ON SUM-PRODUCT REPRESENTATIONS IN $\mathbb{Z}_q$

Mei-Chu Chang

Abstract The purpose of this paper is to investigate efficient representations of the residue classes modulo q, by performing sum and product set operations starting from a given subset A of $\mathbb{Z}_q$. We consider the case of very small sets A and composite q for which not much seemed known (nontrivial results were recently obtained when q is prime or when $\log |A| \sim \log q$). Roughly speaking we show that all residue classes are obtained from a k-fold sum of an r-fold product set of A, where $r \ll \log q$ and $\log k \ll \log q$, provided the residue sets $\pi_{q'}(A)$ are large for all large divisors q' of q. Even in the special case of prime modulus q, some results are new, when considering large but bounded sets A. It follows for instance from our estimates that one can obtain r as small as $r \sim \frac{\log q}{\log |A|}$ with similar restriction on k, something not covered by earlier work of Konyagin and Shparlinski(see KS). On the technical side, essential use is made of Freiman's structural theorem on sets with small doubling constant. Taking for $A = H$ a possibly very small multiplicative subgroup, bounds on exponential sums and lower bounds on $\min_{a\in\mathbb{Z}_q^*} \max_{x\in H} \| \frac{ax}{q} \|$ are obtained. This is an extension to the results obtained by Konyagin, Shparlinski and Robinson on the distribution of solutions of $x^m = a \pmod q$ to composite modulus q.

0. Introduction

In this paper, we consider the following problem. Consider a subset $H \subset \mathbb{Z}_q^*$ ($q \in \mathbb{N}$ arbitrary) such that $|\pi_p(H)| > 1$ for all prime divisors $p|q$. Let kH be the k-fold sum set, and H^r the r-fold product set of H. Then $kH = \mathbb{Z}_q$ for some $k \in \mathbb{N}$. One may for instance take $k = q^3$ (see proof of Theorem 2). Assume now we allow both addition and multiplication and seek for a representation $\mathbb{Z}_q = kH^r$, how small may we take k and r? In this context, we show the following:

Theorem A. *There is a function $\kappa' = \kappa'(\kappa, M)$ such that $\kappa' \to 0$ if $\kappa \to 0, M \to \infty$ with the following property.*

Let $q \in \mathbb{N}$ be odd and $H \subset \mathbb{Z}_q^*$ such that

$$|\pi_p(H)| > 1 \textit{ for all prime divisors } p \textit{ of } q \tag{0.1}$$

$$|\pi_{q'}(H)| > M \textit{ for all divisors } q'|q, q' > q^\kappa \tag{0.2}$$

Then

$$\mathbb{Z}_q = kH^r \textit{ with } k < q^{\kappa'} \textit{ and } r < \kappa' \log q. \tag{0.3}$$

(This will be proved in §6).

The main motivation for this work comes from a recent line of reseach in combinatorial number theory and its applications to exponential sums in finite fields and residue classes. (cf [BKT], [BGK], [BC],[B].)

If we consider in particular a subset $A \subset \mathbb{F}_p$, p prime, such that $|A| > p^\epsilon$ for some fixed (and arbitrary) $\epsilon > 0$, then $kA^k = \mathbb{F}_p$ provided $k > k(\epsilon)$ and also

$$\max_{(a,p)=1} \Big| \sum_{x_1,\dots,x_k \in A} e_p(ax_1 \dots x_k)\Big| < p^{-\delta(\epsilon)} \, |A|^k$$

for some $\delta(\epsilon) > 0$. This and related estimates had very significant application to the theory of Gauss sums and various issues related to pseudo-randomness (see [B], [BKSSW], [BIW] for instance). One of the main shortcomings of the results that are presently available is the break-down of the method, starting from the sum-product theorem in [BKT], if we let $\epsilon = \epsilon(p)$ be small. The boundary of the assumption here is $\varepsilon \gtrsim \frac{1}{\log\log p}$, which is likely much stronger than necessary for such results to hold. More precisely, letting $H < \mathbb{F}_p^*$, one could expect an equidistribution result of the form

$$\max_{(a,p)=1} \Big| \sum_{x \in H} e_p(ax)\Big| < o(|H|) \qquad (*)$$

to hold whenever $\log |H| \gg \log\log p$, which at this stage we can only establish if $\log |H| > \frac{\log p}{(\log\log p)^\varepsilon}$ (see [BGK]).

It became apparently clear that the underlying ideas as developed in [BKT], [BGK] are insufficient to reach this goal (in particular they seem unable to produce a result such as the theorem stated above). Our purpose here is to explore the use of Freiman's Theorem in sum-product problems which was not used in [BKT]). Freiman's Theorem (see [N] for instance) is one of the deepest result in additive number theory, providing a very specific description of subsets A of a torsion-free Abelian group with small sumset, i.e. $|2A| = |A+A| < K|A|$, with K not too large.

The results of this paper are new and based on a new approach. They do not provide the answers to the primary questions we are interested in, such as understanding when (*) holds, but bring new techniques into play through related and more modest aims.

Our bound in (0.3) is essentially optimal. Consider a composite $q = p_1 p_2$, where p_1 and p_2 are prime. Let $p_1 \approx \frac{1}{2} q^\kappa$. Define

$$H = \{1, \theta\} + p_1\{0, 1, \dots, p_2 - 1\}$$

where θ is of multiplicative order 2 $(\mathrm{mod}\, p_1)$. Hence $H \subset \mathbb{Z}_q^*$. Obviously (0.1), (0.2) hold. Since

$$kH^r = kH \subset \{x + y\theta : x, y \in \mathbb{N}, x + y = k\} + p_1\{0, 1, \dots, p_2 - 1\}$$

(0.3) requires $k \geq p_1 \sim \frac{1}{2} q^\kappa$, hence $\kappa' \geq \kappa$.

The argument used to prove Theorem A has the following interesting consequence for subsets $A \subset \mathbb{Z}_p, p$ prime.

Theorem B. *Given $K > 1$, there is $K' = K'(K) \to \infty$, as $K \to \infty$ such that the following holds:*

Let $\theta \in \mathbb{Z}_p$ be such that θ is not a root of any polynomial in $\mathbb{Z}_p[x]$ of degree at most K and coefficients bounded by K (as integers). Then, if $A \subset \mathbb{Z}_p$ is an arbitrary set and $K < |A| < \frac{p}{K}$, we have

$$|A + \theta A| > K'|A|.$$

Remark. For a similar result over characteristic 0, by Konyagin and Laba, see [KL].

Returning to exponential sums with prime modulus $\big($see (6.20)$\big)$, we do obtain the following extension for composite modulus

Theorem C. *Let $H < \mathbb{Z}_q^*$ (q arbitrary) and assume $|H| \geq M > 1$. Then*

$$\max_{(a,q)=1} \Big| \sum_{x \in H} e_q(ax) \Big| < |H| - cq^{-\delta(M)} \tag{0.4}$$

where $\delta(M) \to 0$ for $M \to \infty$ (independently of q).

This theorem will be proved in §8.

In the proof, two cases are distinguished. If H contains an element θ of large multiplicative order, it turns out that one may proceed by a slight modification of the proof of (6.20). (Theorem 4.2 in [KS] for q prime.) If all elements of H are of low order, we use the sum-product type results developed earlier in the paper.

In the case q is a prime, Theorem A and Theorem C may be gotten by combining a theorem by Konyagin and a theorem in the book by Konyagin and Shparlinski [KS], except that the bound on r is slightly weaker. (See Remark 6.2.) Konyagin's theorem uses deep results in algebraic number theory such as Lehmer's Conjecture on the heights of algebraic integers which are not roots of unity. There are several motivations to consider this type of problems. Konyagin's motivation was to prove the Heilbronn Conjecture on the Warring problem and certain partial cases on Stechkin Conjecture on Gauss sums for composite moduli (see [KS], §6). This is also related to the work of Robinson on the distribution of the solution of $x^m \equiv a$ in residue classes (see [R]).

