \equiv u_1/u_2 \pmod p$. Thus $S(u_1, u_2; p) = S(w_1, w_2; p)$ and the result follows from Corollary 4.3.

Lemma 4.5. *Let $a + b + c = 0$, where $abc \neq 0$. Then $\sigma(a, b) + \sigma(b, c) + \sigma(c, a) = 0$.*

Proof. Write $c = -a - b \neq 0$, so that

$$\begin{aligned}\sigma(b, c) = -\sigma(b, a + b) &= \frac{1}{4\pi^2} \sum_{\substack{br+(a+b)s=0\\ r,s\in\mathbb{Z}^*}} \frac{1}{rs} = \frac{1}{4\pi^2} \sum_{\substack{as+b(r+s)=0\\ r,s\in\mathbb{Z}^*}} \frac{1}{rs}\\ &= \frac{1}{4\pi^2} \sum_{\substack{am+bn=0\\ m,n-m\in\mathbb{Z}^*}} \frac{1}{m(n-m)} = \frac{1}{4\pi^2} \sum_{\substack{am+bn=0\\ m,n\in\mathbb{Z}^*}} \frac{1}{m(n-m)},\end{aligned}$$

since a, b and $a + b$ are non-zero by hypothesis. Together with the analogous expression for $\sigma(a, c)$, we find that

$$\sigma(a, c) + \sigma(b, c) = \frac{1}{4\pi^2} \sum_{\substack{am+bn=0\\ m,n\in\mathbb{Z}^*}} \left(\frac{1}{m(n-m)} + \frac{1}{n(m-n)}\right) = -\sigma(a, b),$$

as required.

Define

$$\sigma(a, b; J) := \sum_{\substack{ar+bs=J\\ r,s\in\mathbb{Z}^*}} \frac{1}{rs} \left(= (-2i\pi)^2 \int_0^1 e(-Jt)\psi(at)\psi(bt)dt\right).$$

Note that $\sigma(a, a, J) = -2a^2/J^2$ if $a|J$, and 0 otherwise. If $a + b + c = 0$ and $J \neq 0$ then

$$\sigma(a, b; J) + \sigma(b, c; J) + \sigma(c, a; J) = -\frac{1}{2}(\sigma(a, a; J) + \sigma(b, b; J) + \sigma(c, c; J)).$$

5. Theorem A and beyond

5a. Proof of Theorem A.

We rewrite (2.2) as

$$\left\{\frac{b_0n}{p}\right\} + \left\{\frac{b_1n}{p}\right\} + \cdots + \left\{\frac{b_kn}{p}\right\} = 1 \tag{5.1}$$

By (2.1) the sum on the left-hand side is always a positive integer not exceeding k. Therefore

$$\frac{1}{(k-1)!} \prod_{j=2}^{k} \left(j - \sum_{i=0}^{k} \left\{\frac{b_in}{p}\right\}\right) = \begin{cases} 1 & \text{if (5.1) holds,}\\ 0 & \text{otherwise,}\end{cases}$$

so that, since $\{t\} = \psi(t) + \frac{1}{2}$,

$$\begin{aligned} M(b_0, b_1, \ldots, b_k; p) &= \sum_{n=1}^{p-1} \frac{1}{(k-1)!} \prod_{j=2}^{k} \left(j - \left(\frac{k+1}{2} \right) - \sum_{i=0}^{k} \psi \left(\frac{b_i n}{p} \right) \right) \\ &= \sum_{m=0}^{k-1} c_{k,m} \sum_{n=1}^{p-1} \left(\sum_{i=0}^{k} \psi \left(\frac{b_i n}{p} \right) \right)^m \\ &= \sum_{m=0}^{k-1} c_{k,m} \sum_{i_1, i_2, \ldots, i_m \in \{0, \ldots, k\}} S(b_{i_1}, b_{i_2}, \ldots, b_{i_m}; p) \qquad (5.2) \end{aligned}$$

where we define $c_{k,m}$ as the coefficient of X^m in

$$\sum_{m=0}^{k-1} c_{k,m} X^m := \frac{1}{(k-1)!} \prod_{j=2}^{k} \left(j - \left(\frac{k+1}{2} \right) - X \right).$$

In (5.2) we need only consider those terms with m even, since the value of the inner double sum is 0 when m is odd. Thus, for $k = 2$ we have $c_{2,0} = \frac{1}{2}$ so that $M(b_0, b_1, b_2; p) = (p-1)/2$, which we already observed! For $k = 3$, we have $c_{3,0} = 0$ and $c_{3,2} = \frac{1}{2}$, so that

$$\begin{aligned} M(b_0, b_1, b_2, b_3; p) &= 2S(1, 1; p) + \sum_{0 \le i < j \le 3} S(b_i, b_j; p) \\ &= \frac{p}{6} + O(1) + \sum_{0 \le i < j \le 3} S(b_i, b_j; p), \qquad (5.3) \end{aligned}$$

since $S(1, 1, p) = \frac{p}{12} - \frac{1}{4} + \frac{1}{6p}$ by (4.1).
For $k = 4$, we have $c_{4,0} = -\frac{1}{16}$ and $c_{4,2} = \frac{1}{4}$, so that

$$M(b_0, b_1, \ldots, b_4; p) = \frac{p}{24} + O(1) + \frac{1}{2} \sum_{0 \le i < j \le 4} S(b_i, b_j; p). \qquad (5.4)$$

The asymptotic formulae in Theorem A follow from Lemma 2.1, and using Corollary 4.4 in the last two equations.

5b. Beyond Theorem A.

We remark that by the above two equations and (4.1) we can obtain more precise results if the b_i are pairwise coprime: For $k = 3$

$$M(\mathbf{b}; p) = \frac{p}{12} \left(2 + \sum_{0 \le i < j \le 3} \theta_p(b_i, b_j) \right) - \left(2 + \sum_{0 \le i \ne j \le 3} S(b_i, p; b_j) \right); \qquad (5.5)$$

and for $k = 4$, we have

$$M(\mathbf{b}; p) = \frac{p}{24} \left(1 + \sum_{0 \le i < j \le 4} \theta_p(b_i, b_j) \right) - \frac{1}{2} \left(3 + \sum_{0 \le i \ne j \le 4} S(b_i, p; b_j) \right). \qquad (5.6)$$

5c. A reciprocity rule for residue races.

The reciprocity rule (2.5) was inspired by the two equations above and noticing that by taking a suitable sum we may obtain cancellation using the reciprocity law (4.1) for Dedekind sums. In this way we proved (2.5) for $k = 4$ and $k = 5$, with $\ell = 1$. However (2.5) can be given a direct and easier proof:

Proof of the reciprocity rule (2.5). Define $B(t) := \{b_0t\}+\{b_1t\}+\cdots+\{b_kt\}$, so that $(b_0n)_b+\cdots+(b_kn)_b = \ell b$ is equivalent to $B(n/b) = \ell$. Note that $B(t) = -([b_0t] + [b_1t] + \cdots + [b_kt])$ and so is an integer. Moreover, for $t \in (0, 1)$, we have $0 < B(t) < k + 1$ and so $B(t)$ is always one of the integers $1, 2, \dots,$ or k. Write the set of fractions $\{0, 1\} \cup \cup_{i=0}^{k}\{n/|b_i| : 1 \le n \le |b_i| - 1\}$ as $t_0 = 0 < t_1 < t_2 < \cdots < t_r < t_{r+1} = 1$. Let $\tau_i = b_i/|b_i|$ so that

$$M(\mathbf{b}_i; b_i) = \sum_{\substack{1\le j\le r \\ B(t_j)=\ell \text{ with } t_j=n/|b_i| \text{ for some } n}} \tau_i;$$

and so

$$(*) \qquad \sum_{i=0}^{k} M(\mathbf{b}_i; b_i) = \sum_{\substack{1\le j\le r \\ B(t_j)=\ell \text{ with } t_j=n/|b_{i(j)}|}} \tau_{i(j)} = \sum_{\nu=1}^{r} \tau_{i(j_\nu)},$$

where $j_1 \le j_2 \le \cdots \le j_r$ are precisely those values of j with $B(t_j) = \ell$.

Notice that $B(t) = -([b_0t]+[b_1t]+\cdots+[b_kt])$ does not change value in any interval (t_j, t_{j+1}). However $B(t)$ does change value at each t_j, for $1 \le j \le r$: A simple calculation reveals that if $b_i > 0$ then $B(t_j^+) = B(t_j) = B(t_j^-) - 1$, and if $b_i < 0$ then $B(t_j^-) = B(t_j) = B(t_j^+) - 1$. Therefore if $B(t_j) = \ell$ then either $B(t_j^-) > \ell$ and $B(t_j^+) = \ell$ in which case $\tau_{i(j)} = 1$, or $B(t_j^+) > \ell$ and $B(t_j^-) = \ell$ in which case $\tau_{i(j)} = -1$. Thus $\tau_{i(j_\nu)} = -\tau_{i(j_{\nu+1})}$, and so the sum in (*) equals $(\tau_{i(j_1)} + \tau_{i(j_r)})/2$.

