When are subset sums equidistributed modulo m?

Stan Wagon[1]
Macalester College, St. Paul, MN 55105 (wagon@macalstr.edu)

and

Herbert S. Wilf[2]
University of Pennsylvania, Philadelphia, PA 19104 (wilf@central.cis.upenn.edu)

January 30, 1994

Abstract. For a triple (n, t, m) of positive integers, we attach to each t-subset $S = \{a_1, \ldots, a_t\} \subseteq \{1, \ldots, n\}$ the sum $f(S) = a_1 + \cdots + a_t$ (modulo m). We ask: for which triples (n, t, m) are the $\binom{n}{t}$ values of $f(S)$ uniformly distributed in the residue classes mod m? The obvious necessary condition, that m divides $\binom{n}{t}$, is not sufficient, but a q-analogue of that condition is both necessary and sufficient, namely:

$$\frac{q^m - 1}{q - 1} \quad \text{divides the Gaussian polynomial} \quad \binom{n}{t}_q.$$

We show that this condition is equivalent to: for each divisor $d > 1$ of m, we have $t \bmod d > n \bmod d$. Two proofs are given, one by generating functions and another via a bijection. We study the analogous question on the full power set of $[n]$: given (n, m); when are the 2^n subset sums modulo m equidistributed into the residue classes? Finally we obtain some asymptotic information about the distribution when it is not uniform, and discuss some open questions.

[1] Until July, 1994: P. O. Box 1782, Silverthorne, CO 80498 (71043.3326@compuserve.com)

[2] Supported by the Office of Naval Research

1. Introduction

While working on a problem related to lotteries, Larry Carter, of IBM, and the first author were led to the question of the title. Positive integers n, t, and m are given. By a *t-ticket* we mean a subset of $\{1, 2, \ldots, n\}$ of size t. The *value* of a t-ticket is the modulo-m sum of its entries. Our question is: for which triples (n, t, m) are the values of the t-tickets equally distributed among the m residue classes? Let us call a triple *uniform* if equidistribution holds.

There is an obvious necessary condition, namely that $\binom{n}{t}$ be divisible by m, but this is not sufficient, as the example $(n, t, m) = (5, 2, 2)$ shows. A special case of this question was considered by Snevily [4].

In this paper we will describe some of the experimentation that went into formulation of a conjecture about the necessary and sufficient condition. We then will prove that the conjecture is true, using the method of generating functions. Then we will give a bijective proof of the fact that (n, t, m) is uniform when the conditions of the theorem hold.

The following recurrence was used in our computations. For nonnegative integers (n, t, m), and for residue classes i modulo m, let $f(i, n, t, m)$ be the number of t-tickets from $\{1, 2, \ldots, n\}$ whose value is congruent to i mod m. Then we have

$$f(i, n, t, m) = f(i, n-1, t, m) + f(i-n, n-1, t-1, m). \qquad (1)$$

The proof is immediate, by considering separately those t-tickets that contain n and those that do not.

From this formula and suitable initial values it is easy to generate images of the uniform triples (we used *Mathematica*), by fixing m and varying t and n. Figure 1 shows twelve cases (moduli), where each plotted point indicates a uniform triple. The data suggest some definite patterns, but the statement that covers all cases does not immediately leap out.

Larry Carter made the observation from these data that the cases in which uniformity holds can be summarized by a succinct arithmetical condition (condition 3 in the theorem below).

Theorem. *The following properties of a triple (n, t, m) of positive integers are equivalent:*

1. *(n, t, m) is uniform;*
2. *$(q^m - 1)/(q - 1)$ divides the Gaussian polynomial $\binom{n}{t}_q$;*
3. *For all $d > 1$ that divide m, we have $t \bmod d > n \bmod d$ (here $a \bmod b$ denotes the least nonnegative residue).*

