A GENERALIZATION OF AN IMO PROBLEM

Alex Fink[1]
Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada
finka@math.ucalgary.ca

Received: 8/15/05, Revised: 5/2/06, Accepted: 5/12/06, Published: 5/17/06

Abstract

Bill Sands has conjectured that for no integer $n \geq 3$ does there exist a vector of n integers whose dot products with all permutations of $(1, \ldots, n)$ form a complete residue system mod $n!$. In this paper we verify this conjecture when $n + 1$ is not prime, $n = 4$, and $n = 6$. We also suggest a generalization of the problem.

1. Introduction

In the 2001 International Mathematical Olympiad ([4, 1], or p. 118 of [3]), the following was posed as Problem 4. We have adapted the notation slightly.

> Let n be an odd integer greater than 1, and let $a_1, a_2, \ldots, a_n$ be given integers. For each of the $n!$ permutations $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ of $1, 2, \ldots, n$, let
>
> $$T(\mathbf{b}) = \sum_{i=1}^{n} a_i b_i.$$
>
> Prove that there are two permutations $\mathbf{b}$ and $\mathbf{b}'$, $\mathbf{b} \neq \mathbf{b}'$, such that $n!$ is a divisor of $T(\mathbf{b}) - T(\mathbf{b}')$.

It will be convenient for our purposes to consider permutations of $0, 1, \ldots, n-1$ rather than $1, 2, \ldots, n$; this makes no fundamental difference to the problem.

This problem was proposed by Bill Sands, who conjectures ([3], p. 143) that the result holds for all integers $n > 2$. It is clearly false for $n = 1$ and $n = 2$, with $a_1 = 0$ and $(a_1, a_2) = (0, 1)$, respectively, providing counterexamples.

[1] The author's work was done while holding a NSERC Undergraduate Research Fellowship in 2003 and was supported by NSERC Discovery Grant #8306.

Our main result addresses a generalization of the above problem, verifying Sands's conjecture for many more $n > 2$.

Theorem 1 *Let n be a positive integer such that $n+1$ is not prime, and let $a_1, a_2, \ldots, a_n$ be integers. There exist distinct permutations $\mathbf{b}$ and $\mathbf{b}'$ of $0, 1, \ldots, n-1$ for which*

$$\sum_{i=1}^{n} a_i b_i \equiv \sum_{i=1}^{n} a_i b_i' \pmod{n!}.$$

In particular, Theorem 1 applies when $n > 2$ is odd, and so the IMO problem follows as a special case of this theorem.

We will call a vector $\mathbf{a} = (a_1, \ldots, a_n)$ of integers **nice** (in the sense of "showing fine discrimination") if there do not exist such permutations $\mathbf{b} \neq \mathbf{b}'$, i.e. if

$$\{\mathbf{a} \cdot \mathbf{b} \mid \mathbf{b} \text{ a permutation of } \{0, \ldots, n-1\}\}$$

is a complete set of residues modulo $n!$. Thus Theorem 1 asserts that *there exist no nice vectors of length n, for $n+1$ not prime.*

In the next section, we present some preliminaries. We then present a proof of Theorem 1, followed by independent proofs that there are no nice vectors for the cases $n = 4$ and $n = 6$, which are the two smallest cases not covered by Theorem 1. Finally we comment on some open problems.

2. Preliminaries

Any nonzero rational q can be uniquely written as

$$q = \pm t_1^{a_1} t_2^{a_2} \ldots t_k^{a_k},$$

where $t_1, t_2, \ldots, t_k$ are distinct primes and each a_i is a nonzero integer. For a prime t_i, we define $\mathrm{ord}_{t_i}(q)$, the *order* of t_i in q, to be the exponent a_i of t_i in the above expression, or 0 if t_i does not appear. We also set $\mathrm{ord}_t(0) = \infty$ for any prime t, and will adopt the usual arithmetical conventions regarding ∞, in particular: $\infty + \infty = \infty + n = \infty$ and $n < \infty$ for all positive integers n. Then the following lemma is easy to prove.

Lemma 1 *For any prime t and rationals q and r,*

(a) $\mathrm{ord}_t(q \pm r) \geq \min(\mathrm{ord}_t(q), \mathrm{ord}_t(r))$*, and equality holds if* $\mathrm{ord}_t(q) \neq \mathrm{ord}_t(r)$*;*

(b) $\mathrm{ord}_t(qr) = \mathrm{ord}_t(q) + \mathrm{ord}_t(r)$*;*

The Bernoulli numbers $B_0, B_1, B_2, \ldots$ (e.g., see §6.5 of [2]) are rational numbers defined by the recurrence

$$B_0 = 1, \qquad \sum_{i=0}^{k-1} \binom{k}{i} B_i = 0 \text{ for } k \geq 2.$$

So $B_1 = -1/2$, $B_2 = 1/6$, $B_3 = 0$, $B_4 = -1/30$, etc. It is known (e.g., page 301 of [2]) that for t prime,

$$\mathrm{ord}_t(B_{t-1}) = -1, \qquad \mathrm{ord}_t(B_i) \geq 0 \text{ for all } i < t-1. \tag{1}$$

One of the most familiar properties of the Bernoulli numbers is that they satisfy

$$\sum_{i=0}^{x-1} i^{t-1} = \frac{1}{t} \sum_{j=0}^{t-1} B_j \binom{t}{j} x^{t-j} \tag{2}$$

for all positive integers t. In particular, this demonstrates that the function

$$S_t(x) = \sum_{i=0}^{x-1} i^t = \frac{1}{t+1} \sum_{j=0}^{t} B_j \binom{t+1}{j} x^{t+1-j}$$

is a polynomial in x of degree $t+1$ for each $t \geq 0$.

