On a problem of Graham

By E. ERDŐS and E. SZEMERÉDI (Budapest)

GRAHAM stated the following conjecture: Let p be a prime and $a_1, \dots, a_p$ p non-zero residues (mod p). Assume that if $\sum_{i=1}^{p} \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1 (not all $\varepsilon_i = 0$) is a multiple of p then $\sum_{i=1}^{p} \varepsilon_i$ is uniquely determined. The conjecture states that in this case there are only two distinct residues among the a's.

We are going to prove this conjecture for all sufficiently large p, in fact we will prove a sharper result. To extend our proof for the small values of p would require considerable computation, but no theoretical difficulty.

Our proof is surprisingly complicated and we are not convinced that a simpler proof is not possible, but we could not find one.

First we prove

Theorem 1. *Let η_0 be sufficiently small, $\eta < \eta_0$, $p > p_0(\eta)$: $A = \{a_1, \dots, a_l\}$, $l > \eta^{1/10} p$ is a set of non-zero residues* mod p. *Assume that for every t the number of indices i satisfying $a_i \equiv t$* (mod p) *is less than $\eta \cdot p$. Then*

$$\sum_{i=1}^{l} \varepsilon_i a_i \equiv r \pmod p \quad \varepsilon_i = 0 \quad \text{or } 1, \text{ not all } \quad \varepsilon_i = 0$$

is solvable for every r (mod p).

This theorem is perhaps of some interest in itself and easily implies Grahams conjecture in case each residue ossurs with a multiplicity $< \eta_0 p$. To see this observe that if $n_0^{1/10} < \frac{1}{2}$ we can split our set $a_1, \dots, a_p$ into two disjoint sets which satisfy the requirements of Theorem 1 and thus $\sum_{i=1}^{p} \varepsilon_i$ cannot be unique for $\sum_{i=1}^{p} \varepsilon_i a_i \equiv 0$ (mod p).

Now we prove Theorem 1. Put $\eta^{1/10} = \delta$. First we prove the following.

Now denote by $F(D)$ the set of all residues of the form $\sum_{x_i \in D} \varepsilon_i x_i$ and with $X + Y = \{x + y; x \in X, y \in Y\}$.

Lemma. *Let $B \subset A$, $|B| > \frac{|A|}{2}$, $(|A| = l > \delta p)$. Then there is a $D \subset B$ so that $|F(D)|$ is greater than $\frac{1}{2\delta^2} |D|$.*

To prove the Lemma observe that we can assume that there is a $B_1 \subset B$, $|B_1| > \frac{1}{2}|B|$ that every residue occurs in B_1 with a multiplicity at least $\eta^2 p^{1/2}$. For if not then a simple argument shows that B contains more that $3p^{1/2}$ distinct residues and then by a theorem of Erdős and Heilbronn $\sum_{a_i \in A} \varepsilon_i a_i \equiv r \pmod{p}$ is solvable for all r [1] which contradicts our hypothesis.

Henceforth we only consider B_1. By the theorem of Dirichlet to every $b \in B_1$ there is an integer $t_b < \frac{1}{\delta^2}$ so that the residue of $t_b \cdot b \pmod{p}$ is an absolute value $< \delta^2 p$. We want to show that there is a $b \in B_1$ for which this $t_b b \pmod{p}$ is an absolute value $> \frac{\delta^3}{8\eta}$. The number of distinct b's in B_1 is greater than $\frac{\delta}{4\eta}$ (B_1 has at least $\frac{\delta}{4}p$ elements and at most ηp of them are in the same congruence class). Now there are at most $\frac{1}{\delta^2}$ choices for t_b thus there are at most $\frac{1}{\delta^2}$ distinct $b's$ for which $t_b \cdot b$ is in the same residue class, hence there are at most $\frac{1}{\delta^2} \cdot 2\frac{\delta^3}{8\eta} = \frac{\delta}{4\eta}$ distinct values of b for which $t_b \cdot b$ is not greater than $\frac{\delta^3}{8\eta}$, but since there are more than $\frac{\delta}{4\eta}$ distinct b's in B_1 there is a $b \in B_1$ for which

$$\frac{\delta^3}{8\eta} < |t_b \cdot b| < \delta^2 p \tag{1}$$

as stated.

