EQUAL SUMS OF LIKE POWERS

E. M. Wright

Principal, University of Aberdeen

In what follows small latin letters denote rational integers (whole numbers) and we write

$$S_h = S_h(a) = a_1^h + \ldots + a_s^h = \Sigma a_i^h$$

Let us consider the system of k equations

$$S_h(a) = S_h(b) \qquad (1 \leq h \leq k), \tag{1}$$

that is

$$\begin{aligned} a_1 + \ldots + a_s &= b_1 + \ldots + b_s, \\ a_1^2 + \ldots + a_s^2 &= b_1^2 + \ldots + b_s^2, \\ &\cdots\cdots\cdots \\ a_1^k + \ldots + a_s^k &= b_1^k + \ldots + b_s^k. \end{aligned}$$

These equations are obviously satisfied if the b are a permutation of the a; such a solution we call trivial. We prove first that, if $s \leq k$, then all solutions are trivial. If $s < k$, we put $a_{s+1} = \ldots = a_k = b_{s+1} = \ldots = b_k = 0$. Hence we may take $s = k$. Then (1) implies that

$$\Sigma a = \Sigma b, \qquad \Sigma a_1 a_2 = \Sigma b_1 b_2,$$

$$\Sigma a_1 a_2 a_3 = \Sigma b_1 b_2 b_3, \quad a_1 \ldots a_k = b_1 \ldots b_k$$

Hence the b are the roots of the same equation of the k-th

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press

degree as are the a. Thus the b are a permutation of the a.

When $s > k$, there may be non-trivial solutions. Let us write $P(k,2)$ for the least s such that the equations (1) have a non-trivial solution. We have proved above that

$$P(k,2) \geq k+1, \tag{2}$$

a result due to Bastien [1].

We may generalise our problem a little. Let us write

$$S_{hu} = a_{1u}^h + a_{2u}^h + \ldots + a_{su}^h,$$

and write $P(k,j)$ for the least value of s such that the set of $k(j-1)$ equations

$$S_{h1} = S_{h2} = \ldots = S_{hj} \qquad (1 \leq h \leq k) \tag{3}$$

is soluble with no set $a_{1u},\ldots,a_{su}$ a permutation of any set $a_{1v},\ldots,a_{sv}$, unless $u = v$. Clearly

$$P(k,j) \geq P(k,2) \geq k+1. \tag{4}$$

On the other hand, we can prove by an enumerative argument that

$$P(k,j) \leq \tfrac{1}{2}k(k+1) + 1. \tag{5}$$

Consider all the sets of integers $a_1, a_2, \ldots, a_s$ such that $1 \leq a_i \leq n$ $(1 \leq i \leq s)$. There are n^s such sets. For each such set

$$s \leq S_h(a) \leq sn^h,$$

and so there are at most

$$\prod_{h=1}^{k} sn^h = s^k n^{\frac{1}{2}k(k+1)}$$

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press

different sets $S_1, \ldots, S_k$.

If

$$n^s \geq (s!\,j)\, s^k\, n^{\frac{1}{2}k(k+1)}, \tag{6}$$

there is at least one set of values $S_1, \ldots, S_k$ which corresponds to at least $s!\,j$ different sets $(a_1, \ldots, a_s)$. Since there are at most $s!$ different permutations of any set $a_1, \ldots, a_s$, this set of values $S_1, \ldots, S_k$ must correspond to at least j different sets $a_1, \ldots, a_s$, no one of which is a permutation of any other. Hence, provided (6) is true, the equations (3) have a non-trivial solution. Now (6) is satisfied if $s = \frac{1}{2}k(k+1)+1$ and n is large enough; in fact, it is enough if $n > s!\,j s^k$.

We remark that, if any set $\{a_{iu}\}$ $(1 \leq i \leq s,\ 1 \leq u \leq j)$ is a solution of (3), so is the set $\{t + a_{iu}\}$ for any integer t, since

$$S_h(t + a_i) = \sum_{m=0}^{h} \binom{h}{m} t^{h-m} S_m(a_i).$$

Hence we need not bother whether our a_{iu} are all positive.

For <u>odd</u> k, we can improve (5) to

$$P(k, j) \leq \tfrac{1}{2}(k^2+3) \tag{7}$$

as follows. Take s even and replace $a_{1u}, \ldots, a_{su}$ by

$$b_{1u}, \ldots, b_{\frac{1}{2}s,u}, -b_{1u}, -b_{2u}, \ldots, -b_{\frac{1}{2}s,u}$$

Then $S_{hu} = 0$ if h is odd, and we have only to satisfy (3) for even h. An enumerative argument, similar to our earlier one,

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press

applied only to even values of h, shows that $s \geq \frac{1}{2}(k^2+3)$ is enough and so (7) follows.