Write $[x^j]P(x)$ to denote the coefficient of x^j in the polynomial $P(x)$.

Lemma 2 *For any prime t and any integer $j \geq 0$,*

$$\mathrm{ord}_t([x^j]S_{t-1}(x)) \geq -1,$$

and

$$\mathrm{ord}_t([x^j]S_{k-1}(x)) \geq 0$$

for all integers $k < t$.

Proof. In case $j = 0$, it suffices to notice that $[x^0]S_{t-1}(x)$ is the constant term of $S_{t-1}(x)$ and is thus 0, so $\mathrm{ord}_t([x^j]S_{t-1}(x)) = \infty$. So let $j > 0$ henceforth.

Since t is prime, $t \mid \binom{t}{j}$ for $1 \leq j \leq t-1$. Hence, by (1) and Lemma 1(b), for any integer $j \in [2, t-1]$,

$$\mathrm{ord}_t([x^j]S_{t-1}(x)) = \mathrm{ord}_t\left(\frac{1}{t} B_{t-j} \binom{t}{t-j}\right) \geq -1 + 0 + 1 = 0;$$

also

$$\mathrm{ord}_t([x]S_{t-1}(x)) = \mathrm{ord}_t\left(\frac{1}{t} B_{t-1} \binom{t}{t-1}\right) = \mathrm{ord}_t(B_{t-1}) = -1$$

and

$$\mathrm{ord}_t([x^t]S_{t-1}(x)) = \mathrm{ord}_t\left(\frac{1}{t} B_0 \binom{t}{0}\right) = \mathrm{ord}_t(\frac{1}{t}) = -1.$$

Also, for each integer $k < t$ and each $1 \le j \le k$, again by (1) and Lemma 1(b),

$$\mathrm{ord}_t([x^j]S_{k-1}(x)) = \mathrm{ord}_t\left(\frac{1}{k}B_{k-j}\binom{k}{k-j}\right) = \mathrm{ord}_t(B_{k-j}) \ge 0.$$

□

For positive integers m and t, define $\mathcal{D}_{m,t}$ to be the set of all t-tuples of distinct integers from $0, 1, \ldots, m-1$. Let $\mathbf{q} = (q_1, q_2, \ldots, q_t)$ be a t-tuple of positive integers, and define

$$s_{\mathbf{q}}(m) = \sum_{\mathbf{b}\in\mathcal{D}_{m,t}} \prod_{i=1}^{t} b_i^{q_i},$$

where we write $\mathbf{b} = (b_1, b_2, \ldots, b_t)$. Note that if $m < t$, then the sum is empty and $s_{\mathbf{q}}(m) = 0$.

Lemma 3 *For each fixed* $\mathbf{q}$, $s_{\mathbf{q}}(m)$ *is a polynomial in* m, *with* $(m-k)$ *as a factor for each* $k = 0, 1, \ldots, t-1$.

We present two proofs of Lemma 3.

First proof. We will expand the sum $s_{\mathbf{q}}(m)$ with a general form of the inclusion-exclusion principle. Consider the statements $h_j = h_k$ for each $1 \le j < k \le t$. Call the set of all such statements P. The sum can then be written as

$$s_{\mathbf{q}}(m) = \sum_{P'\subseteq P} (-1)^{|P'|} \sum_{\mathbf{h}\models P'} \prod_{i=1}^{t} h_i^{q_i},$$

where, for any $P' \subseteq P$, $\mathbf{h} \models P'$ means that the sum ranges over all t-tuples $\mathbf{h} = (h_1, h_2, \ldots, h_t)$ of integers from $[0, m-1]$ for which every member of P' is true. Now, to each such subset P' there corresponds a graph G on $\{1, 2, \ldots, t\}$ defined as follows: the edge $\{j, k\}$ is in G if and only if the statement $h_j = h_k$ is in P'. Then for any j and k, h_j and h_k are forced to be equal in the inner sum if and only if vertices j and k are in the same component of G. Let $C_{G,1}, C_{G,2}, \ldots, C_{G,s_G}$ denote the components of G, and let Q_i denote the sum $\sum_{j\in C_{G,i}} q_j$. Then $s_{\mathbf{q}}(m)$ can be rewritten

$$s_{\mathbf{q}}(m) = \sum_{G} (-1)^{e(G)} \sum_{\mathbf{h}} \prod_{i=1}^{s_G} h_i^{Q_i},$$

where, for each G, $\mathbf{h}$ ranges over all s_G-tuples of integers from $[0, m-1]$, and where $e(G)$ is the number of edges of G. Now, the term inside the rightmost sum is a product of powers of independent variables, so we can switch the sum and the product, obtaining

$$s_{\mathbf{q}}(m) = \sum_{G} (-1)^{e(G)} \prod_{i=1}^{s_G} \sum_{k=0}^{m-1} k^{Q_i} = \sum_{G} (-1)^{e(G)} \prod_{i=1}^{s_G} S_{Q_i}(m). \tag{3}$$

But $S_{Q_i}(m)$ is a polynomial in m. Furthermore, $s_G \leq |G| = t$, and the number of graphs G is at most $2^{|P|} = 2^{\binom{t}{2}}$, both bounded for fixed $\mathbf{q}$. So, since $s_{\mathbf{q}}(m)$ is a sum of products of polynomials in m, we conclude that it can also be expressed as a polynomial in m.

