Canad. Math. Bull. Vol. **18** (3), 1975

A RESULT ON SUMS OF SQUARES

BY
J. L. DAVISON

In this note we give an elementary proof of the following.

THEOREM 1. *Let $n \geq 1$ be an integer. Then, every positive even integer less than or equal to $n(n^2-1)/3$ can be expressed as a sum of n squares of integers from the set* $\{0, 1, 2, \ldots, n-1\}$.

Theorem 1 follows from Lagrange's Four Square Theorem. Indeed, using Lagrange's Theorem we can show that $[n/3]+5$ squares are sufficient (a number smaller than n, for $n>7$). This will be proved in Theorem 2. The virtue of Theorem 1, is that the proof is completely elementary, requiring no Number Theory and moreover gives a constructive method for finding such a representation.

Theorem 1 is obtained from some remarks on permutation groups. Let S_n denote the permutation group on $\{1, 2, \ldots, n\}$. If $\sigma \in S_n$, let $m(\sigma)=\sum_{i=1}^n |\sigma(i)-i|^2$. Note that if i is the identity permutation, then $m(\iota)=0$ and if ρ is the reverse permutation, given by $\rho(i)=n+1-i$, then $m(\rho)=n(n^2-1)/3$.

PROPOSITION 1. *For $\sigma \in S_n$, $m(\sigma)$ is even and lies in the interval* $[0, n(n^2-1)/3]$.

Proof. We show in fact that

$$m(\sigma)+m(\rho \circ \sigma) = \frac{n(n^2-1)}{3} \tag{1}$$

Expanding we obtain

$$m(\sigma) = \sum_{i=1}^n \sigma(i)^2 + \sum_{i=1}^n i^2 - 2\sum_{i=1}^n i\sigma(i)$$

Thus

$$m(\sigma) = 2\sum_{i=1}^n i^2 - 2\sum_{i=1}^n i\sigma(i), \tag{2}$$

which shows that $m(\sigma)$ is even,
Similarly,

$$m(p \circ \sigma) = 2\sum_{i=1}^n i^2 - 2\sum_{i=1}^n i(n+1-\sigma(i)) \tag{3}$$

From the fact that $\sum_{i=1}^n i^2 = n(n+1)(2n+1)/6$, we find that adding (2) and (3) gives us (1).

PROPOSITION 2. *Let $n \geq 4$, and let w be an even integer between 0 and $n(n^2-1)/3$. Then, there exists a $\sigma \in S_n$ with $m(\sigma)=w$.*

https://doi.org/10.4153/CMB-1975-078-1 Published online by Cambridge University Press

Proof. The proof is by induction. For $n=4$, the result is true by inspection. So let $n>4$. From equation (1), we can assume that $w \leq n(n^2-1)/6$. Since $n(n^2-1)/6 \leq (n-2)(n-1)(n)/3$ for $n \geq 5$, it follows that $w \leq (n-2)(n-1)(n)/3$. So by the inductive hypothesis, there exists $\hat{\sigma} \in S_{n-1}$ such that $m(\hat{\sigma})=w$. We let $\sigma(i)=\hat{\sigma}(i)$, $1 \leq i \leq n-1$ and $\sigma(n)=n$ and thus $m(\sigma)=w$.

Proof of Theorem 1. If $n=1$, 2 or 3 the result is true by inspection. If $n \geq 4$, the result follows from Proposition 2 and the fact that $|\sigma(i)-i| \in \{0, 1, \ldots, n-1\}$.

REMARK. This proof gives us a constructive method for finding an expression for the integer w as a sum of squares. For example, if $w=62$, $n=6$. The problem is to solve $m(\sigma)=62$, $\sigma \in S_6$.

For $n=6$, $n(n^2-1)/3=70$ so, we have $m(\rho \circ \sigma)=8$

From S_4 we see that if $\hat{\sigma}=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ then $m(\hat{\sigma})=8$.

So $\rho \circ \sigma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix}$ and hence

$\sigma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$

i.e. $62=5^2+1^2+1^2+1^2+3^2+5^2$

THEOREM 2. *Let $n \geq 1$. Then every positive integer not greater than $n(n^2-1)/3$ can be expressed as a sum of* $[n/3]+5$ *squares of integers from the set* $\{0, 1, 2, \ldots, n-1\}$.

Proof. If $n=1$ or 2, the proof is trivial. Let $n \geq 3$, and $1 \leq w \leq n(n^2-1)/3$. Then $w=k(n-1)^2+\ell$, where $0 \leq \ell < (n-1)^2$. By Lagrange's Theorem [1], ℓ is a sum of 4 squares of integers from $\{0, 1, 2, \ldots, n-2\}$.
Now

$$k = \left[\frac{w}{(n-1)^2}\right] \leq \left[\frac{n(n^2-1)}{3(n-1)^2}\right] = \left[\frac{n(n+1)}{3(n-1)}\right]$$

But $n(n+1)/3(n-1) \leq (n/3)+1$ so it follows that $k \leq [n/3]+1$. Thus, the number of squares required is at most $[n/3]+5$, which concludes the proof.

REFERENCE

1. G. H. Hardy & E. M. Wright, *An Introduction to The Theory of Numbers* (Oxford Press), 1960, p. 302.

DEPARTMENT OF MATHEMATICS,
LAURENTIAN UNIVERSITY