POLYNOMIAL IDENTITIES

J. B. ROBERTS[1]

In this paper we are concerned with various generalizations of certain known theorems about the splitting of finite sets of numbers into equinumerous classes such that the sums of powers of the numbers in a given class is independent of the class. In certain cases lower bounds, which are quite large, are given for the number of possible splittings. In addition we give a method which enables one to compute these splittings with facility.

Let $n_1, n_2, n_3, \cdots$ be a fixed sequence of integers each $\geqq 2$. Define $p_0=1$, $p_1=n_1$, $p_2=n_1n_2$, $p_3=n_1n_2n_3, \cdots$. Then every integer has a unique representation in the form

$$(1)\qquad n = a_0 + a_1p_1 + a_2p_2 + \cdots + a_kp_k, \qquad k \geqq 0, 0 \leqq a_i \leqq n_{i+1}.$$

We shall use this fact below.

DEFINITION.

$$\left(\sum_{n=0}^{r-1} f(n)n^t\right) * \left(\sum_{n=0}^{s-1} g(n)n^t\right) = \sum_{n=0}^{rs-1} f(n - r[n/r])g([n/r])n^t.$$

We use $[x]$ for the largest integer $\leqq x$. Note that $n-r[n/r]$ and $[n/r]$ are just the digits in the expansion of n, $0\leqq n<rs$, in the form $n=a_0+a_1r$, $0\leqq a_0<r$, $0\leqq a_1<s$.

A short computation shows that the $*$ operation is associative.

THEOREM 1. *Let n_i and p_i be as defined above and let the a_i be those functions of n defined by* (1). *Then*

$$(2)\qquad \left(\sum_{n=0}^{n_1-1} f_1(n)n^t\right) * \cdots * \left(\sum_{n=0}^{n_k-1} f_k(n)n^t\right) = \sum_{n=0}^{p_k-1} f_1(a_0) \cdots f_k(a_{k-1})n^t.$$

PROOF. The proof is by induction on k. (a) Let $k=2$. Then

$$\left(\sum_{n=0}^{n_1-1} f_1(n)n^t\right) * \left(\sum_{n=0}^{n_2-1} f_2(n)n^t\right) = \sum_{n=0}^{p_2-1} f_1(n - n_1[n/n_1])f_2([n/n_1])n^t.$$

But if $n=a_0+a_1p_1$, $0\leqq a_0<n_1$, $0\leqq a_1<n_2$, then

$$a_0 = n - p_1[n/p_1], \qquad a_1 = [n/p_1].$$

This proves the theorem for $k=2$. (b) Suppose theorem true for $k\leqq j-1$. Then

Received by the editors December 23, 1959.

[1] This work was done under National Science Foundation research grant G-5252.

$$\left(\sum_{n=0}^{n_1-1} f_1(n)n^t\right) * \cdots * \left(\sum_{n=0}^{n_j-1} f_j(n)n^t\right)$$
$$= \left(\sum_{n=0}^{p_{j-1}-1} f_1(a_0) \cdots f_{j-1}(a_{j-2})n^t\right) * \left(\sum_{n=0}^{n_j-1} f_j(n)n^t\right)$$
$$= \left(\sum_{n=0}^{p_{j-1}-1} F(n)n^t\right) * \left(\sum_{n=0}^{n_j-1} f_j(n)n^t\right)$$
$$= \sum_{n=0}^{p_j-1} F(n - p_{j-1}[n/p_{j-1}])f_j([n/p_{j-1}])n^t$$

where $F(n) = f_1(a_0) \cdots f_{j-1}(a_{j-2})$ when $n = a_0 + a_1p_1 + \cdots + a_{j-2}p_{j-2}$. Let $n = a_0 + a_1p_1 + \cdots + a_{j-1}p_{j-1}$. Then

$$F(n - p_{j-1}[n/p_{j-1}]) = F(a_0 + a_1p_1 + \cdots + a_{j-2}p_{j-2})$$
$$= f_1(a_0) \cdots f_{j-1}(a_{j-2})$$

and

$$f_j([n/p_{j-1}]) = f_j(a_{j-1})$$

and the proof is complete.

