PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 2, June 1980

LAGRANGE'S THEOREM WITH $N^{1/3}$ SQUARES

S. L. G. CHOI, PAUL ERDÖS AND MELVYN B. NATHANSON[1]

ABSTRACT. For every $N > 1$ we construct a set A of squares such that $|A| < (4/\log 2)N^{1/3} \log N$ and every nonnegative integer $n \leqslant N$ is a sum of four squares belonging to A.

Let A be an increasing sequence of nonnegative integers and let $A(x)$ denote the number of elements of A not exceeding x. If every nonnegative integer up to x is a sum of four elements of A, then $A(x)^4 \geqslant x$ and so $A(x) \geqslant x^{1/4}$. In 1770, Lagrange proved that every integer is a sum of four squares. If A is a subsequence of the squares such that every nonnegative integer is a sum of four squares belonging to A, then we say that Lagrange's theorem holds for A. Since there are $1 + [x^{1/2}]$ nonnegative squares not exceeding x, it is natural to look for subsequences A of the squares such that Lagrange's theorem holds for A and A is "thin" in the sense that $A(x) \leqslant cx^{\alpha}$ for some $\alpha < 1/2$.

Härtter and Zöllner [2] proved that there exist infinite sets S of density zero such that Lagrange's theorem holds for $A = \{n^2 | n \notin S\}$. It is still true in this case that $A(x) \sim x^{1/2}$. Using probabilistic methods, Erdös and Nathanson [1] proved that, for every $\varepsilon > 0$, Lagrange's theorem holds for a sequence A of squares satisfying $A(x) \leqslant cx^{(3/8)+\varepsilon}$.

In this paper we study a finite version of Lagrange's theorem. For every $N > 1$, we construct a set A of squares such that $|A| < (4/\log 2)N^{1/3} \log N$ and every $n \leqslant N$ is the sum of four squares belonging to A. This improves the result of Erdös and Nathanson in the case of finite intervals of integers. We conjecture that for every $\varepsilon > 0$ and $N \geqslant N(\varepsilon)$ there exists a set A of squares such that $|A| \leqslant N^{(1/4)+\varepsilon}$ and every $n \leqslant N$ is the sum of four squares in A.

Let $|A|$ denote the cardinality of the finite set A and let $[x]$ denote the greatest integer not exceeding x.

LEMMA. *Let $a \geqslant 1$. Let $n \geqslant a^2$ and $n \not\equiv 0 \pmod 4$. Then either $n - a^2$ or $n - (a-1)^2$ is a sum of three squares.*

PROOF. If the positive integer m is not a sum of three squares, then m is of the form $m = 4^s(8t + 7)$. If $s = 0$, then $m \equiv 3 \pmod 4$. If $s \geqslant 1$, then $m \equiv 0 \pmod 4$.

Received by the editors May 11, 1979 and, in revised form, September 21, 1979.
1980 *Mathematics Subject Classification*. Primary 10J05; Secondary 10L05, 10L02, 10L10.
Key words and phrases. Sums of squares, Lagrange's theorem, addition of sequences.
[1]The research of the third author was supported in part by the National Science Foundation under grant no. MCS78-07908.

Since $a-1$, a are two consecutive numbers, there exist $i, j \in \{0, 1\}$ such that $a-i$ is even and $a-j$ is odd, hence $(a-i)^2 \equiv 0 \pmod 4$ and $(a-j)^2 \equiv 1 \pmod 4$. If $n \equiv 1$ or $2 \pmod 4$, then

$$n-(a-i)^2 \equiv n \equiv 1 \quad \text{or} \quad 2 \pmod 4,$$

and so $n-(a-i)^2$ is a sum of three squares. If $n \equiv 3 \pmod 4$, then

$$n-(a-j)^2 \equiv n-1 \equiv 2 \pmod 4,$$

and so $n-(a-j)^2$ is a sum of three squares. This proves the lemma.

THEOREM. *For every $N \geqslant 2$ there is a set A of squares such that*

$$|A| < \left(\frac{4}{\log 2}\right) N^{1/3} \log N$$

and every nonnegative integer $n \leqslant N$ is a sum of four squares belonging to A.

PROOF. Let $N \geqslant 6$. Let $A_1 = \{a^2 | 0 \leqslant a \leqslant 2N^{1/3} \text{ and } a^2 \leqslant N\}$ and let A_2 consist of the squares of all numbers of the form $[k^{1/2}N^{1/3}] - i$, where $4 \leqslant k \leqslant N^{1/3}$ and $i \in \{0, 1\}$. Then $|A_1| \leqslant 2N^{1/3} + 1$ and $|A_2| \leqslant 2N^{1/3} - 6$. Let $A_3 = A_1 \cup A_2$. Then $|A_3| < 4N^{1/3}$.