Now $B(t_1^-) = \sum_i b_it_1^- + \sum_{i:\ b_i<0} 1 = \#\{i :\ b_i < 0\}$ so that $\tau_{i(j_1)} = -1$ if $\#\{i :\ b_i < 0\} \le \ell$, and $= 1$ otherwise. Similarly $B(t_r^+) = \#\{i :\ b_i > 0\}$ so that $\tau_{i(j_r)} = 1$ if $\#\{i :\ b_i > 0\} \le \ell$, and $= -1$ otherwise. The result follows.

6. When is $N(\mathbf{a}, p) = 0$?

Lemma 1.1 (where $b_0 + b_2 = 0$) may be rephrased and generalized as follows.

Lemma 6.1. *If non-zero $b_0, b_1, \dots, b_k$ satisfy (2.1), and I is a proper subset of $\{0, 1, \dots, k\}$ for which $\sum_{i\in I} b_i \equiv 0 \pmod p$ then $M(b_0, b_1, \dots, b_k; p) = 0$.*

Proof. Re-ordering the b_is as necessary, we may assume that $\sum_{0\le i\le\ell} b_i = 0$, where $\ell < k$. Then $\sum_{0\le i\le\ell}(b_in)_p \equiv \sum_{\ell<i\le k}(b_in)_p \equiv 0 \pmod p$, and so both sums are $\ge p$, since each is composed of positive terms. But then the sum in (2.2) must be $\ge 2p$, so that (2.2) cannot be satisfied.

When we examined $k = 4$ we discovered another general phenomena that forces $M(\mathbf{b}; p) = 0$:

Lemma 6.2. *If non-zero $b_0, b_1, \dots, b_k$ satisfy (2.1), I is a proper subset of J and M is a proper subset of L, where J and L are disjoint subsets of $\{0, 1, \dots, k\}$, and if*

$$\sum_{i\in I} b_i + \sum_{j\in J} b_j = \sum_{m\in M} b_m + \sum_{\ell\in L} b_\ell = 0$$

then $M(b_0, b_1, \dots, b_k; p) = 0$.

Proof. Re-ordering the b_is as necessary, we may assume that $I = \{0, \dots, i\}$, $J = I \cup \{i + 1, \dots, j\}$, $M = \{j + 1, \dots, m\}$, $L = M \cup \{m + 1, \dots, \ell\}$, so that $a_i + a_j \equiv a_m + a_\ell \equiv 0 \pmod p$. Therefore $(a_i n)_p + (a_j n)_p = p = (a_m n)_p + (a_\ell n)_p$, so that we cannot have $(a_i n)_p < (a_j n)_p < (a_m n)_p < (a_\ell n)_p$.

Proof of second part of Corollary 1. Select $a_j \not\equiv 0 \pmod p$ (for some $j, 2 \le j \le k - 1$), and then $a_1 \not\equiv 0$ or $a_j \pmod p$ and let $a_k \equiv a_j - a_1 \pmod p$. The remaining a_i can take any non-zero values $\pmod p$ so that the set $a_1, \dots, a_k \pmod p$ are distinct. Thus if (1.1) is satisfied we have $(na_i)_p < (na_j)_p < (na_k)_p$, contradicting Lemma 6.1.

One can easily improve "$k - 2$" in Corollary 1 to $\binom{k}{3}$ by selecting any $i < j < \ell$ and ensuring $a_j \equiv a_i + a_\ell \pmod p$; and one can go further by using other configurations that ensure $N = 0$. One of the key open problems is to determine all sets $a_1, \dots, a_k \pmod p$ for which $N = 0$ for p sufficiently large. As we shall see, for $k = 3$ this is straightforward, and for $k = 4$ we succeeded in finding all possibilities. However, we do not know how to do so for larger k. At the start of section 3 we gave a geometric interpretation of this question which may shed further light on it.

6b. Identities involving Dedekind sums. By Lemma 6.1 we know that if $b_4 = -b_0$ then $M(\mathbf{b}; p) = 0$ and $S(b_0, b_i; p) + S(b_4, b_i; p) = 0$ for any b_i. Therefore (5.3) becomes: If $b_1 + b_2 + b_3 = 0$ then

$$S(b_1, b_2, ; p) + S(b_2, b_3; p) + S(b_3, b_1; p) = \frac{p-1}{8} - \frac{3}{2} S(1, 1; p) = \frac{1}{4} - \frac{1}{4p};$$

so we have a new, easy proof of (4.2).

7. The typical residue race

In this section we shall give two quite different proofs of the first part of Corollary 1. It is not hard to deduce this from well-known results on discrepancies but we give two proofs more in tone with the rest of this paper.

7a. The tail of $\sigma(\mathbf{u})$.
We prove the following useful result:

Proposition 7.1. *For any non-zero integers $u_1, \dots, u_k$,*

$$\sum_{\substack{m_1,\dots,m_k\in\mathbb{Z}^* \\ m_1u_1+\cdots+m_ku_k=0 \\ \max_i |m_i|\ge y}} \frac{1}{|m_1 m_2 \dots m_k|} \ll_k \frac{(\log y)^{k-1}}{y}$$

for any positive integer y, where the constant is independent of the choice of the u_i.

Proof. We will partition the sum above into subsums indexed by integers j, $1 \le j \le k$ and $\ell \ge 0$ where we have $|m_j| > |m_i|$ for $i < j$ and $|m_j| \ge |m_i|$ for $i > j$, and $z := y2^\ell \le |m_j| < y2^{\ell+1}$. From the linear equation $m_1u_1 + \cdots + m_ku_k = 0$ we see that m_j is determined by the other m_i and thus this subsum is

$$\le \sum_{\substack{m_i \in \mathbb{Z}^*,\ |m_i| \le 2z \\ \text{for all } 1 \le i \le k,\ i \ne j}} \frac{1}{|m_1 m_2 \dots m_k|} \le \frac{1}{z} \prod_{\substack{1 \le i \le k \\ i \ne j}} \sum_{\substack{m_i \in \mathbb{Z}^* \\ |m_i| \le 2z}} \frac{1}{|m_i|} \le \frac{1}{z}(2\log z + O(1))^{k-1}.$$

Summing over j and ℓ gives the result.

Remark. It would be interesting to know what the "best possible" result is here. Certainly if we take each $u_i = 1$ then the sum is $\gg (\log y)^{k-2}/y$; we guess that this gives the "correct" power on $\log y$.

(First) proof of the first part of Corollary 1. For any $(m_1, \dots, m_k) \in (\mathbb{Z}/p)^k - \{0\}$ there are exactly p^{k-1} vectors $\mathbf{u}$ in $(\mathbb{Z}/p)^k$ with $\mathbf{m}{\cdot}\mathbf{u} \equiv 0 \pmod p$. Thus there are $\ll y^k p^{k-1}$ vectors $\mathbf{u}$ for which there exists some non-zero $\mathbf{m}$ with $\mathbf{u} \cdot \mathbf{m} \equiv 0 \pmod p$ and each $|m_i| \le y$. Therefore for all but $O_k(y^k p^{k-1})$ vectors $\mathbf{u}$ we have

$$\sum_{\substack{m_1, \dots, m_k \in \mathbb{Z}^* \\ \mathbf{m}\cdot\mathbf{u} = 0}} \frac{1}{m_1 \dots m_k} \ll \frac{\log^{k-1} y}{y}.$$

by Proposition 7.1, since in any other solution to $\mathbf{m}{\cdot}\mathbf{u} = 0$ we have some $|m_i| > y$. Applying this to each "non-diagonal" term in (5.2) using Lemma 4.1, we find that $M(b_0, \dots, b_k; p)$ equals the sum of diagonal terms in (5.2) plus an error of $O(\log^{k-1} y/y)$ (a "diagonal term" is a $S(b_{i_1}, \dots, b_{i_m}; p)$ where the b_{i_j} are all equal), for all but $O_k(y^k p^{k-1})$ choices of vectors $\mathbf{b}$. Therefore, in such cases, $M(b_0, \dots, b_k; p)$ equals $cp + O(p \log^{k-1} y/y)$ for some constant c. We could compute c, with some difficulty, directly from (5.2), since $S(b, \dots, b; p) = S(1, 1, \dots, 1, p) = 1/(m{+}1)2^m$. However, if we average over all possibilities for $b_0, \dots, b_k$ satisfying (2.1), then the average of m's is $p/k!$, which equals, by the above, $cp + O(p(\log y)^{k-1}/y + y^k)$ so that $c = 1/k!$ by taking $y = \eta(p)^{1/k}$.

7b. Mean and Variance of Dedekind sums.

Assume k is even, else $S(\mathbf{b}; p) = 0$ for all $\mathbf{b} \pmod p$. Since $\psi(-t) + \psi(t) = 0$ we see that $S(b_1, \dots, b_{k-1}, b_k; p) = -S(b_1, \dots, b_{k-1}, -b_k; p)$; and so $S(\mathbf{b}; p)$ is zero on average, running over the distinct vectors $\mathbf{b} \pmod p$. Now

$$\sum_{b_1, b_2, \dots, b_k \pmod p} S(b_1, \dots, b_k; p)^2 = \sum_{m,n \pmod p} \prod_{i=1}^{k} \left\{ \sum_{b_i \pmod p} \psi\left(\frac{b_i m}{p}\right) \psi\left(\frac{b_i n}{p}\right) \right\}$$

$$= \sum_{m,n \pmod p} S(m, n; p)^k. \tag{7.1}$$

For each nonzero $r \pmod p$ define a_r and $b_r > 0$ to be those coprime integers with $\max\{|a_r|, b_r\}$ minimal and $a_r \equiv rb_r \pmod p$. There are exactly $p-1$ non-zero pairs $m, n \pmod p$ with $m \equiv rn \pmod p$. By Corollary 4.4 we see that $|S(m,n;p)| = p/12|a_r|b_r + O(\sqrt{p})$, for each such pair m, n.