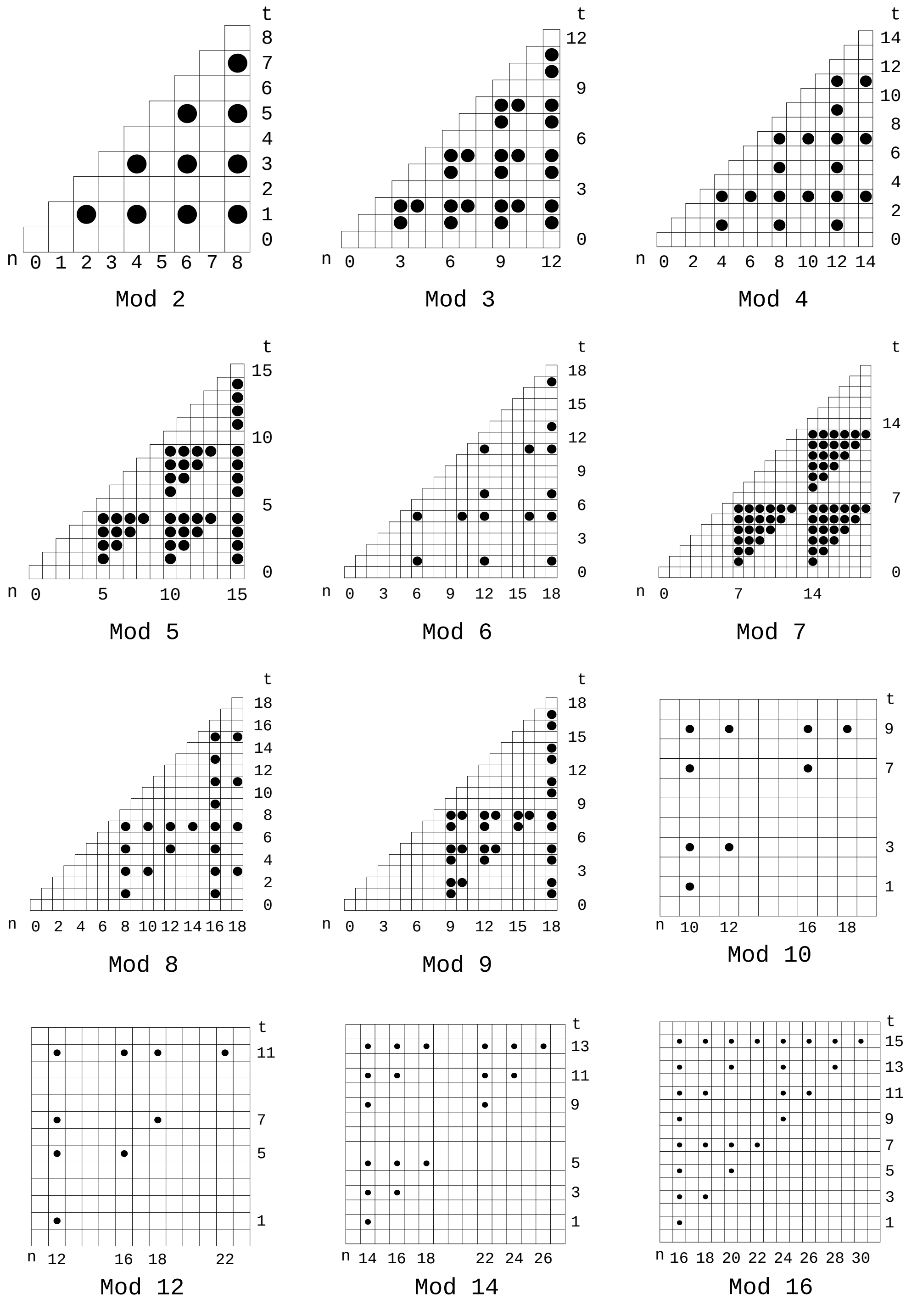

FIGURE 1. Dots indicate that t-subset sums from $[n]$ are equidistributed modulo m. By fixing m and varying t and n, various patterns are revealed. For example there is an m-periodicity in both the t- and the n-directions; thus for the moduli 10, 12, 14 and 16, we show only a fundamental region.

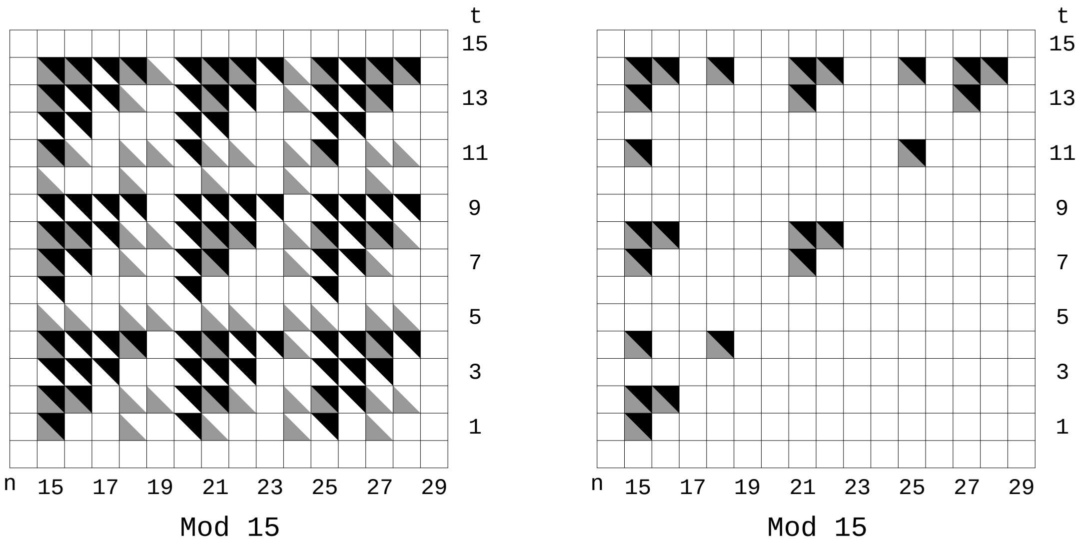

FIGURE 2. The uniform pairs (n, t) for modulus $m = 15$ arise from those for $m = 3$ and $m = 5$. The left chart shows the uniform pairs for 3 (gray triangles) and 5 (black triangles). A pair (n, t) is uniform modulo 15 iff it is uniform modulo 3 and 5 and t mod $15 > n$ mod 15, as in chart on right.

2. A proof by generating functions

To prove the theorem, we start with the following lemma.

Lemma 1. *Let $h(q)$ denote the t^{th} elementary symmetric function of the n quantities $q, q^2, \ldots, q^n$. Then the subset sums are equidistributed modulo m if and only if $h(q)$ is divisible by $(q^m - 1)/(q - 1)$.*

Proof. First, for each $i = 0, 1, 2, \ldots$, let a_i be the number of these sums that are *equal* to i. Then clearly the t^{th} elementary symmetric function of the n quantities $q, q^2, \ldots, q^n$ is

$$\sum_{1 \le i_1 < i_2 < \cdots < i_t \le n} q^{i_1} q^{i_2} \cdots q^{i_t} = \sum_{1 \le i_1 < i_2 < \cdots < i_t \le n} q^{i_1 + i_2 + \cdots + i_t} = \sum_i a_i q^i. \tag{2}$$

As before, let $f(i, n, t, m)$ denote the number of these sums that fall into residue class i mod m, and note that $h(q)$ is the sum in (2) above. Then $\sum_{i=0}^{m-1} f(i, n, t, m) q^i$ is equal to $h(q)$ modulo $(q^m - 1)$.

