An interesting result about subset sums

Nitu Kitchloo
Lior Pachter

November 27, 1993

Abstract

We consider the problem of determining the number of subsets $B \subseteq \{1, 2, \ldots, n\}$ such that $\sum_{b \in B} b \equiv k \bmod n$, where k is a residue class mod n $(0 < k \leq n)$. If the number of such subsets is denoted N_n^k then

$$N_n^k = \frac{1}{n} \sum_{\substack{s|n \\ s\,odd}} 2^{\frac{n}{s}} \frac{\varphi(s)}{\varphi(\frac{s}{(k,s)})} \mu(\frac{s}{(k,s)}).$$

Here φ denotes the Euler phi function and μ is the Möbius function. This elaborates on a result by Erdős and Heilbronn. We also derive a similar result for finite abelian groups.

1 Introduction

Let $A_n = \{1, 2, \ldots, n\}$. There have been a number of results in the past about how large a subset $A \subseteq A_n$ has to be so that the sums of the elements of A possess a certain property, [1], [2], [3]. In particular, Erdős and Heilbronn [2] proved the following result:

Let n be a positive integer, $a_1, \ldots, a_k$ distinct residue classes mod n, and N a residue class mod n. Let $F(N; n; a_1, \ldots, a_k)$ denote the number of solutions of the congruence

$$e_1 a_1 + \ldots + e_k a_k \equiv N \bmod n$$

where $e_1, \ldots, e_k$ take the values of 0 or 1.

Theorem 1 (Erdős, Heilbronn) *Let a_i be nonzero for every i and let p be a prime. Then*

$$F(N; p; a_1, \ldots, a_k) = 2^k p^{-1}(1 + o(1))$$

if $k^3 p^{-2} \to \infty$ as $p \to \infty$.

We consider the related problem of explicitly determining the number of subsets $A \subseteq A_n$ with the property that the sum of the elements of A is congruent to $k \bmod n$. Note that this is equivalent to determining $F(k; n; a_1, \ldots, a_n)$ when $0 < k \leq n$. This follows if we accept the convention that the elements of the empty set sum up to $0 \bmod n$. We will denote $F(k; n; a_1, \ldots, a_n)$ by N_n^k.

Clearly $N_n^k \geq 1$. This is because for any n, k, the subset $\{k\}$ of A_n has the desired property. Another subset of A_n with this property for $n \geq 3, k = 0$ is the subset $B = \{x \in A_n : gcd(x, n) = 1\}$. This is a well known result.

2 Calculation of N_n^k

Proposition 2 *Consider the polynomial $P_n(x)$ defined as follows:*

$$P_n(x) = \prod_{j=1}^{n} (1 + x^j) = \sum_{r=0}^{\frac{n(n+1)}{2}} a_{n,r} x^r.$$

Let $\omega_n = e^{\frac{2\pi i}{n}}$ be a primitive nth root of unity. Then

$$N_n^k = \frac{1}{n} \sum_{j=1}^{n} \omega_n^{-kj} P_n(\omega_n^j).$$

Proof: Notice that each coefficient of x^r in $P_n(x)$ is equal to the number of subsets of A_n that sum to r. N_n^k is the sum over the coefficients of x^r where n divides $r - k$. Therefore,

$$N_n^k = \sum_{\lambda : \lambda n + k \geq 0} a_{n, \lambda n + k}. \tag{1}$$

We will prove the proposition using (1) and the following Lemma:

Lemma 3 *Let λ be a positive integer. Then $\sum_{j=0}^{n-1} \omega_n^{\lambda j} = 0$ when $n \not| \lambda$ and n when $n | \lambda$.*

Proof: Consider the equation $x^n - 1 = 0$. We factor this as

$$(x - 1)(1 + x + x^2 + \ldots + x^{n-2} + x^{n-1}) = 0.$$

Note that ω_n^λ is a root of $x^n - 1$ for every λ. Hence it is a root of the second factor if and only if $\omega_n^\lambda - 1 \neq 0$. The result follows.