Now we are ready to construct D. We can assume without loss of generality that 1 occurs in B_1 (and is different from the b which we just constructed). Now our set D consists of $t_b \left[\frac{1}{\delta^2}\right]$ b's and $\left[\frac{\delta^3}{8\eta}\right]$ 1's (by our conditions we have at least $\eta^2 p^{1/2}$ 1's and b's). It easily follows from (1) that the number of sums $\sum \varepsilon_i d_i$, $d_i \in D$ is at least

$$\left[\frac{1}{\delta^2}\right]\left[\frac{\delta^3}{8\eta}\right] > \frac{\delta}{9\eta} > \frac{1}{2\delta^2}\left(t_b\left[\frac{1}{\delta^2}\right] + \left[\frac{\delta^3}{8\eta}\right]\right) \tag{2}$$

(2) follows from $t_b \leq \left[\frac{1}{\delta^2}\right]$ and $\delta = \eta^{1/10}$ which proves the Lemma.

Unit D from A and apply the Lemma repeatedly. Thus we obtain disjoint sets D_i, $1 \leq i \leq r$ each of which satisfy the Lemma and their union has at least $\frac{|A|}{2}$ elements (since by the Lemma if

$$\left|A - \bigcup_{i=1}^{r} D_i\right| > \frac{1}{2}|A| \geq \frac{\delta}{2}p \tag{3}$$

we can select another set D_{r+1}).

Now denote by $F(D_i)$ the set of all residues of the form $\sum_{d_j \in D_i} \varepsilon_i d_i$ by our Lemma

$$|F(D_i)| > |D_i| \frac{1}{2\delta^2}. \tag{4}$$

Now clearly

$$F\left(\bigcup_{i=1}^{r} D_i\right) = F(D_1) + F(D_2) + \dots + F(D_r). \tag{5}$$

By the Cauchy—Davenport theorem [2]

$$\left|F\left(\bigcup_{i=1}^{r} D_i\right)\right| \geqq \min\left(p, \sum_{i=1}^{r} |F(D_i)|\right) = p$$

by (3), (4) and (5), which completes the proof of Theorem 1.

Henceforth we can assume that at least one residue occurs at least $\eta_0 p$ times amongst the a's. Without loss of generality we can assume that this residue is 1 and that 1 occurs $t \geqq \eta_0 p$ times.

We have to distinguish several cases. First assume $t > \frac{9}{10} p$. Several subcases have to be distinguished. First assume that all a's are $\leqq p-t$, $1 < a_1 < \dots < a_{p-t} \leqq p-t$. Let $a_r + \dots + a_k \geqq p-t$ be the smallest k with this property, $k < p-t$ is easy to see also $a_1 + \dots + a_{k+1} < p$ is obvious thus

$$a_1 + \dots + a_k + (p - a_1 - a_2 - \dots - a_k)1 \quad \text{and} \quad a_1 + \dots + a_{k+1} + (p - a_1 - \dots - a_{k+1})1$$

give two representations of 0 with different $\sum_{i=1}^{p} \varepsilon_i$.

Thus at least one of the a's are $> p-t$. Clearly one cannot have two incongruent a's in $(p-t, p)$ otherwise $\sum \varepsilon_i$ is clearly not unique. Let $p-t < a_{p-t} < p$. If $a_{p-t} \geqq t$ it must clearly occur with multiplicity one (since otherwise $t > \frac{9}{10} p$ again gives non-uniqueness for $\sum \varepsilon_i$). Observe that in this case $a_1 + \dots + a_{p-t-1} \geqq 2(p-t-1) \geqq$ $\geqq p-t$ since $t \leqq p-2$. Let now k be the smallest integer satisfying

$$t > a_1 + \dots + a_k \geqq p-t$$

and now $a_{p-t} + (p - a_{p-t})1$ and $a_1 + \dots + a_k + (p - a_1 - \dots - a_k)1$ give two different values for $\sum_{i=1}^{p} \varepsilon_i$ what is contradiction.

Thus we can assume $a_{p-t} < t$. But then $a_1 + a_{p-t} < p$ and thus we again get using $p - a_{p-t}$ resp. $p - a_1 - a_{p-t}$ ones two different values of $\sum_{i=1}^{p} \varepsilon_i$. This disposes the case $t > \frac{9}{10} p$.