Now, if $0 < |a|, b < \sqrt{p/2}$ are coprime integers then $a_r = a$ and $b_r = b$ where $r \equiv a/b \pmod p$, since $a_r b - b_r a \equiv 0 \pmod p$ and $|a_r b - b_r a| \leq 2\max\{|a|, b\}^2 < p$ and thus $a_r b - b_r a = 0$. If $|a_r|$ or b_r is $> \sqrt{p/2}$ then $|S(m,n;p)| = O(\sqrt{p})$ by the above. Combining all of this information gives for $k \geq 2$:

$$\begin{aligned}\sum_{m,n \pmod p} S(m,n;p)^k &= (p-1) \sum_{\substack{0<|a|,b<\sqrt{p/2} \\ (a,b)=1}} \left(\frac{p}{12ab} + O(\sqrt{p})\right)^k + O(p^{2+k/2}) \\ &= \frac{2\zeta(k)^2}{12^k \zeta(2k)} p^{k+1} + O(p^{k+1/2} + p^{2+k/2}),\end{aligned}$$

where $\zeta(s)$ is the Riemann zeta function.

Combining the last two displayed equations gives, for $k \geq 2$,

$$\frac{1}{p^k} \sum_{\mathbf{b} \pmod p} S(\mathbf{b};p)^2 \ll_k p,$$

and so, by (5.2),

$$\frac{1}{p^k} \sum_{\substack{b_0,b_1,\dots,b_k \pmod p \\ b_0+b_1+\cdots+b_k \equiv 0 \pmod p}} \left| M(\mathbf{b};p) - \frac{p-1}{k!} \right|^2 \ll_k p.$$

The first part of Corollary 1 follows immediately from this estimate.

The attractive identity (7.1) generalizes as follows: For any positive integers k, ℓ

$$\sum_{b_1,b_2,\dots,b_k \pmod p} S(b_1,\dots,b_k;p)^\ell = \sum_{u_1,u_2,\dots,u_\ell \pmod p} S(u_1,\dots,u_\ell;p)^k; \tag{7.2}$$

though note that this is vacuous for $k = \ell$.

8. More analysis

We note that

$$\frac{1}{2\pi^2} \sum_{k \in \mathbb{Z}^*} \frac{1 - e(k\theta)}{k^2} = \theta(1-\theta) \quad \text{for } 0 \leq \theta \leq 1. \tag{8.1}$$

This may be established noting that the identity is trivial for $\theta = 0$ and then that the derivatives of both sides are equal in our range by the Fourier expansion of $\psi(t)$.

Next we prove a useful lemma:

Lemma 8.1. *Suppose p is prime and constants α_i, β_i are given with $|\alpha_i|, |\beta_i| \ll 1$ for $1 \le i \le p$. Let $\alpha_{i+p} = \alpha_i$ and $\beta_{i+p} = \beta_i$ for all i. For any non-zero $a \pmod p$ select integers r and s with $a \equiv r/s \pmod p$ and $\max\{|r|, |s|\}$ minimal. Then*

$$\sum_{1\le|i|\le(p-1)/2} \frac{\alpha_i}{i}\frac{\beta_{ai}}{(ai)_p} = \frac{1}{rs}\sum_{j\in\mathbb{Z}^*}\frac{\alpha_{sj}\beta_{rj}}{j^2} + O\left(\frac{1}{\sqrt{p}}\right)$$

where $(t)_p$ is the least residue of $t \pmod p$ in absolute value.

Proof. By Lemma 4.2 we have $\max\{|r|, |s|\} < \sqrt{p}$. If $|i| < \sqrt{p}/2$ and $|(ai)_p| < \sqrt{p}/2$ then $|ri - s(ai)_p| < p$ and divisible by p, so that $i = js$ and $(ai)_p = jr$ for some integer j. All such terms from the left side are part of the sum on the right. Moreover the terms in the sum on the right which arise this way are precisely those with $|j| \le (p-1)/(2\max\{|r|, |s|\})$, and so the extra terms contribute $\ll (1/rs)\max\{|r|, |s|\}/p \ll 1/p$.
We need to bound those terms $1/ij$ on the left side with $j \equiv ai \pmod p$ and either $|i| \ge \sqrt{p}/2$ or $|j| \ge \sqrt{p}/2$. We shall work under the assumption that $|i| \le |j|$ (the estimate for the other terms may be obtained by replacing a by $1/a$ in the argument), so that $|j| > \sqrt{p}/2$.
Those terms on the left side with $|j| > \sqrt{p}\log p$ contribute $\ll \sum_{1\le i\le p} 1/(i\sqrt{p}\log p) \ll 1/\sqrt{p}$. So we may now assume that $|j| \le \sqrt{p}\log p$. Now for $\ell = 1, \ldots, L := [\log\log p] + 1$, consider those terms with $e^{\ell-1}\sqrt{p/2} < |j| \le e^{\ell}\sqrt{p/2}$. The contribution of the terms with $(1/e^{\ell})\sqrt{p/2} < |i| < e^{\ell}\sqrt{p/2}$ is $\ll \ell/e^{\ell}\sqrt{p} \ll 1/2^{\ell}\sqrt{p}$. Now consider the terms with $|i| < (1/e^{\ell})\sqrt{p/2}$. If i', j' are another such pair then $|i'j - ij'| < p$ and is divisible by p, so equals 0. Thus for some pair of coprime integers $u, v > 0$ we have $i = ku$ and $j = kv$ for some integer k. The contribution to the sum above is $\le \sum_{k\ge\sqrt{p/2}/|v|} 1/k^2|uv| \ll 1/|u|\sqrt{p}$. We claim that there is no more than one such pair u, v with $u < \log p$ for if there were another such pair u', v' then $|uv' - u'v| < 2\sqrt{p}\log^2 p < p$ and is divisible by p and so equals 0, which is impossible. The total contribution from these terms is then $\ll 1/\sqrt{p} + L/\sqrt{p}\log p \ll 1/\sqrt{p}$.

We also note an elementary identity that will come in useful: If $0 \le \alpha, \beta \le 1$ then

$$\frac{1}{2}((\alpha-\alpha^2) + (1-\beta-(1-\beta)^2) - (\{1+\alpha-\beta\} - \{1+\alpha-\beta\}^2)) = \min\{\alpha,\beta\} - \alpha\beta. \tag{8.2}$$

Proposition 8.2. *For a given prime p, integers $1 \le a, M, N \le p-1$, with $\alpha = N/p$ and $\beta = M/p$, and integers r and $s > 0$ with $a \equiv r/s \pmod p$ and $\max\{|r|, |s|\}$ minimal, we have*

$$\sum_{\substack{n\le N,\ m\le M\\ m\equiv an \pmod p}} 1 = \frac{MN}{p} + \frac{p}{2rs}(\min\{\{r\alpha\}, \{s\beta\}\} - \{r\alpha\}\{s\beta\}) + O(\sqrt{p}). \tag{8.3}$$

Proof. The left side of (8.3) equals

$$\sum_{n\le N,\ m\le M}\frac{1}{p}\sum_{k=0}^{p-1} e\left(\frac{k(sm-rn)}{p}\right) = \frac{MN}{p} + \frac{1}{p}\sum_{k=1}^{p-1}\left(\frac{1-e\left(\frac{ksM}{p}\right)}{1-e\left(\frac{-ks}{p}\right)}\right)\left(\frac{1-e\left(\frac{-krN}{p}\right)}{1-e\left(\frac{kr}{p}\right)}\right).$$

Now since $1/(1-e(-t/p)) \asymp p/2i\pi t + O(1)$ for $0<|t| \ll p$, we get from Lemma 8.1,

$$= \frac{MN}{p} + \frac{p}{4rs\pi^2} \sum_{k=1}^{p-1} \frac{(1-e(ks\beta))(1-e(-kr\alpha))}{k^2} + O(\sqrt{p}),$$

and then the result follows from (8.1) and (8.2).