Now consider

$$P_n(\omega_n^j) = \sum_{k=0}^{\frac{n(n+1)}{2}} a_{n,k} \omega_n^{jk}.$$

Then

$$\begin{aligned}
\sum_{j=1}^{n} \omega_n^{-kj} P_n(\omega_n^j) &= \sum_{j=1}^{n} \omega_n^{-kj} \sum_{r=0}^{\frac{n(n+1)}{2}} a_{n,r}\omega_n^{rj} \\
&= \sum_{r=0}^{\frac{n(n+1)}{2}} a_{n,r} \sum_{j=1}^{n} \omega_n^{(r-k)j} \\
&= n \sum_{\lambda:\lambda n+k \geq 0} a_{n,\lambda n+k} \\
&= n(N_n^k).
\end{aligned}$$

Proposition 4 *$P_n(\omega_n^j) = 2^{(n,j)}$ if $\frac{n}{(j,n)}$ is odd and 0 otherwise. Here (n,j) denotes the g.c.d. of n, j $(1 \leq j \leq n)$.*

Proof: We shall first prove two technical lemmas and then combine them to obtain the required result.

Lemma 5

$$P_n(\omega_n^j) = [P_{\frac{n}{(n,j)}}(\omega_{\frac{n}{(n,j)}})]^{(n,j)}.$$

Proof: Note that

$$\begin{aligned}
P_n(\omega_n^j) &= \prod_{r=1}^{n} (1 + [\omega_n^j]^{r\frac{(n,j)}{(n,j)}}) \\
&= \prod_{r=1}^{n} (1 + [\omega_n^{(n,j)}]^{\frac{jr}{(n,j)}}).
\end{aligned}$$

Now $\omega_n^{(n,j)} = \omega_{\frac{n}{(n,j)}}$. Hence

$$P_n(\omega_n^j) = \prod_{r=1}^{n} (1 + [\omega_{\frac{n}{(n,j)}}^{\frac{j}{(n,j)}}]^r).$$

Furthermore, $(\frac{j}{(n,j)}, \frac{n}{(n,j)}) = 1$ so $\omega_{\frac{n}{(n,j)}}^{\frac{j}{(n,j)}}$ is a primitive $\frac{n}{(n,j)}$th root of unity. Therefore as r ranges from 1 to n, the factors repeat themselves (n,j) times, i.e.

$$\begin{aligned}
P_n(\omega_n^j) &= [\prod_{r=1}^{\frac{n}{(n,j)}} (1 + [\omega_{\frac{n}{(n,j)}}^{\frac{j}{(n,j)}}]^r)]^{(n,j)} \\
&= [P_{\frac{n}{(n,j)}}(\omega_{\frac{n}{(n,j)}}^{\frac{j}{(n,j)}})]^{(n,j)}.
\end{aligned}$$

Recalling that $(\frac{j}{(n,j)}, \frac{n}{(n,j)}) = 1$ we notice that $P_{\frac{n}{(n,j)}}(\omega_{\frac{n}{(n,j)}}^{\frac{j}{(n,j)}})$ is just a permutation of the factors in $P_{\frac{n}{(n,j)}}(\omega_{\frac{n}{(n,j)}})$. Hence,

$$P_{\frac{n}{(n,j)}}(\omega_{\frac{n}{(n,j)}}^{\frac{j}{(n,j)}}) = P_{\frac{n}{(n,j)}}(\omega_{\frac{n}{(n,j)}})$$

which gives the result

$$P_n(\omega_n^j) = [P_{\frac{n}{(n,j)}}(\omega_{\frac{n}{(n,j)}})]^{(n,j)}.$$

Lemma 6 $P_r(\omega_r) = 1 - (-1)^r$.