For even k and j = 2, we replace $a_{11}, \ldots, a_{s1}$ by

$$c_1, c_2, \ldots, c_{s/2}, -d_1, -d_2, \ldots, -d_{s/2},$$

and $a_{12}, \ldots, a_{s2}$ by the negatives of these numbers. We require that

$$\sum_{i=1}^{s/2} c_i^h = \sum_{i=1}^{s/2} d_i^h \quad (h \text{ odd}, \ 1 \leq h \leq k)$$

and this leads to the result that

$$P(k,2) \leq \frac{1}{2}(k^2+4).$$

The enumerative method used to establish (5) and (7) does not, of course, exhibit actual solutions of (3) or of (1). On the other hand, if we can find actual solutions for any particular k, j and s, this value of s provides an upper bound for P(k, j). Much of the work in this field consists of finding actual solutions to (1) or to (3).

It seems probable that

$$P(k,j) = k+1 \qquad \text{(all } j\text{)} \tag{8}$$

and, in view of (2), it is only necessary to show that $P(k,j) \leq k+1$, i.e., to find a solution of (3) with $s = k+1$. Gloden [3] gave elegant methods of constructing such a solution for $k = 2, 3, 5$ and any j, so that (8) is proved for these three values of k (see pp. 330, 331 of [4] for a slightly different presentation of Gloden's constructions). Whether (8) is true for any other k is not known.

The result

$$P(k,2) = k+1 \tag{9}$$

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press

is known for $k \leq 9$, actual solutions of (1) being known for these k with $s = k + 1$. Let us write (1) in the form

$$[a_1, \ldots, a_s]_k = [b_1, \ldots, b_s]_k \tag{10}$$

Then it is not difficult to show that, for any d,

$$[a_1, \ldots, a_s, b_1+d, \ldots, b_s+d]_{k+1} = [a_1+d, \ldots, a_s+d, b_1, \ldots, b_s]_{k+1} \tag{11}$$

follows from (1). For example, $[0,3]_1 = [1,2]_1$ and so, with $d = 3$, we get $[1,2,3,6]_2 = [0,3,4,5]_2$, that is $[1,2,6]_2 = [0,4,5]_2$. Continuing this process with $d = 5, 7, 8, 13, 11$ in succession, we get solutions of (10) for $k = 3, 4, 5, 6, 7$ and $s = 4, 5, 6, 8, 8$ respectively. Thus (9) is true for $k \leq 5$ and for $k = 7$. Other solutions have been found for $k = 6, 8, 9$ (see [4]).

Tarry and Escott (c. 1910, see [2]) used this method to prove (in the obvious way) that $P(k,2) \leq 2^k$. As a result the whole subject is usually called the Tarry-Escott problem. In fact, Prouhet [8] announced in 1851 a correct rule for finding a solution of (3) for any j and $s = j^k$. He gave no proof, but his is the kind of result which is easier to prove than to guess. His result was overlooked until Lehmer [7] rediscovered his solution (in a generalised form) and gave a proof. A more suitable name for the whole topic is therefore the Prouhet-Lehmer problem, but, of course, many theorems and problems are wrongly named.

Prouhet's theorem is as follows. Express each number a $(0 \leq a \leq j^{k+1} - 1)$ as a "decimal" in the scale of j. If the least positive residue (mod j) of the sum of the digits of a in this scale is u, assign a to the set Ω_u. Then there are just j^k different a in each Ω_u, and they may be taken as the a_{iu} $(1 \leq i \leq j^k)$ in a solution of (3) with $s = j^k$. There are proofs of this in [7], [9] and [10]; the last-named contains a fuller account of the historical point.

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press

It is simplest to prove a slightly more general theorem due to Lehmer, from which Prouhet's result follows. Let us write

$$\xi = \sum_{i=0}^{k} c_i \mu_i \qquad (0 \leq c_i \leq j-1)$$

and

$$T(r) = \sum_{\sum c_i \equiv r \pmod{j}} \xi^h .$$

Consider $\Lambda(r,t) = T(r) - T(t)$, which is clearly a homogeneous polynomial of degree h in $\mu_0, \mu_1, \ldots, \mu_k$. If $\mu_k = 0$, we have

$$T(r) = \sum_{c_0, \ldots, c_{k-1}=0}^{j-1} \xi^h = T(t), \quad \Lambda(r,t) = 0 .$$

Hence $\Lambda(r,t)$ has a factor μ_k. Similarly, it has $\mu_0, \ldots, \mu_{k-1}$ as factors and so

$$\Lambda(r,t) = \mu_0 \ldots \mu_k F(r,t) ,$$

where $F(r,t)$ is a polynomial in the μ_i. Hence, if $h < k+1$, we have $\Lambda(r,t) = 0$ and so

$$T(0) = T(1) = \ldots = T(j-1) \qquad (1 \leq h \leq k) .$$

If we now write $\mu_i = j^i$, all the values of ξ are different integers and we have Prouhet's result.

A related problem arises in connection with the so-called "easier" Waring's problem. We shall require a solution of (1), viz.

$$(1) \qquad S_h(a) = S_h(b) \qquad (1 \leq h \leq k) ,$$

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press

such that

$$S_{k+1}(a) \neq S_{k+1}(b) . \tag{12}$$

We write $M(k)$ for the least s for which (1) and (12) are both true. Of course $P(k,2)$ is the least s for which (1) is true.