The method we use here is totally different from Konyagin's. The main ingredients of the proof are Freiman's theorem and certain geometric techniques from Bilu's proof of Freiman's Theorem (see [Bi]).

§1.

Notation.

1. For $q \in \mathbb{N}$, $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$.

2. Let $x = (x_1, \cdots, x_d), y = (y_1, \cdots, y_d) \in \mathbb{R}^d$. Then $xy^T = \sum_i x_i y_i$, where y^T is the transpose of the matrix y. If $x \in \mathbb{Z}^d$ and $y \in \mathbb{Z}_q^d$, then the matrix multiplication is done over $\mathbb{Z}_q$.

3. Let $\xi = (\xi_1, \dots, \xi_d) \in \mathbb{Z}_q^d$, $P = \prod_{i=1}^d [A_i, B_i] \subset \mathbb{R}^d$, and $\mathbb{P} = P \cap \mathbb{Z}^d$. A *generalized arithmetic progression* is $\mathcal{P} = \{x\xi^T : x \in \mathbb{P}\}$. When a progression $\mathcal{P}$ is give, P and $\mathbb{P}$ are used with the above meaning. Sometimes we refer to a progression by (ξ, P), or $(\xi, \mathbb{P})$.

4. A progression $\mathcal{P}$ given by $\xi, P = \prod_{i=1}^d [1, J_s]$ is *proper* if $|\mathcal{P}| = |\mathbb{P}|$. We say $\mathcal{P}$ is *proper with respect to* L if

$$\{x\xi^T : x \in \prod_{i=1}^d [1, LJ_s] \cap \mathbb{Z}^d\}$$

is proper.

5. For $A, B \subset Z_q$, and $k \in \mathbb{N}$,

$$\begin{aligned} A + B =& \{a + b : a \in A, b \in B\}, \quad kA = (k-1)A + A, \\ AB =& \{ab : a \in A, b \in B\}, \quad A^k = A^{k-1}A, \\ a \cdot B =& \{a\}B \text{ (mod } q), \quad \text{for } a \in \mathbb{Z}, \\ aB =& \{a\}B, \quad \text{for } a \in \mathbb{Z}_q. \end{aligned}$$

6. For $q \in \mathbb{N}$, $e_q(\theta) = e^{2\pi i\theta}$.

7. $\|x\|$ = the distance from x to the nearest integer.

Lemma 1.0. *Let $y = (y_1, \cdots, y_d) \in \mathbb{Z}^d$ with $\gcd(y_1, \cdots, y_d) = 1$. Then there exists $S \in SL_d(\mathbb{Z})$ with y as an assigned row or column.*

Proof. We do induction on d.

Let $a = \gcd(y_2, \cdots, y_d)$. The assumption implies $\gcd(a, y_1) = 1$. Hence there exist $b, c \in \mathbb{Z}$, $|b| \le |a|, |c| \le |y_1|$ such that

$$y_1 b - ac = 1.$$

Let $y_i = ay'_i$ for $i = 2, \cdots, d$, and let $S' = (s_{i,j}) \in SL_{d-1}(\mathbb{Z})$ be given by induction with $(y'_2, \cdots, y'_d)$ as the first row. Then

$$S = \begin{pmatrix} y_1 & y_2 & \cdots & y_d \\ c & y'_2 b & \cdots & y'_d b \\ 0 & s_{2,1} & \cdots & s_{2,d-1} \\ 0 & & \cdots & \\ 0 & s_{d-1,1} & \cdots & s_{d-1,d-1} \end{pmatrix} \in SL_d(\mathbb{Z}).$$

Remark 1.0.1. It is clear from our proof that $S(i,j)$, the (i,j)-cofactor of S is bounded by $|y'_1 \cdots \widehat{y'_j} \cdots y'_d|$.

To prove the next lemma, we need the following from Bilu's work on Freiman's Theorem. These are Lemma 6.6 and part of the proof of Theorem 1.2 in [Bi]. We include them here for the reader's convenience.

B1. For $x \in \mathbb{R}^m, B \subset \mathbb{R}^m$,

$$\|x\|_B := \inf\{\lambda^{-1} : \lambda x \in B\}.$$

B2. Let $e_1, \cdots, e_m$ be a basis of $\mathbb{R}^m$, $W = \langle e_1, \cdots, e_{m-1}\rangle$, and $\pi : \mathbb{R}^m \to W$ be the projection. Let B be a symmetric, convex body. Then

$$\mathrm{vol}_{m-1}(\pi(B)) \leq \frac{m}{2}\ \|e_m\|_B\ \mathrm{vol}_m(B),$$

where $\mathrm{vol}_m(B)$ is the volume of $B \subset \mathbb{R}^m$.

B3. Let $\lambda_1, \cdots, \lambda_m$ be consecutive minima related to $\|\cdot\|_B$. Then there is a basis $f_1, \cdots, f_m \in \mathbb{Z}$ (called Mahler basis) such that

$$\begin{aligned} &\|f_1\|_B \leq \lambda_1, \\ &\|f_i\|_B \leq \frac{i}{2}\lambda_i, \text{ for } i = 2, \cdots, m. \end{aligned}$$

B4. Let $f_1, \cdots, f_m \in \mathbb{Z}$ be the Mahler basis as given in B3 and $\rho_i = \|f_i\|_B$. Then for $x = \sum_i x_i f_i$,

$$\|x\|_\rho := \max_i \rho_i\ |x_i|.$$

B5. For $x \in \mathbb{R}^m$, we have

$$m^{-1}\|x\|_B \leq \|x\|_\rho \leq \frac{m!^2}{2^{m-1}}\ \|x\|_B.$$

Lemma 1.1. *Let a progression $\mathcal{P}$ be given by $\xi \in \mathbb{Z}_q^d$, and $P = \prod_{i=1}^d [-J_i, J_i]$. Assume there exists $L > 0$ such that the progression $(\xi, \prod_{i=1}^d [1, LJ_i])$ is not proper.*

Then there exists $v \in \mathbb{N}$, and a progression $\mathcal{P}'$ given by $\xi' \in \mathbb{Z}_q^{d-1}$, $P' = \prod_{i=1}^{d-1}[-J_i', J_i']$, satisfying

(i). $v < L \min_i J_i$, and $v|q$

(ii). $\prod_{i=1}^{d-1} J_i' < C_d \frac{L}{v} \prod_{i=1}^d J_i$, where $C_d = d\big[\frac{(d-1)!^2}{2^{d-2}}\ (d-1)\big]^{d-1}$.

(iii). $v \cdot \{x\xi^T : x \in \mathbb{P}\} \subset \{x'\xi'^T : x' \in \mathbb{P}'\}$

Proof. Let $v =\ \gcd(y_1, \cdots, y_d)$. We may clearly assume that $v|q$.

Let $y' = (y_1', \ldots, y_d') = (\frac{1}{v}y_1, \ldots, \frac{1}{v}y_d)$. Hence $\gcd(y_1', \ldots, y_d') = 1$.

Let $e_1, \cdots, e_d$ be the standard basis of $\mathbb{R}^d$, and let $S \in SL_d(\mathbb{Z})$ with $e_d S = y'$ be given by Lemma 1.0.

For $x \in \mathbb{P}$, let $\bar{x} \in \mathbb{Z}^{d-1}$ and $\bar{\xi} \in \mathbb{Z}_q^{d-1}$ be defined by

$$xS^{-1} = (\bar{x}, *), \tag{1.1}$$

and

$$vS\xi^T = (\bar{\xi}, 0)^T. \tag{1.2}$$

Hence

$$vx\xi^T = (xS^{-1})(vS\xi^T) = \bar{x}\bar{\xi}^{\,T}. \tag{1.3}$$

Let

$$B = PS^{-1}. \tag{1.4}$$

Then

$$\mathrm{vol}(B) = 2^d \prod_{i=1}^{d} J_i. \tag{1.5}$$

Denote π the orthonormal projection on $[e_1, \dots, e_{d-1}]$. Let $f_1, \cdots, f_{d-1}$ be a Mahler basis for $\pi(B) \subset [e_1, \cdots, e_{d-1}]$.