Since $s_{\mathbf{q}}(m) = 0$ when $m < t$, as a polynomial $s_{\mathbf{q}}(m)$ must have the factor $m(m-1)\cdots(m-t+1)$. □

Second proof. We will show inductively on t that $s_{\mathbf{q}}(m)$ can be expressed as a polynomial in m. When $t = 1$, $s_{\mathbf{q}}(m) = S_{q_1}(m)$, which is a polynomial in m.

Suppose $t > 1$. Let $\mathbf{q}' = (q_1, q_2, \ldots, q_{t-1})$, and for each $1 \leq i \leq t-1$, let $\mathbf{q}_i = (q_1, q_2, \ldots, q_{i-1}, q_i + q_t, q_{i+1}, \ldots, q_{t-1})$. Then we can write

$$s_{\mathbf{q}}(m) = \left(\sum_{i=0}^{m-1} i^{q_t}\right) s_{\mathbf{q}'}(m) - \sum_{i=1}^{t-1} s_{\mathbf{q}_i}(m) = S_{q_t}(m) s_{\mathbf{q}'}(m) - \sum_{i=1}^{t-1} s_{\mathbf{q}_i}(m).$$

This equation holds even if $m < t$. $S_{q_t}(m)$ is a polynomial in m, and inductively $s_{\mathbf{q}'}(m)$ and $s_{\mathbf{q}_i}(m)$ for each i are polynomials in m. Thus so is $s_{\mathbf{q}}(m)$.

Again $s_{\mathbf{q}}(m) = 0$ when $0 \leq m < t$, so $s_{\mathbf{q}}(m)$ must have the given factors. □

3. Proof of Theorem 1

Let $n > 2$ be an integer with $n+1$ not prime. Towards a contradiction, let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ be a nice vector. Then as $\mathbf{b} = (b_1, \ldots, b_n)$ ranges over all permutations of $0, 1, \ldots, n-1$ (i.e. over the elements of $\mathcal{D}_{n,n}$),

$$T(\mathbf{b}) = \sum_{i=1}^{n} a_i b_i$$

takes on a value congruent to each of the integers $0, 1, \ldots, n! - 1$ at most once. Since $|\mathcal{D}_{n,n}| = n!$, $T(\mathbf{b})$ must take on a value congruent to each of $0, 1, \ldots, n! - 1$ exactly once.

Our condition on n guarantees that we may choose a prime $p < n$ for which $n \equiv -1 \pmod{p}$. Then $T(\mathbf{b})^{p-1}$ is congruent to each of $0^{p-1}, 1^{p-1}, \ldots, (n!-1)^{p-1}$ mod $n!$ as $\mathbf{b}$ ranges over the elements of $\mathcal{D}_{n,n}$. So

$$L := \sum_{\mathbf{b} \in \mathcal{D}_{n,n}} \left(\sum_{i=1}^{n} a_i b_i\right)^{p-1}$$

must be congruent modulo $n!$ to

$$R := \sum_{i=0}^{n!-1} i^{p-1} = S_{p-1}(n!).$$

By the multinomial theorem,

$$\begin{aligned} L &= \sum_{\mathbf{b}\in\mathcal{D}_{n,n}} \sum_{\mathbf{q}} \binom{p-1}{q_1 \quad q_2 \quad \cdots \quad q_n} \prod_{j=1}^{n} (a_j b_j)^{q_j} \\ &= \sum_{\mathbf{b}\in\mathcal{D}_{n,n}} \sum_{\mathbf{q}} \binom{p-1}{q_1 \quad q_2 \quad \cdots \quad q_n} \prod_{j=1}^{n} a_j^{q_j} \prod_{j=1}^{n} b_j^{q_j} \\ &= \sum_{\mathbf{q}} \binom{p-1}{q_1 \quad q_2 \quad \cdots \quad q_n} \left(\prod_{j=1}^{n} a_j^{q_j} \right) \sum_{\mathbf{b}\in\mathcal{D}_{n,n}} \prod_{j=1}^{n} b_j^{q_j}. \end{aligned}$$

as $\mathbf{q}$ ranges over every n-tuple of non-negative integers $(q_1, q_2, \ldots, q_n)$ satisfying $\sum_{i=1}^{n} q_i = p-1$.

For any such $\mathbf{q}$, let $t_{\mathbf{q}}$ be the number of its components which are nonzero. For any given permutation $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ of the integers $0, 1, \ldots, n-1$, consider the set of all permutations $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ such that $b_i = c_i$ for all i such that q_i is nonzero. There will be $(n - t_{\mathbf{q}})!$ such permutations $\mathbf{b}$, and for each of these permutations the product $\prod_{j=1}^{n} b_j^{q_j}$ will take the same value. Therefore, we can write

$$\begin{aligned} L &= \sum_{\mathbf{q}} \binom{p-1}{q_1 \quad q_2 \quad \cdots \quad q_n} \left(\prod_{j=1}^{n} a_j^{q_j} \right) (n - t_{\mathbf{q}})! \sum_{\mathbf{b}\in\mathcal{D}_{n,t_{\mathbf{q}}}} \prod_{j=1}^{t_{\mathbf{q}}} b_j^{q'_j} \\ &= \sum_{\mathbf{q}} \binom{p-1}{q_1 \quad q_2 \quad \cdots \quad q_n} \left(\prod_{j=1}^{n} a_j^{q_j} \right) (n - t_{\mathbf{q}})! s_{\mathbf{q}'}(n). \end{aligned}$$

where $\mathbf{q}' = (q'_1, q'_2, \ldots, q'_{t_{\mathbf{q}}})$ is obtained from $\mathbf{q}$ by deleting all of the zero components. Note that $\sum_{i=1}^{t_{\mathbf{q}}} q'_i = \sum_{i=1}^{n} q_i = p-1$.