Moreover, if for all i, the $f(i, n, t, m)$ are equal, then what they are equal to must be $\binom{n}{t}/m$, so we must then have

$$\sum_{i=0}^{m-1} f(i, n, t, m) q^i = \frac{1}{m}\binom{n}{t} \sum_{i=0}^{m-1} q^i = \frac{1}{m}\binom{n}{t} \frac{q^m - 1}{q - 1} = h(q) \bmod (q^m - 1).$$

Hence in this case
$$h(q)=Q(q)(q^m-1)+\frac{1}{m}\binom{n}{t}\frac{q^m-1}{q-1}$$
and therefore $h(q)$ must be divisible by $(q^m-1)/(q-1)$.

Conversely, if
$$h(q)=p(q)\frac{q^m-1}{q-1}$$
for polynomial p, then $h(1)=\binom{n}{t}=p(1)m$ implies that $p(1)=\binom{n}{t}/m$. Thus
$$h(q)=p(q)\frac{q^m-1}{q-1}=(p(1)+(q-1)Q(q))\frac{q^m-1}{q-1}=Q(q)(q^m-1)+\frac{1}{m}\binom{n}{t}\frac{q^m-1}{q-1}.$$
Hence $h(q)$ modulo (q^m-1) has its coefficients all equal, and the sums are equidistributed modulo m. ∎

Lemma 2. *Let $g(q)$ be the rational function*
$$\frac{(1-q^{a_1})\cdots(1-q^{a_t})}{(1-q^{b_1})\cdots(1-q^{b_m})},$$
in which all of the a's and b's are positive integers. Define, for every integer $k\geq 1$, $e(k)$ to be the excess of the number of multiples of k that occur among the a_i's over the number that occur among the b_i's. Then in order that the rational function $g(q)$ be a polynomial, it is necessary and sufficient that $e(k)\geq 0$ for every positive integer k.

Proof. Write each expression $1-q^s$ as $\prod_{d\backslash s}F_d(q)$, where the F's are the cyclotomic polynomials. If we imagine replacing each factor in (4) by its cyclotomic factorization, then since the cyclotomic polynomials are irreducible, the quantity in (4) is a polynomial iff each fixed cyclotomic polynomial $F_k(q)$ appears there with a nonnegative exponent. But the exponent with which a given $F_k(q)$ appears is the excess of the number of multiples of k that appear among the a's over the number that appear among the b's. ∎

To prove the theorem, we need, by Lemma 1, to describe the conditions under which $h(q)$ is divisible by $(q^m-1)/(q-1)$. But $h(q)$ is the t^{th} elementary symmetric function of $q,q^2,\ldots,q^n$, and is therefore the coefficient of y^t in $\prod_{l=1}^n(1+yq^l)$ (this statement is identical with the recurrence (1) above).

However, the product $\prod_{l=1}^n(1+yq^l)$ is well known in combinatorics to be the generating function for the Gaussian polynomials $\binom{n}{j}_q$. Precisely, we have
$$\prod_{l=1}^{n}(1+yq^l)=\sum_{j=0}^{n}y^jq^{\binom{j+1}{2}}\binom{n}{j}_q.$$
Thus we see that the coefficient of y^t is
$$h(q)=q^{\binom{t+1}{2}}\binom{n}{t}_q=q^{\binom{t+1}{2}}\frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-t+1})}{(1-q)(1-q^2)\cdots(1-q^t)}.$$

Thus *necessary and sufficient for equidistribution is that*

$$\frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-t+1})}{(1-q^m)(1-q^2)\cdots(1-q^t)}$$

be a polynomial.

To determine when this is a polynomial we use Lemma 2. Let $e(k)$ denote the excess that must be nonnegative, according to the statement of Lemma 2.

Fix some $k \geq 1$. Then $e(k)$ in (4) is the number of multiples of k in $[n-t+1, n]$ minus the number of multiples of k in $[2, t]$ minus one more if k divides m. If we write $n = \alpha k + \beta$ and $t = \gamma k + \delta$, with $0 \leq \beta, \delta < k$, then $e(k)$ is exactly

$$\left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{n-t}{k} \right\rfloor - \left\lfloor \frac{t}{k} \right\rfloor + \left\lfloor \frac{1}{k} \right\rfloor - \tau(k \backslash m) = \tau(\beta < \delta) + \tau(k = 1) - \tau(k \backslash m),$$

($\tau(\cdots)$ is the truth value of the statement "$\cdots$") which must be nonnegative for all $k \geq 1$. If $\beta < \delta$ or $k = 1$ or k does not divide m, this is surely nonnegative. If $k > 1$ and k divides m then we must require that $\beta < \delta$, i.e., that $n \bmod k < t \bmod k$ for every $k > 1$ that divides m. ■

We remark that the proof shows that whether or not the conditions of the theorem hold, we always have

$$r(q) \stackrel{\text{def}}{=} \sum_{i=0}^{m-1} f(i, n, t, m) q^i = q^{t(t+1)/2} \binom{n}{t}_q \text{ modulo } (q^m - 1). \tag{3}$$

This makes it easy to compute the numbers of subset sums in each residue class mod m whether or not the tickets are equidistributed, by looking at the remainder of the division of $q^{t(t+1)/2}$ times the Gaussian polynomial by $(q^m - 1)$. For example the triple $(n, t, m) = (17, 10, 16)$ is not uniform. After dividing $q^{55}\binom{17}{10}_q$ by $q^{16} - 1$ we find a remainder of

$$\begin{aligned} &1212 + 1219\,q + 1212\,q^2 + 1219\,q^3 + 1212\,q^4 + 1219\,q^5 + 1212\,q^6 + 1219\,q^7 \\ &+ 1212\,q^8 + 1219\,q^9 + 1212\,q^{10} + 1219\,q^{11} + 1212\,q^{12} + 1219\,q^{13} + 1212\,q^{14} + 1219\,q^{15}, \end{aligned}$$

in which the coefficient of each q^i is $f(i, 17, 10, 16)$.