For $\bar{x} = \sum_{i=1}^{d-1} x_i' f_i \in \pi(B)$, the second inequality in B5 implies

$$|x_i'| \le \frac{(d-1)!^2}{2^{d-2}} \|\bar{x}\|_{\pi(B)} \rho_i^{-1} \le c_d \rho_i^{-1}, \quad \forall i \tag{1.6}$$

where $c_d = \frac{(d-1)!^2}{2^{d-2}}$.

Let

$$J_i' = c_d \rho_i^{-1}, \tag{1.7}$$

and

$$P' = \prod_{i=1}^{d-1} [-J_i', J_i']. \tag{1.8}$$

Denote

$$x' = (x_1', \cdots, x_{d-1}'),$$

$$F = \begin{pmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_{d-1} \end{pmatrix} \in \mathrm{GL}_{d-1}(\mathbb{Z}),$$

and

$$\xi'^T = F\bar{\xi}^T.$$

Then

$$\bar{x}\bar{\xi}^T = (x'F)\bar{\xi}^T = x'\xi'^T.$$

Hence (1.3) implies

$$vx\xi^T = x'\xi'^T. \tag{1.9}$$

This is property (iii) in our conclusion.

From the choice of S, we have

$$e_d = y' S^{-1} = \frac{y}{v} S^{-1} \in \frac{L}{v} P S^{-1} = \frac{L}{v} B. \tag{1.10}$$

Hence (cf B1)

$$\|e_d\|_B \leq \frac{L}{v}. \tag{1.11}$$

Combining (1.11), B2, and (1.5) we have

$$\mathrm{vol}(\pi(B)) < \frac{dL}{2v} \mathrm{vol}(B) = 2^d \, \frac{dL}{2v} \prod_{i=1}^{d} J_i. \tag{1.12}$$

On the other hand, the first inequality in B5 on $\pi(B)$ gives

$$\{x : |x_i| \leq \rho_i^{-1}\} \subset \{x : \|x\|_{\pi(B)} \leq d - 1\}$$

Hence

$$2^{d-1} \prod_{i=1}^{d-1} \rho_i^{-1} \leq (d-1)^{d-1} \mathrm{vol}(\pi(B)). \tag{1.13}$$

Putting (1.7), (1.13) and (1.12) together , we have

$$\begin{aligned} \prod_{i=1}^{d-1} J_i' = c_d^{d-1} \prod \rho_i^{-1} &\leq c_d^{d-1} 2^{-(d-1)} (d-1)^{d-1} \mathrm{vol}(\pi(B)) \\ &\leq c_d^{d-1} 2^{-(d-1)} (d-1)^{d-1} 2^d \frac{dL}{2v} \prod_{i=1}^{d} J_i. \end{aligned} \tag{1.14}$$

This is (ii) in the Lemma. □

Remark 1.1.1. In Lemma 1.1, we take $P = \prod_{i=1}^d [-J_i, J_i]$ for the convenient notation, because we need a symmetric body to use Bilu's result. Clearly, we can apply the lemma to the progression $\mathcal{P} = (\xi, P)$ with $P = \prod_{i=1}^d [1, J_i]$. Then $\mathcal{P}'$ is given by $(\xi', \prod_{i=1}^{d-1} [1, J_i'])$

§2

Lemma 2.1. *Let $\mathcal{P} = (\xi, P)$ be the progression with $\xi = (\xi_1, \cdots, \xi_d) \in \mathbb{Z}_q^d$, and $P = \prod_{s=1}^d [1, J_s] \subset \mathbb{R}^d$, where the integers*

$$J_1 \geq \cdots \geq J_d > 0.$$

Assume there exists $\varepsilon > 0$ and $a \in \mathbb{Z}_q^*$ satisfying

$$|\mathcal{P} \cap a\mathcal{P}| > \varepsilon |\mathcal{P}|. \tag{2.1}$$

Then for any index $i = 1, \ldots, d$, one of the following alternatives hold.

(i). $J_i < \frac{2}{\varepsilon}$

(ii). $\mathcal{P}$ is not proper with respect to $\frac{9}{\varepsilon}$

(iii). there exists $k_i \in \mathbb{Z}$, and $k' = (k'_1, \cdots, k'_d) \in \mathbb{Z}^d$, such that

$$0 < k_i < \frac{1}{\varepsilon},$$

$$|k'_s| < \frac{8}{\varepsilon^2} \quad \text{for all } i \le s \le d,$$

and

$$ak_i\xi_i = k'\xi^T.$$

Proof. Denote

$$\Omega = \{x \in \mathbb{P} : ax\xi^T \in \mathcal{P} \cap a\mathcal{P}\}. \tag{2.2}$$

Assume (ii) fails. In particular, the arithmetic progression $\mathcal{P}$ in $\mathbb{Z}_q$ is proper. It follows from (2.1) that

$$|\Omega| > \varepsilon|\mathcal{P}| = \varepsilon J_1 \cdots J_d\,. \tag{2.3}$$

Hence there exist $x_1, \cdots, \widehat{x_i}, \cdots, x_d \in \mathbb{Z}$ such that

$$|\{x_i : x = (x_1, \cdots, x_d) \in \Omega\}| > \varepsilon J_i\,.$$

Assume (i) fails as well. Then $\varepsilon J_i \ge 2$ and there is $k_i \in \mathbb{Z}$,

$$0 < k_i < \frac{1}{\varepsilon} \tag{2.4}$$

with $ak_i\xi_i \in \mathcal{P} - \mathcal{P}$. Hence

$$ak_i\xi_i = k'\xi^T \text{ with } k' = (k'_1, \cdots, k'_d) \in \prod_{s=1}^{d} \big[-J_s, J_s\big] \cap \mathbb{Z}^d. \tag{2.5}$$

To show assumption (iii) holds, we need to show $|k'_s| < \frac{8}{\varepsilon^2}$, for $i \le s \le d$. We assume

$$|k'_t| \ge \frac{8}{\varepsilon^2} \text{ for some } t \in \{i, \cdots, d\}. \tag{2.6}$$

Let

$$R = \left[\frac{4}{\varepsilon}\right], \tag{2.7}$$

$$\ell = 2 \min_s \frac{J_s}{|k'_s|}, \tag{2.8}$$

$$S = \{x\xi^T + r\ell k_i\xi_i : x \in \Omega, r = 1, \cdots, R\}, \tag{2.9}$$

and

$$\mathbb{S} = \{x + r\ell k_i e_i : x \in \Omega, r = 1, \cdots, R\}.$$

For $r \in \mathbb{N}$, $1 \leq r \leq R$, by (2.7), (2.8), (2.4) and (2.6), we have

$$r\ell k_i < \frac{4}{\varepsilon}\, 2\, \frac{J_t}{|k_t'|}\, \frac{1}{\varepsilon} \leq J_t \leq J_i\,. \tag{2.10}$$

Hence

$$\mathbb{S} \subset \mathbb{P} + [0, J_i]e_i.$$

The above inclusion and the assumption that $\mathcal{P}$ is proper with respect to $\frac{9}{\varepsilon}$ imply

$$|aS| = |S| = |\mathbb{S}| < 2J_1 \cdots J_d. \tag{2.11}$$

On the other hand, for any $x \in \Omega$, we have by (2.2)

$$ax\xi^T = \bar{x}\xi^T \in \mathcal{P} \tag{2.12}$$

for some $\bar{x} = \bar{x}(x) \in \mathbb{P}$. Let $\bar{\Omega} \subset \mathbb{P}$ be the set of all such $\bar{x}$. Then there is a one-to-one correspondence between Ω and $\bar{\Omega}$. Putting (2.5) and (2.12) together, we have (as any element in $a \cdot S$,) $\big($cf (2.9)$\big)$

$$ax\xi^T + ar\ell k_i\xi_i = (\bar{x} + r\ell k')\xi^T. \tag{2.13}$$

Since for $s \in \{1, \cdots, d\}$,

$$|r\ell k_s'| < \frac{4}{\varepsilon}\, 2\, \frac{J_s}{|k_s'|}|k_s'| \; < \frac{8}{\varepsilon}J_s, \tag{2.14}$$

we have

$$\bar{x} + r\ell k' \in \prod_{s=1}^{d} \Big[-\Big(1 + \frac{8}{\varepsilon}\Big)J_s\,, \Big(1 + \frac{8}{\varepsilon}\Big)J_s\Big]. \tag{2.15}$$

The failure of assumption (ii) and (2.15) imply that $a \cdot S$ is proper.