By (3), for any integer m, $s_{\mathbf{q}'}(m)$ can be expressed as a sum of products of the form $S_{i_1}(m) \ldots S_{i_k}(m)$, with $\sum_{j=1}^{k} i_j = p-1$. In each such product, no $i_j > p-1$, and at most one $i_j = p-1$. Thus, by Lemma 2, the order of p in the coefficients of each S_i is at least 0, with one possible exception, where it may be -1. So if $S(x)$ is any of these products above, then for any integer a, $\mathrm{ord}_p([x^a]S(x)) \geq -1$ by Lemma 1(b), and consequently $\mathrm{ord}_p([x^a]s_{\mathbf{q}'}(x)) \geq -1$ by Lemma 1(a). Since this holds for any $\mathbf{q}'$, we can choose a positive integer h such that for any $\mathbf{q}'$, $hs_{\mathbf{q}'}(x)$ has integer coefficients, and that $p^2 \nmid h$; we can further require that $p! \mid h$, so that in particular $\mathrm{ord}_p(h) = 1$.

By Lemma 3, we may define the polynomial

$$s'_{\mathbf{q}'}(m) = \frac{s_{\mathbf{q}'}(m)}{m(m-1)\cdots(m-t_{\mathbf{q}}+1)}$$

for any $t_{\mathbf{q}}$-tuple $\mathbf{q}'$ of positive integers. We then set

$$\sigma = \sum_{\mathbf{q}} \binom{p-1}{q_1 \quad q_2 \quad \cdots \quad q_n} \left(\prod_{j=1}^{n} a_j^{q_j} \right) hs'_{\mathbf{q}'}(n),, \tag{4}$$

where the sum ranges over all n-tuples $\mathbf{q} = (q_1, \ldots, q_n)$ with sum $p-1$, so that $L = \sigma \cdot n!/h$. Now,

$$\begin{aligned} hs'_{\mathbf{q}'}(p-1) &= \frac{hs_{\mathbf{q}'}(p-1)}{(p-1)(p-2)\ldots(p-t_{\mathbf{q}})} \\ &= p \cdot s_{\mathbf{q}'}(p-1) \cdot \left(\frac{h}{p(p-1)(p-2)\ldots(p-t_{\mathbf{q}})} \right). \end{aligned}$$

Since the second and third factors of the last expression are both integers (in the latter case, by choice of h), we see that $p \mid hs'_{\mathbf{q}'}(p-1)$. But $hs_{\mathbf{q}'}$ is a polynomial with integer coefficients by our choice of h, so recalling the definition of $s'_{\mathbf{q}'}$, $hs'_{\mathbf{q}'}$ must also be a polynomial with integer coefficients. Consequently, the congruence class of $hs'_{\mathbf{q}'}(m)$ modulo p depends only on the congruence class of m mod p. In particular, since $p \mid hs'_{\mathbf{q}'}(p-1)$ and $n \equiv -1 \pmod p$, $p \mid hs'_{\mathbf{q}'}(n)$. This holds for arbitrary $\mathbf{q}'$, which means that p divides each term under the summation in (4), so $p \mid \sigma$, that is, there is an integer f for which $\sigma = pf$. Then $L = n!pf/h$.

We now turn our attention to R. From (2), x is a factor of $S_t(x)$ and $S_t(x)/x$ is a polynomial. Letting $S'_{p-1}(m) = S_{p-1}(m)/m$, we have by (2) that

$$\begin{aligned} S'_{p-1}(n!) &= \frac{S_{p-1}(n!)}{n!} = \frac{1}{n!p} \sum_{j=0}^{p-1} B_j \binom{p}{j} (n!)^{p-j} \\ &= \frac{(n!)^{p-1}}{p} + \sum_{j=1}^{p-2} \frac{1}{p} \binom{p}{j} B_j (n!)^{p-1-j} + B_{p-1}. \end{aligned}$$

But note that $p \mid n!$ (since $p < n$), and by (1) $\mathrm{ord}_p(B_j) \geq 0$ for $j < p-1$, $\mathrm{ord}_p(B_{p-1}) = -1$, thus $\mathrm{ord}_p(S'_{p-1}(n!)) = -1$ by Lemma 1(a). Because $\mathrm{ord}_p(h) = 1$ we then have that $\mathrm{ord}_p(hS'_{p-1}(n!)) = 0$ by Lemma 1(b). Therefore we can write

$$R = S_{p-1}(n!) = \frac{n!}{h} \cdot hS'_{p-1}(n!) = \frac{n!}{h} \cdot k$$

for rational k such that $\mathrm{ord}_p(k) = 0$.

