Mathematics

G. A. Freiman

1961

SovietRxiv

Abstract

Full Text

Mathematics

G. A. Freiman

INVERSE PROBLEMS OF ADDITIVE NUMBER THEORY

On the Addition of Sets of Residues Modulo a Prime

(Presented by Academician I. M. Vinogradov, June 30, 1961)

Notation. K and M are finite sets of rational integers:

$$K = \{a_0, a_1, \dots, a_{k-1}\}, \qquad M = \{b_0, b_1, \dots, b_{m-1}\}.$$

We assume that $a_0 = 0,\ a_i < a_{i+1},\ i = 0, 1, \dots, k-2;\ b_0 = 0,\ b_j < b_{j+1},\ j = 0, 1, \dots, m-2;\ a_{k-1} < p$ and $b_{m-1} < p;\ p$ is a prime number. $(2K)_p,\ (K+M)_p$ are the sets of all distinct residues modulo p from $2K,\ K+M$. $T(2K), T(K+M)$ are the number of numbers in $2K,\ K+M$. $T_p(2K), T_p(K+M)$ are the number of distinct residues in $2K,\ K+M$ modulo p.

Results describing the structure of K and M when $T_p(K+M) = k+m-1$ were obtained by Vosper ([1]).

Theorem 1. If $T_p(2K) < 2.4k - 3$ and $k < p/35$, then the residues from K are contained in an arithmetic progression modulo p of length $k+b$, where b is determined from the equality $T = 2k - 1 + b$.

Proof. Let

$$I = \sum_{x_1, x_2 \in K} \sum_{x_3 \in (2K)_p} \sum_{a=0}^{p-1} e^{2\pi i a \frac{x_1 + x_2 - x_3}{p}} = \sum_{a=0}^{p-1} S_1^2 S,$$

where

$$S_1 = \sum_{j=0}^{k-1} e^{2\pi i \frac{a}{p} a_j}, \qquad S = \sum_{x \in (2K)_p} e^{-2\pi i \frac{a}{p} x}.$$

If one assumes that for $a \neq 0$

$$|S_1| \leq 0.6k,$$

then

$$|I| \leq k^2 T_p + \sum_{a=1}^{p-1} |S_1|^2 |S| \leq k^2 T_p + 0.6k \left[\sum_{a=0}^{p-1} |S_1|^2 \sum_{a=0}^{p-1} |S|^2 \right]^{1/2} < k^2 p.$$

Since $I = k^2 p$, there exists a' such that

$$|S_1(a')| = \left| \sum_{j=0}^{k-1} e^{2\pi i \frac{a'}{p} a_j} \right| > 0.6k. \tag{1}$$

Lemma. Given k complex numbers

$$e^{2\pi i \alpha_0},\ e^{2\pi i \alpha_1}, \ldots,\ e^{2\pi i \alpha_{k-1}},$$

where α_i are real numbers.

Let $k_1(\beta)$ be the number of numbers for which

$$\begin{array}{ll} \beta \leqslant \{\alpha_i\} < \beta + \frac{1}{2}, & \text{if } 0 \leqslant \beta \leqslant \frac{1}{2}, \\ \beta \leqslant \{\alpha_i\} \text{ or } \{\alpha_i\} < \beta - \frac{1}{2}, & \text{if } \frac{1}{2} < \beta < 1. \end{array}$$

If for every β

$$k_1(\beta) < ck,$$

then

$$\left| \sum_{j=0}^{k-1} e^{2\pi i \alpha_j} \right| \leqslant (2c-1)k.$$

From this lemma and from (1) it follows that there exist integers u and v (the latter may be determined by means of the congruence $a'v \equiv 1 \pmod{p}$) such that among the numbers

$$u + vs, \qquad 0 \leqslant s \leqslant \frac{p-3}{2} \tag{2}$$

there are k_1 numbers congruent to numbers of K, and

$$k_1 \geqslant 0.8k.$$

Let the numbers from (2) that are congruent to numbers of K be obtained for the values s equal to

$$s_0, s_1, \dots, s_{k_1-1}, \qquad s_i < s_{i+1}, \quad i = 0, 1, \dots, k_1 - 2.$$

We may assume that $s_0 = 0$.

If $(s_1, s_2, \dots, s_{k_1-1}) = d > 1$, then instead of the number v one may take the number vd. We may therefore suppose that $d = 1$.

If $s_{k_1-1} \geqslant 2k_1 - 2$, then from Theorem VI in ([2]) it follows that

$$T_p(2K) \geqslant 3k_1 - 3 \geqslant 2.4k - 3.$$

Thus, $s_{k_1-1} \leqslant 2k_1 - 3$. If in K there existed a residue congruent to $u + vs$ for

$$4k_1 - 6 < s < p - (2k_1 - 3),$$

then we would have $T_p \geqslant 2k_1 - 1 + k_1 = 3k_1 - 1$.

Thus, all residues from K are congruent to the numbers $u + vs$ for

$$-(2k_1 - 3) \leqslant s \leqslant 4k_1 - 6.$$

Hence, and from Theorem V in ([2]), follows the validity of the theorem being proved.

The theorem is also valid for $T_p < 2.3k - 3$ and $k < p/12$.