Let σ be such that $\frac{J_\sigma}{|k_\sigma'|} = \min_s \frac{J_s}{|k_s'|}$. Then $\ell k_\sigma' = 2J_\sigma$ and the sets $\mathbb{P} + \ell k', \mathbb{P} + 2\ell k', \cdots, \mathbb{P} + R\ell k'$ are disjoint. Hence the sets $\Omega + \ell k', \Omega + 2\ell k', \cdots, \Omega + R\ell k'$ are all disjoint. Therefore,

$$|aS| = \Big| \bigsqcup_{r=1}^{R} (\bar{\Omega} + r\ell k')\xi^T \Big| = |\bar{\Omega}|\; R > \varepsilon J_1 \cdots J_d\; R > 3J_1 \cdots J_d,$$

which contradicts (2.11). □

Proof of Theorem B.

We will use the notion $c(K')$ for various (maybe different) constants depending on K'.

Assume $A \subset \mathbb{Z}_p$ such that $K < |A| < \frac{p}{K}$ and $|A + \theta A| < K'|A|$, where $\theta \in \mathbb{Z}_p^*$ satisfies the assumption of Theorem B . By Ruzsa's inequality

$$|A - A| \leq \frac{|A + B|^2}{|B|}$$

for $|A| = |B|$, we have

$$|A - A| < (K')^2 |A|.$$

Identifying $\mathbb{Z}_q \simeq \{0, 1, \dots, q-1\}$, we apply Freiman's theorem to A, first considered as a subset of $\mathbb{Z}$ with doubling constant $\leq 2{K'}^2$ and $A = -A$. it follows from Freiman's theorem that $A \subset \mathcal{P}$, where $\mathcal{P}$ is a generalized d-dimensional progression with $d < c(K')$, $\frac{|\mathcal{P}|}{|A|} < c(K')$. Since $|A + \theta A| < K'|A|$, there is $c \in \mathbb{F}_p$ such that

$$|(c - A) \cap \theta A| \geq \frac{|A|^2}{|A + \theta A|} > \frac{|A|}{K'},$$

and thus

$$|(A - A) \cap \theta(A - A)| > \frac{|A|}{K'}.$$

Let $\hat{\mathcal{P}} = \mathcal{P} - \mathcal{P}$. Then $|\hat{\mathcal{P}}| = c(K')\ |\mathcal{P}|$. We get

$$|\hat{\mathcal{P}} \cap \theta\hat{\mathcal{P}}| > c(K')|\hat{\mathcal{P}}| \tag{2.16}$$

Our aim is to apply Lemma 2.1 with $\epsilon = c(K')$ and $a = \theta$. Some simplifications occur because q being prime. We want to rule out alternatives (i) and (ii). If (i) holds for some $i = 1, \cdots, d$, we may clearly replace $\hat{\mathcal{P}}$ by a progression $\mathcal{P}_1 \subset \hat{\mathcal{P}}$ of dimension $d - 1$, $\frac{c(K')}{2}|\hat{\mathcal{P}}| \leq |\mathcal{P}_1|$ and still satisfying

$$|\mathcal{P}_1 \cap \theta\mathcal{P}_1| > c_1(K')|\mathcal{P}| \geq c_1(K')|\mathcal{P}_1|. \tag{2.17}$$

If (ii) holds, apply Lemma 1.1 to obtain a reduction of d to $d - 1$. Observe that since the integer v in Lemma 1.1 satisfies $v|p$ and

$$v < c(K') \min J_i < c(K')|A| < c(K')\frac{p}{K} < p,$$

necessarily $v = 1$ (assuming K large enough). Thus by Lemma 1.1, $\mathcal{P} \subset \mathcal{P}_1$, where $|\mathcal{P}_1| < c(K')|\mathcal{P}|$ and $\mathcal{P}_1$ of dimension $d - 1$. In both cases (either (i) or (ii)), we obtain $\mathcal{P}_1$ of dimension $d - 1$ such that

$$c(K')|\mathcal{P}| < |\mathcal{P}_1| < c(K')|\mathcal{P}|$$

and (2.17) holds.

Continuing the process, we get a progression $\bar{\mathcal{P}}$ satisfying (2.17) and alternative (iii) of Lemma 2.1, for all $i = 1, \cdots, d_1$, where d_1 is the dimension of $\bar{\mathcal{P}}$ and $\epsilon = \epsilon(K')$. Thus

$$\bar{\mathcal{P}} = \left\{ \sum_{i=1}^{d_1} x_i \xi_i : 0 \leq x \leq J_i, x_i \in \mathbb{Z} \right\}$$

and for all $i = 1, \cdots, d_1$ there are $k_i \in \mathbb{Z}, k'_{i,s} \in \mathbb{Z}(1 \leq s \leq d_1)$ satisfying

$$\theta k_i \xi_i = \sum_{s=1}^{d_1} k'_{i,s} \xi_s \tag{2.18}$$

and

$$0 < k_i < c(K'), \tag{2.19}$$

$$|k'_{i,s}| < c(K')\,\frac{J_s}{J_i}\ , \qquad \text{for all } s = 1, \cdots, d_1. \tag{2.20}$$

For (2.20), we use (2.10) which is valid for all $s = 1, \cdots, d_1$ $\big($rather than (2.6) which is a consequence$\big)$.

Returning to (2.18), it follows that the polynomial

$$p(x) = \det\Big[(xk_i - k'_{i,i})e_{i,i} - \sum_{i \neq j} k'_{i,j} e_{i,j}\Big] \in \mathbb{Z}_p[x] \tag{2.21}$$

has θ as a root, where $e_{i,j}$ is the matrix with $(i,j)-$entry 1 and 0 elsewhere. Clearly $p(x)$ is of degree $d_1 \leq d \leq c(K')$ with non-vanishing x^{d_1}-coefficient by (2.19). By (2.19), (2.20) all coefficients of (2,21) are bounded by

$$\sum_{\pi \in Sym(d_1)} \prod_{i=1}^{d_1} (|k_i|\ \delta_{i,\pi(i)} + |k'_{i,\pi(i)}|) < c(K')^{d_1} \sum_{\pi} \prod_{i=1}^{d_1} \frac{J_{\pi(i)}}{J_i} < c'(K').$$

This contradicts to the assumption on θ for K sufficiently large. $\square$

Remark. Quantitatively speaking, the previous argument will require K' to be at most sublogarithmic in p, since we do rely on Freiman's theorem (cf [C]). Thus we may ask the question how large the quantity

$$\min_{p^\varepsilon < |A| < p^{1-\varepsilon}} \frac{|A + \theta A|}{|A|} \tag{2.22}$$

can be made to some $\theta \in \mathbb{F}_p$. Considering sets A of the form

$$A = \Big\{\sum_{i=1}^{d} x_i \theta^i : 0 \leq x_i \leq M\Big\},$$

it is easily seen that (2.22) is less than $\exp(\sqrt{\log p})$.

§3.