By partial summation on (8.3), or by a direct calculation, one can deduce that

$$\sum_{n\le N} \psi\left(\frac{an}{p}\right) = \frac{p}{2rs}(\{r\alpha\}^2 - \{r\alpha\}) + O(\sqrt{p}). \tag{8.4}$$

Corollary 8.3. *Fix integer $k \ge 42$. For a given prime p, and integer $1 \le a \le p-2$, define integers r and $s>0$ with $a \equiv r/s \pmod p$ and $\max\{|r|,|s|\}$ minimal. Let $w_1 < w_2 < ... < w_{p-1}$ be the set of integers $\{n+(an)_p : 1 \le n \le p-1\}$ put in ascending order (where $(t)_p$ is now the least positive residue of $t \pmod p$). Then*

$$w_1 + w_2 + \cdots + w_{[p/k]} \ge 2p^2/k^2 + O(p^{3/2}),$$

unless $r/s = 1, 1/2$ or 2 in which case it equals $(r+s)p^2/2k^2 + O(p^{3/2})$

Proof. The numbers $w_1 < w_2 < ... < w_{p-1}$ run through a reduced residue system mod p and are all in $[2, 2p-2]$. Therefore $n+(an)_p = ((a+1)n)_p$ or $p+((a+1)n)_p$. We are interested in the smaller w_i, that is when $n+(an)_p = ((a+1)n)_p$. A characteristic function for this happening is $1/2 + \psi((a+1)n/p) - \psi(n/p) - \psi(an/p)$. We wish to count how often this happens with $((a+1)n)_p < N$ so let's write $m = ((a+1)n)_p$ and our characteristic function becomes $1/2 + \psi(m/p) - \psi(rm/(r+s)p) - \psi(sm/(r+s)p)$. Therefore

$$\begin{aligned} \#\{n: \ n+(an)_p \le N\} &= \sum_{m\le N} m/p - \psi(rm/(r+s)p) - \psi(sm/(r+s)p) \\ &= \frac{N^2}{2p} + \frac{p}{2(r+s)}\left(\frac{\{r\alpha\}-\{r\alpha\}^2}{r} + \frac{\{s\alpha\}-\{s\alpha\}^2}{s}\right) + O(\sqrt{p}). \end{aligned}$$

by (8.4). Let $N_k = w_{[p/k]}$. Note that $\{t\} - \{t\}^2 = \{|t|\} - \{|t|\}^2$.
We start by considering $r > 0$:
If $\alpha < 1/\max\{r,s\}$ then $\{r\alpha\} = r\alpha$ and $\{s\alpha\} = s\alpha$, so that $\#\{j : w_j \le N\} = N/(r+s) + O(\sqrt{p})$. Thus if $k \ge (r+s)\max\{r,s\}$ then $N_k = (r+s)p/k + O(\sqrt{p})$, and so, by partial summation $w_1 + w_2 + \cdots + w_{[p/k]} = (r+s)p^2/2k^2 + O(p^{3/2})$.
If $r+s \ge 8$ and $4rs < k$ then $\{r\alpha\} = r\alpha$ and $\{s\alpha\} = s\alpha$ for all $\alpha \le 4/k < 1/\max\{r,s\}$, and so $\#\{j : w_j \le N\} = N/(r+s) + O(\sqrt{p})$, and in particular $\#\{j : w_j \le 4p/k\} = 4p/k(r+s) + O(\sqrt{p}) < p/2k + O(\sqrt{p})$ so that $w_1 + w_2 + \cdots + w_{[p/k]} \ge (p/2k + O(\sqrt{p}))(4p/k) = 2p^2/k^2 + O(p^{3/2})$.

Now, since $t-t^2\le 1/4$ for $t\in[0,1)$, we deduce that $\#\{j: w_j\le N\}\le N^2/2p+p/8rs+O(\sqrt{p})$. If $4rs\ge k$ then $\#\{j: w_j\le N\}\le N^2/2p+p/2k$; and so $N_k\ge p/\sqrt{k}$. But then, by partial summation we deduce that $w_1+w_2+\cdots+w_{[p/k]}\ge p^2/3k^{3/2}$.

Now we consider $r<0$. By changing a to $1/a$ if necessary we may assume that $s>|r|$. If $\alpha<1/s$ then $\#\{j: w_j\le N\}=0$ by the above formula; therefore if $s\le 2k/3$ then $\#\{j: w_j\le 3p/2k\}=0$, so that $w_1+w_2+\cdots+w_{[p/k]}\ge\sum_{3p/2k<w<5p/2k} w\ge 2p^2/k^2$. If $s>2k/3$, then $4s(s+r)>2k$ so that $\#\{j: w_j\le N\}\le N^2/2p+p/8s(s+r)+O(\sqrt{p})\le N^2/2p+p/2k+O(\sqrt{p})$; and so by partial summation we deduce that $w_1+w_2+\cdots+w_{[p/k]}\ge p^2/3k^{3/2}+O(p^{3/2})$.

Corollary 8.4. *Fix $1<\tau\le 2$. For a given prime p, and integer $1\le a\le p-2$, define integers r and $s>0$ with $a\equiv r/s \pmod p$ and $\max\{|r|,|s|\}$ minimal. Let $\mathcal{N}$ be a set of $[p/k]$ integers all $\le \tau p/k$. Then*

$$\sum_{n\in\mathcal{N}}(an)_p\ge O(\sqrt{p})+\begin{cases}\frac{p^2}{2\tau k} & \text{if } rs<0\\ \frac{p^2}{2\tau k}\left(1-\frac{\tau}{2s}\right)^2 & \text{if } rs>0 \text{ and } s>\tau/2\\ \frac{p^2}{2\tau k}\left(1+\frac{k}{2\tau r}\right)^{-1} & \text{if } rs>0\end{cases}\cdot$$

Proof. Taking $\delta=\{\tau r/k\}$, equation (8.3) becomes

$$\sum_{\substack{n\le\tau p/k,\ m\le M\\ m\equiv an \pmod p}}1=\frac{\tau M}{k}+\frac{p}{2rs}(\min\{\delta,\{s\beta\}\}-\delta\{s\beta\})+O(\sqrt{p}).$$

If $rs<0$ then this is $\le\tau M/k+O(\sqrt{p})$, and so by partial summation this gives the first result. Now assume $rs>0$. If $r\ge k/\tau$ then $rs\ge k(s/\tau)\ge k(s/\tau)\delta$. If $r<k/\tau$ then $\delta=\tau r/k$ and so $rs=k(s/\tau)\delta$. Since $\min\{\delta,\{s\beta\}\}-\delta\{s\beta\}\le\delta$ thus the above bound is $\le\tau M/k+p/2k(s/\tau)+O(\sqrt{p})$, which yields the second result by partial summation. If $rs>0$ then $\min\{\delta,\{s\beta\}\}-\delta\{s\beta\}\le s\beta$ so the above bound is $\le M(\tau/k+1/2r)+O(\sqrt{p})$, which yields the final result by partial summation.

9. Upper bounds on N

As we stated in the introduction, we believe that $N(a_1,\dots,a_k;p)\le[p/k]$. Moreover that for $k\ge 3$, equality holds if and only if $\{b_0,b_1,\dots,b_k\}=\{g,g,\dots,g,-kg\}$, for some non-zero $g \pmod p$. We have shown this for $k=3$ and 4.

One can prove $N(a_1,\dots,a_k;p)<2p/(k+1)$ as follows: Let $\mathcal{N}$ be the set of residues n for which (2.2) holds. Note that since $\{(bn)_p:\ 1\le n\le p-1\}=\{n:\ 1\le n\le p-1\}$, we have $\sum_{n\in\mathcal{N}}(b_in)_p\ge\sum_{m\le N}m=N(N+1)/2$, where $N=N(a_1,\dots,a_k;p)=|\mathcal{N}|$. Therefore

$$pN=\sum_{n\in\mathcal{N}}((b_0n)_p+(b_1n)_p+\cdots+(b_kn)_p)\ge(k+1)N(N+1)/2,$$

and the result follows.

Getting rid of that extra factor of “2” has taken us considerable effort; however we do suspect that there is a simple geometric proof (that $\nu(a_1,\dots,a_k)\le 1/k$).

Theorem 9.1. *Let $k \geq 42$ be a given integer. If p is sufficiently large (as a function of k) then $N(a_1, \dots, a_k; p) \leq [p/k]$.*

Tracing through the arguments below we get Theorem 9.1 for $p \gg k^C$ for some absolute constant C.

Corollary 9.2. *For $k = 2, 3, 4$ and all $k \geq 42$, we have $\nu(a_1, \dots, a_k) \leq 1/k$.*

Our proof needs certain complicated hypotheses. First note that by (2.1) (changing b_0 by a suitable multiple of p, if necessary) we have $b_0 + b_1 + \cdots + b_k = 0$. Thus at least one b_i is negative, and at least one b_i is positive. We may assume that the majority are positive and that $b_0 < 0$; this assumption is valid since we can multiply the b_i through by any constant that is nonzero mod p. Note that (2.2) is equivalent to the statement

$$(b_1 n)_p + \cdots + (b_k n)_p < p, \tag{9.1}$$

since $0 < (b_0 n)_p < p$ and $(b_0 n)_p + (b_1 n)_p + \cdots + (b_k n)_p \equiv 0 \pmod p$. Let us assume we have a set $\mathcal{N}$ of $[p/k]$ distinct $n \pmod p$ for which (9.1) is satisfied. The one solution we know is the case where $b_1 = b_2 = \cdots = b_k$. Let us assume that there is another such solution (that is, where the b_i's are not all equal).