We note, following [2], that the factorization of $1 - q^i$ into cyclotomic polynomials means that $\binom{n}{t}_q$ is the product of precisely those cyclotomic polynomials $F_d(q)$ for which the number of multiples of d in $[n-t+1, n]$ is greater than the number in $[1, t]$. But this excess is $\lfloor n/d \rfloor - \lfloor (n-t)/d \rfloor - \lfloor t/d \rfloor$, which is 0 unless $\bar{t} > \bar{n}$†, when it is 1. We can restate this as a relationship between the cyclotomic factors of the Gaussian polynomial and uniform triples, which at the same time gives a nice way of computing the Gaussian polynomials, as follows.

† We use the abbreviation $\bar{t}$ (mod d) for the least nonnegative residue of t mod d.

Proposition. *The Gaussian polynomial* $\binom{n}{t}_q$ *is the product of exactly those cyclotomic polynomials* $F_j(q)$ *for which the triple* (n,t,j) *is uniform.*

We can express the distribution function $r(q)$, of (3) explicitly in terms of the values of the Gaussian polynomials at the roots of unity. Indeed (3) implies that

$$q^{t(t+1)/2}\binom{n}{t}_q = (q^m - 1)Q(q) + r(q)$$

for some quotient polynomial $Q(q)$. If $\omega^m = 1$, let $q = \omega$ in the above, to find that $r(\omega) = \omega^{t(t+1)/2}\binom{n}{t}_\omega$ at every mth root of unity ω. Hence by Lagrange interpolation,

$$r(q) = \frac{1}{m}\sum_{\omega^m=1}\frac{q^m-1}{q-\omega}\omega^{1+t(t+1)/2}\binom{n}{t}_\omega. \tag{4}$$

Note that the single term $\omega = 1$ has the value $\binom{n}{t}$ and that, by (3), this actually accounts for all of $r(q)$ precisely when the conditions of our theorem hold, for then and only then is it true that all $f(i,n,t,m) = \binom{n}{t}/m$.

By matching coefficients of powers of q on both sides of (4) we obtain the following formula for the occupancies of each residue class:

$$f(j,n,t,m) = \frac{1}{m}\sum_{\omega^m=1}\omega^{t(t+1)/2-j}\binom{n}{t}_\omega.$$

Hence the frequency vector is essentially the Fourier transform of the vector of values of the Gaussian polynomials at the roots of unity. This last formula is a nice way to compute the occupancy numbers, and in fact the images in Figure 3 below were found in a few seconds by this method.

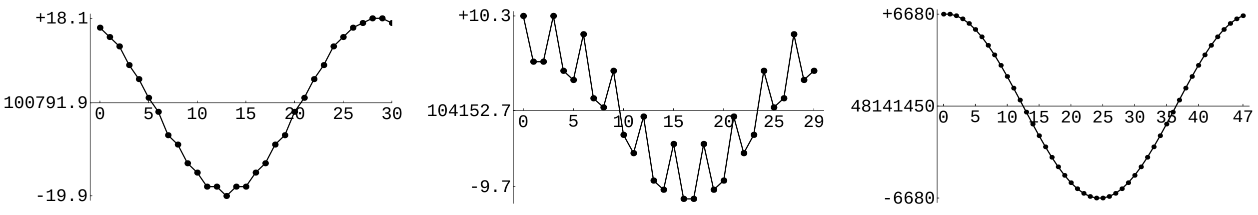

FIGURE 3. The first two panels show two frequency vectors for 9-tuples from [26]. The modulus in the first is 31, with a down-and-up pattern characteristic of primes. In the second panel the modulus is 30, and the vector's behavior is more complex. The frequencies in the third panel are from the triple $(36, 13, 48)$.

3. A bijective proof

In this section we attack the problem using elementary combinatorial arguments. We present a bijective proof of the positive direction of the theorem ((3) $\Rightarrow$ (1)). The method also yields the negative, nonuniform, direction of the theorem ((1) $\Rightarrow$ (3)) if m is a prime power. As a bonus we get some formulas for the residue frequencies as well as an elementary proof of the m-periodicity that is so striking in Figure 1. We begin with the general proof of the positive direction, in which we recursively construct a bijection.

Proof of the positive direction. Fix n and t and suppose m satisfies the hypothesis of the theorem: $\bar{t} > \bar{n} \pmod{d}$, for each $d > 1$ that divides m. The proof will be by induction on m. To this end, note that the hypothesis is satisfied for triples (n, t, d) if d divides m; more important, it is satisfied for any triple (n', t', d) where $n' \equiv n$ and $t' \equiv t \pmod{d}$.

Now let km be the largest multiple of m with $km \leq n$; call numbers in $[km]$ *small.* Let w be the number of small entries in a ticket T, and let $d = \gcd(w, m)$. We will call d the *type* of T. Our hypothesis tells us that $d < m$. For suppose otherwise. Then m divides w, which implies that $t - w = \bar{t} \pmod{m}$, since $t - w$, being the number of nonsmall entries in T, is at most $n - km$, which is less than m by definition of k. But also $t - w \leq \bar{n}$ (mod m) because $t - w \leq n - km$. Therefore $\bar{t} \leq \bar{n} \pmod{m}$, contradicting the hypothesis.