Lemma 3.1. *Let $\mathcal{P} = (\xi, P)$ be a progression with $\xi = (\xi_1, \cdots, \xi_d) \in \mathbb{Z}_q^d$, and $P = \prod_{s=1}^{d} [1, J_s] \subset \mathbb{R}^d$, where the integers*

$$J_1 \geq \cdots \geq J_d > 0.$$

Assume

$$\delta_0 \prod J_i < |\mathcal{P}| < q^{1-3\gamma} \tag{3.1}$$

with $\gamma > 0$ a constant.

Let $\varepsilon > 0, M > 0$ (ε small, M large) satisfy

$$\delta_0^{-1}\left(\frac{1}{\varepsilon}\right)^{3^{d+10}} < M < q^{\gamma/2}. \tag{3.2}$$

Assume

$$|\pi_{q'}(\mathcal{P})| > M \textit{ for all } q'|q, q' > q^\gamma. \tag{3.3}$$

Let $B \subset \mathbb{Z}_q^*$ such that

$$|\pi_{q'}(B)| > M \textit{ for all } q'|q, q' > q^{\gamma/10d} \tag{3.4}$$

denoting

$$\pi_{q'} : \mathbb{Z}_q \to \mathbb{Z}_{q'}$$

the quotient map mod q'.

Then there is $a \in B$ such that

$$|a\mathcal{P} \cap \mathcal{P}| < \varepsilon|\mathcal{P}|. \tag{3.5}$$

Lemma 3.1 will be proved by assuming $|a\mathcal{P} \cap \mathcal{P}| > \varepsilon|\mathcal{P}|$ for all $a \in B$, applying Lemma 2.1 (on a progression which may have fewer generators) and ruling out alternatives (i)-(iii) to get a contradiction.

We will first make a possible reduction of the number d of generators of $\mathcal{P}$ to ensure properness with respect to some constant, using Lemma 1.1.

The reduction.

We take

$$\varepsilon_0 = \varepsilon. \tag{3.6}$$

Assume

$$\delta_0|\mathbb{P}| \le |\mathcal{P}|, \tag{3.7}$$

and

$$\mathcal{P} \text{ is not proper with respect to } \frac{9}{\varepsilon_0}.$$

Lemma 1.1 allows then a reduction of the dimension of the progression $\mathcal{P}$ in the following sense:

There is $v_0 \in \mathbb{N}$, and $\xi^{(1)} \in \mathbb{Z}_q^{d-1}, \mathbb{P}_1 = \prod_{i=1}^{d-1}[1, J_{1,i}] \cap \mathbb{Z}^{d-1}$ satisfying

$$v_0 < \frac{9}{\varepsilon_0}\min J_i, \quad v_0|q,$$

$$|\mathbb{P}_1| < \frac{C}{\varepsilon_0 v_0}\,|\mathbb{P}|, \tag{3.8}$$

$$v_0 \cdot \mathcal{P} \subset \mathcal{P}_1. \tag{3.9}$$

By (3.9), (3.7) and (3.8),

$$|\mathbb{P}_1| \geq |\mathcal{P}_1| \geq \frac{|\mathcal{P}|}{v_0} > \frac{\delta_0}{v_0}\ |\mathbb{P}| > \delta_1\ |\mathbb{P}_1|, \tag{3.10}$$

with

$$\delta_1 = c\varepsilon_0\delta_0. \tag{3.11}$$

Take

$$\varepsilon_1 = \varepsilon\delta_1. \tag{3.12}$$

and repeat the preceding.

If $\mathcal{P}_1$ is not proper with respect to $\frac{9}{\varepsilon_1}$, apply one more time Lemma 1.1 to obtain $v_1 \in \mathbb{N}$, and $\xi^{(2)} \in \mathbb{Z}_q^{d-2}, \mathbb{P}_2 = \prod_{i=1}^{d-2}[1, J_{2,i}]\ \cap \mathbb{Z}^{d-2}$ satisfying

$$v_1 < \frac{9}{\varepsilon_1}\min J_{1,i}, \quad v_1|q,$$

$$|\mathbb{P}_2| < \frac{C}{\varepsilon_1 v_1}\ |\mathbb{P}_1|, \tag{3.13}$$

$$v_1 \cdot \mathcal{P}_1 \subset \mathcal{P}_2. \tag{3.14}$$

By (3.14), (3.10) and (3.13),

$$|\mathbb{P}_2| \geq |\mathcal{P}_2| \geq \frac{|\mathcal{P}_1|}{v_1} > \frac{\delta_1}{v_1}\ |\mathbb{P}_1| > \delta_2\ |\mathbb{P}_2|, \tag{3.15}$$

with

$$\delta_2 = c\varepsilon_1\delta_1. \tag{3.16}$$

Notice that

$$\mathcal{P}_2 \supset v_0 v_1 \mathcal{P}. \tag{3.17}$$

Take

$$\varepsilon_{r-1} = \varepsilon\delta_{r-1}. \tag{3.18}$$

After applying Lemma 1.1 r times, we have $v_{r-1} \in \mathbb{N}$, and $\xi^{(r)} \in \mathbb{Z}_q^{d-r}, \mathbb{P}_r = \prod_{i=1}^{d-r}[1, J_{r,i}]\ \cap \mathbb{Z}^{d-r}$ satisfying

$$v_{r-1} < \frac{9}{\varepsilon_{r-1}}\min J_{r-1,i}, \quad v_{r-1}|q, \tag{3.19}$$

$$|\mathbb{P}_r| < \frac{C}{\varepsilon_{r-1}v_{r-1}}\ |\mathbb{P}_{r-1}|, \tag{3.20}$$

$$v_{r-1} \cdot \mathcal{P}_{r-1} \subset \mathcal{P}_r. \tag{3.21}$$

Same reasoning as before,

$$|\mathbb{P}_r| \geq |\mathcal{P}_r| > \delta_r\ |\mathbb{P}_r|, \tag{3.22}$$

with

$$\delta_r = c\varepsilon_{r-1}\delta_{r-1}. \tag{3.23}$$

Also,

$$v_0 v_1 \cdots v_{r-1}\mathcal{P} \subset \mathcal{P}_r. \tag{3.24}$$

We have the following

1. $c\varepsilon_0\varepsilon_1\cdots\varepsilon_{r-1}\delta_0 = \delta_r$

2. $\delta_r = c\varepsilon\delta_{r-1}^2$

3. $\varepsilon_{r-1} = c(\varepsilon\delta_0)^{2^{r-1}}$

3'. Assume $\delta_0 > \varepsilon$. Then $\varepsilon_{r-1} > c\,\varepsilon^{2^r} > (c\varepsilon)^{2^d}$

3". $\varepsilon_0\varepsilon_1\cdots\varepsilon_{r-1} > c\,\varepsilon\varepsilon^{2^2+2^3+\cdots+2^r} > c\,\varepsilon^{2^{r+1}} \geq c\,\varepsilon^{2^{d+1}}$

4. $|\mathbb{P}\,| > c\,\varepsilon_0\varepsilon_1\cdots\varepsilon_{r-1}v_0v_1\ldots v_{r-1}|\mathbb{P}_r|$

4'. $\frac{C}{\varepsilon_0\varepsilon_1\cdots\varepsilon_{r-1}}\,|\mathbb{P}| > v_0v_1\cdots v_{r-1}$

5. $\left(\frac{C}{\varepsilon}\right)^{2^{d+1}}|\mathbb{P}| > v_0v_1\ldots v_{r-1}$

To see the above (in)equalities hold, we note that our notations (3.11), (3.16), ... , (3.23) imply (1); (3.18) and (3.23) imply (2); (3.18) and (2) imply (3); (3.8), (3.13), ... , (3.20) imply (4); (4') and (3") imply (5).

