A NEW PROOF OF A THEOREM OF LEHMER

J. B. ROBERTS

In 1851 Prouhet **(2)** stated that any b^{k+1} consecutive positive integers (b a positive integer $\geqslant 2$) can be separated into b sets $\bar{C}_0, \ldots, \bar{C}_{b-1}$ each with b^k members in such a way that

$$\sigma_t(\bar{C}_0) = \ldots = \sigma_t(\bar{C}_{b-1}), \qquad 0 \leqslant t \leqslant k,$$

where $\sigma_t(\bar{C}_j)$ designates the sum of the tth powers of the numbers in $\bar{C}_j$. In 1947 Lehmer **(1)** generalized this result.

This paper contains a new proof of Lehmer's theorem. The proof gives a slightly more general result which is immediate from the less general form. The method of proof is similar to that of Lehmer except that it makes use of difference operators rather than differentiation. Two other proofs of Lehmer's theorem which are based on rather different ideas were given by Wright **(3)**.

1. Lehmer's theorem.

THEOREM. *Let $\alpha_0, \ldots, \alpha_k$ be an arbitrary set of $k+1$ complex numbers (distinct or not) and let b be an integer $\geqslant 2$. Let C be the collection of all numbers of the form $j_0\alpha_0 + \ldots + j_k\alpha_k$ where the j_i are integers satisfying $0 \leqslant j_i \leqslant b-1$. Further, let C_j, $0 \leqslant j \leqslant b-1$, be the collection of elements of C for which $j_0 + \ldots + j_k \equiv j \pmod{b}$. Then for $P(x)$, a complex polynomial of degree smaller than or equal to k,*

$$\sum_{n \in C_i} P(x+n) = \sum_{n \in C_j} P(x+n), 0 \leqslant i \leqslant b-1, 0 \leqslant j \leqslant b-1.$$

2. Proof of the theorem via operators. Let $E(c)$, where c is an arbitrary complex number, be an operator which maps the (complex) polynomial $P(x)$ onto the polynomial $P(x+c)$. Then $E(a+c) = E(a)E(c)$.

Throughout the remainder of this paper b is to be a fixed integer $\geqslant 2$ and ω any bth root of unity.

LEMMA 1.

$$\prod_{m=0}^{k} \sum_{j=0}^{b-1} \omega^j E(j\alpha_m) = \sum_{n \in C} \omega^{v(n)} E(n),$$

where $v(n) = j_0 + \ldots + j_k$ when $n = j_0\alpha_0 + \ldots + j_k\alpha_k$. Further, if a number $n \in C$ has more than one representation of the specified kind the right-hand sum includes a term for each representation.

Received May 6, 1957.

The proof of this lemma is immediate upon multiplying out the left side of the equation.

If we now take $\omega \neq 1$ we find

$$\sum_{j=0}^{b-1} \omega^j E(j\alpha_m)P(x) = \sum_{j=0}^{b-1} \omega^j P(x+j\alpha_m) = a_q x^q \sum_{j=0}^{b-1} \omega^j + \sum_{j=0}^{b-1} \omega^j Q(x,j)$$

where a_q is the leading coefficient of $P(x)$ and $Q(x,j)$ is a polynomial of degree smaller than that of $P(x)$. Now, since

$$\sum_{j=0}^{b-1} \omega^j = 0$$

we have

LEMMA 2.

$$\sum_{j=0}^{b-1} \omega^j E(j\alpha_m),\ \omega \neq 1,$$

maps a polynomial $P(x)$ onto a polynomial of smaller degree.

An immediate consequence of this lemma is that when $P(x)$ has degree smaller than or equal to k the operator on the left side of the equation in Lemma 1 maps $P(x)$ onto 0. Hence

$$(1)\quad \sum_{n\epsilon C} \omega^{v(n)}E(n)P(x) = \sum_{n\epsilon C} \omega^{v(n)}P(x+n) = \sum_{j=0}^{b-1} \omega^j \sum_{n\epsilon C j} P(x+n) = 0.$$

Equation (1) holds for all bth roots of unity other than 1. But when $c_{b-1}x^{b-1} + \ldots + c_0 = 0$ for all bth roots of unity other than 1 we must have

$$\begin{aligned} c_{b-1}x^{b-1} + \ldots + c_0 &= c_{b-1}(x-\omega_1)\ldots(x-\omega_{b-1}) = c_{b-1}(x^{b-1}+\ldots+1) \\ &= c_{b-1}x^{b-1} + \ldots + c_{b-1} \end{aligned}$$

for all x. Hence $c_i = c_{b-1}$ for $0 \leqslant i \leqslant b-1$. ($\omega_1, \ldots, \omega_{b-1}$ are the bth roots of unity other than 1.) Applying this result to (1) we find that

$$\sum_{n\epsilon C j} P(x+n)$$

is independent of j. This completes the proof of Lehmer's theorem.