We claim that within the family of tickets of type d there is equidistribution among values modulo d. This claim suffices, for if c_i is the frequency of the residue class i within type d, then the claim implies, for each $j \leq d - 1$:

$$c_0 + c_d + c_{2d} + \cdots + c_{(\frac{m}{d}-1)d} = c_j + c_{j+d} + \cdots + c_{j+d(\frac{m}{d}-1)}. \tag{5}$$

We can now construct a bijection showing that $c_j = c_{j+id}$ as follows. If T is a ticket of value j and type d, let w be the number of small entries in T; write w as Ld where $\gcd(L, m) = 1$. Then add iL^{-1} (the inverse is modulo m) to each of the small entries of T (reducing modulo km and using km for 0). This adds $wiL^{-1} = LdiL^{-1} = di$ to the mod-m value, as desired. These bijections, together with (5), imply that each $c_0 m/d$ equals $c_j m/d$, and so $c_0 = c_j$. This is true within each type d, proving uniformity.

It remains to prove the claim. We will show here a remarkable fact. If S is some fixed set of small elements, consider the collection of all tickets whose set of small elements is exactly S. We claim that *within this collection, the modulo d frequencies are all equal.* Indeed, for tickets T in such a family the mod-d frequencies are a translation of the mod-d frequencies of $T \cap [km + 1, n]$. But these intersections are all possible $(t - w)$-subsets from $[km + 1, n]$. Since d divides m, as far as mod-d values are concerned such a subset may be viewed as a $(t - w)$-subset of $[\bar{n} \bmod m]$. But $d < m$, so we can invoke induction to get uniformity, provided we verify the hypothesis for the triple $(\bar{n} \bmod m, t - w, d)$. But, modulo d, $\bar{n} \bmod m$ is congruent to n. Since $t - w \equiv t \pmod{d}$, the observation at the beginning of the proof shows that the hypothesis is preserved and induction yields the desired uniformity. The base case is $m = 1$, which is trivial. ∎

If m is a prime p then the bijection in the previous proof is easy to describe. Any ticket has w elements in $[kp]$, the largest multiple of p less than or equal to n, where w is not divisible by p Let u be the mod-p inverse of w and add uj to each small entry of T, reducing modulo kp, and using kp for 0. This changes a ticket of value 0 to one of value j.

For the negative direction, our argument succeeds only for prime power moduli. A ticket is said to be k-*good* if $|T \cap [km]|$ is not a multiple of m (m will be clear from the context).

Proof of the negative direction, (1) $\Rightarrow$ (3), for prime power moduli. Suppose that, for $m = p^r$ the hypothesis fails for (n,t). Let $q = p^{r-1}$. If the hypothesis fails for the modulus q, then by induction the tickets are nonuniform modulo q and so nonuniform modulo p^r. So we may assume uniformity modulo q, which implies

$$c_0 + c_q + c_{2q} + \cdots + c_{(p-1)q} = c_j + c_{j+q} + \cdots + c_{j+(p-1)q}.$$

As in the proof of the positive direction, the k-good tickets for $k \le n/p^r$ are equidistributed. If, for every $k \le n/p^r$, T fails to be k-good, then each interval $[1, p^r]$, $[p^r+1, 2p^r]$, $[2p^r+1, 3p^r]$, and so on, either contains or is disjoint from T. If $p \ne 2$ the effect of these parts of T on T's value is 0, since p^r divides $p^r(p^r+1)/2$; if $p = 2$ each interval contributes 2^{r-1} and the net contribution is 0 if $\lfloor t/2^r \rfloor$ is even and 2^{r-1} otherwise. Thus the value of T is primarily determined by its intersection with the last interval, $[\lfloor n/p^r \rfloor p^r + 1, n]$. But this remainder has the same value as the corresponding $\bar{t}$ ticket from $[\bar{n}]$ (note that our assumptions imply that $\bar{t} \le \bar{n}$), and these are nonuniform because p^r does not divide $\binom{\bar{n}}{\bar{t}}$. [Proof: Use the well-known formula for the power of a prime in a factorial; then observe that if $1 \le b \le r-1$ then

$$\left\lfloor \frac{\bar{n}}{p^b} \right\rfloor - \left\lfloor \frac{\bar{t}}{p^b} \right\rfloor - \left\lfloor \frac{(\bar{n}-\bar{t})}{p^b} \right\rfloor \le 1,$$

but when $b \ge r$ each of the three terms is 0.] ∎

The preceding proof yields some useful formulas. First define

$$h = h(t,m) = \begin{cases} m/2, & \text{if } m \text{ is even and } \lfloor t/m \rfloor \text{ is odd;} \\ 0, & \text{otherwise,} \end{cases}$$

and write $s = \binom{\lfloor n/m \rfloor}{\lfloor t/m \rfloor}$. Then if $m = p$ is prime we have

$$f(i,n,t,p) = f(i-h, \bar{n}, \bar{t}, p)s + \frac{\binom{n}{t} - s\binom{\bar{n}}{\bar{t}}}{p}. \tag{6}$$

The first summand gives the contribution for tickets that are not k-good for any k; the second is an equal share of the remainder (the number of bad ticket is subtracted from the total). This formula shows that the frequency vector for (n,t) is a translation of a scalar multiple of that for $(\bar{n}, \bar{t})$; thus its shape is the same.