Assume $a \in \mathbb{Z}_q$ and

$$|\mathcal{P} \cap a\mathcal{P}| > \varepsilon|\mathcal{P}|.$$

By (3.24), (3.7), (4), (1), and (3.18),

$$\begin{aligned}
|\mathcal{P}_r \cap a\mathcal{P}_r| &\geq |(v_0v_1\ldots v_{r-1}\mathcal{P}) \cap a(v_0\ldots v_{r-1}\mathcal{P})| \\
&\geq (v_0v_1\ldots v_{r-1})^{-1}|\mathcal{P}\cap a\mathcal{P}| \\
&> (v_0\ldots v_{r-1})^{-1}\varepsilon\delta_0\;|\mathbb{P}| \\
&> c\varepsilon\varepsilon_0\ldots\varepsilon_{r-1}\delta_0\;|\mathbb{P}_r| \\
&= c\varepsilon\delta_r|\;\mathbb{P}_r| \\
&= c\varepsilon_r|\mathcal{P}_r|,
\end{aligned} \tag{3.25}$$

where

$$\varepsilon_r = \varepsilon\delta_r. \tag{3.26}$$

We need the following little fact from algebra to prove Lemma 3.2.

Fact A. Let $A \subset \mathbb{Z}_q$, $k \in \mathbb{Z}$, and $q' = \frac{q}{\gcd(k,q)}$. Then $|\pi_{q'}(A)| = |k \cdot A|$.

Proof of Lemma 3.1. We assume after r reductions $\mathcal{P}_r$ is proper with respect to $\frac{9}{\varepsilon_r}$. (If $\mathcal{P}$ is already proper with respect to $\frac{9}{\varepsilon}$, then $r = 0$ and $\mathcal{P}_0 = \mathcal{P}$.) We apply Lemma 2.1 to $\mathcal{P}' = \mathcal{P}_r$, replacing ε by ε_r. By our construction, alternative (ii) in Lemma 2.1 is ruled out.

Assume $J'_i := J_{r,i}$ ordered decreasingly $J'_1 \geq J'_2 \geq \cdots \geq J'_{d'}$.

Let $\xi'_i = \xi_i^{(r)} \in \{1, 2, \dots, q-1\} \simeq \mathbb{Z}_q \backslash \{0\}$ and define

$$\begin{aligned} q_1 = &\ \gcd(\xi'_1,\ q) \\ q_2 = &\ \gcd(\xi'_1,\ \xi'_2,\ q) \\ &\ \vdots \\ q_{d'} = &\ \gcd(\xi'_1,\ \cdots, \xi'_{d'},\ q). \end{aligned}$$

Claim. $q_{d'} \leq q^{1-\gamma}$.

Proof of Claim. Assume

$$q_{d'} > q^{1-\gamma}.$$

Let $w = \frac{q}{q_{d'}} < q^\gamma$. Then (5), (3.1) and (3.2) imply

$$v_0 v_1 \cdots v_{r-1} w \leq \left(\frac{C}{\varepsilon}\right)^{2^{d+1}} |\mathbb{P}|\, q^\gamma < \left(\frac{C}{\varepsilon}\right)^{2^{d+1}} \frac{1}{\delta_0} q^{1-2\gamma} < q^{1-\gamma}. \tag{3.27}$$

Also,

$$w\xi'_1 = \cdots = w\xi'_{d'} = 0 \pmod{q},$$

hence, from (3.24)

$$v_0 v_1 \cdots v_{r-1} w \mathcal{P} = 0 \pmod{q}.$$

By Fact A,

$$\pi_{q'}(\mathcal{P}) = 0 \tag{3.28}$$

with $\big($by (3.27)$\big)$

$$q' = \frac{q}{\gcd(q, v_0 \dots v_{r-1} w)} > q^\gamma.$$

This contradicts (3.3). □

Therefore, there is $i \in \{1, \dots, d'\}$ such that

$$\frac{q_{i-1}}{q_i} > q^{\frac{\gamma}{d}}. \tag{3.29}$$

$$\frac{q}{q_1}, \frac{q_1}{q_2}, \dots, \frac{q_{i-2}}{q_{i-1}} \leq q^{\frac{\gamma}{d}} \tag{3.30}$$

Apply Lemma 2.1 considering this particular index i. Alternative (ii) is ruled out by construction.

Claim. Alternative (i) fails.

Proof. If (i) holds, we get

$$\left(\frac{C}{\varepsilon}\right)^{2^{d+1}} > \frac{2}{\varepsilon_r} > J'_i \geq J'_{i+1} \geq \cdots \geq J'_{d'}. \tag{3.31}$$

Let

$$v = v_0 \dots v_{r-1} \frac{q}{q_{i-1}}.$$

By (3.30), (5), (3.1) and (3.2),

$$v \le v_0 \cdots v_{r-1} q^\gamma < \left(\frac{C}{\varepsilon}\right)^{2^{d+1}} |\mathbb{P}|\, q^\gamma < c q^{1-3\gamma+\frac{\gamma}{2}} q^\gamma < q^{1-\gamma}$$

Hence, from the definition of q_{i-1}

$$\begin{aligned} v\mathcal{P} = v_0 v_1 \cdots v_{r-1} \frac{q}{q_{i-1}} \mathcal{P} \subset \frac{q}{q_{i-1}} \mathcal{P}_r \\ = \frac{q}{q_{i-1}} \Big\{ \sum_{s \ge i} x_s \xi'_s : x_s \le J'_s \Big\}. \end{aligned} \tag{3.32}$$

(3.31), (3.32) imply

$$|v\mathcal{P}| \le J'_i J'_{i+1} \ldots J'_{d'} < \left(\frac{C}{\varepsilon}\right)^{d2^{d+1}} < M.$$

Hence Fact A implies

$$|\pi_{q'}(\mathcal{P})| = |v\mathcal{P}| < M$$

with $q' = \frac{q}{\gcd(q,v)} > q^\gamma$ again contradicting (3.3). □

So alternative (iii) holds and there are k_i, $(k'_s)_{1\le s\le d'} \in \mathbb{Z}$ such that

$$0 < k_i < \frac{1}{\varepsilon_r} \tag{3.33}$$

$$|k'_s| < \frac{8}{\varepsilon_r^2} \quad \text{for } i \le s \le d' \tag{3.34}$$

$$a k_i \xi'_i = \sum_{s=1}^{d'} k'_s \xi'_s \pmod q. \tag{3.35}$$

Since $q_{i-1} = \gcd(\xi'_1, \ldots, \xi'_{i-1}, q)$, (3.35) implies

$$a k_i \xi'_i = \sum_{s \ge i} k'_s \xi'_s \pmod{q_{i-1}}. \tag{3.36}$$

By (3.33), (3.34), (3') and (3.2), the coefficients $(k_i, k'_i, \ldots, k'_{d'})$ in (3.36) ranges in a set of at most $\frac{1}{\varepsilon_r}\big(\frac{8}{\varepsilon_r^2}\big)^{d'} < \big(\frac{C}{\varepsilon}\big)^{(2d+1)2^{d+1}} < M^{1/2}$ elements.

Recalling (3.29) and (3.4)

$$\left|\pi_{\frac{q_{i-1}}{q_i}}(B)\right| > M \tag{3.37}$$

and we may consider elements $\bar{B} \subset B, |\bar{B}| > M$, such that $\pi_{\frac{q_{i-1}}{q_i}}\big|_{\bar{B}}$ is one-to-one. Assuming $|\mathcal{P} \cap a\mathcal{P}| > \varepsilon|\mathcal{P}|$ for all $a \in \bar{B}$, we have for all $a \in \bar{B}$, cf. (3.25)

$$|\mathcal{P}' \cap a\mathcal{P}'| > c\varepsilon_r |\mathcal{P}'| \tag{3.38}$$

and the preceding applies, providing in particular a representation (3.36).

In view of the bound on the number of coefficients in (3.36), there is $B' \subset \bar{B}$, $|B'| > M^{1/2}$ such that for all $a \in B'$, (3.36) holds with the same coefficients $k_i, k'_s (s \geq i)$. Taking any a_1, a_2 in B'

$$
\begin{aligned}
&(a_1 - a_2) k_i \xi'_i = 0 \pmod{q_{i-1}} \\
&(a_1 - a_2) k_i = 0 \quad \Big(\text{mod } \frac{q_{i-1}}{q_i}\Big)
\end{aligned}
\tag{3.39}
$$

implying

$$1 = \big|\pi_{\frac{q_{i-1}}{q_i}}(k_i B')\big| \geq \frac{1}{|k_i|} \big|\pi_{\frac{q_{i-1}}{q_i}}(B')\big| = \frac{|B'|}{|k_i|} > \varepsilon_r M^{1/2}$$

a contradiction.