If $P(k,2) = k+1$, then $M(k) = P(k,2)$. But, if we do not know that $P(k,2) = k+1$, it is surprisingly difficult to prove that $M(k) = P(k,2)$, though one certainly expects this to be so. Observe that, for any k, either (i) $P(k,2) = P(k+1,2)$ or (ii) $M(k) = P(k,2)$.

Hua [5] proved that

$$M(k) \leq (k+1)\left(\left[\frac{\log \frac{1}{2}(k+2)}{\log (1+1/k)}\right] + 1\right) \sim k^2 \log k$$

for large k, and he can improve this to something like $\frac{1}{2}k^2 \log k$ for large k. This should be compared with the upper bound $[(k^2+4)/2]$ for $P(k,2)$. Hua's ingenious and elegant proof, while still "elementary", is much more elaborate than the simple enumerative proof of the result for $P(k,2)$.

Waring's problem is to determine $g(k)$, the least value of s such that every positive n can be expressed as a sum of s numbers from the set

$$0, 1^k, 2^k, 3^k, \ldots .$$

In general (with possibly a few exceptions), it is known that

$$g(k) = 2^k + [(3/2)^k] - 2 .$$

We write $G(k)$ to denote the least value of s such that every large enough n is the sum of s k-th powers.

What I called the "easier" Waring's problem (in [11]) is that of finding $v(k)$, the least value of s such that every positive n can be expressed as a sum of s numbers from the set

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press

$$0,\ 1^k,\ 2^k,\ 3^k,\ \ldots,\ -1^k,\ -2^k,\ -3^k,\ \ldots\ .$$

It is "easier" in the sense that $v(k) \leq g(k)$ but, as $v(k)$ is only known for $k = 2$, it has not proved to be easier in any other sense.

First

$$2m = (m+1)^2 - m^2 - 1$$

and

$$2m + 1 = (m+1)^2 - m^2 .$$

Hence $v(2) \leq 3$. But 6 is neither the sum nor the difference of two squares and so $v(2) = 3$.

Again

$$n^3 - n = n(n-1)(n+1) = 6t$$

and

$$n = n^3 - 6t = n^3 - (t+1)^3 - (t-1)^3 + 2t^3 ,$$

so that $v(3) \leq 5$. Since $x^3 \equiv 0, 1$ or $-1 \pmod 9$, numbers of the form $n = 9u + 4$ require 4 cubes at least, and so $v(3) = 4$ or 5.

There exist a and b such that

$$\sum_{i=1}^{s} a_i^h = \sum_{i=1}^{s} b_i^h \qquad (1 \leq h \leq k-2),$$

$$\Sigma a_i^{k-1} \neq \Sigma b_i^{k-1}$$

with $s = M(k-2)$. Hence

$$\Sigma(x+a_i)^k - \Sigma(x+b_i)^k = Cx + D \quad (C \neq 0) .$$

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press

If no more than $\Delta(k, C)$ k-th powers represent any residue mod C, we have

$$v(k) \leq \Delta(k, C) + 2s = \Delta(k, C) + 2M(k-2) .$$

Lower bounds for $v(k)$ can be found by considering congruences.

Thus I showed [11] that $8 \leq v(4) \leq 12$. Davenport improved this to $v(4) \leq 11$ and Hunter [6] improved it further to $9 \leq v(4) \leq 10$. But it is unknown whether $v(4)$ is 9 or 10.

For large k, this method is surpassed by the use of Vinogradoff's inequality

$$G(k) \leq 6\, k \log k + (4 + \log 216)\, k$$

and the obvious inequality $v(k) \leq G(k) + 1$.

REFERENCES

1. L. Bastien, Sphinx-Oedipe 8(1913), 171-172.

2. L. E. Dickson, History of the Theory of Numbers, vol. 2, Washington, 1920, Ch. 24.

3. A. Gloden, Mehrgradige Gleichungen, Groningen, 1944.

4. G. H. Hardy and E. M. Wright, Introduction to the Theory of Numbers, 4th ed. (Oxford 1960), 328-32.

5. L. K. Hua, Quart. J. of Math. 9(1938), 315-20.

6. W. Hunter, Journ. London Math. Soc. 16(1941), 177-9.

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

8. E. Prouhet, C. R. Acad. Sci. (Paris) 33(1851), 225.

9. E. M. Wright, Equal sums of like powers, Proc. Edinburgh Math. Soc. 8(1949), 138-42.

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press

_____, Prouhet's 1851 solution of the Tarry-Escott problem of 1910, Amer. Math. Monthly 66(1959), 199-201.

_____, An easier Waring's problem, Journ. London Math. Soc. 9(1934), 267-72.

https://doi.org/10.4153/CMB-1965-015-7 Published online by Cambridge University Press