Finally, because we have assumed L and R to be congruent modulo $n!$, we must have $L - R = n!d$ for some integer d. However, $hd = h(L-R)/n! = pf - k$, so $k = pf - hd$. In particular, k is integral. But $p \mid h$, while $p \nmid k$, a contradiction. This completes the proof. □

4. Two other cases

The following lemmas will be convenient to reduce the number of cases in the treatment of other values of n.

Lemma 4 *Suppose that* $\mathbf{a} = (a_1, \ldots, a_n)$ *is nice. Then:*

(a) any rearrangement of $\mathbf{a}$ *is nice;*

(b) for any integer k, $\mathbf{a}+k=(a_1+k,\ldots,a_n+k)$ *is nice; and*

(c) for any integer k *with* $(k,n!)=1$, $k\mathbf{a}=(ka_1,\ldots,ka_n)$ *is nice.*

Proof. Part (a) is easy to prove. For part (b), we have

$$\sum_{i=1}^{n}(a_i+k)b_i=\sum_{i=1}^{n}a_ib_i+\sum_{i=1}^{n}kb_i=\sum_{i=1}^{n}a_ib_i+\frac{1}{2}n(n+1)k.$$

The map $\phi(x)=x+\frac{1}{2}n(n+1)k$ is a bijection on the integers mod $n!$, so this expression takes each value mod $n!$ exactly once. This proves part (b). Similarly, when $(k,n!)=1$,

$$\sum_{i=1}^{n}(ka_i)b_i=k\sum_{i=1}^{n}a_ib_i.$$

As $\phi'(x)=kx$ is a bijection on the integers mod $n!$, this takes on every value mod $n!$ exactly once, proving part (c). $\square$

Recall that in the last section, we defined

$$T(\mathbf{b})=\sum_{i=1}^{n}a_ib_i$$

where $\mathbf{b}=(b_1,\ldots,b_n)$ is a permutation of $0,\ldots,n-1$.

Lemma 5 *Let* $\mathbf{a}=(a_1,\ldots,a_n)$ *be nice.*

(a) Let $m\mid n!$. *As* $\mathbf{b}$ *varies over all permutations of* $0,\ldots,n-1$, $T(\mathbf{b})$ *takes a value in each congruence class mod* m *exactly* $n!/m$ *times.*

(b) If n *is even, then* $\sum a_i$ *is odd.*

Proof. Part (a) follows easily from the observations that, modulo $n!$, $T(\mathbf{a})$ will be congruent to each integer $[0,n!-1]$ exactly once, and that each congruence class mod m is a union of $n!/m$ classes mod $n!$.

As for part (b), let $S_{\mathbf{a}}=\sum T(\mathbf{b})$ as $\mathbf{b}$ ranges over all permutations of $0,\ldots,n-1$. Then, modulo $n!$,

$$S_{\mathbf{a}}\equiv\sum_{i=0}^{n!-1}i=\frac{n!(n!-1)}{2}\equiv\frac{n!}{2}.$$

However, for any given integer $0\le k\le n-1$ and any index $1\le i\le n$, $b_i=k$ holds of just $(n-1)!$ different permutations $\mathbf{b}$. So if we consider the expansions of the $n!$ summands $T(\mathbf{b})$, we see that a_i occurs multiplied by k in exactly $(n-1)!$ of the summands, corresponding to those permutations $\mathbf{b}$ such that $b_i = k$. Hence, $S_{\mathbf{a}}$ can also be written (mod $n!$) as

$$S_{\mathbf{a}} = \sum_{i=1}^{n} a_i \cdot (n-1)! \sum_{k=0}^{n-1} k = \frac{(n-1)!n(n-1)}{2} \sum_{i=1}^{n} a_i = \frac{n!(n-1)}{2} \sum_{i=1}^{n} a_i.$$

So $n!/2 \equiv n!/2 \sum a_i \pmod{n!}$, and thus $\sum a_i$ must be odd. $\square$

In the upcoming proofs, congruence of vectors is to be interpreted componentwise. That is,

$$(a_1, \ldots, a_n) \equiv (b_1, \ldots, b_n) \pmod{t}$$

if and only if $a_i \equiv b_i \pmod{t}$ for all i.

We now handle the case $n = 4$, for which Sands also had a proof ([3], p. 143).

Theorem 2 *There exist no nice vectors of length $n = 4$.*

Proof. Suppose that $\mathbf{a} = (a_1, a_2, a_3, a_4)$ were nice. By Lemma 5(b), the sum of the components of $\mathbf{a}$ is odd, so the number of odd components of $\mathbf{a}$ is either 1 or 3. If it is 1, then $(a_1 + 1, \ldots, a_4 + 1)$ is a solution with three odd components by Lemma 4(b). So we may assume that $\mathbf{a}$ has three odd components. By Lemma 4(a), we can assume without loss of generality that $\mathbf{a} \equiv (0, 1, 1, 1) \bmod 2$.

Go on to consider $\mathbf{a}$ mod 8. Of the three odd components of $\mathbf{a}$, either two are congruent mod 8 or not. Suppose two of the components of $\mathbf{a}$ are congruent mod 8, and, without loss of generality, that these are a_2 and a_3. Then the permutations $\mathbf{b} = (1, 0, 3, 2)$ and $\mathbf{b}' = (1, 3, 0, 2)$ achieve

$$T(\mathbf{b}) - T(\mathbf{b}') = \sum_{i=1}^{4} a_i b_i - \sum_{i=1}^{4} a_i b_i' = 3(a_3 - a_2).$$

Since $8 \mid (a_3 - a_2)$, it follows that $T(\mathbf{b}) \equiv T(\mathbf{b}') \pmod{24}$, which contradicts that $\mathbf{a}$ is nice.