Proof: Consider the polynomial $x^r - 1$. Then $1, \omega_r, \omega_r^2, \ldots, \omega_r^{r-1}$ are the distinct r roots of this polynomial. Thus

$$x^r - 1 = (x-1)(x-\omega_r)(x-\omega_r^2)\cdots(x-\omega_r^{r-1}).$$

Substituting $x = -1$ we get

$$((-1)^r - 1) = (-1)^r(1+\omega_r)(1+\omega_r^2)\cdots(1+\omega_r^r).$$

i.e. $1 - (-1)^r = P_k(\omega_r)$. Now

$$\begin{aligned} P_n(\omega_n^j) &= [P_{\frac{n}{(n,j)}}(\omega_{\frac{n}{(n,j)}})]^{(n,j)} \\ &= [1 - (-1)^{\frac{n}{(n,j)}}]^{(n,j)}. \end{aligned}$$

This is equal to $2^{(n,j)}$ when $\frac{n}{(n,j)}$ is odd and 0 otherwise.

Proposition 7 *Suppose* $t|n$, $\delta = \frac{n}{t}$. *Then*

$$\sum_{x \in \mathbf{Z}_\delta^\times} \omega_n^{-ktx} = \frac{\varphi(\delta)}{\varphi(\frac{\delta}{(k,\delta)})} \sum_{x \in \mathbf{Z}^\times_{\frac{\delta}{(k,\delta)}}} \omega^x_{\frac{\delta}{(k,\delta)}}.$$

Proof: First note that $\omega_n^{tx} = \omega_\delta^x$. Also x and $-x$ are both elements of $\mathbf{Z}_\delta^\times$. Therefore

$$\sum_{x \in \mathbf{Z}_\delta^\times} \omega_n^{-ktx} = \sum_{x \in \mathbf{Z}_\delta^\times} \omega_\delta^{kx}.$$

Now rewrite ω_δ^{kx} as $\omega_{\frac{\delta}{(\delta,k)}}^{\frac{k}{(\delta,k)}x}$. Hence

$$\begin{aligned} \sum_{x \in \mathbf{Z}_\delta^\times} \omega_\delta^{kx} &= \sum_{x \in \mathbf{Z}_\delta^\times} \omega_{\frac{\delta}{(\delta,k)}}^{\frac{k}{(\delta,k)}x} \\ &= \frac{\varphi(\delta)}{\varphi(\frac{\delta}{(k,\delta)})} \sum_{x \in \mathbf{Z}^\times_{\frac{\delta}{(k,\delta)}}} \omega_{\frac{\delta}{(\delta,k)}}^{\frac{k}{(\delta,k)}x}. \end{aligned}$$

This is because $\frac{\varphi(\delta)}{\varphi(\frac{\delta}{(k,\delta)})}$ summands are identical $\forall x \in \mathbf{Z}_\delta^\times$. Finally, since $(\frac{k}{(\delta,k)}, \frac{\delta}{(\delta,k)}) = 1$ this reduces to

$$\frac{\varphi(\delta)}{\varphi(\frac{\delta}{(k,\delta)})} \sum_{x \in \mathbf{Z}^\times_{\frac{\delta}{(k,\delta)}}} \omega^x_{\frac{\delta}{(k,\delta)}}$$

which completes the proof of the proposition.

Proposition 8

$$\sum_{t\in \mathbf{Z}_n^\times} \omega_n^t = \mu(n).$$

Proof: Let $\Phi_n(x)$ denote the nth cyclotomic polynomial. Then $\sum_{t\in \mathbf{Z}_n^\times} \omega_n^t$ is just the negative of the coefficient of $x^{\varphi(n)-1}$ in $\Phi_n(x)$.

Claim 9 *$\Phi_n(x) = \Phi_d(x^m)$ where $n = dm$ and d is the product of all the distinct prime factors of n.*

Proof: It is well known that $\Phi_n(x) = \prod_{r|n}(x^{\frac{n}{r}} - 1)^{\mu(r)}$. For a proof of this result see [4], page 353. Now $\Phi_d(x^m) = \prod_{s|d}(x^{\frac{n}{s}} - 1)^{\mu(s)}$. If $s|n$ and $s > d$ then s is divisible by the square of some prime and so $\mu(s) = 0$. Hence the claim.