There is an analogous formula in the prime power case. If (n, t, p^{r-1}) is uniform then the formula is identical with that of the prime case

$$f(i,n,t,m) = f(i-h, \bar{n}, \bar{t}, m)s + \frac{\binom{n}{t} - s\binom{\bar{n}}{\bar{t}}}{m}.$$

If (n,t,p^{r-1}) is not uniform then the tickets fall into two classes, those that are k-good for some appropriate k (call these simply *good*) and those that are not (call them *bad*). As before, the number of bad tickets with value i is $f(i-h,\bar{n},\bar{t},m)s$. The good tickets, on the other hand, have modulo-m values that are equidistributed among the p classes $i, i+q, \ldots, i+(p-1)q$, where $q=p^{r-1}$. The number of all tickets that have such values is $f(i,n,t,q)$. We can therefore subtract the number of bad ones and divide by p, obtaining

$$f(i,n,t,m) = f(i-h,\bar{n},\bar{t},m)s + \frac{f(i,n,t,m/p) - s\sum_{z=0}^{p-i} f(i+zq-h,\bar{n},\bar{t},m)}{p}.$$

This formula is, like (1), a recurrence, but it is much faster for computation since the arguments go down through the powers of p.

4. Multisets and power sets

Aside from the case of t-subsets of an n-set, there are other contexts in which the uniform distribution of sums arises naturally. We mention two of these in this section. Then we study the asymptotics of the distribution into residue classes when that distribution is not uniform, in the case of the full power set. Our aim is shed some light on the question of how nonuniform the distribution can be.

First we allow repetition in the t-subsets, and we consider t-multisets: sets consisting of a_1 1's, …, a_n n's, where $\sum a_i = t$. The criterion for uniformity turns out to be virtually unchanged.

The *sum* of a multiset is $\sum_i ia_i$. Let $g(i,n,t)$ (resp. $f(i,n,t)$) be the number of t-multisets (resp. t-subsets) of $[n]$ whose sum is i.

Multiset Theorem. *The triple (n,t,m) is uniform for multisets iff $(n+t-1,t,m)$ is uniform. In fact, $g(i,n,t) = f(i+\binom{t}{2}, n+t-1, t)$.*

Proof. The first assertion follows from the second. A t-multiset from $[n]$ may be viewed as an $(n-1)$-subset of $[n+t-1]$ by the usual "stars and bars" argument: Consider $n+t-1$ blanks and fill in $n-1$ of them with markers ("stars"). Then place 1's in the blanks that precede the first marker, 2's in the next string of consecutive blanks, and so on. If $\{b_1,\ldots,b_{n-1}\}$ is the set of marker positions then the corresponding multiset has sum

$$\sum_{i=1}^{n} i(b_i - b_{i-1} - 1) = nb_n - \binom{n+1}{2} - \sum_{i=1}^{n-1} b_i = \binom{t}{2} + \sum B,$$

where $\sum B$ is the sum of the entries in B, the t-set of non marker positions. ∎

Next we consider the question of equidistribution of all 2^n of the subset sums of the set $[n]$, modulo m. This question is easier than the one previously treated, but here we are able not only to get the equidistribution criterion, but also to discuss the asymptotics of the distribution of subset sums when they are not uniform.

Power Set Theorem. *The 2^n subset sums of $[n]$ are equidistributed into the residue classes modulo m iff $m \le 2n$ and m is a power of 2.*

To prove this we expand $f(x) = \prod_{j=1}^n (1+x^j)$ as a polynomial,

$$\prod_{j=1}^n (1+x^j) = \sum_r c_r x^r,$$

then each c_r is clearly the number of subsets of $[n]$ whose sum is r. To reduce modulo m we proceed as before: $f(x)$ modulo $(x^m - 1)$ generates the number of subsets of $[n]$ whose mod m sum is r. If these sums are equidistributed then there are $2^n/m$ in each residue class (whence m must divide 2^n), so it must be true in this case that

$$\prod_{j=1}^n (1+x^j) \text{ modulo } (x^m - 1) = \frac{2^n}{m}(1 + x + x^2 + \ldots + x^{m-1}),$$

which is to say that

$$\prod_{j=1}^n (1+x^j) = p(x)(x^m - 1) + \frac{2^n}{m}\frac{x^m - 1}{x - 1}$$

where $p(x)$ is some polynomial of degree $< m$. If in this equation we let x be an mth root of unity other than $x = 1$, then we see that the left side must vanish at x because the right side does. But if the product vanishes it must be that there is a j, $1 \le j \le n$, such that $x^j = -1$. Now $x = \exp(2\pi i\mu/m)$, where $1 \le \mu \le m-1$, so x^j is $\exp(2\pi i j\mu/m)$, and this must be equal to -1. Thus we must have $2j\mu/m = 2k+1$. Hence, for each integer μ, $1 \le \mu \le m-1$ there exists a j, $1 \le j \le n$, such that $2j\mu/m$ is an odd integer.

Suppose $m > 2n$. Then take $\mu = 1$. We have $2j\mu/m < 2j\mu/2n = j/n \le 1$. Hence $2j\mu/m$ cannot be an odd integer, a contradiction. So m must be a power of 2 that is $\le 2n$.

Conversely, suppose $m \le 2n$ and m is a power of 2. Choose μ, $1 \le \mu \le m-1$. Then we can choose j to be the largest power of 2 that is $\le n$, say $j = 2^b$. With that choice we have $2j\mu/m = j\mu/(m/2)$. But the denominator is a power of 2 that is $\le n$. Hence $j/(m/2)$ is an integer. ∎

For the positive direction of this theorem, we can give a bijective proof: Use induction on n. First suppose n is not a power of 2, say $2^i < n < 2^{i+1}$. Any subset of $[n]$ is either a subset of $[n-1]$ or is obtained from such a subset by adjoining n. By the induction hypothesis, the subset-sums from $[n-1]$ are equidistributed modulo 2^{i+1}, and hence so are the subset-sums from $[n]$.