Corresponding to any set of k integers $\{b_1, \dots, b_k\}$ there is a (unique) "frequency sequence" $d_1 \geq d_2 \geq \cdots \geq d_\ell \geq 1$, where $d_1 + d_2 + \cdots + d_\ell = k$, and there are distinct integers $c_1, \dots, c_\ell$ such that $d_j = \#\{i : \ b_i = c_j\}$ for each j. We can order these frequency sequences lexicographically; that is $(d_1, d_2, \dots, d_\ell) > (D_1, D_2, \dots, D_L)$ if there exists integer I such that $d_i = D_i$ for $1 \leq i \leq I - 1$, and $d_I > D_I$. The frequency sequence of the one solution we have is simply (k). Under our assumption that there is another solution we select that with the next largest frequency sequence in our ordering (that is, the largest other than our known solution).

We now show that there exists m such that $\#\{i : b_i = m \text{ or } 2m\} > v := [(k+1)/2]$. If not, we re-order the b_i as follows: First take those $b_i \equiv 1 \pmod p$, then those $b_i \equiv 2 \pmod p$, $b_i \equiv 4 \pmod p$, and so on until we get those $b_i \equiv 2^{h-1} \pmod p$ for h is the order of 2 mod p. Then we start with a reduced residue not already accounted for, call it R, and then take those $b_i \equiv R \pmod p$, then those $b_i \equiv 2R \pmod p$, and so on. By our assumption, in this re-ordered sequence, $b_i/b_{i+v} \not\equiv 1, 1/2$ or $2 \pmod p$. Thus $\sum_{n \in \mathcal{N}} (b_i n)_p + (b_{i+v} n)_p \geq 2p^2/k^2 + O(p^{3/2})$ by Corollary 8.3. Therefore

$$\begin{aligned} 2p[p/k] &= 2 \sum_{n \in \mathcal{N}} ((b_0 n)_p + (b_1 n)_p + \cdots + (b_k n)_p) \\ &= \sum_{i=0}^{k} \sum_{n \in \mathcal{N}} (b_i n)_p + (b_{i+v} n)_p \geq 2(k+1)p^2/k^2 + O(p^{3/2}), \end{aligned}$$

giving a contradiction.

We shall now prove that either $\#\{i : b_i = m\} \leq 1$ or $\#\{i : b_i = 2m\} \leq 1$, so that $d_1 \geq [(k+1)/2]$:

First, assume $\#\{i : b_i = m\} \geq \#\{i : b_i = 2m\} \geq 2$, so that $\#\{i : b_i = m\} > k/4$. Divide all the b_i through by $m \pmod p$ (that is, we may take $m = 1$). Select I so that $b_I = 2$. If (9.1) holds then we must have $n \leq 4p/k$. In this range $(2n)_p = 2n$ and so we can construct a new sequence satisfying (9.1) for all $n \in \mathcal{N}$, by taking $B_i = b_i$ if $b_i \neq 2$ or $i = I$, and $B_i = 1$ if $b_i = 2$ and $i \neq I$. Evidently this new sequence has larger frequency sequence than the original sequence, contradicting hypothesis.

Now, assume $\#\{i : b_i = 2m\} \geq \#\{i : b_i = m\} \geq 2$, so that $\#\{i : b_i = 2m\} > k/4$. Divide all the b_i through by $2m \pmod p$. Select I so that $b_I = 1$. If (9.1) holds then we must have $n \leq 4p/k$. If n is odd then $(n/2)_p = (p+n)/2 > p/2$ but there are ≥ 2 values of i with $b_i = 1/2$, so that (9.1) cannot hold. Thus we must have $n = 2q$ for some integer $q < 2p/k$. But now we can construct a new sequence satisfying (9.1) for all $n \in \mathcal{N}$, by taking $B_i = b_i$ if $b_i \neq 1$ or $i = I$, and $B_i = 1/2$ if $b_i = 1$ and $i \neq I$. Evidently this new sequence has larger frequency sequence than the original sequence, contradicting hypothesis.

By scaling by an appropriate constant we may now assume that $\#\{i : b_i = 1\} = d_1 \geq [(k+1)/2] \geq k/2$. Therefore in any solution of (9.1) we must have $n \leq 2p/k$.

Define integers r_i and $s_i > 0$ with $b_i \equiv r_i/s_i \pmod p$ and $\max\{|r_i|, |s_i|\}$ minimal. Let $\mathcal{L}$ be the set of i with $r_i < 0$, or $r_i \geq k/5$ or $s_i \geq 3$. By Corollary 8.4 with $\tau = 2$, we find that $\sum_{n\in\mathcal{N}} (b_i n)_p \geq p^2/9k + O(\sqrt{p})$ for $i \in \mathcal{L}$, and so

$$\begin{aligned} p^2/k > p[p/k] &= \sum_{n\in\mathcal{N}} ((b_0 n)_p + (b_1 n)_p + \cdots + (b_k n)_p) \\ &\geq |\mathcal{L}| p^2/9k + (k+1-|\mathcal{L}|)p^2/2k^2 + O(p^{3/2}); \end{aligned}$$

therefore $|\mathcal{L}| < 5$, that is $|\mathcal{L}| \leq 4$.

Other elements of our sequence have $1 \leq r_i < k/5$ and $s_i = 1$ or 2. Now $r_i n \leq 2p/5$ and so $(b_i n)_p = b_i n$ if $s_i = 1$; and $(b_i n)_p = r_i n/2$ or $(p + r_i n)/2$ if $s_i = 2$, depending on whether n is even or odd. Either way $((b_i - 1)n)_p < (b_i n)_p$ for all $n \in \mathcal{N}$ if $b_i > 1$. Let J be the i with $s_i = 2$. We may assume $r_i = 1$ for all $i \in J$, else we can construct a new sequence satisfying (9.1) for all $n \in \mathcal{N}$, by taking $B_i = b_i$ if $i \notin J$, and $B_i = 1/2$ if $i \in J$. Evidently this new sequence has larger frequency sequence than the original sequence, contradicting hypothesis. We claim that J cannot contain more than one element else, arguing as above, every $n \in \mathcal{N}$ must be an even integer so we can construct a new sequence satisfying (9.1) for all $n \in \mathcal{N}$ with larger frequency sequence. Let P be the i with $s_i = 1 < r_i$. We claim that P has at most one element if $\mathcal{L} \cup J$ contains just $\{0\}$; otherwise $\mathcal{P}$ is empty. In the latter case we can construct a new sequence satisfying (9.1) for all $n \in \mathcal{N}$, by taking $B_i = b_i$ if $i \notin P$, and $B_i = 1$ if $i \in P$, but this has a larger frequency sequence. In the former case we take some $j \in P$ and set $B_j = 2$ in our new sequence.

In summary, we have now proved that there are at most 5 integers i for which $b_i \neq 1$. This means that $n \leq p/(k-4)$ in any solution of (9.1) so we can now take $\tau = 21/19$ in Corollary 8.4 (since $k \geq 42$). Now let $\mathcal{L}$ be the set of i with $r_i < 0$, or $r_i \geq k/\tau$ or $s_i \geq 2$. Proceeding as above we find that $\sum_{n\in\mathcal{N}} (b_i n)_p \geq 3025p^2/12768k + O(\sqrt{p})$ for $i \in \mathcal{L}$; and thus deduce that $|\mathcal{L}| < 3$ so that $|\mathcal{L}| \leq 2$. Arguing as above (but now noting that s_i can only be 1), we see that there are at most 2 integers i for which $b_i \neq 1$. In fact there are exactly two such integers for if there were just one we would be in the case $b_1 = \cdots = b_k = 1,\ b_0 = -k$. This means that $n \le p/(k-1)$ in any solution of (9.1) so we can now take $\tau = 1.05$ in Corollary 8.4 which implies that $\sum_{n\in\mathcal{N}}(b_i n)_p \ge p^2/4k$ for $i \in \mathcal{L}$, and thus $|\mathcal{L}| < 2$ so that $|\mathcal{L}| = 1$. Arguing as above this means that our set must be $b_1 = \cdots = b_{k-1} = 1,\ b_k = 2,\ b_0 = -k-1$, but then $\mathcal{N}$ has just $[p/(k+1)]$ elements giving a contradiction.

10. Spectra

10a. The case $k = 3$. Given non-zero integers $b_0, \dots, b_3$, whose sum is 0, we wish to understand the values taken by

$$\omega(\mathbf{b}) := 12\nu(a_1, a_2, a_3) = 2 + \sum_{0\le i<j\le 3} \frac{(b_i, b_j)^2}{b_i b_j}.$$

By Lemma 6.1 we know that if $b_i/b_j = -1$ for some i, j then $\omega(\mathbf{b}) = 0$, so we may assume $b_i/b_j \ne -1$, and therefore $(b_i, b_j)^2/b_i b_j \ge -1/2$. But at most 4 numbers amongst $\{b_i b_j : 0 \le i < j \le 3\}$ can be negative so that $\omega(b) \ge 2 + 4(-\frac{1}{2}) + 2*$ positive terms > 0. Thus

$$\omega(\mathbf{b}) = 0 \ \text{ if and only if } \ b_i + b_j = 0 \text{ for some } i, j.$$

Since the sum of the b_i's is 0 at least one of them is negative and at least one is positive. Reordering if necessary we may assume $b_0 < 0 < b_3$. Since $\omega(\mathbf{b}) = \omega(-\mathbf{b})$ we may also assume $b_2 > 0$. So we have two cases to consider, as $b_1 > 0$ or $b_1 < 0$. We now look at how small $\omega(\mathbf{b})$ can get.

