NOTES ON NUMBER THEORY II

On a theorem of van der Waerden

Leo Moser

(received August 28, 1959)

A well known theorem of van der Waerden [1] states that given any two positive integers k and t, there exists a positive integer m such that in every distribution of the numbers 1, 2, ..., m into k classes, at least one class contains an arithmetic progression of t + 1 terms. Other proofs and generalizations of this theorem have been given by Grünwald [2], Witt [3] and Lukomskaya [4]. The last mentioned proof appears in the booklet of Khinchin "Three pearls of number theory" in which van der Waerden's theorem plays the role of the first pearl.

Let $W = W(k,t)$ denote the least integer m such that in every distribution of 1, 2, ..., m into k classes at least one class contains an arithmetic progression of t + 1 terms. All known upper estimates for W for general k and t are far beyond the range of explicit expressions in terms of common algebraic operations. The first non-trivial lower estimate was given by Erdös and Radó [5]. They proved

$$W(k,t) > (2tk^t)^{\frac{1}{2}} . \tag{1}$$

This result was obtained by an averaging argument which does not yield any method for finding the desired distribution except the obvious but impractical method of examining all possible distributions of 1, 2, ..., $(2tk^t)^{\frac{1}{2}}$ into k classes. The object of this note is to construct a distribution which yields

$$W(k,t) > tk^{c \log k} \tag{2}$$

where c is a fixed constant. It is clear that for k sufficiently large compared to t, (2) is stronger than (1).

We will first prove (2) in the case t = 2, i.e. for

$$m = [2k^c \log k] \tag{3}$$

we will split 1, 2, ..., m into k classes in such a way that no class contains the average of two of its elements. Let n be the integer determined by

$$2^{(n-1)^2} \leq m < 2^{n^2} . \tag{4}$$

Express every $x \leq m < 2^{n^2}$ in the base 2^n, so that

$$x = a_0 + a_1 2^n + a_2 (2^n)^2 + \ldots + a_{n-1}(2^n)^{n-1},\ 0 \leq a_i < 2^n . \tag{5}$$

As is well known, the a_i will be uniquely determined by x. Let us further define b_i by

$$a_i \equiv b_i \pmod 2,\ b_i = 0 \text{ or } 1,\ i = 0, 1, 2, \ldots, n-1 \tag{6}$$

and

$$M(x) = \sum_{i=0}^{n-1} b_i 2^i . \tag{7}$$

Finally we define N(x) by

$$N(x) = \sum_{i=0}^{n-1} a_i^2 . \tag{8}$$

We now distribute 1, 2, ..., m into classes putting x and y in the same class if and only if

$$M(x) = M(y) \text{ and } N(x) = N(y) . \tag{9}$$

We will show that in this distribution the number of classes does not exceed k and that each class is "progression free". Since $x \leq m < 2^{n^2}$ we have by (5) and (8)

$$N(x) < n \cdot 2^{2n} . \tag{10}$$

Also (6) and (7) yield

$$M(x) < 2^n . \tag{11}$$

Hence the number of classes does not exceed $n \cdot 2^{3n} < 2^{4(n-1)}$ for $n > 6$. But now $2^{(n-1)^2} < m < 2k^c \log k$ implies $(n-1)^2 < c_1 (\log k)^2$ and $2^{4(n-1)} < k$ if c and c_1 are suitable constants.

We next show that our classes are progression-free. Suppose that x and y are in the same class and that the digits of x are $a_0^{(1)}, a_1^{(1)}, \ldots, a_{n-1}^{(1)}$ and those of y are $a_0^{(2)}, a_1^{(2)}, \ldots, a_{n-1}^{(2)}$. Since M(x) = M(y) we have

https://doi.org/10.4153/CMB-1960-005-9 Published online by Cambridge University Press

$a_i^{(1)} \equiv a_i^{(2)} \pmod 2$. Hence the digits of $z = \frac{1}{2}(x+y)$ will be $a_i^{(3)}$ where $a_i^{(3)} = \frac{1}{2}(a_i^{(1)} + a_i^{(2)})$. But now

$$\sum_{i=0}^{n-1} (a_i^{(3)})^2 = \sum \left\{\tfrac{1}{2}(a_i^{(1)} + a_i^{(2)})\right\} 2$$

$$\leq \tfrac{1}{2} \left\{ \sum (a_i^{(1)})^2 + \sum (a_i^{(2)})^2 \right\} = \tfrac{1}{2} \{N(x) + N(y)\} = N(x).$$

with equality if and only if $a_i^{(1)} = a_i^{(2)}$ for $i = 0, 1, 2, \ldots, n-1$. Thus if x and y are distinct and in the same class then $\frac{1}{2}(x+y)$ is in another class, and the proof of (2) is complete for the case $t = 2$.

Suppose now that $t > 2$. We split the integers $1, 2, \ldots, m = [2k^c \log k]$ into k classes as before. Further, we put two integers in the same class if $x \equiv y \pmod m$. If the resulting distribution of $1, 2, \ldots, m\,[t/2]$ contains a class with t numbers in arithmetic progression, then this class will also contain an arithmetic progression of 3 terms in an interval $[rm, (r+1)m]$, and hence there will be an arithmetic progression of three terms in the interval $[1, m]$ which, as we have seen, is not possible. Thus we have $W > \frac{1}{2} t\, k^c \log k$. However, the 2 in the last result can be absorbed by changing the constant c. Hence the proof is complete.

REFERENCES

1. B.L. van der Waerden, Beweis einer Baudetschen Vermutung, Nieuw Archief voor Wiskunde 15 (1921), 212-216.

2. R. Radó, Note on combinatorial analysis, Proc. Lond. Math. Soc. 48 (1945), 122-160.

3. E. Witt, Ein kombinatorischer Satz der Elementargeometrie, Math. Nachrichten 6 (1952), 261-262.

4. A.Y. Khinchin, Three Pearls of Number Theory, (Rochester, 1952), 11-17.

5. P. Erdös and R. Radó, Combinatorial theorems on classification of subsets of a given set, Proc. Lond. Math. Soc. 2 (1952), 417-439.

University of Alberta

https://doi.org/10.4153/CMB-1960-005-9 Published online by Cambridge University Press