Now suppose we are dealing with subsets of $[2^i]$. The induction hypothesis tells us that the subset-sums from $[2^i - 1]$ are equidistributed modulo 2^i. If f_j denotes the number of subsets whose mod-2^{i+1} sum is j, then this means that

$$f_0 + f_{2^i} = f_1 + f_{1+2^i} = f_2 + f_{2+2^i} = \cdots = f_{2^i-1} + f_{2^{i+1}-1}.$$

Now consider the function that takes a subset of $[2^i]$ and deletes 2^i if 2^i is in the subset, and adjoins 2^i otherwise. This is a bijection and its effect on the mod-2^{i+1} value of the sum of a set is to add $\pm 2^i$, which is the same as adding 2^i. This bijection therefore shows that each $f_j = f_{j+2^i}$, which combines with the equations above to yield equidistribution. ∎

5. Asymptotics of the distribution for the power set

We work out an exact and an asymptotic expression for the standard deviation, $\sigma(n,m)$, of the occupancies of the residue classes modulo m in the power set case. It shows that the ratio of standard deviation to mean goes to zero exponentially, for fixed m, as $n \to \infty$, at least in the case where n goes to ∞ through multiples of m. The rate at which the ratio approaches zero depends on the smallest odd prime factor of m, which refines the fact, discussed in the previous section, that for equidistribution m must be a power of 2.

Theorem. *Fix an integer $m > 0$.*

(a) *If m is a power of 2, then $\sigma(n,m) = 0$ if n is a multiple of m.*

(b) *If m is not a power of 2, and the odd part of m, say m'', is prime, then when n is a multiple of m we have*

$$\frac{\sigma(n,m)}{\mathrm{mean}(n,m)} = \frac{\sqrt{m''-1}}{2^{n(1-1/m'')}}.$$

(c) *If m is not a power of 2, and the odd part of m, say m'', is composite, then asymptotically, as $n \to \infty$ through multiples of m, we have*

$$\frac{\sigma(n,m)}{\mathrm{mean}(n,m)} \sim 2^{-n(1-1/p_2)},$$

where p_2 is the smallest odd prime factor of m.

For n, m fixed, let $c(n,m,j)$ be the number of subsets of $[n]$ whose sum is j modulo m. Then we know that

$$f_{n,m}(q) \stackrel{\mathrm{def}}{=} \sum_{j=0}^{m-1} c(n,m,j)q^j = \prod_{j=1}^{n}(1+q^j) \quad (\text{modulo } q^m - 1),$$

which means that

$$g_n(q) \stackrel{\mathrm{def}}{=} \prod_{j=1}^{n}(1+q^j) = p(q)(q^m-1) + f_{n,m}(q),$$

for some polynomial p. Now it is well known and easy to check that if $f(q)$ is any real polynomial of degree $m-1$, then the sum of the squares of the coefficients of f is equal to

$$\frac{1}{m} \sum_{\omega^m=1} |f(\omega)|^2.$$

Hence

$$\sum_{j=0}^{m-1} c(n,m,j)^2 = \frac{1}{m}\sum_{\omega^m=1} |g_n(\omega)|^2.$$

Now we will suppose that n is a multiple of m, say $n = km$. Then, if $\omega = e^{2\pi ir/m}$ is a fixed mth root of unity, the sequence $\{\omega^j\}_{j\geq 0}$ is periodic in j of period m. Hence

$$|g_n(\omega)| = \prod_{j=1}^{n} |(1+\omega^j)| = \Big(\prod_{j=1}^{m} |(1+\omega^j)|\Big)^k = \Big(\prod_{j=1}^{m} |2\cos\frac{\pi rj}{m}|\Big)^k.$$

Suppose $(r,m) = 1$. Then in the last product above, rj runs through a complete system of residues modulo m, so in that case

$$\prod_{j=1}^{m} |2\cos\frac{\pi rj}{m}| = \prod_{j=1}^{m} |2\cos\frac{\pi j}{m}| = \begin{cases} 2 & \text{if } m \text{ is odd;} \\ 0 & \text{if } m \text{ is even.} \end{cases}$$

If, on the other hand, $(r,m) = d \geq 1$, then put $m' = m/d, r' = r/d$, and find

$$|g_n(\omega)| = \prod_{j=0}^{m-1} |(2\cos\frac{\pi jr'}{m'})| = \left|\prod_{j=0}^{m'-1}(2\cos\frac{\pi j}{m'})\right|^d = \begin{cases} 2^d & \text{if } m' \text{ is odd;} \\ 0 & \text{if } m' \text{ is even.} \end{cases}$$

Now for the variance of the occupancy numbers, when $n = km$, we have

$$\begin{aligned} \sigma^2(km,m) &= \frac{1}{m^2}\sum_{r=1}^{m-1} |g_n(\omega_r)|^2 = \frac{1}{m^2}\sum_{r=1}^{m-1} |g_m(\omega_r)|^{2k} \\ &= \frac{1}{m^2}\sum_{\substack{r=1 \\ m/(m,r)\ \text{odd}}}^{m-1} 2^{2k\, gcd(m,r)} = \frac{1}{m^2}\sum_{r''=1}^{m''-1} 2^{k2^{a+1} gcd(m'',r'')}, \end{aligned} \tag{7}$$

where $m = 2^a m''$, m'' odd.

Now, as r'' runs through its range, in the last displayed sum, the largest possible value that the gcd can take is m''/p_2, where p_2 is the smallest prime factor of m'', unless m'' is itself prime. In the former case, m'' is the odd part of m, so $p_2 = p_2(m)$ is the smallest *odd* prime factor of m. In the case where m'' is prime, the last member of (7) above is exactly $(m''-1)2^{2n/m''}/m^2$.