The set A_1 contains all squares not exceeding $\min(N, 4N^{2/3})$. Thus, if $0 \leqslant n \leqslant \min(N, 4N^{2/3})$, then n is a sum of four squares in $A_1 \subseteq A_3$. We shall show that if $4N^{2/3} < n \leqslant N$ and $n \not\equiv 0 \pmod 4$, then there is an integer $b^2 \in A_2$ such that $0 \leqslant n - b^2 \leqslant 4N^{2/3}$ and $n - b^2$ is a sum of three squares. Since each of these squares does not exceed $4N^{2/3}$, it follows that $n - b^2$ is a sum of three squares in A_1, hence n is a sum of four squares in $A_1 \cup A_2 = A_3$.

Suppose $4N^{2/3} < n \leqslant N$ and $n \not\equiv 0 \pmod 4$. Let $k = [n/N^{2/3}]$. Then $4 \leqslant k \leqslant N^{1/3}$. Let $a = [k^{1/2}N^{1/3}]$. Then $a^2 \leqslant n$. Moreover, $a^2 \in A_2$ and $(a-1)^2 \in A_2$. By the lemma, $n - b^2$ is a sum of three squares for either $b = a$ or $b = a - 1$. We must now show that $0 \leqslant n - b^2 \leqslant 4N^{2/3}$. Since $kN^{2/3} \leqslant n < (k+1)N^{2/3}$ and $a \leqslant k^{1/2}N^{1/3} < a + 1$, it follows that

$$n - b^2 \geqslant n - a^2 \geqslant kN^{2/3} - (k^{1/2}N^{1/3})^2 = 0.$$

Since $k \leqslant N^{1/3}$ and $4 < 3N^{1/6}$ for $N \geqslant 6$, it follows that

$$\begin{aligned} n - b^2 &< (k+1)N^{2/3} - (a-1)^2 \\ &< (k+1)N^{2/3} - (k^{1/2}N^{1/3} - 2)^2 \\ &< (k+1)N^{2/3} - (kN^{2/3} - 4k^{1/2}N^{1/3}) \\ &= N^{2/3} + 4k^{1/2}N^{1/3} \\ &\leqslant N^{2/3} + 4N^{1/2} \\ &< 4N^{2/3}. \end{aligned}$$

Therefore, if $0 \leqslant n \leqslant N$ and $n \not\equiv 0 \pmod 4$, then n is a sum of four squares belonging to A_3.

Construct the finite set A of squares as follows:

$$A = \{4^r a^2 | a^2 \in A_3, r \geqslant 0, 4^r a^2 \leqslant N\}.$$

Then $A_3 \subseteq A$ and

$$|A| \leqslant \left(\frac{\log N}{\log 4} + 1\right)|A_3| < \left(\frac{2 \log N}{\log 4}\right) 4N^{1/3}$$
$$= \left(\frac{4}{\log 2}\right) N^{1/3} \log N.$$

Let $0 \leqslant n \leqslant N$. Then $n = 4^r m$, where $r \geqslant 0$ and $m \not\equiv 0 \pmod 4$. Consequently, $m = a_1^2 + a_2^2 + a_3^2 + a_4^2$, where $a_i^2 \in A_3$. Then

$$n = 4^r m = 4^r a_1^2 + 4^r a_2^2 + 4^r a_3 + 4^r a_4^2$$
$$= (2^r a_1)^2 + (2^r a_2)^2 + (2^r a_3)^2 + (2^r a_4)^2$$

is a sum of four squares in A. This proves the theorem for $N \geqslant 6$.

For $N < 6$, it suffices to consider the set $A = \{0, 1\}$ for $N = 2, 3$ and the set $A = \{0, 1, 4\}$ for $N = 4, 5$. This completes the proof.

References

1. P. Erdös and M. B. Nathanson, *Lagrange's theorem and thin subsequences of squares*, Contributions to Probability: A Collection of Papers Dedicated to Eugene Lukacs, (J. Gani and V. K. Rohatgi, eds.), Academic Press, New York (to appear).

2. E. Härtter and J. Zöllner, *Darstellungen natürlichen Zahlen als Summe und als Differenz von Quadraten*, Norske Vidensk. Selsk. Skr. (Trondheim) 1 (1977), 1–8.

Department of Mathematics, Southern Illinois University, Carbondale, Illinois 62901