Claim 10 *$\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$ if p is a prime that does not divide n.*

Proof: Once again we use the fact that $\Phi_n(x) = \prod_{r|n}(x^{\frac{n}{r}} - 1)^{\mu(r)}$. In our case we have

$$\begin{aligned}
\Phi_{pn}(x) &= \prod_{r|pn}(x^{\frac{np}{r}} - 1)^{\mu(r)} \\
&= \prod_{r|pn: p\nmid r}(x^{\frac{np}{r}} - 1)^{\mu(r)} \prod_{r|pn: p|r}(x^{\frac{np}{r}} - 1)^{\mu(r)} \\
&= \prod_{t|n}(x^{\frac{np}{t}} - 1)^{\mu(t)} \prod_{s|n}(x^{\frac{n}{s}} - 1)^{\mu(sp)}.
\end{aligned}$$

However μ is a multiplicative function hence $\mu(sp) = -\mu(s)$ so

$$\Phi_{pn}(x) = (\Phi_n(x^p))(\Phi_n(x))^{-1}.$$

If $p^2|n$ for some prime p then by Claim 9 the coefficient of $x^{\varphi(n)-1}$ in $\Phi_n(x)$ is 0. So assume that $n = \prod_{i=1}^m p_i$, where the p_i's are distinct. We now use induction on m and Claim 10 to obtain that $\sum_{t\in \mathbf{Z}_n^\times} \omega_n^t = \mu(n)$.

Theorem 11

$$N_n^k = \frac{1}{n}\sum_{\substack{s|n \\ s\ odd}} 2^{\frac{n}{s}} \frac{\varphi(s)}{\varphi(\frac{s}{(k,s)})}\mu(\frac{s}{(k,s)}).$$

Proof: Using Proposition 2 we obtain that

$$N_n^k = \frac{1}{n}\sum_{j=1}^{n} \omega_n^{-kj} P_n(\omega_n^j).$$

Now we use Proposition 4 to obtain

$$N_n^k = \frac{1}{n} \sum_{j:\frac{n}{(j,n)} odd} \omega_n^{-kj} 2^{(j,n)}.$$

Now let $(j,n) = t$. Then

$$N_n^k = \frac{1}{n} \left(\sum_{t|n:\frac{n}{t} odd} 2^t \sum_{x \in \mathbf{Z}^{\times}_{\frac{n}{t}}} \omega_n^{-ktx} \right)$$

since as x ranges over $\mathbf{Z}^{\times}_{\frac{n}{t}}$, tx ranges over the elements r such that $(r,n) = t$. Applying Proposition 10 we obtain

$$N_n^k = \frac{1}{n} \left(\sum_{t|n:\frac{n}{t} odd} 2^t \frac{\varphi(\frac{n}{t})}{\varphi(\frac{\frac{n}{t}}{(k,\frac{n}{t})})} \sum_{x \in \mathbf{Z}^{\times}_{\frac{\frac{n}{t}}{(k,\frac{n}{t})}}} \omega^x_{\frac{\frac{n}{t}}{(k,\frac{n}{t})}} \right).$$

Finally, we use Proposition 7 to conclude that

$$N_n^k = \frac{1}{n} \sum_{t|n:\frac{n}{t} odd} 2^t \frac{\varphi(\frac{n}{t})}{\varphi(\frac{\frac{n}{t}}{(k,\frac{n}{t})})} \mu(\frac{\frac{n}{t}}{(k,\frac{n}{t})}).$$

Substituting $s = \frac{n}{t}$ this reduces to

$$N_n^k = \frac{1}{n} \sum_{\substack{s|n \\ s\, odd}} 2^{\frac{n}{s}} \frac{\varphi(s)}{\varphi(\frac{s}{(k,s)})} \mu(\frac{s}{(k,s)}).$$

For the case when $k = n$ this formula can easily be simplified to obtain

$$N_n^n = \frac{1}{n} \sum_{\substack{s|n \\ s\, odd}} 2^{\frac{n}{s}} \varphi(s).$$

3 A Theorem About Finite Abelian Groups

A natural generalization of the problem discussed in the previous section is a similar problem for finite abelian groups. That is, if G is a finite abelian group of order n, we want to calculate the number of subsets of G whose elements sum up to the identity element $(\overline{0})$ of G.