So we can assume that all of the odd components of $\mathbf{a}$ are distinct mod 8. Using Lemma 4 to multiply by an odd integer, and rearranging if necessary, it suffices to consider $\mathbf{a}$ congruent to $(0, 1, 5, 3)$ mod 8.

So assume $\mathbf{a} \equiv (0, 1, 5, 3) \pmod{8}$. In this case, we count the permutations $\mathbf{b}$ of $0, 1, 2, 3$ for which $T(\mathbf{b}) \equiv 2 \pmod{8}$. Examining the 24 cases, we find that the only such permutations are $(2, 0, 3, 1)$ and $(2, 1, 0, 3)$; since there are fewer than three of these, this case is impossible, by Lemma 5(a). This completes the proof. $\square$

Finally, we examine the case $n = 6$.

Theorem 3 *There exist no nice vectors of length $n = 6$.*

Proof. Suppose that $\mathbf{a} = (a_1, \cdots, a_6)$ were nice. By Lemma 5(b), we know that $\sum a_i$ is odd. By Lemma 4, we may assume without loss of generality that $\mathbf{a}$ is congruent to either $(0, 1, 1, 1, 1, 1)$ or $(0, 0, 0, 1, 1, 1)$ mod 2 (analogously to the case $n = 4$).

Now, consider $\mathbf{a}$ mod 4. If $\mathbf{a}$ is congruent to $(0, 1, 1, 1, 1, 1)$ mod 2, then by Lemma 4, we can assume that the even element of $\mathbf{a}$ is congruent to 0 mod 4 by adding 2 to $\mathbf{a}$ if necessary; also, by possibly multiplying by -1 we can assume that $\mathbf{a}$ has more elements congruent to 1 than to 3 mod 4. We then need to consider only the cases in which $\mathbf{a}$ is congruent to

$$(0, 1, 1, 1, 1, 1),\ (0, 1, 1, 1, 1, 3), \text{ and } (0, 1, 1, 1, 3, 3) \bmod 4.$$

If $\mathbf{a}$ is congruent to $(0, 0, 0, 1, 1, 1)$ mod 2, then we can assume that there there are more elements of $\mathbf{a}$ congruent to 0 mod 4 than to 2, and more congruent to 1 mod 4 than to 3. Furthermore, if $\mathbf{a} = (0, 0, 2, 1, 1, 1)$, the nice vector $-\mathbf{a}+1$ will be congruent to $(0, 0, 0, 1, 1, 3)$ mod 4. So we must also consider the cases in which $\mathbf{a}$ is congruent to

$$(0, 0, 0, 1, 1, 1),\ (0, 0, 0, 1, 1, 3), \text{ and } (0, 0, 2, 1, 1, 3) \bmod 4.$$

Altogether, we have six cases to consider. For most of the cases, we will need the fact, from Lemma 5(a), that we must have $6!/4 = 180$ values of $T(\mathbf{b})$ in each congruence class mod 4.

Case (i): $\mathbf{a} \equiv (0, 1, 1, 1, 1, 1)$

For any permutation $\mathbf{b}$, there are $5! = 120$ permutations (including $\mathbf{b}$) with the same first component, and the values of $T(\mathbf{b})$ for each of these values of $\mathbf{b}$ are congruent mod 4. Therefore, 120 divides the number of values of $T(\mathbf{b})$ in any congruence class mod 4. But $120 \nmid 180$, so there cannot be equally many values in each congruence class, and we can reject this case.

Case (ii): $\mathbf{a} \equiv (0, 1, 1, 1, 1, 3)$

Similarly to case (i), we obtain sets of $4! = 24$ permutations $\mathbf{b}$ for which the values of $T(\mathbf{b})$ are congruent mod 4, and $24 \nmid 180$, so we can reject this case as well.

Case (iii): $\mathbf{a} \equiv (0, 1, 1, 1, 3, 3)$

Consider the equivalence relation $\sim$ under which two permutations $\mathbf{b} = (b_1, \ldots, b_6)$ and $\mathbf{b}' = (b'_1, \ldots, b'_6)$ satisfy $\mathbf{b} \sim \mathbf{b}'$ iff $\{b_2, b_3, b_4\} = \{b'_2, b'_3, b'_4\}$ and $\{b_5, b_6\} = \{b'_5, b'_6\}$. Note that when $\mathbf{b} \sim \mathbf{b}'$, we will obtain $T(\mathbf{b}) \equiv T(\mathbf{b}')$. Each equivalence class of $\sim$ has size $3!2! = 12$. Thus, it suffices to consider one representative of each equivalence class and ascertain whether we obtain $180/12 = 15$ values of $T(\mathbf{b})$ in each congruence class mod 4.