If $b_0 < 0 < b_1, b_2, b_3$ then, since $b/c \ge (b,c)^2/bc$ for any positive integers b and c, we have

$$\omega(\mathbf{b}) > 2 + \sum_{j=1}^{3}(b_0, b_j)^2/b_0 b_j \ge 2 + \sum_{j=1}^{3} b_j/b_0 = 2 - 1 = 1.$$

If $b_0, b_1 < 0 < b_2, b_3$ and $\omega(\mathbf{b}) \leqq 1$ then

$$\max_{i=0,1} \sum_{j=2}^{3} \frac{(b_i, b_j)^2}{|b_i| b_j} \ge \frac{1}{2}\sum_{i=0}^{1}\sum_{j=2}^{3} \frac{(b_i, b_j)^2}{|b_i| b_j} > \frac{1}{2}(2 - \omega(\mathbf{b})) \ge \frac{1}{2}.$$

Swapping b_0 and b_1 if necessary, we thus deduce that the values of $(b_0, b_j)^2/|b_0|b_j$ for $j = 2$ and 3 are $1/3$ and $1/m$, for $m = 3, 4$ or 5, or $1/2$ and $1/m$ for some $m \ge 2$.

If $\theta_p(b_0, b_2) = \theta_p(b_0, b_3) = -1/3$ then $\mathbf{b} = \{-3, -7, 1, 9\}$ so that $\omega(\mathbf{b}) = 4/3$.

If $\theta_p(b_0, b_2) = -1/3$ and $\theta_p(b_0, b_3) = -1/m$ for $m = 4$ or 5 then $\mathbf{b} = \{-1, -(m+2), 3, m\}, \{-(2m+1), -m, 3m, 1\}$ or $\{-(3m-2), -3, 1, 3m\}$. Thus $\omega(-1, -6, 3, 4) = 1$, and $\omega(\mathbf{b}) > 1$ otherwise.

We can now assume that $b_2 = -2b_0$, so $\mathbf{b} = \{m, -2m, n, m-n\}$ for some coprime integers $m, n > 0$.

If m is even then $\omega(\mathbf{b}) = 3/2{+}3/2n(m{-}n)$, which is > 1 unless $\{m, n\} = \{-1, 1\}, \{-2, 1\}, \{1, 2\}$ or $\{2, 3\}$. Excluding those cases with $b_i + b_j = 0$ we are left with $\omega(\{1, 4, -2, -3\}) = 1$.
If m is odd we may assume n is even (swapping n and $m - n$ if necessary) so that $\omega(\mathbf{b}) = 3/2 + 3/2m(m - n)$, giving rise to $\omega(\{1, 4, -2, -3\}) = \omega(\{-1, 3, 4, -6\}) = 1$.

We now look at how large $\omega(\mathbf{b})$ can be. Notice that $\omega(\{1, 1, 1, -3\}) = 4$. Since $b_0 + b_1 + b_2 + b_3 = 0$, at most 3 of the numbers $\{(b_i, b_j)^2/b_ib_j : 0 \leq i < j \leq 3\}$ can be positive; and their sum is $> \omega(\mathbf{b}) - 2$. If $\omega(\{1, 1, 1, -3\}) \geq 4$, then their sum is > 2 so at least two of them equal 1 (else their sum is $\leq 1 + 1/2 + 1/2 = 2$). Thus either $b_0 = b_1$ and $b_2 = b_3$, so that $b_2 = -b_0$ and $\omega(\mathbf{b}) = 0$ by Lemma 6.1, or $b_1 = b_2 = b_3$ and we find that $\mathbf{b}= \{1, 1, 1, -3\}$ up to scalar multiples.
The Spectrum beyond the first accumulation points: In the spectrum of values of ω the smallest accumulation point, other than 0, is 3/2. Since $\omega(\mathbf{b}) = 3/2 - 3/2d$ where $d = n(n - m)$ or $m(n - m)$ is odd, for $\mathbf{b}= \{m, -2m, n, m - n\}$, we see that 3/2 is indeed an accumulation point. To show it is the smallest we now determine all $\mathbf{b}$ for which $\omega(\mathbf{b}) < 3/2 - \epsilon$, for some given $\epsilon > 0$, which is a finite set: First note that

$$\sum_{\substack{0\leq i<j\leq 3\\ b_ib_j<0}} \frac{(b_i, b_j)^2}{|b_ib_j|} > \frac{1}{2} + \epsilon,$$

so that the largest two of the values of $(b_i, b_j)^2/|b_ib_j|$ with $b_ib_j < 0$ are $-1/2$ and $-1/m$ where $m < 3/\epsilon$, or $\{-1/n, -1/m\}$ where $3 \leq n \leq m < 6n/(n - 2)$ with $n \leq 7$. Thus we have finitely many possibilities as claimed. If one of the ratios is $-1/2$ we return to the sets $\mathbf{b}= \{m, -2m, n, m{-}n\}$ considered above. Otherwise we find, by computing all possibilities, that the values taken by $\omega(\mathbf{b}) \leq 3/2$ are all of the form $3/2 - 3/2d$, or equal 3/2. For example, $\omega(1, -3, -10, 12) = 7/5$, $\omega(1, -4, -9, 12) = 4/3$, and $\omega(3, -4, -15, 16) = 3/2$. Thus

The set of values of $\nu(a_1, a_2, a_3)$ which are $\leq 1/8$ are precisely the numbers of the form $(1/8)(1 - 1/d)$ with d odd, and 1/8 itself. Indeed note that $\nu(1, -1, d) = (1/8)(1 - 1/d)$ for odd d, and $\nu(4, 1, 16) = 1/8$.

As we will see below, the largest accumulation point occurs at 3, created by having $b_i = b_j$ for some $i \neq j$. In fact if $\mathbf{b}= \{m, m, 2n, -2(m + n)\}$ with $(2n, m) = 1$ then $\omega(\mathbf{b}) = 3$. If $\mathbf{b}= \{m, m, n, -2m - n\}$ with $(n, 2m) = 1$ then $\omega(\mathbf{b}) = 3 + 3/n(n + 2m)$, which equals $3 + 3/d$ where $d = n(n + 2m)$ is odd. Any odd d can be written in this form, and thus arises from such a set $\mathbf{b}$, except when $d = 1$ since then we would have $m = 0$.
Now assume $\omega(\mathbf{b}) \geq 3$ and $b_i \neq b_j$ for all $i \neq j$. Proceeding as at the end of the last subsection, we note that at most 3 of the numbers $\{(b_i, b_j)^2/b_ib_j : 0 \leq i < j \leq 3\}$ can be positive; and, under our assumptions here, their sum is > 1, whereas they are each $\leq 1/2$. Therefore we must have three positive terms, and they would have to be $1/2 + 1/2 + 1/m$ for any $m \geq 2$, or $1/2 + 1/3 + 1/m$ for $m = 3, 4$ or 5. If the latter case the third ratio would have to be 1/6 giving a contradiction. In the first case the only configuration that could arise is from $\mathbf{b}= \{1, 2, 4, -7\}$, in which case $\omega(\mathbf{b}) = 3$. Thus

The set of values of $\nu(a_1, a_2, a_3)$ which are $\geq 1/4$ are precisely the numbers of the form $(1/4)(1 + 1/d)$ with $d \geq 3$ odd, and $1/4$ itself. Indeed note that $\nu(m, m + 1, -m) = (1/4)(1 + 1/(2m + 1))$, and $\nu(1, 2, 4) = 1/4$.

The Accumulation Points: 2 is an accumulation point, since $\omega(\mathbf{b}) \to 2$ if $b_1 = 1$ and $b_2, b_3 \to \infty$ so that $(b_2, b_3) = (b_2, b_3 - 1) = (b_3, b_2 - 1) = 1$.
If $|\omega(\mathbf{b}) - 2| > \epsilon$ then

$$\max_{0\leq i<j\leq 3} \frac{(b_i, b_j)^2}{|b_i b_j|} \geq \frac{1}{6} \sum_{0\leq i<j\leq 3} \frac{(b_i, b_j)^2}{|b_i b_j|} \geq \frac{|\omega(\mathbf{b}) - 2|}{6} > \epsilon/6,$$

so there are only finitely many possibilities for this largest fraction; that is, $b_i/b_j = r/s$ for some coprime integers r and s with $|rs| < 6/\epsilon$. Then $\mathbf{b}= \{rm, sm, n, -n - (r + s)m\}$ for some integer n, with $mn(r + s) > 0$ and $(n, m) = 1$, and so

$$\left|\omega(\mathbf{b}) - \left(2 + \frac{1}{rs}\right)\right| \leqq \frac{r^2}{|rmn|} + \frac{s^2}{|smn|} + \frac{r^2}{|rmn|} + \frac{s^2}{|smn|} + \frac{|r + s|^2}{|nN|} \ll \frac{1}{|n|}$$

where $|N| = |n+(r+s)m| > |n|$. Therefore the accumulation points are precisely points of the form $2 + \frac{1}{rs}$ with r, s coprime. Now any integer d can be written as rs with $r = d$ and $s = 1$, so the accumulation points are all of the form $2 + 1/d, d \in \mathbb{Z}^*$. However if $d = -1$ then $rm + sm = 0$ so this is not allowed. Thus we deduce

The set of accumulation points of $\nu(a_1, a_2, a_3)$ are precisely $1/6$ and the numbers of the form $1/6+1/12d$ with d an integer other than 0 or -1. Indeed $\nu(1, d+1, n) \to 1/6+1/12d$ as $n \to \infty$.