For the purposes of this section we will use the following notation: Let $\underline{S}$ denote a k-tuple of numbers, i.e. $\underline{S} = (s_1, s_2, \ldots, s_k)$. Given two k-tuples $\underline{J}$ and $\underline{N}$ define

$$\sum_{\underline{0} < \underline{J} \leq \underline{N}} = \sum_{j_1=1}^{j_1=n_1} \sum_{j_2=1}^{j_2=n_2} \cdots \sum_{j_k=1}^{j_k=n_k}.$$

Will will denote the number of subsets of a finite abelian group G whose elements sum up to $\overline{0}$ by N_G.

Theorem 12 *Let $G = \mathbf{Z}_{n_1} \bigoplus \mathbf{Z}_{n_2} \bigoplus \ldots \bigoplus \mathbf{Z}_{n_k}$ be a finite abelian group of order $n = n_1 n_2 \cdots n_k$. Given a k-tuple $\underline{J}$ define T_J =g.c.d.$(\frac{j_1 n}{n_1}, \ldots, \frac{j_k n}{n_k})$ and let $\underline{N} = (n_1, n_2, \ldots, n_k)$. Then*

$$N_G = \frac{1}{n} \sum_{\underline{0} < \underline{J} \leq \underline{N}} [1 - (-1)^{\frac{n}{(n,T_J)}}]^{(n,T_J)}.$$

We shall prove this theorem using the same ideas as before.

Proposition 13 *Consider the polynomial*

$$F(x_1, x_2, \ldots, x_k) = \prod_{\underline{0} < \underline{S} \leq \underline{N}} (1 + x_1^{s_1} x_2^{s_2} \cdots x_k^{s_k}) = \sum_{\underline{\alpha}} a_{\underline{\alpha}} x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}.$$

Then

$$N_G = \frac{1}{n} \sum_{\underline{0} < \underline{J} \leq \underline{N}} F(\omega_{n_1}^{j_1}, \ldots, \omega_{n_k}^{j_k}).$$

Proof: The proof is identical to that of Proposition 2.

Proposition 14

$$F(\omega_{n_1}^{j_1}, \ldots, \omega_{n_k}^{j_k}) = [1 - (-1)^{\frac{n}{(n,T_J)}}]^{(n,T_J)}.$$

Proof: Note that $\omega_{n_i}^{j_i s_i} = \omega_n^{\frac{j_i s_i n}{n_i}}$. Therefore

$$\begin{aligned} F(\omega_{n_1}^{j_1}, \ldots, \omega_{n_k}^{j_k}) &= \prod_{\underline{0} < \underline{S} \leq \underline{N}} (1 + \omega_{n_1}^{j_1 s_1} \omega_{n_2}^{j_2 s_2} \cdots \omega_{n_k}^{j_k s_k}) \\ &= \prod_{\underline{0} < \underline{S} \leq \underline{N}} (1 + \omega_n^{\sum_i \frac{j_i s_i n}{n_i}}). \end{aligned}$$

Consider the exponent in one factor of the above product for a fixed $\underline{S}$, i.e.

$$\sum_i s_i (\frac{j_i n}{n_i}) = T_J (\sum_i s_i (\frac{j_i n}{n_i T_J})).$$

Claim 15 *For every m ($0 \leq m \leq n$) there exists a k-tuple $\underline{S}$ such that*

$$T_J (\sum_i s_i (\frac{j_i n}{n_i T_J})) \equiv T_J m \bmod n.$$

Proof: Note that g.c.d.$(\frac{j_1 n}{n_1 T_J}, \ldots, \frac{j_k n}{n_k T_J}) = 1$ and therefore for any integer m there exists $s_i \in \mathbf{Z}$ such that

$$m = \sum_i \frac{s_i j_i n}{n_i T_J}.$$

Equivalently,

$$T_J m = T_J(\sum_i \frac{s_i j_i n}{n_i T_J}).$$

Now note that if any s_i is replaced by $s_i + n_i$ in the above equation then we still have equality (mod n). Thus every s_i can be chosen to be less than n_i.