Henceforth assume $\eta_0 p < t \leqq \frac{9}{10} p$. Again we have to distinguish several cases. First assume that there are at most $\frac{t}{100}$ residues amongst the a's greater than

$\frac{t}{100}$. Since there are $p-t$ a's not congruent 1 there clearly are at least $\frac{p-t}{2}+1$ a's greater than one but less than $\frac{t}{100}$. Their sum is thus greater than $p-t$. Let $a_1+\dots+a_r$ the smallest r for which $a_1+\dots+a_r \geqq p-t$ then also $a_1+\dots+a_r+a_{r+1} < p-t+\frac{t}{50} < p$ thus $a_1+\dots+a_r+(p-a_1-\dots-a_r)\cdot 1$ and $a_1+\dots+a_r+a_{r+1}+(p-a_1-\dots-a_r-a_{r+1})1$ again give two different values for $\sum_{i=1}^{p} \varepsilon_i$.

Henceforth we can assume that there are at least $\frac{t}{100}$ a's greater than $\frac{t}{100}$ and in fact we can assume that they are all less than $\frac{p-t}{2}$ (since as we proved in the previous case at most one a can be greater than $\frac{p-t}{2}$).

Let now S_1 be a set of $\frac{t}{100}$ a's which are congruent one and S_2 a disjoint set of $\frac{t}{200}$ a's which are also congruent one. Let a be one of the residues in $\left(\frac{t}{100}, \frac{p-t}{2}\right)$. Clearly

$$|F(a \cup S_1)| \geqq \frac{2t}{100} = \frac{t}{50} \quad \text{and} \quad |F(A-S_1-S_2-a)| > \tag{6}$$
$$|A|-|S_1|-|S_2|-1 \geqq p-\frac{t}{100}-\frac{t}{200}-1.$$

Thus by Cauchy-Davenport

$$|F(a \cup S_1 \cup A-S_1-S_2-a)| \geqq \min\{p_1 |F(a \cup S_1)|+|F(A-S_1-S_2-a)|\} = p.$$

Hence

$$0 \equiv \alpha_1 \cdot 1 + \sum_i \alpha_{a_i} a_i, \quad \alpha_1 \leqq t-\frac{t}{100}. \tag{7}$$

Now we again have to distinguish two cases. Assume first

$$\sum_i \alpha_{a_i} > \eta_0^2 p \quad (t \geqq \eta_0 p).$$

As stated previously we can assume by the theorem of Erdős and Heilbronn that the number of distinct a's is less than $3\sqrt{p}$ thus we can assume $\alpha_{a_1} > \frac{\eta_0^2}{3} p^{1/2}$. Thus by the theorem of Dirichlet there is an $s \leqq \frac{\alpha_{a_1}}{2}$ for which

$$|sa_1| < p^{1/2} \frac{3}{\eta_0^2} < \frac{t}{200}.$$

If $sa_1 > p - \frac{t}{200}$ then $sa_1 + (p - sa_1)1$ and $2sa_1 - (p - 2sa_1)1$ give two representations of D with different $\sum \varepsilon_i$. Thus we can assume $sa_1 < \frac{t}{200}$ but then sa_1 can be replaced by sa_1 ones from S_2 and since $sa_1 \neq s$ this again gives two distinct value of $\sum_i \varepsilon_i$.

Thus we can assume $\sum \alpha_{a_i} < \eta_0^2 p$. Thus we have at least $p - t - \eta_0^2 p > \frac{p-t}{2}$ a's distinct from 1 which have not been used in (7). By Erdős—Heilbronn (as used before) at least one of these a's have a high multiplicity and thus there is an $sa < \frac{t}{100}$. Thus $\alpha_1 < \frac{t}{100}$ since otherwise we could replace sa of the ones by sa and thus we again get two distinct values of $\sum \varepsilon_i$.

Now we omit from A all the a's occuring in (6) and we obtain a new set A'. Using (6) for A' we again get representation of 0 (7′) (we remark that we can assume that α_1 in (7) and α_1' in (7′) are both $\leqq t - \frac{t}{100}$ thus we do not run out of ones). Adding the two representations of D we obtain our contradiciton.

References

[1] P. Erdős and H. Heilbronn, On the addition of residue classes mod p, *Acta Arithmetica* **9** (1964), 149—159.
[2] H. Halberstam and K. F. Roth, Sequences, *Oxford*, 1969.

(Received February 14, 1974.)