THEOREM 2. *Suppose* $\sum_{n=0}^{r-1} f(n)n^t = 0$, $\sum_{n=0}^{s-1} g(n)n^t = 0$ *for all integers t satisfying* $0 \leqq t \leqq \alpha_1$, $0 \leqq t \leqq \alpha_2$ *respectively. Then*

$$\left(\sum_{n=0}^{r-1} f(n)n^t\right) * \left(\sum_{n=0}^{s-1} g(n)n^t\right) = 0$$

for all integers t satisfying $0 \leqq t \leqq \alpha_1 + \alpha_2 + 1$.

PROOF. The $*$ product is

$$\sum_{n=0}^{rs-1} f(a_0)g(a_1)(a_0 + a_1r)^t = \sum_{a_0=0}^{r-1} \sum_{a_1=0}^{s-1} f(a_0)g(a_1)(a_0 + a_1r)^t$$
$$= \sum_{a_0=0}^{r-1} \sum_{a_1=0}^{s-1} f(a_0)g(a_1) \sum_{k=0}^{t} \binom{t}{k} a_0^k (a_1r)^{t-k}$$
$$= \sum_{k=0}^{t} \binom{t}{k} r^{t-k} \left(\sum_{a_0=0}^{r-1} f(a_0)a_0^k\right)\left(\sum_{a_1=0}^{s-1} g(a_1)a_1^{t-k}\right).$$

When $0 \leqq t \leqq \alpha_1 + \alpha_2 + 1$ then either $0 \leqq k \leqq \alpha_1$ or $0 \leqq t - k \leqq \alpha_2$ and therefore one of the two inside sums on the right vanishes. This completes the proof.

COROLLARY. *Suppose for each j,* $1 \leqq j \leqq m$, $\sum_{n=0}^{n_j-1} f_j(n)n^t = 0$ *for all integers t satisfying* $0 \leqq t \leqq \alpha_j$. *Then*

$$\sum_{n=0}^{p_m-1} f_1(a_0) \cdots f_m(a_{m-1})n^t = 0$$

for all integers t satisfying

$$0 \leqq t \leqq \alpha_1 + \cdots + \alpha_m + (m-1).$$

This corollary follows immediately from the theorem and Theorem 1.

It should be noted that the corollary remains true if for some j the sum $\sum_{n=0}^{n_j-1} f_j(n)n^t$ does not vanish for any integral t providing we replace α_j by -1.

Suppose now that $A = \{\beta_0, \beta_1, \cdots\}$ is an arbitrary sequence of complex numbers. Define A_n, for n given by (1), to be

$$A_n = a_0\beta_0 + a_1\beta_1 + \cdots + a_k\beta_k.$$

Elementary algebraic manipulations involving the binomial theorem show that if $\sum_{n=0}^{r-1} f(n)n^t = 0$ for all integers t, $0 \leqq t \leqq \alpha$, then also $\sum_{n=0}^{r-1} f(n)A_n^t = 0$ for these same t. Further this latter proposition is equivalent to the proposition that $\sum_{n=0}^{r-1} f(n)P(x+A_n) = 0$ for all polynomials $P(x)$ of degree $\leqq \alpha$.

These remarks and the above results prove the

THEOREM 3. *Let m be a positive integer and $\alpha_1, \cdots, \alpha_m$ be integers each $\geqq -1$. Suppose further $\sum_{n=0}^{n_j-1} f_j(n)n^t = 0$ for $0 \leqq t \leqq \alpha_j$. Then, for every polynomial $P(x)$ of degree $< \alpha_1 + \cdots + \alpha_m + m$,*

$$\sum_{n=0}^{p_m-1} f_1(a_0) \cdots f_m(a_{m-1})P(x + A_n) = 0. \tag{3}$$

If in Theorem 3 each function f_j is periodic of period n_j then, since $a_j \equiv [n/p_j]$ (mod n_j), we may write (3) as

$$\sum_{n=0}^{p_m-1} \prod_{j=1}^{m} f_j([n/p_{j-1}])P(x + A_n) = 0. \tag{4}$$

We write next a theorem, a special case of which we shall combine with Theorem 3 to obtain some further identities.