Therefore by the above claim we obtain

$$\begin{aligned} \prod_{\underline{0} < \underline{S} \leq \underline{N}} (1 + \omega_n^{\sum_i \frac{j_i s_i n}{n_i}}) &= \prod_{m=0}^{n-1} (1 + \omega_n^{T_J m}) \\ &= P_n(\omega_n^{T_J}) \\ &= [1 - (-1)^{\frac{n}{(n,T_J)}}]^{(n,T_J)} \end{aligned}$$

and so we have proved the proposition.

Proof (main theorem): The theorem now follows immediately by combining Propositions 13 and 14:

$$\begin{aligned} N_G &= \frac{1}{n} \sum_{\underline{0} < \underline{J} \leq \underline{N}} F(\omega_{n_1}^{j_1}, \ldots, \omega_{n_k}^{j_k}) \\ &= \frac{1}{n} \sum_{\underline{0} < \underline{J} \leq \underline{N}} [1 - (-1)^{\frac{n}{(n,T_J)}}]^{(n,T_J)}. \end{aligned}$$

4 Further Results

Another problem related to the calculation of N_n^k is the calculation of $N_{n,m}^n$ where $0 < m < \frac{n(n+1)}{2}$. $N_{n,m}^n$ is defined to be the number of subsets $B \subseteq \{1, 2, \ldots, n\}$ such that $\sum_{b \in B} b \equiv 0 \bmod m$. We Remark that $N_{n,m}^n$ is easily obtained when $m|n$.

Proposition 16 *Let n, m be positive integers with $m|n$. Then*

$$N_{n,m}^n = \frac{1}{m} \sum_{\substack{s|m \\ s\, odd}} 2^{\frac{n}{s}} \varphi(s).$$

Proof: Using Lemma 3 and the same proof as given in Proposition 2 we obtain that:

$$N_{n,m}^n = \frac{1}{m} \sum_{j=1}^{m} P_n(\omega_m^j).$$

Now $1+(\omega_m^j)^{m+i} = 1+(\omega_m^j)^i$ so the factors in $P_n(\omega_m^j)$ repeat themselves $\frac{n}{m}$ times. Therefore $P_n(\omega_m^j) = [P_m(\omega_m^j)]^{\frac{n}{m}}$. Now we proceed as before to get

$$N_{n,m}^n = \frac{1}{m} \sum_{\substack{s|m \\ s\ odd}} 2^{\frac{n}{s}} \varphi(s).$$

Snevily, [5] has proposed the following conjecture:

Conjecture 17 *The sequence* $\{N_{n,m}^n\}_{m=1}^{\frac{n(n+1)}{2}}$ *is monotonically decreasing.*

We also mention an interesting connection between our problem and two other counting problems in combinatorics. Let C_n denote the number of circular sequences of 0's and 1's, where two sequences obtained by a rotation are considered the same. This problem is discussed in [6], page 75. The solution is

$$C_n = \frac{1}{n} \sum_{t|n} \varphi(t) 2^{\frac{n}{t}}.$$

This is indentical in form to our formula for N_n^n except that in our case we sum over all $t|n$ where t is odd. Another related problem is the calculation of the number of monic irreducible polynomials of degree n over a field of q elements where q is prime ([6], page 116). If the number of such polynomials is denoted M_n^q then

$$M_n^q = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

For $q = 2$ this has the exact same form as our formula for N_n^k where $(k,n) = 1$. Once again, the only difference is that our sum is over $d|n$ such that d is odd.

References

[1] N. Alon and G. Freiman, On sums of a subset of a set of integers, *Combinatorica*, **8**(4) (1988), 297-306.

[2] P. Erdős and H. Heilbronn, On the addition of residue classes mod p, *Acta Arithmetica*, **9** (1964), 149-159.

[3] J. Olson, An additive theorem modulo p, *J. Combinatorial Theory*, **5** (1968), 45-52.

[4] R. Dean, *Classical Abstract Algebra*, Harper and Row, Publishers, New York, 1990.

[5] H. Snevily, personal communication.

[6] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press 1992.

Nitu Kitchloo

Department of Mathematics
MIT
Cambridge, MA

Lior Pachter

Department of Mathematics
Caltech
Pasadena, CA