Equal Sums of Like Powers

By E. M. Wright

(*Received* 6*th March*, 1948. *Read* 7*th May*, 1948.)

1. In this note all small latin letters denote rational integers. We write $k \geqq 1$, $s \geqq 1$ and consider the simultaneous equations

$$\sum_{i=1}^{j} x_{i1}{}^h = \sum_{i=1}^{j} x_{i2}{}^h = \ldots\ldots = \sum_{i=1}^{j} x_{is}{}^h \qquad (1 \leqq h \leqq k). \qquad (1)$$

A solution of these equations is said to be non-trivial if no set $\{x_{iu}\}$ is a permutation of another set $\{x_{iv}\}$. In 1851 Prouhet[1] constructed a non-trivial solution of these equations with $j = s^k$ and Lehmer[2] has recently found a parametric solution for the same j. Here I give two alternative elementary proofs of Lehmer's result. Lehmer's own proof depends on the ideas of generating functions, exponentials, differentiation, matrices, and complex roots of unity, though all at a fairly simple level. One of my proofs requires only the factor theorem for a polynomial and the other only the multinomial theorem for a positive integral index.

I also show how to construct solutions for general k and any $s \leqq 2^m$ with $j = m2^k$. This result is an advance on Prouhet's, since my value of j is in general less than his value s^k. My method is almost trivial.

Many authors[3] have found solutions of (1) for particular values of k, s and j (especially $s = 2$) and Gloden[4] has shown how to construct solutions for $k = 2$, 3 or 5, any s and $j = k + 1$. So far as I know, only Prouhet and Lehmer have considered the problem for general k and s. Elsewhere[5] I have shown that solutions exist for

---

[1] *Comptes Rendus* (Paris), 33 (1851), 225.

[2] *Scripta Math.* 13 (1947), 37-41.

[3] Dickson's *History of the Theory of Numbers* II, chap. 24, lists 65 articles on this topic between 1878 and 1920.

[4] *Mehrgradige Gleichungen* (Groningen 1944), 71-90.

[5] *Bull. Amer. Math. Soc.* **54** (1948), 755-757.

general k and s when

$$j = \tfrac{1}{2}(k^2 + k + 2) \quad (k \text{ even}), \qquad j = \tfrac{1}{2}(k^2 + 3) \quad (k \text{ odd}),$$

values of j which are much less than Prouhet's s^k or my $m2^k$ and which are, in fact, independent of s. But the method proves only the existence of solutions and cannot be adapted to construct a solution.

2. *The Prouhet-Lehmer Theorem.* We take $n \geqq 2$ and suppose the numbers a_i $(1 \leqq i \leqq n)$ to satisfy $0 \leqq a_i \leqq s - 1$. Any set $(a_1, \ldots, a_n)$ such that

$$a_1 + a_2 + \ldots + a_n \equiv r \pmod{s} \tag{2}$$

is called an (n, r) set. If $r \equiv t \pmod{s}$, every (n, r) set is an (n, t) set and conversely. If $\phi = \phi(a_1, \ldots, a_n)$, we say that $\sum_{(n,r)} \phi$, the sum of ϕ over all (n, r) sets, is *independent of* r if

$$\sum_{(n,0)} \phi = \sum_{(n,1)} \phi = \ldots = \sum_{(n,s-1)} \phi.$$

We may enumerate all the (n, r) sets by letting each of $a_1, \ldots, a_{n-1}$ take independently the values 0 to $s - 1$ and choosing a_n for each set so that (2) is satisfied. From this it follows that there are just s^{n-1} different (n, r) sets and also that, if ϕ does not depend on a_n, $\sum_{(n,r)} \phi$ is independent of r. More generally

LEMMA 1. *If ϕ does not depend on one of the a_i, the sum $\sum_{(n,r)} \phi$ is independent of r.*

Lehmer's result is as follows.

THEOREM 1. If $\mu_1, \ldots, \mu_n$ *are any numbers and*

$$\xi = a_1 \mu_1 + a_2 \mu_2 + \ldots + a_n \mu_n,$$

then $\sum_{(n,r)} \xi^h$ *is independent of r for $1 \leqq h \leqq n - 1$.*

If we put $n = k + 1$ and $\mu_1, \ldots, \mu_n$ any non-zero integers, Theorem 1 provides us with a solution of the equations (1). Prouhet's result is the particular case of Theorem 1 in which $\mu_l = s^{l-1}$ $(1 \leqq l \leqq n)$, so that the ξ corresponding to the (n, r) sets are just those integers between 0 and $s^{k+1} - 1$ inclusive, the sum of whose digits in the scale of s is congruent to $r \pmod{s}$. This solution is obviously non-trivial. The case $s = 2$ of Theorem 1 is due to Escott.[1]

[1] *Quart. Jour. of Math.*, 41 (1910), 145.

Lehmer also proves

THEOREM 2. *If* $\mu_1 \mu_2 \ldots \mu_n \neq 0$, then $\sum_{(n,r)} \xi^n$ *is not independent of* r.