THEOREM 4. *Suppose $\sum_{n=0}^{m-1} f(n)n^t = 0$ for all integers t, $0 \leqq t \leqq \alpha$. Then putting $f(-1) = f(m) = 0$ we have*

$$\sum_{n=0}^{m} (f(n) - f(n-1))n^t = 0 \qquad \text{for } 0 \leqq t \leqq \alpha + 1.$$

PROOF.

$$\sum_{n=0}^{m}(f(n)-f(n-1))n^t = \sum_{n=0}^{m-1} f(n)(n^t-(n+1)^t)$$

$$= -\sum_{n=0}^{m-1} f(n)\sum_{s=0}^{t-1}\binom{t}{s}f(n)n^s = -\sum_{s=0}^{t-1}\binom{t}{s}\sum_{n=0}^{m-1}f(n)n^s = 0.$$

A special case of the result in Theorem 4 enables us to give an easy inductive proof of the well known formula

$$(5)\qquad \sum_{n=0}^{q}(-1)^n\binom{q}{n}n^t = 0, \qquad 0 \leqq t \leqq q-1.$$

Indeed this formula is true for $q=1$ and assuming its truth for q we see, with

$$f(n) = (-1)^n\binom{q-1}{n},$$

that

$$\sum_{n=0}^{q+1}\left((-1)^n\binom{q}{n} - (-1)^{n-1}\binom{q}{n-1}\right)n^t = \sum_{n=0}^{q+1}(-1)^n\binom{q+1}{n}n^t = 0.$$

$$0 \leqq t \leqq q.$$

If we now take each

$$f_j(n) = (-1)^n\binom{n_j-1}{n}$$

and $\alpha_j = n_j - 2$ we deduce from (5) and Theorem 3 the

THEOREM 5. *For $P(x)$ any polynomial of degree $< n_1 + \cdots + n_m - m$,*

$$\sum_{n=0}^{p_m-1}(-1)^{a_0+\cdots+a_m}\binom{n_1-1}{a_0}\cdots\binom{n_m-1}{a_{m-1}}P(x+A_n) = 0.$$

Specializing this result by choosing all $n_i = b \geqq 2$ gives the main polynomial identity (Equation (7)) of [2].

If we take each $f_j(n) = \epsilon_j^n$, where ϵ_j is an n_jth root of unity we see that f_j is periodic of period n_j and $\sum_{n=0}^{n_j-1} f_j(n) = \sum_{n=0}^{n_j-1}\epsilon_j^n = 0$ for $\epsilon_j \neq 1$. Hence from Theorem 3 and (4) we may write the

THEOREM 6. *Let ν be the number of $\epsilon_1, \cdots, \epsilon_m$ which equal* 1 *and suppose $P(x)$ is any polynomial of degree $< m - \nu$. Then*

$$\sum_{n=0}^{p_m-1}\epsilon_1^{[n/p_0]}\cdots\epsilon_m^{[n/p_{m-1}]}P(x+A_n) = 0.$$

Specializing this result by choosing all $n_i = b \geqq 2$ gives the main polynomial identity (Equation (1)) of [**3**].

We insert a known lemma which will be used in deducing our next result.

LEMMA. *If $\sum_{n=0}^{q-1} c_n x^n = 0$ for all qth roots of unity other than* 1 *then all the c_i are equal.*

PROOF. A polynomial of degree $q-1$ is determined to within a multiplicative constant by $q-1$ distinct zeros. The zeros of the given polynomial are also zeros of the polynomial $1+x+x^2+ \cdots +x^{q-1}$. Hence the given polynomial is a constant times this one. Equating coefficients gives the result.

Let now $\epsilon_j = e^{2\pi s i/n^j} = e(s/n_j)$, $j \geqq 1$, where $i = (-1)^{1/2}$. Then if L_{m-1} is the least common multiple of $n_1, \cdots, n_m$ we have

$$\begin{aligned}\epsilon_1^{[n/p_0]} \cdots \epsilon_m^{[n/p_{m-1}]} &= e\left(s \sum_{j=1}^{m} [n/p_{j-1}]/n_j\right) \\ &= e\left((s/L_{m-1}) \sum_{j=1}^{m} L_{m-1}[n/p_{j-1}]/n_j\right).\end{aligned}$$

Define C_r to be the set of those n, $0 \leqq n \leqq p_m$, for which

$$\sum_{j=1}^{m} \mathrm{L}_{m-1}[n/p_{j-1}]/n_j \equiv r \pmod{L_{m-1}}.$$

Then

$$\begin{aligned}\sum_{n=0}^{p_m-1} \epsilon_1^{[n/p_0]} \cdots \epsilon_m^{[n/p_{m-1}]} &P(x+A_n) \\ &= \sum_{r=0}^{L_{m-1}-1} e(rs/L_{m-1}) \sum_{n \in C_r} P(x+A_n).\end{aligned} \tag{6}$$