3. Special Cases.

(a) If we take $\alpha_i = b^i$, $0 \leqslant i \leqslant k$, in the theorem then C_j, $0 \leqslant j \leqslant b-1$, consists of those integers from 0 to $b^{k+1}-1$ whose base b digit sum is congruent to j modulo b. Hence, if we take $P(x) = x^t$ and put $x = a+1$, $a \geqslant 0$, the theorem yields

$$\sigma_t(\bar{C}_0) = \ldots = \sigma_t(\bar{C}_{b-1}), \qquad 0 \leqslant t \leqslant k,$$

where $\bar{C}_j$ consists of those integers m from $a+1$ to $a+b^{k+1}$ such that $m-(a+1) \in C_j$. This is Prouhet's result applied to the b^{k+1} consecutive integers $a+1, \ldots, a+b^{k+1}$.

(b) Take the α_i as in (a) and let $P(x) = (j + mx) \dots (j + mx - q + 1)/q!$ When one puts $x = p/q$, in this case the theorem yields the result that

$$\sum_{n \in C_j} \binom{j + q + mn}{q}$$

is independent of j. The C_j are as in (a).

4. Calculation of the C_j when $\alpha_i = b^i$. We illustrate the calculation by means of an example. We take $b = 3$, $k = 2$. The aim is to construct a string of twenty-seven symbols of three kinds which, when attached to the integers 0 through twenty-six, have the property that two of these integers are in the same C_j, $0 \leqslant j \leqslant 2$ in this case, if and only if they have the same attached symbol. We use α, β, γ as our three kinds of symbols. The construction proceeds as follows.

$$\alpha\beta\gamma$$
$$\alpha\beta\gamma \ \beta\gamma\alpha \ \gamma\alpha\beta$$
$$\alpha\beta\gamma \ \beta\gamma\alpha \ \gamma\alpha\beta \ \beta\gamma\alpha \ \gamma\alpha\beta \ \alpha\beta\gamma \ \gamma\alpha\beta \ \alpha\beta\gamma \ \beta\gamma\alpha$$

If k had been 3 we would have continued one more step to get a string of 81 digits, the first twenty-seven of which would have been those in the third line above, the next twenty-seven of which would have been the cyclic permutation of those above beginning with the second block of 9, and the last twenty-seven would have been the cyclic permutation of those above beginning with the last block of 9.

In our case we have

α	β	γ	β	γ	α	γ	α	β	β	γ	α	γ	α	β	α	β	γ	γ	α	β
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

α	β	γ	β	γ	α
21	22	23	24	25	26

and therefore

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

Hence, to split the 27 positive integers $r, r + 1, \dots, r + 26$ into three classes satisfying Prouhet's result we take the a of section 3(a) to be $r - 1$ and find

$$\bar{C}_0 = \{r, r + 5, r + 7, r + 11, r + 13, r + 15, r + 19, r + 21, r + 26\}$$
$$\bar{C}_1 = \{r + 1, r + 3, r + 8, r + 9, r + 14, r + 16, r + 20, r + 22, r + 24\}$$
$$\bar{C}_2 = \{r + 2, r + 4, r + 6, r + 10, r + 12, r + 17, r + 18, r + 23, r + 25\}.$$

If $r = 1$, for instance, we have

$$\begin{aligned} &1^t + 6^t + 8^t + 12^t + 14^t + 16^t + 20^t + 22^t + 27^t \\ &= 2^t + 4^t + 9^t + 10^t + 15^t + 17^t + 21^t + 23^t + 25^t \\ &= 3^t + 5^t + 7^t + 11^t + 13^t + 18^t + 19^t + 24^t + 26^t, \qquad 0 \leqslant t \leqslant 2. \end{aligned}$$

References

1. D. H. Lehmer, *The Tarry-Escott problem*, Scripta Math., *13* (1947), 37–41.

2. M. E. Prouhet, *Memoire sur quelques relations entre les puissances des nombres*, C.R. Acad. Sci., *33* (Paris, 1851), 225.

3. E. M. Wright, *Equal sums of like powers*, Proc. Edin. Math. Soc., (2), *8* (1949), 138–142.

Wesleyan University
Middletown, Conn.
and
Reed College
Portland, Oregon