Suppose the odd part of m is not prime. Then asymptotically, as $k \to \infty$, $n = km$, we have

$$\sigma^2(km,m) \sim \frac{1}{m^2} 2^{k2^{a+1}m''/p_2} = \frac{2^{2mk/p_2}}{m^2} = \frac{2^{2n/p_2}}{m^2}.$$

Since the mean occupancy of a residue class is $2^n/m$, we have

$$\frac{\sigma(km,m)}{\text{mean}(km,m)} \sim 2^{-n(1-1/p_2)},$$

as claimed.

If the odd part of m is prime then we have an exact evaluation, as stated in the theorem above. ∎

6. Questions

1. Can the negative direction of the theorem, i.e. that (3) $\Rightarrow$ (1), be given an elementary proof?
2. We have shown that for the full power set, the standard deviation of the distribution is an asymptotically vanishing fraction of the mean, on certain subsequences of $n \to \infty$. Is the same true in the case of t-subsets of $[n]$?
3. THE PRIME MODULUS CONJECTURE. Let $f(n,t,m)$ denote the entire sequence of frequencies $\{f(i,n,t,m)\}_{i=0}^{m-1}$. For an odd prime modulus p, computations suggest that $f(n,t,m)$ is a unimodal sequence, provided we shift to start at the minimum frequency. This means that the frequencies would then go from a minimum to a maximum and then back to the minimum, with no direction changes except at the maximum. We will henceforth use the term *d-wave* for a sequence of d integers that is unimodal after a shift. Note that if $p > t(n-t)$, then the mod-p reduction disappears from the problem and this conjecture is a consequence of the classical unimodality result about the Gaussian polynomials (see [7]).
4. Given (n,t,m) and a divisor d of m with $d > 1$. Say that d is *good* if $\bar{t} > \bar{n} \pmod{d}$; otherwise d is *bad*. This question and the following one are attempts to explain and quantify the observed link between the shape of the frequency vector $f(n,t,m)$ and the shapes of $f(n,t,d)$ for bad divisors d of m. First note that if there are no bad divisors, then the main theorem applies and $f(n,t,m)$ is constant.

Consider the case where m has a single bad divisor, d. Computations lead to the following two conjectures:

   (a) If $d = m$, then $f(n,t,m)$ is an m-wave, as conjectured for prime moduli in Question 3.
   (b) $f(n,t,m) = (d/m)f(n,t,d)*$, where $*$ denotes a periodic extension that turns the d-vector into an m-vector.

At present the simple formula in (b) remains a conjecture. Statements (a) and (b) together imply that the wave behavior for primes holds whenever there is only one bad divisor of m (see the third panel of Figure 3 for an example of this situation with $(n,t,m) = (36,13,48)$ and the only bad divisor being 48).

5. We now formulate a general conjecture that attempts to explain the overall shape of the frequency sequence $f(n,t,m)$ by positing a Fourier-like decomposition of $f(n,t,m)$ into components (waves) corresponding to the bad divisors of m.

The General Conjecture. *For every triple (n,t,d), there is a $d-$wave, $\hat{f}(n,t,d)$, such that, for every triple (n,t,m) $(m>1)$ we have*

$$f(n,t,m) = \sum_{d\in\beta(m)} C_d \hat{f}(n,t,d)*,$$

where the C_d's are rational, and "" indicates that the d-wave is to be extended periodically to an m-sequence, and $\beta(m)$ is the set of bad divisors of m.*

The idea behind this formulation is that $\hat{f}(n,t,m)$ captures the essence of the mod-m nonuniformities in $f(n,t,m)$ caused by m, as opposed to those caused by bad divisors of m. Note first that, if this conjecture is true and p is prime, then $f(n,t,p) = C_p\hat{f}(n,t,p)$. Thus $f(n,t,p)$ has the shame shape as $\hat{f}(n,t,p)$ and $f(n,t,p)$ is a p-wave, which settles the Prime Moduli Conjecture (Question 3). Moreover, if m has a single bad divisor then $f(n,t,m)$ is a periodic extension of a d-wave, as conjectured in Question 4.
As an illustration of the case of two bad divisors, consider $(n,t,m) = (26,9,15)$; the bad divisors are 3 and 15, and we can take

$$\hat{f}(26,9,3) = f(26,9,3) = \{1041554, 1041498, 1041498\},$$

$$\hat{f}(26,9,5) = f(26,9,5) = \{624910, 624910, 624910, 624910, 624910\}.$$

In order to find $\hat{f}(26,9,15)$, we used trial and error to discover that $11/56$ works as the constant C_3. In other words, $f(26,9,15) - (11/56)\hat{f}(26,9,3)$ turns out to be a 15-wave, so we take it as the definition of $\hat{f}(26,9,15)$; moreover, $11/56$ appears to be the unique constant that works in this case. To summarize,

$$f(26,9,15) = \hat{f}(26,9,15) + \frac{11}{56}\hat{f}(26,9,3)$$

is a decomposition of the frequency vector into a 15-wave and a 3-wave. We have not been able to identify any pattern in the coefficients that arise in such decompositions.

References

1. L. Comtet, *Advanced Combinatorics*, Dordrecht: D. Reidel, 1974.
2. D. E. Knuth and H. S. Wilf, The power of a prime that divides a binomial coefficient, *J. für die reine u. angew. Math.* **396** (1989), 212-219.
3. G. Pólya and G. L. Alexanderson, Gaussian binomial coefficients, *Elem. der Math.* **26** (1971), 102-109.
4. H. Snevily, Subsets whose sums are congruent, Problem E3472, *Amer. Math. Monthly* **100** (1993), 503.
5. D. Zeilberger, Kathy O'Hara's constructive proof of the unimodality of the Gaussian coefficients, *Amer. Math. Monthly* **96** (1989), 590-602.