By Theorem 6 the left side of (6) is zero for $P(x)$ any polynomial of degree $< m - \nu_s$ where ν_s is the number of $n_1, \cdots, n_m$ which divide s. Putting $\bar{\nu} = \max \nu_s$, $0 \leqq s < L_{m-1}$, we see that the left side of (6) is zero for all s, $0 \leqq s < L_{m-1}$, when $P(x)$ is a polynomial of degree $< m - \bar{\nu}$. Hence using the lemma and (6) gives

THEOREM 7. *Let C_r be as defined above. Then for $P(x)$ any polynomial of degree $< m - \bar{\nu}$ the sum $\sum_{n \in C_r} P(x+A_n)$ is independent of r, $0 \leqq r \leqq L_{m-1}$.*

Specializing this result by choosing all $n_i = b \geqq 2$ gives Lehmer's theorem (see [**1**; **3**; **4**; **5**; **6**]).

A number of other similar results can be derived from Theorems 5 and 6.

Theorem 7 tells us that the integers $0 \leqq n < p_m$ can be split into L_{m-1} disjoint (equinumerous) classes C_r over which the sum $\sum_{n \in C_r} P(x+A_n)$ is invariant. It is natural to inquire into the number of ways such a splitting can be accomplished. We have investigated this question to some extent, especially in the case where all $n_j = b \geqq 2$. In this case we have obtained a lower bound for the number of splittings of $0 \leqq n < p_m$. This lower bound is $((b-1)!)^m$. We omit the proof of this result but shall give a method which can be used to construct this number of splittings.

For the rest of this paper all $n_j = b \geqq 2$ and $\psi_0, \psi_1, \psi_2, \cdots$ is any sequence of functions defined over the integers each of period b. Using the periodicity of the ψ_i we find by direct computation

$$(7) \qquad \prod_{i=0}^{m-1} \sum_{j=0}^{b-1} \epsilon^{\psi_i(j)} x^{jb^i} = \sum_{n=0}^{b^m-1} \epsilon^{\psi_0([n]) + \cdots + \psi_{m-1}([n/b^{m-1}])} x^n,$$

where ϵ is a bth root of unity. Defining $\phi_m(n)$ for $0 \leqq n < b^m$ by

$$\phi_m(n) = \psi_0([n]) + \cdots + \psi_{m-1}([n/b^{m-1}])$$

we see that (7) yields a generating function for $\phi_m(n)$. From this we see immediately, for $0 \leqq a_i < b$,

$$\phi_m(a_0 + a_1 b + \cdots + a_{m-1} b^{m-1}) \equiv \psi_0(a_0) + \cdots + \psi_{m-1}(a_{m-1}) \pmod{b}.$$

If Ψ_r is the set of n, $0 \leqq n < b^m$, for which

$$\psi_0(a_0) + \cdots + \psi_{m-1}(a_{m-1}) \equiv r \pmod{b}$$

then the proof of Theorem 7 proves that the sum there can be replaced by $\sum_{n \in \Psi_r} P(x+A_n)$.

Hence each sequence of ψ_i yields a splitting which can be obtained by finding those n for which $\phi_m(n) \equiv r \pmod{b}$. We proceed to outline our method for determining these splittings.

We define strings of numbers which we denote by $S_1, S_2, \cdots$. Given two such strings S_i and S_j we shall write $S_i S_j$ for the string obtained when they are juxtaposed in the order indicated. By $\overset{\tau}{S_i}$, where τ is an integer, we shall mean the string obtained from S_i by adding modulo b the number τ to each digit of S_i. For example if $b=6$, $S_i = 501243$, $S_j = 450123$ then

$$S_i S_j = 501243450123 \quad \text{and} \quad \overset{3}{S_i} = 234510.$$

We proceed to the construction of such a sequence of S_i for any given sequence ψ_i of functions defined and with period b over the integers.

$$(8)\qquad \begin{cases} S_1 = \psi_0(0)\psi_0(1)\cdots\psi_0(b-1); \\ S_{m+1} = S_m^{\psi_m(0)}\cdots S_m^{\psi_m(b-1)}, \qquad m \geqq 1. \end{cases}$$

Note that S_1 has the b digits $\psi_0(0), \cdots, \psi_0(b-1)$ and that in general S_m has b^m digits.