10b. The case $k = 4$. In this case we define

$$\omega(\mathbf{b}) := 24\nu(\mathbf{a}) = 1 + \sum_{0\leq i<j\leq 4} \frac{(b_i, b_j)^2}{b_i b_j}.$$

Below we see that the largest accumulation point for ω is 4 created by having $b_2 = b_3 = b_4$, and the smallest, other than 0, is 1/6 created by having $b_2 = -2b_1$ and $b_3 = -3b_1$. All cases for $k = 4$ are considerably harder then for $k = 3$, though one can obtain the results below by essentially the same methods.
There are either four or six positive numbers amongst $\{(b_i, b_j)^2/b_i b_j\}$. If $\omega(\mathbf{b}) \geq 4$ then the sum of these positive numbers is > 3. Suppose for now that no three of the b_is are equal. Then there must be six positive numbers in this set, and one of them must be 1. Testing the five possibilities that arise, the only values ≥ 4 are $\omega(1, 1, 2, 2, -6) = \omega(1, 4, 2, 2, -9) = 4$. If three of the b_i's are equal we either have $\omega(a, a, a, 3b, -3(a+b)) = 4$, or $\omega(a, a, a, b, -(3a + b)) = 4 + 8/b(b + 3a)$ whenever $(b, 3a) = 1$. Now $b(b + 3a)$ with $a, b \neq 0$ represents every integer $\equiv 1 \pmod 3$ except 1; and thus the spectrum contains every number of the form $4 + 8/d$ where $d \equiv 1 \pmod 3$ with $d \neq 1$. Thus

The set of values of $\nu(a_1, a_2, a_3, a_4)$ which are $\geq 1/6$ are precisely the numbers of the form $(1/6)(1 + 2/d)$ with $d \geq 4$ and $d \equiv 1 \pmod 3$, as well as $1/6$ itself. Indeed note that $\nu(m, 2m, 3m, -1) = (1/6)(1 + 2/(3m + 1))$, and $\nu(1, 2, 3, 6) = 1/6$.

The lower end of this spectrum is much more difficult to understand. We start by studying when $\nu(\mathbf{a})= 0$. By Lemmas 6.1 and 6.2 we know that $\nu(\mathbf{a})= 0$ if a subsum of the b_i's is 0, or $\mathbf{b}= \{m, -2m, n, -2n, m + n\}$ for some m and n. Working as above we can restrict our computations to a finite set of cases and establish that, other than those sets $\mathbf{b}$ just described, $\omega(\mathbf{b})= 0$ if and only if $\mathbf{b}$ is one of the sets below:

$-9, -1, 2{,}3, 5$
$-9, -2, 1{,}4, 6$
$-9, -4, 2{,}3, 8$
$-10, -6, 2{,}5, 9$
$-12, -1, 2{,}3, 8$
$-12, -1, 3{,}4, 6$
$-12, -2, 1{,}4, 9$
$-12, -2, 3{,}4, 7$
$-12, -3, 1{,}6, 8$
$-12, -3, 4{,}5, 6$
$-12, -5, 3{,}4, 10$
$-14, -1, 3{,}5, 7$
$-14, -3, 1{,}7, 9$
$-15, -1, 2{,}5, 9$
$-15, -1, 3{,}5, 8$
$-15, -2, 1{,}6, 10$
$-15, -2, 3{,}4, 10$
$-15, -4, 2{,}5, 12$
$-15, -4, 5{,}6, 8$
$-15, -7, 3{,}5, 14$
$-18, -1, 4{,}6, 9$
$-18, -2, 5{,}6, 9$
$-18, -4, 1{,}9, 12$
$-20, -1, 3{,}8, 10$
$-20, -1, 4{,}7, 10$
$-20, -3, 1{,}10, 12$
$-20, -3, 4{,}9, 10$
$-24, -1, 5{,}8, 12$
$-30, -1, 6{,}10, 15$

By the same computation as before we can compute the finitely many sets $\mathbf{b}$ with $\omega(\mathbf{b})< 1/6-\epsilon$. In fact there are the sets $\mathbf{b}$ of the form $\{m, -2m, n, -3n, m+2n\}$, and only finitely many other sets with $\omega(\mathbf{b})< 1/6$. We computed all of them, far too many to include here. The smallest nonzero values found, $< 1/11$, were, in ascending order

$$\begin{aligned}
4/77 &= \omega(-21,-11,3,7,22)\\
2/35 &= \omega(-28,-5,4,14,15)\\
4/65 &= \omega(-26,-3,1,13,15)\\
1/14 &= \omega(-21,-8,6,7,16) = \omega(-21,-4,2,7,16)\\
4/55 &= \omega(-30,-2,6,11,15) = \omega(-22,-6,2,11,15) = \omega(-22,-5,1,11,15)\\
1/13 &= \omega(-24,-3,6,8,13) = \omega(-24,-13,3,8,26)\\
6/77 &= \omega(-28,-1,4,11,14)\\
1/12 &= \omega(-32,-3,1,16,18)\\
12/143 &= \omega(-26,-1,3,11,13)\\
8/91 &= \omega(-21,-1,2,7,13)\\
4/45 &= \omega(-27,-4,2,9,20)\\
12/133 &= \omega(-38,-3,1,19,21)
\end{aligned}$$

To verify this, we note that if $0 < \omega(\mathbf{b}) \leq 4/77$ and the largest two ratios are $1/m + 1/n$ with $2 \leq m \leq n$, then either $n \geq 3$ in which case the third largest ratio is $\leq 4/(73/77 - 1/m - 1/n)$; or $m = n = 2$ and, since we are avoiding the case of Lemma 2, the third largest ratio is $\leq 4/(73/77 - 1/2 - 1/2 + 1/4) < 21$. Either way, with three ratios given, the set $\mathbf{b}$ is determined and there is a finite computation remaining.

Accumulation points: We proceed much as for $k = 3$. By (5.4) the accumulation points are $\frac{1}{24}$, for a "typical" $\mathbf{b}$;

$$\frac{1}{24}\left(1+\frac{1}{m}\right),\ m \in \mathbb{Z}^*,$$

which we obtain from $b = \{1, m, -b_1, -b_2, b_1 + b_2 - (m+1)\}$ as $b_1, b_2 \to \infty$;

$$\frac{1}{24}\left(1+\frac{1}{m}+\frac{1}{n}\right),\ m, n, \in \mathbb{Z} \setminus \{0,-1\},\ m, n \ \text{ not both in } \{-2, -1/2\},$$

which we obtain from $b = \{1, m, b_1, nb_1, -(m+1) - (n+1)b_1\}$ as $b_1 \to \infty$; and

$$\frac{1}{24}\left(1+\frac{1}{AB}+\frac{1}{AC}+\frac{1}{BC}\right) \text{ with } (A,B,C) = 1 \text{ and } A, B, C \in \mathbb{Z}^*.$$

To obtain this last one take $b = \{r, s, t, b, b - r - s - t\}$ with $b \to \infty$ and $(r, s, t) = 1$. We have $\nu(\mathbf{a}) = \frac{1}{24}\left(1 + \frac{(r,s)^2}{rs} + \frac{(r,t)^2}{rt} + \frac{(s,t)^2}{st}\right)$. Writing $g = (r, s), h = (r, t), j = (s, t)$ and $R = r/gh, S = s/gj, T = t/hj$, the internal sum is $1/AB + 1/AC + 1/BC$ with

$A = gT, B = hS, C = jR$. One can check $(A, B, C) = 1$. On the other hand, given $(A, B, C) = 1$ we select

$$g = \prod_{\substack{p|(A,B)\\ p^\lambda||A}} p^\lambda, \ h = \prod_{\substack{p|(B,C)\\ p^\lambda||B}} p^\lambda, \ j = \prod_{\substack{p|(C,A)\\ p^\lambda||C}} p^\lambda,$$

(where $p^\lambda||A$ means that $p^\lambda|A$ but $p^{\lambda+1} \not| A$) and $T = A/g, S = B/h$ and $R = C/j$, and we can recover r, s, t as above.

11. Accumulation points for general k.

Define $\Gamma_k = \{\nu(a_1, \dots, a_k) : a_i$ distinct non-zero integers$\}$ and let $\hat{\Gamma}_k$ be the set of accumulation points of Γ_k.