3. *First Proof.* By the multinomial theorem we have

$$\sum_{(n,r)} \xi^h = \sum_{t_1 + \cdots + t_n = h} \frac{h!}{t_1! \ldots t_n!} \mu_1^{t_1} \ldots \mu_n^{t_n} \left\{ \sum_{(n,r)} a_1^{t_1} \ldots a_n^{t_n} \right\},$$

where $t_1, t_2, \ldots, t_n$ are all non-negative and $0! = 1$ as usual. Let us consider the coefficient of a particular $\mu_1^{t_1} \ldots \mu_n^{t_n}$. If $h < n$, at least one of the t_i must be zero, $a_1^{t_1} \ldots a_n^{t_n}$ does not depend on one of the a_i and so the coefficient of $\mu_1^{t_1} \ldots \mu_n^{t_n}$ is independent of r by Lemma 1. Theorem 1 follows.

If $h = n$, the same argument shows that every term is independent of r except that in $\mu_1 \ldots \mu_n$. Hence Theorem 2 follows from

LEMMA 2. *The sum*

$$Q(n, r) = \sum_{(n,r)} a_1 \ldots a_n$$

is not independent of r.

If $Q(n, r)$ is independent of r, we have for every r

$$\begin{aligned} 0 &= Q(n, r+1) - Q(n, r) \\ &= \sum_{a_n=1}^{s-1} a_n Q(n-1, r+1-a_n) - \sum_{a_n=1}^{s-1} a_n Q(n-1, r-a_n) \\ &= \sum_{a=0}^{s-2} (a+1) Q(n-1, r-a) - \sum_{a=1}^{s-1} a Q(n-1, r-a) \\ &= \sum_{a=0}^{s-2} Q(n-1, r-a) - (s-1) Q(n-1, r-s+1) \\ &= \sum_{a=0}^{s-1} Q(n-1, r-a) - s Q(n-1, r+1). \end{aligned}$$

If a runs through a complete set of residues (mod s) so does $r - a$. Hence

$$\sum_{a=0}^{s-1} Q(n-1, r-a) = \sum_{a_1=0}^{s-1} \cdots \sum_{a_{n-1}=0}^{s-1} a_1 a_2 \ldots a_{n-1} = \{\tfrac{1}{2}s(s-1)\}^{n-1}$$

and so

$$Q(n-1, r+1) = 2^{1-n} s^{n-2} (s-1)^{n-1}$$

is independent of r. Repeating this argument $(n-1)$ times we

https://doi.org/10.1017/S0013091500002698 Published online by Cambridge University Press

find that

$$Q(1, r) = r \qquad (0 \leqq r \leqq s-1)$$

is independent of r. This is absurd and so Lemma 2 is true.

4. *Second proof.* The expression

$$S(r, t) = \sum_{(n, r)} \xi^h - \sum_{(n, t)} \xi^h$$

is a homogeneous form of degree h in $\mu_1, \mu_2, \ldots, \mu_n$. If one of the μ, say μ_n, is zero, ξ does not depend on a_n and so, by Lemma 1, $S(r, t) = 0$. Hence μ_n is a factor of $S(r, t)$ and similarly for $\mu_1, \ldots, \mu_{n-1}$; that is, $S(r, t)$ has the factor $\mu_1 \mu_2 \ldots \mu_n$. If $h < n$, this is impossible unless $S(r, t)$ vanishes identically. This is Theorem 1.

If $h = n$, we have

$$S(r, t) = C\mu_1 \mu_2 \ldots \mu_n,$$

and so[1]

$$\sum_{(n, r)} \xi^n = F(\mu_1, \ldots, \mu_n) + n! \; \mu_1 \ldots \mu_n Q(n, r),$$

where F is independent of r. Theorem 2 follows from Lemma 2 as before.

5. THEOREM 3. *If we have a non-trivial solution of* (1) *for* $s = 2$ *and* $j = J$, *we can construct a non-trivial solution for the same* k, $s = 2^m$ *and* $j = mJ$, *where* m *is any positive whole number.*

Let us suppose that

$$\sum_{i=1}^{J} b_i^h = \sum_{i=1}^{J} c_i^h \qquad (1 \leqq h \leqq k),$$

where the b are not a permutation of the c. By a simple use of the binomial theorem it follows that

$$\sum_{i=1}^{J} (t + b_i)^h = \sum_{i=1}^{J} (t + c_i)^h \qquad (1 \leqq h \leqq k) \qquad (3)$$

for every t. Hence we may suppose every b and every c positive. We choose

$$d > \max(b_1, \ldots, b_J, c_1, \ldots, c_J).$$

[1] Here again we use the multinomial theorem, so that the two proofs of Theorem 2 do not differ greatly.

https://doi.org/10.1017/S0013091500002698 Published online by Cambridge University Press

We now consider a set of mJ numbers divided into m sub-sets. The u-th sub-set consists either of the J numbers $(u-1)d+b_i$ $(1 \leqq i \leqq J)$ or of the J numbers $(u-1)d+c_i$ $(1 \leqq i \leqq J)$. We have thus two choices of each sub-set and so 2^m choices of the set itself, no two of which lead to the same set of numbers. By applying (3) to each corresponding pair of sub-sets we see that the sum of the h-th powers of the numbers of each set is the same, provided that $1 \leqq h \leqq k$.

6. If we use the particular case $s=2$ of Theorem 1, we can thus construct a solution for general s with $j = m\,2^k$, provided $s \leqq 2^m$. For particular k, solutions with smaller j can, of course, be constructed from known solutions for $s=2$.

DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF ABERDEEN.

https://doi.org/10.1017/S0013091500002698 Published online by Cambridge University Press