It is not difficult to see that the nth digit of S_{m+1} is nothing more than the least non-negative residue mod b of $\phi_m(n)$. This enables us to determine the Ψ_r rapidly if we are given the ψ_i.

As an illustration let $b=3$, $m=2$ and define ψ_0, ψ_1, ψ_2 by

k	$\psi_0(k)$	$\psi_1(k)$	$\psi_2(k)$
0	0	0	0
1	2	1	2
2	1	2	1.

Then

$$S_1 = 021,$$
$$S_2 = 021\ 102\ 210,$$
$$S_3 = 021\ 102\ 210\ 210\ 021\ 102\ 102\ 210\ 021.$$

Writing 0, 1, $\cdots$, 26 under these we see immediately that

$$\Psi_0 = \{0,\ 4,\ 8,\ 11,\ 12,\ 16,\ 19,\ 23,\ 24\},$$
$$\Psi_1 = \{2,\ 3,\ 7,\ 10,\ 14,\ 15,\ 18,\ 22,\ 26\},$$
$$\Psi_2 = \{1,\ 5,\ 6,\ 9,\ 13,\ 17,\ 20,\ 21,\ 25\}.$$

To obtain an alternative splitting take all ψ_i to be equal to the identity map as in [**3**; **6**] and obtain

$$S_1 = 012,$$
$$S_2 = 012\ 120\ 201,$$
$$S_3 = 012\ 120\ 201\ 120\ 201\ 012\ 201\ 012\ 120.$$

Therefore

$$C_0 = \{0,\ 5,\ 7,\ 11,\ 13,\ 15,\ 19,\ 21,\ 26\},$$
$$C_1 = \{1,\ 3,\ 8,\ 9,\ 14,\ 16,\ 20,\ 22,\ 24\},$$
$$C_2 = \{2,\ 4,\ 6,\ 10,\ 12,\ 17,\ 18,\ 23,\ 25\}.$$

This gives us two different splittings of 0, 1, $\cdots$, 26 into three distinct classes. According to our bound there are at least two more such splittings obtainable in this way.

References

1. D. H. Lehmer, *The Tarry-Escott problem*, Scripta Math. vol. 13 (1947) pp. 37–41.
2. J. B. Roberts, *A curious sequence of signs*, Amer. Math. Monthly vol. 64 (1957) pp. 317–322.
3. ———, *A new proof of a theorem of Lehmer*, Canad. J. Math. vol. 10 (1958) pp. 191–194.
4. E. M. Wright, *Equal sums of like powers*, Edinburgh Math. Proc. vol. 8 (1949) pp. 138–142.
5. ———, *Equal sums of like powers*, Bull. Amer. Math. Soc. vol. 54 (1948) pp. 755–757.
6. ———, *Prouhet's* 1851 *solution of the Tarry-Escott problem of* 1910, Amer. Math. Monthly vol. 66 (1959) pp. 199–201.

Reed College

A DETERMINANT CONNECTED WITH FERMAT'S LAST THEOREM

L. CARLITZ[1]

Put

$$\Delta_n = \begin{vmatrix} 1 & C_{n,1} & C_{n,2} & \cdots & C_{n,n-1} \\ C_{n,n-1} & 1 & C_{n,1} & \cdots & C_{n,n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ C_{n,1} & C_{n,2} & C_{n,3} & \cdots & 1 \end{vmatrix},$$

where the $C_{n,r}$ are binomial coefficients. Bachmann showed that if

$$x^p + y^p + z^p = 0 \qquad (p \nmid xyz) \tag{1}$$

is solvable then $\Delta_{p-1} \equiv 0 \pmod{p^3}$. However Lubelski showed that for $p \geqq 7$, Δ_{p-1} is divisible by p^8, while E. Lehmer proved that Δ_{p-1} is divisible by $p^{p-2}q_2$, where $q_2 = (2^{p-1}-1)/p$; also $\Delta_n = 0$ if and only if $n = 6k$. For references see [2].

The writer [1] has determined the residue of Δ_{p-1} (mod p^{p-1}). The result is that

Received by the editors December 1, 1959.

[1] Research supported by National Science Foundation, Grant G-9425.