This proves Lemma 3.1.

Following the same arguments as in Lemma 3.1, we also obtain:

Lemma 3.1′. *Under the assumptions of Lemma 3.1, there exit elements* $a_1, \dots, a_R$ *in* B, *with* $R \sim M^{\frac{1}{10}}$ *such that*

$$|a_s \mathcal{P} \cap a_{s'} \mathcal{P}| < \varepsilon |\mathcal{P}| \text{ for } s \neq s'. \tag{3.40}$$

Proof. Let $\bar{B} \subset B$ be the set constructed in the proof of Lemma 3.1.

Assume $a_1, \dots, a_r \in \bar{B}$ obtained satisfying (3.40) and suppose

$$\max_{1 \leq s \leq r} |a_s \mathcal{P} \cap a \mathcal{P}| > \varepsilon |\mathcal{P}| \text{ for all } a \in \bar{B}.$$

Hence, there is some $s = 1, \dots, r$ and $B_1 \subset \bar{B}$ with

$$|B_1| > \frac{1}{r} |\bar{B}| > \frac{M}{R} > M^{9/10}$$

and such that

$$|\mathcal{P} \cap \frac{a}{a_s} \mathcal{P}| > \varepsilon |\mathcal{P}| \text{ for all } a \in B_1. \tag{3.41}$$

It follows that all elements $\frac{a}{a_s}, a \in B_1$, have a representation (3.36). Passing again to a subset B'_1, $|B'_1| > M^{9/10 - 1/2} = M^{2/5}$, we may ensure the same coefficients $k_i, (k'_s)_{s \geq i}$ and get a contradiction as before.

§4.

Let $A \subset \mathbb{Z}_q$ such that

$$|A + A| < K|A| \tag{4.1}$$

and

$$1 \ll |A| < q^{1 - 4\gamma}. \tag{4.2}$$

Identifying $\mathbb{Z}_q \simeq \{0, 1, \dots, q-1\}$, we apply Freiman's theorem to A, first considered as a subset of $\mathbb{Z}$ (with doubling constant $\leq 2K$).

From [C], we obtain

$$d \leq 2K$$

and a progression $\mathcal{P}$ given by $\xi = (\xi_1, \dots, \xi_d) \in \mathbb{Z}^d; P = \prod_i^d [0, J_i]$, with $J_1 \geq J_2 \geq \cdots \geq J_d$ in $\mathbb{N}$, such that

$$A \subset \mathcal{P} = \left\{x\xi^T : x \in \mathbb{P}\right\} \tag{4.3}$$

and

$$|\mathbb{P}| < C^{K^3}|A|. \tag{4.4}$$

Applying $\pi_q : \mathbb{Z} \to \mathbb{Z}_q$, $\mathcal{P}$ becomes a progression in $\mathbb{Z}_q$ containing $A \subset \mathbb{Z}_q$. Assuming

$$C^{K^3} < q^{\gamma/2}, \tag{4.5}$$

by (4.5), (4.4), (4.2) and (4.4), we have

$$q^{1-3\gamma} > C^{K^3} q^{1-4\gamma} > |\mathbb{P}| \geq |\mathcal{P}| \geq |A| > C^{-K^3}|\mathbb{P}|. \tag{4.6}$$

Thus assumption 3.1 in Lemma 3.1 holds with $\delta_0 = C^{-K^3}$.

Let ε, M satisfy (3.2), i.e.

$$C^{K^3}\left(\frac{1}{\varepsilon}\right)^{10^{K+5}} < M < q^{\gamma/2} \tag{4.7}$$

and moreover

$$\varepsilon < C^{-K^3}.$$

Assume $B \subset \mathbb{Z}_q^*$ such that $|\pi_{q'}(B)| \leq |\pi_{q'}(A)|$, (e.g. B ,contained in a translate of A) for all $q'|q$ and $q' > q^\gamma$. Furthermore, assume B satisfies

$$|\pi_{q'}(B)| > M, \quad \text{if } q'|q \text{ and } q' > q^{\frac{\gamma}{20K}}. \tag{4.8}$$

Since by assumption also

$$|\pi_{q'}(\mathcal{P})| \geq |\pi_{q'}(A)| \geq |\pi_{q'}(B)| > M, \quad \text{if } q'|q \text{ and } q' > q^\gamma,$$

conditions (3.3), (3.4) of Lemma 3.1 are satisfied.

Apply Lemma 3.1'.

Let $a_1, \dots, a_R \in B$ satisfy (3.5). (We take $R < M^{\frac{1}{10}}$.) Write

$$\begin{aligned}\left|\bigcup_{r\leq R} a_r A\right| &\geq R|A| - \sum_{r\neq s} |a_r A \cap a_s A| \\ &\geq R|A| - \sum_{r\neq s} |a_r\mathcal{P} \cap a_s\mathcal{P}| \\ &> R|A| - R^2\varepsilon C^{K^3}|A|. \end{aligned} \tag{4.9}$$

Taking $R = \frac{1}{2\,\varepsilon}\, C^{-K^3}$, (4.9) implies

$$|AB| \geq \left|\bigcup_{r\leq R} a_r A\right| > \frac{R}{2}|A| > \frac{1}{\varepsilon} C^{-K^3}|A|. \tag{4.10}$$

Assume

$$M > C^{50^{K+10}} \tag{4.11}$$

$\big($which implies the first inequality of (4.7), hence it also implies (4.5) $\big)$ and take

$$\frac{1}{\varepsilon} = M^{10^{-K-6}}.$$

From (4.10) and (4.11)

$$|AB| > M^{10^{-K-7}}|A|. \tag{4.12}$$

Replacing 4γ by γ and summarizing, we proved the following:

Lemma 4.1. *Let $A \subset \mathbb{Z}_q$ satisfy*

$$|A| < q^{1-\gamma} \tag{4.13}$$

$$|A+A| < K|A|. \tag{4.14}$$

Let M satisfy

$$C^{50^{K+10}} < M < q^{\gamma/8}. \tag{4.15}$$

Let $B \subset \mathbb{Z}_q^*$ such that

$$|\pi_{q'}(B)| \le |\pi_{q'}(A)|, \quad \text{if } q'|q \textit{ and } q' > q^\gamma,$$

also

$$|\pi_{q'}(B)| > M, \quad \textit{if } q'|q \textit{ and } q' > q^{\gamma/80K}. \tag{4.16}$$

Then

$$|AB| > M^{10^{-K-7}}|A|. \tag{4.17}$$

§**5.**

Proposition 1.

Let $\kappa > 0$ be a small and M a large constant.

Let $H \subset \mathbb{Z}_q^*$ (q large) satisfy

$$|\pi_{q'}(H)| > M \textit{ whenever } q'|q, q' > q^\kappa. \tag{5.1}$$

Then there is $k, r \in \mathbb{N}$ such that

$$k < q^{\kappa'} \tag{5.2}$$

$$r < \log_2 q^{\kappa'} \tag{5.3}$$

$$|kH^r| > q^{1-\kappa'} \tag{5.4}$$

where

$$\kappa' = \kappa'(\kappa, M) \to 0 \textit{ for } \kappa \to 0, M \to \infty \textit{ (independent of } q).$$

Proof.

We describe the construction. Given any

$$\kappa_1 > \kappa^{1/2} \tag{5.5}$$

and denote

$$K = \min\left\{ (\log\log M)^{1/2}, \frac{\kappa_1}{100\kappa} \right\}. \tag{5.6}$$

Let $A_0 = H$ and $A_\alpha = k_\alpha H^{r_\alpha}$ be the set obtained at stage α. Assume $|A_\alpha| < q^{1-\kappa_1}$.