Theorem 2. If $3k - 3 \leqslant T(2K) < \frac{10}{3}k - 5$, $(a_1, a_2, \dots, a_{k-1}) = 1$, $c_1 k < a_{k-1}$, $k > c_2$, where c_1 and c_2 are sufficiently large positive constants, then the set K is contained in two arithmetic progressions with the same difference, of total length not exceeding $k+b$, where b is determined from the equality $T = 3k-3+b$ (see ([3])).

Using this result instead of Theorem VI in ([2]), it is easy to strengthen the result of Theorem 1.

Theorem 3. If $T_p < 2.68k$, then there exist positive numbers β and c such that, when the condition $c < k < \beta p$ is satisfied, the assertion of Theorem 1 is valid.

Theorem 4. If $T = k + m - 1 + b$, where $b \leqslant \min(k, m) - 3$, $(a_1, a_2, \dots, a_{k-1}, b_1, b_2, \dots, b_{m-1}) = 1$, then $a_{k-1} \leqslant k + b - 1$, $b_{m-1} \leqslant m + b - 1$.

Theorem 5. If $k \geqslant m$,

$$T_p(K + M) \leqslant k + m + \theta m - 3, \qquad k < \beta p, \quad \beta \leqslant \tfrac{1}{12}, \tag{3}$$

where $\theta \geqslant 0$ satisfies the condition

$$\eta^3\theta^3+(\eta^3+2\eta^2)\theta^2+\left(\eta^2+\frac{5}{4}\eta\right)\theta+\frac{\eta+1}{4}-2(1-3\beta)^2\eta^{3/2}<0, \qquad \eta=m/k \tag{4}$$

then the sets K and M are situated in progressions with the same difference modulo p, of lengths respectively equal to $k+b$ and $m+b$, where b is determined from the equality $T=k+m-1+b$.

Proof. Suppose

$$|S_1S_2|<\gamma km,$$

where

$$\gamma=(1-3\beta)^2\frac{\sqrt{km}}{k+m+\theta m}, \qquad S_1=\sum_{j=0}^{k-1}e^{2\pi ia\frac{a_j}{p}}, \qquad S_2=\sum_{j=0}^{m-1}e^{2\pi ia\frac{b_j}{p}}, \qquad p\nmid a,$$

leads to a contradiction:

$$\begin{aligned} pkm &= \sum_{x_1\in K}\sum_{x_2\in M}\sum_{x_3\in(K+M)_p}\sum_{a=0}^{p-1}e^{\frac{2\pi ia}{p}(x_1+x_2-x_3)}=\sum_{a=0}^{p-1}S_1S_2S_3< \\ &< kmT+\left[\sum_{a=1}^{p-1}|S_1|^2|S_2|^2\sum_{a=0}^{p-1}|S_3|^2\right]^{1/2}\leqslant \\ &\leqslant kmT+\sqrt{\gamma kmTp}\left[\sum_{a=0}^{p-1}|S_1|^2\sum_{a=0}^{p-1}|S_2|^2\right]^{1/4}<pkm. \end{aligned}$$

Thus there exists an a for which

$$|S_1|\geqslant\gamma_1k, \qquad |S_2|\geqslant\gamma_2m, \tag{5}$$

where $\gamma_1\gamma_2=\gamma$.

From (5) and the lemma there follows the existence of integers u, u_1, and v such that, with the numbers (2), the numbers

$$u_1+vt, \qquad 0\leqslant t\leqslant\frac{p-3}{2} \tag{6}$$

are congruent respectively to k_1 numbers from K and m_1 numbers from M, where

$$k_1 \geqslant \frac{1+\gamma_1}{2}\, k, \qquad m_1 \geqslant \frac{1+\gamma_2}{2}\, m.$$

Let the numbers from (6) congruent to numbers from M be obtained for the values t equal to $t_0, t_1, \dots, t_{m_1-1}$, with $t_j < t_{j+1}$, $j = 0, 1, \dots, m_1 - 2$, $t_0 = 0$.

If $\max(s_{k_1-1}, t_{m_1-1}) \geqslant k_1 + m_1 - 3$, then, in view of Theorem 4,

$$T_p(K+M) \geqslant k_1 + m_1 + \min(k_1, m_1) - 3.$$

In view of (4), this contradicts (3).

If $\max(s_{k_1-1}, t_{m_1-1}) \leqslant k_1 + m_1 - 4$, then every number from K (respectively M) is congruent to one of the numbers $u + vs$ (respectively $u_1 + vt$) for

$$-(k_1 + m_1 - 4) \leqslant s, \quad t \leqslant 2k_1 + 2m_1 - 8.$$

Applying Theorem 4, we complete the proof.

Steklov Mathematical Institute
of the Academy of Sciences of the USSR

Received
19 VI 1961

REFERENCES

1. A. G. Vosper, *J. London Math. Soc.*, **31**, No. 122, 200 (1956).
2. G. A. Freiman, *Izv. Vyssh. uchebn. zaved., Matem.*, No. 6 (13), 202 (1959).
3. G. A. Freiman, *Uch. zap. Elabuzhsk. gos. ped. inst.*, **8**, 72 (1960).

Note: Figure translations are in progress. See original paper for figures.