We will count the vectors $\mathbf{b}$ for which $T(\mathbf{b}) \equiv -1 \pmod 4$. Observe that

$$T(\mathbf{b}) \equiv \sum_{i=1}^{6} b_i + 2(b_5 + b_6) - b_1 \equiv -1 + 2(b_5 + b_6) - b_1.$$

Consequently $2(b_5+b_6)-b_1 \equiv 0 \pmod 4$ and $b_1 \equiv 0 \pmod 2$. In the case that b_1 is either 0 or 4, we then have $2(b_5+b_6) \equiv 0 \pmod 4$, so $b_5+b_6 \equiv 0 \pmod 2$, implying b_5 and b_6 have the same parity. Of the components $b_2, \ldots, b_6$, two are even and three are odd, so there are four choices of b_5 and b_6. If b_1 is 2, we have $2(b_5+b_6) \equiv 2 \pmod 4$, so $b_5+b_6 \equiv 1 \pmod 2$, so b_5 and b_6 are of opposite parity. Since there remain two even and three odd bs, this can be done in 6 ways. Altogether, we have $4+4+6=14$ vectors, not the 15 we needed, ruling out the case $\mathbf{a} \equiv (0,1,1,1,3,3)$.

Case (iv): $\mathbf{a} \equiv (0,0,0,1,1,3)$

The permutations $\mathbf{b}$ can be placed in classes of size $3!2! = 12$ analogous to the classes of the last case. We count vectors $\mathbf{b}$, disregarding the order of b_1, b_2, b_3 and of b_4, b_5, for which $T(b) \equiv b_4+b_5-b_6 \equiv 0 \pmod 4$. This requires that $b_4+b_5-b_6 \equiv 0 \pmod 2$, so b_4, b_5, and b_6 either are all even or else consist of one even and two odd integers. If they are all even, they must be 0, 2, and 4, and it can be seen that this yields no solution to $b_4+b_5-b_6 \equiv 0 \pmod 4$. Suppose now that b_4 and b_5 are odd, and wlog $b_4 < b_5$. Then we get 5 solutions, as tabulated here:

b_4	b_5	b_6	Number of solutions
1	3	0, 4	2
1	5	2	1
3	5	0, 4	2

Otherwise, exactly one of b_4 and b_5, say b_4, is odd, as is b_6. This yields 8 solutions:

b_4	b_6	b_5	Number of solutions
1	5	0, 4	2
5	1	0, 4	2
1	3	2	1
3	1	2	1
3	5	2	1
5	3	2	1

We obtain 13 solutions in total, not 15, so we have shown it impossible that $\mathbf{a} \equiv (0,0,0,1,1,3)$.

Case (v): $\mathbf{a} \equiv (0,0,2,1,1,3)$

For this value of $\mathbf{a}$ our equivalence classes of $\mathbf{b}$s have size $2!2! = 4$, and for each congruence class of $T(\mathbf{b})$ mod 4 we will require $180/4 = 45$ vectors $\mathbf{b}$. We want $T(\mathbf{b}) \equiv 2b_3+b_4+b_5-b_6 \equiv 0 \pmod 4$. First, note that when b_3 is even, this reduces to the case $b_4+b_5-b_6 \equiv 0 \pmod 4$, whose solutions we counted in the discussion of case (iv). Since we found 13 solutions then, and each of them had two even numbers among b_1, b_2, and b_3, we obtain 26 solutions in this case. Now suppose b_3 is odd. We then require $b_4 + b_5 - b_6 \equiv 2 \pmod 4$. We will again tabulate the possible solutions. If b_4, b_5, and b_6 are all even, we assume that $b_4 < b_5$; then we have 9 solutions:

b_4	b_5	b_6	b_3	Number of solutions
0	2	4	1,3,5	3
0	4	2	1,3,5	3
2	4	0	1,3,5	3

If two of b_4, b_5, and b_6 are odd, still assuming that $b_4 < b_5$ we have 14 solutions:

b_4	b_5	(b_6, b_3)	Number of solutions
0	1	(3,5)	1
0	3	(1,5), (5,1)	2
0	5	(3,1)	1
1	2	(5,3)	1
1	3	(2,5)	1
1	4	(3,5)	1
1	5	(0,3), (4,3)	2
2	3		0
2	5	(1,3)	1
3	4	(1,5), (5,1)	2
3	5	(2,1)	1
4	5	(3,1)	1

Altogether we have $26 + 9 + 14 = 49$ possible vectors, and not 45, showing that $\mathbf{a} \equiv (0, 0, 2, 1, 1, 3)$ is impossible.

Case (vi): $\mathbf{a} \equiv (0, 0, 0, 1, 1, 1)$

We will examine this case mod 8. Of the three components congruent to 0 mod 4 in $\mathbf{a}$, at least two must be congruent mod 8, and of the three components congruent to 1 mod 4, at least two must also be congruent mod 8. Suppose without loss of generality that $a_1 \equiv a_2$ and $a_4 \equiv a_5$ mod 8. Then, we can place the permutations $\mathbf{b}$ into classes of size $2!2! = 4$, such that two vectors within one class differ only in a possible exchange of b_1 and b_2, or of b_4 and b_5, or both. Two vectors $\mathbf{b}$ in the same class yield congruent values of $T(\mathbf{b})$ mod 8. Thus the number of values of $T(\mathbf{b})$ in any given congruence class mod 8 is divisible by 4. Yet there should be $6!/8 = 90$ values in each congruence class by Lemma 5(a), and $4 \nmid 90$. Thus, this case as well is impossible.

We have now reached a contradiction in every case, and the proof is finished. □

5. Open problems

The least values of n for which the result of Theorem 1 is unknown are $n = 10$ and $n = 12$. It is likely that a proof for any particular one of the unknown cases, along the lines of that for $n = 6$ above, could be found, but a general technique is still lacking.