Proposition 11.1. *If $\nu(a_1, \dots, a_n) \in \Gamma_k \setminus \{0\}$ then $\nu_j^*(a_1, \dots, a_k) \in \hat{\Gamma}_{k+1}$ for any $j, 0 \leq j \leq k$, where*

$$v_j^*(a_1, \dots, a_k) := \int\limits_{\substack{0 \leq t \leq 1\\ (3.2) \text{ holds}}} \{b_j t\} dt.$$

Proof. Note that $v_j^*(\mathbf{a}) = \lim_{p\to\infty} v_{j,p}^*(\mathbf{a})$ where we define

$$v_{j,p}^*(\mathbf{a}) := \frac{1}{p^2} \sum_{n \in A} (b_j n)_p$$

where A is the set of $n \pmod p$ for which (1.1) is satisfied. Let $N_j(\mathbf{a}, t; p)$ be the number of $n \in A$ satisfying the additional inequality

$$(a_{j-1}n)_p < (tn)_p < (a_j n)_p. \tag{11.1}$$

Then

$$\frac{1}{p} \sum_{t \pmod p} N_j(\mathbf{a}, t, p) = \frac{1}{p} \sum_{t \pmod p} \sum_{n\in A:\ (11.1) \text{ holds}} 1 = \frac{1}{p} \sum_{n\in A} \sum_{\substack{t \pmod p:\\ (11.1) \text{ holds}}} 1$$
$$= \frac{1}{p} \sum_{n \in A} ((a_j n)_p - (a_{j-1}n)_p - 1) = pv_{j,p}^* - |A|/p = pv_{j,p}^* + O(1).$$

Also

$$\frac{1}{p} \sum_{t \pmod p} N_j(\mathbf{a}, t_j; p)^2 = \frac{1}{p} \sum_{m,n \in A} \sum_{\substack{t \pmod p\\ (11.1) \text{ holds for}\\ m \text{ and } n}} 1$$

Now, Proposition 8.2 gives

$$\frac{1}{p} \sum_{\substack{t \pmod p \\ (11.1) \text{ holds for } m \text{ and } n}} 1 = \frac{(b_j m)_p}{p} \frac{(b_j n)_p}{p} + O\left(\frac{1}{\sqrt{p}} + \frac{1}{|uv|} \right)$$

where $u/v \equiv m/n \pmod p$ with $|u|, |v| < \sqrt{p}$. There are $p-1$ pairs $m, n \pmod p$ for given u and v, and so the above sum becomes

$$\sum_{m,n \in A} \left(\frac{(b_j m)_p}{p} \frac{(b_j n)_p}{p} + O\left(\frac{1}{\sqrt{p}} \right) \right) + O\left(p \sum_{|u|,|v| < \sqrt{p}} \frac{1}{|uv|} \right) = (pv_{j,p}^*)^2 + O(p^{3/2}).$$

Thus $N_j(\mathbf{a}, t; p)$ has normal order $pv_{j,p}^*$, and the result is proved, varying over t.

12. Generalizations

One can generalize our question to residue races between given polynomials. That is, if $f_1(x), f_2(x), \dots, f_k(x) \in \mathbb{Z}[x]$ then define $N(f_1, f_2, \dots, f_k; p)$ to be the number of residues $n \pmod p$ for which

$$(f_1(n))_p < (f_2(n))_p < \cdots < (f_k(n))_p; \tag{12.1}$$

(1.1) is the case where the f_i's are all linear with no constant term. Even when $k = 2$ this question can be a little tricky:

12a. Two polynomials race.
Notice that $(f(n))_p < (g(n))_p$ if and only if $\{f(n)/p\} + \{(g-f)(n)/p\} = \{g(n)/p\}$, and so

$$\begin{aligned} N(f, g; p) &= \sum_{n \pmod p} \left(1 + \left\{ \frac{g(n)}{p} \right\} - \left\{ \frac{f(n)}{p} \right\} - \left\{ \frac{(g-f)(n)}{p} \right\} \right) \\ &= \frac{p}{2} + \sum_{n \pmod p} \left(\psi\left(\frac{g(n)}{p} \right) - \psi\left(\frac{f(n)}{p} \right) - \psi\left(\frac{(g-f)(n)}{p} \right) \right). \end{aligned}$$

For non-constant polynomials $f(x)$ of small degree (compared to p) one can show that $\sum_{n \pmod p} \psi(f(n)/p) = o(p)$. Therefore $N(f, g; p) \sim p/2$ provided none of f, g and $f - g$ are constants.

12b. Three linear polynomials race.
We briefly investigate $N(f_1, f_2, f_3; p)$ where each $f_i(x) = b_i x + c_i$. Imitating (4.3) we find that

$$\frac{1}{p} S(f_1, f_2; p) = -\frac{1}{4\pi^2} \sum_{\substack{h_1, h_2 \in \mathbb{Z}^* \\ h_1 b_1 + h_2 b_2 \equiv 0 \pmod p}} \frac{1}{h_1 h_2} e\left(\frac{c_1 m_1 + c_2 m_2}{p} \right);$$

and then, as in the proof of Theorem A, this equals

$$\begin{aligned}\frac{1}{4\pi^2}\,\frac{(b_1,b_2)^2}{b_1b_2}\sum_{t\in\mathbb{Z}^*}\frac{1}{t^2}e\left(\frac{t(c_1b_2-c_2b_1)}{p(b_1,b_2)}\right)+O(\frac{\log p}{\sqrt{p}})\\ =\frac{1}{p}S(b_1,b_2;p)+o(1)-\sum_{0\le i<j\le 3}\frac{1}{\beta_{i,j}\beta_{j,i}}\frac{\gamma_{i,j}(1-\gamma_{i,j})}{2},\end{aligned}$$

by (8.1), where $\beta_{i,j}=b_i/(b_i,b_j)$ and $\gamma_{i,j}=\{(\beta_{i,j}c_j-\beta_{j,i}c_i)/p\}$. When none of the ratios b_i/b_j has a small numerator the last term here is swallowed up by the "$o(1)$", so that $S(f_1,f_2;p)=o(p)$. When some b_i/b_j has a small numerator the calculation is evidently more intricate.

12c. General distribution problems.

Let $u_1,u_2,\dots,u_q$ be a set of points in $\mathbb{T}^k$ and let $\Omega\subset\mathbb{T}^k$. One estimates $\#\{1\le i\le q:\ u_i\in\Omega\}/q$, and enquires whether this is approximately $\mathrm{Vol}(\Omega)$?

In our problem (1.1) above $q=p-1$ and $u_n=(\{a_1n/p\},\{a_2n/p\},\dots,\{a_kn/p\})$, with $\Omega=\{(t_1,t_2,\dots,t_k):\ 0<t_1<t_2<\dots<t_k<1\}$. The points u_n may be described as follows: Take all points on the line $\mathcal{L}$ which is the x-axis mod p, in other words, $\{n:\ 0\le n\le p-1\}$, and then consider the map $\phi:\mathcal{L}\to\mathbb{T}^k$ given by $n\to\mathbf{a}n/p$. Here we had $\mathrm{Vol}(\Omega)=1/k!$ and we found that $\#\{1\le i\le q:\ u_i\in\Omega\}/q$ is close to $\mathrm{Vol}(\Omega)$ provided there is no linear relation with small coefficients involving the a_i's (see the first proof of the first part of Corollary 1). Moreover when $k=3$ and 4 we have seen that if there is a linear relation with small coefficients involving the a_i's then the value of $\#\{1\le i\le q:\ u_i\in\Omega\}/q$ is often quite different from $\mathrm{Vol}(\Omega)$, and can be determined in terms of the linear relations involving the a_i's. Note that the linear relations satisfied by the a_i determine a subspace of $\mathbb{T}^k$ in which $\phi(\mathcal{L})$ lives.

In (12.1) we consider the map $\phi:\mathcal{L}\to\mathbb{T}^k$ given by

$$\phi(n)=(f_1(n)/p,f_2(n)/p,\dots,f_k(n)/p)\pmod 1;$$

this provides our u_n.

More generally we can replace the line $\mathcal{L}$ by any curve $\mathcal{C}$ and consider any rational map $\phi:\mathcal{C}\to\mathbb{T}^k$, letting the u_n be the images of the $\mathbb{F}_p$-rational points on $\mathcal{C}$. In the very simple examples above we found that when $\#\{1\le i\le q:\ u_i\in\Omega\}/q$ is not close to $\mathrm{Vol}(\Omega)$, it transpires that $\phi(\mathcal{C})$ lives in a (linear) subspace S of $\mathbb{T}^k$ described by linear equations with small coefficients. In [2] it is shown that this is also true in the level of generality described at the start of this paragraph; moreover that $\#\{1\le i\le q:\ u_i\in\Omega\}/q$ is very close to $\mathrm{Vol}(\Omega\cap S)$. Thus the difficulty in such (seemingly deep) distribution problems boils down to the same (difficult) linear algebra problems we are having in our seemingly much simpler question.

References

1. P. Borwein, *The arc length of the lemniscate* $|p(z)|=1$, Proc. Amer. Math. Soc. **123** (1995), 797–799.

2. A. Granville, I. Shparlinski and A. Zaharescu, *On the distribution of rational functions along a curve of* $\mathbb{F}_p$ *and Residue Races* (to appear).
3. R. R. Hall and P. Shiu, *The distribution of totatives*, Canadian Mathematical Bulletin **45** (2002), 109–114.
4. H. Rademacher and E. Grosswald, *Dedekind sums*, Carus Mathematical Monographs, XIV, Mathematical Assoc. Amer., 1972.

Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA
E-mail address: andrew@math.uga.edu, dshiu@math.uga.edu

Department of Mathematics, Loughborough University, Leics LE11 3TU, England
E-mail address: P.Shiu@lboro.ac.uk