Here is another open problem. Instead of requiring the vectors $\mathbf{b}$, $\mathbf{b}'$ as in Theorem 1 to be permutations of $0, \ldots, n-1$, let them be permutations of any fixed multiset S of n integers.

> *Problem.* Characterise the multisets S such that for every vector $\mathbf{a}$ of length $n = |S|$, there do not exist distinct permutations $\mathbf{b}$, $\mathbf{b}'$ of S such that
>
> $$\mathbf{a} \cdot \mathbf{b} \equiv \mathbf{a} \cdot \mathbf{b}' \pmod{n!}.$$

We will present some basic observations on this problem, including its solution for $n \leq 3$.

We shall say that a vector $\mathbf{a}$ is **nice for** S if $\{\mathbf{a} \cdot \mathbf{b} | \mathbf{b}$ a permutation of $S\}$ is a complete set of residues modulo $n!$; we shall also say that a multiset S of size n **allows nice vectors** if there exists some $\mathbf{a}$ that is nice for S. Then the above problem asks for all multisets S which allow nice vectors.

There is a sort of symmetry in this problem between $\mathbf{a}$ and S. Given $\mathbf{a}$ and S, let S' be the multiset of all components of $\mathbf{a}$ and $\mathbf{a}'$ the vector of all elements of S. Let $S = \{s_1, \ldots, s_n\}$, and $S' = \{s'_1, \ldots, s'_n\}$. Any permutation $\mathbf{b}$ of S can be written $(s_{\sigma(1)}, \ldots, s_{\sigma(n)})$, where σ is a permutation of $\{1, \ldots, n\}$; if we then let $\mathbf{b}' = (s'_{\sigma^{-1}(1)}, \ldots, s'_{\sigma^{-1}(n)})$, it is easy to confirm that $\mathbf{a} \cdot \mathbf{b} = \mathbf{a}' \cdot \mathbf{b}'$. This establishes a bijection between the permutations of S and those of S'. In particular, if $\mathbf{a}$ is nice for S, then $\mathbf{a}'$ is nice for S'.

As this symmetry might suggest, an analogue of Lemma 4 holds in this new problem in which $\mathbf{a}$ is replaced by S. The more direct analogue of Lemma 4 continues to hold as well. We won't prove this statement here.

We will now consider particular values of n, starting with $n = 1$. Any multiset S of size 1 allows nice vectors. Indeed, if $|S| = 1$, there is only one possible permutation of S, so any vector $\mathbf{a}$ is vacuously nice.

For $|S| = 2$, if S has two elements of the same parity, it is clear that $\mathbf{a} \cdot \mathbf{b}$ has the same parity for either permutation $\mathbf{b}$ of S, so that S does not allow nice vectors. Otherwise, the multiset S has one even and one odd element. Then S must be congruent mod 2 to $\{0, 1\}$, and this problem reduces to our main problem. In particular, S allows nice vectors.

However, we claim that *no multiset S with $|S| = 3$ allows nice vectors*. Let $S = \{s_1, s_2, s_3\}$. We consider two cases, according as whether S contains two elements congruent modulo 3.

Suppose, without loss of generality, that $s_1 \equiv s_2 \pmod 3$. There must exist two components of $\mathbf{a} = (a_1, a_2, a_3)$, say a_1 and a_2, which are congruent mod 2. Then it is easily seen that for $\mathbf{b} = (s_1, s_2, s_3)$ and $\mathbf{b}' = (s_2, s_1, s_3)$, $T(\mathbf{b}) \equiv T(\mathbf{b}') \pmod{3!}$. So S does not allow nice vectors.

Now assume S has no two elements congruent modulo 3. S is congruent mod 6 to either $\{k, k+1, k+2\}$ or $\{k, k+2, k+4\}$ for some integer k, as we can see by examining all eight possibilities for S mod 6. Assume that $\mathbf{a}$ is nice for S. By the analogue of Lemma 4 for S that we mentioned above, $\mathbf{a}$ is then also nice for either $\{0, 1, 2\}$ or $\{0, 2, 4\}$. But the first of these cases is our main problem, and we have seen that $\{0, 1, 2\}$ does not allow nice vectors. As for $S = \{0, 2, 4\}$, $\mathbf{a} \cdot \mathbf{b}$ must be even for any permutation $\mathbf{b}$ of S, so $\{0, 2, 4\}$ does not allow nice vectors either. This verifies our claim.

Thus it remains to be resolved: *Are there any multisets S of size at least 4 which allow nice vectors?*

Acknowledgements

I would like to thank Bill Sands, my supervisor for the NSERC USRA Fellowship, under which this work was done, for his support, and in particular his many helpful suggestions regarding this paper. I also thank Richard Guy for suggesting the terminology "nice".

References

[1] Titu Andreescu and Zuming Feng, *USA and International Mathematical Olympiads 2001*, Mathematical Association of America, 2002.

[2] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley, 1989.

[3] A. M. Storozhev, J. B. Henry, and A. Di Pasquale. *Mathematics Contests 2001: The Australian Scene*, Australian Mathematics Trust, 2001.

[4] *The Official Scoring Site of the International Mathematical Olympiad 2001.* http://imo.wolfram.com/. Retrieved July 25, 2004.