We distinguish the following cases.

(i) $|A_\alpha + A_\alpha| > K|A_\alpha|$

Take then $k_{\alpha+1} = 2k_\alpha$ and $r_{\alpha+1} = r_\alpha$

(ii) $|A_\alpha + A_\alpha| \leq K|A_\alpha|$

Apply Lemma 4.1 with $A = A_\alpha, B = H, \gamma = \kappa_1$. In (5.1) we can assume $M < q^{\frac{\gamma}{10}}$. Conditions (4.15) and (4.16) clearly hold, because of (5.6). Hence

$$|A_\alpha H| > M^{10^{-K-7}} |A_\alpha| > K|A_\alpha|.$$

The second inequality is again by (5.6). Hence

$$|k_\alpha H^{r_\alpha + 1}| > K|A_\alpha|.$$

In this case we take $k_{\alpha+1} = k_\alpha$ and $r_{\alpha+1} = r_\alpha + 1$.

Therefore

$$|A_{\alpha+1}| > K|A_\alpha|, \tag{5.7}$$

with

$$\begin{aligned} k_{\alpha+1} &\leq 2k_\alpha \\ r_{\alpha+1} &\leq r_{\alpha+1}. \end{aligned} \tag{5.8}$$

To reach size $q^{1-\kappa_1}$, the number of steps is at most $\frac{\log q}{\log K}$, because after s steps, by (5.7)

$$q \geq |A_{\alpha+1}| > K^s |H| \geq K^s.$$

By (5.8), we have in (5.2)

$$k \leq 2^{\frac{\log q}{\log K}} = q^{\kappa_2}.$$

Hence

$$\kappa_2 = \frac{\log 2}{\log K} \sim \frac{1}{\min\{\log\log\log M, \log\frac{1}{\kappa}\}},$$

by (5.5) and (5.6).

We conclude the proof of Proposition 1 by taking $\kappa = \max\{\kappa_1, \kappa_2\}$.

§6.

We need the following to prove Theorem A.

Let $\nu, \nu' : \mathbb{Z}_q \to \mathbb{R}$ be functions. We recall

F1. $\hat{\nu}(\xi) = \sum_{x \in \mathbb{Z}_q} \nu(x) e_q(-x\xi)$. If ν is a probability measure, i.e. $0 \le \nu(x) \le 1$, then $|\hat{\nu}(\xi)| \le 1$.

F2. $\nu * \nu'(x) = \sum_{y \in \mathbb{Z}_q} \nu(x-y)\nu'(y)$.

F3. $\operatorname{supp}(\nu * \nu') \subset \text{ Supp } \nu + \text{ Supp } \nu'$.

F4. $\nu(x) = \frac{1}{q} \sum_{\xi \in \mathbb{Z}_q} \hat{\nu}(\xi) e_q(x\xi)$.

F5. $\widehat{\nu * \nu'}(\xi) = \hat{\nu}(\xi)\hat{\nu}'(\xi)$.

Let $0 \le x \le \frac{5\pi}{6}$. Then

T1. $\sin x > \frac{x}{2\pi}$. Therefore, $|e_q(1) - 1| > \frac{1}{q}$.

T2. $\cos x < 1 - \frac{x^2}{4\pi}$. Therefore, $|e_q(1) + 1| < 2 - \frac{\pi}{2}\,\frac{1}{q^2}$.

T3. $|e_q(x) - e_q(y)| = |2 \sin \frac{2\pi}{2q}(x-y)|$.

Proof of Theorem A. Let $\kappa > 0$, M be constants as in Proposition 1. Let $q \in \mathbb{N}$ be odd. Let $H \subset \mathbb{Z}_q^*$ satisfy the following conditions:

$$|\pi_p(H)| \ge 2 \text{ for all primes } p|q \tag{6.1}$$

$$|\pi_{q'}(H)| > M \text{ for all } q'|q, q' > q^\kappa \tag{6.2}$$

We want to show that

$$k_1 H^r = \mathbb{Z}_q$$

for some $k_1, r \in \mathbb{N}$ satisfying

$$r < \log q^{\kappa'} \tag{6.3}$$

$$k_1 < q^{5\kappa'}. \tag{6.4}$$

By (6.2), Proposition 1 applies. Let k, r satisfy (5.2)-(5.4).

Denote

$$\mathcal{D} = \big\{q' \in \mathbb{N} : q' \ne 1 \text{ and } q'|q\big\},$$

hence

$$|\mathcal{D}| < q^{\frac{1}{\log\log q}}. \tag{6.5}$$

For $q' \in \mathcal{D}$, we have

$$|\pi_{q'}(kH^r)| \ge \frac{|kH^r|}{q/q'} > \frac{q^{1-\kappa'}}{q/q'} = q' q^{-\kappa'} \tag{6.6}$$

while by (6.1), also

$$|\pi_{q'}(kH^r)| \ge |\pi_{q'}(H)| \ge 2. \tag{6.7}$$

Take a subset $\Omega_{q'} \subset kH^r$ such that $\pi_{q'}|\Omega_{q'}$ is one-to-one and

$$|\Omega_{q'}| \geq \max\{2, q'q^{-\kappa'}\}. \tag{6.8}$$

Define the probability measures

$$\mu_{q'} = \frac{1}{|\Omega_{q'}|} \sum_{x \in \Omega_{q'}} \delta_x, \tag{6.9}$$

δ_x being the indicator function, and their convolution

$$\begin{aligned} \mu(x) &= \underset{q' \in \mathcal{D}}{*} \ \mu_{q'}(x) \\ &= \sum_{y_1, \cdots, y_{|\mathcal{D}|-1}} \mu_{q_{|\mathcal{D}|}}(x - y_1 - \cdots - y_{|\mathcal{D}|-1}) \cdots \mu_{q_2}(y_2)\mu_{q_1}(y_1). \end{aligned} \tag{6.10}$$

Then by F3,

$$\operatorname{supp} \mu \subset \sum_{q' \in \mathcal{D}} \operatorname{supp} \mu_{q'} \subset \sum_{q' \in \mathcal{D}} \Omega_{q'} \subset |\mathcal{D}|kH^r. \tag{6.11}$$

We estimate the Fourier coefficients

$$\hat{\mu}\left(\frac{a}{q}\right) = \sum_{x \in \mathbb{Z}_q} e_q(-ax)\mu(x)$$

for $0 < a < q$.

Let $\frac{a}{q} = \frac{a'}{q'}$ where $q'|q$ and $(a', q') = 1$. From (6.10) and F5

$$\left|\hat{\mu}(\frac{a}{q})\right| \leq \left|\widehat{\mu_{q'}}\left(\frac{a'}{q'}\right)\right| = \frac{1}{|\Omega_{q'}|}\left|\sum_{x \in \Omega_{q'}} e_{q'}(a'x)\right|. \tag{6.12}$$

Claim 1. $\left|\hat{\mu}\left(\frac{a}{q}\right)\right| < 1 - \frac{1}{16}q^{-2\kappa'}$.

Proof of Claim 1.

Assume $\left|\hat{\mu}\left(\frac{a}{q}\right)\right| > 1 - \tau$. We want to find a lower bound on τ. Squaring both sides of (6.12), we obtain

$$\sum_{x, y \in \Omega_{q'}} \cos \frac{2\pi a'}{q'}(x - y) > (1 - \tau)^2 |\Omega_{q'}|^2. \tag{6.13}$$

Choose an element $x_0 \in \Omega_{q'}$ such that

$$\sum_{y \in \Omega_{q'}} \cos \frac{2\pi a'}{q'}(x_0 - y) > (1 - \tau)^2 |\Omega_{q'}|. \tag{6.14}$$

By T3, we write

$$|e_{q'}(a'x_0) - e_{q'}(a'y)|^2 = \left[2 \sin \frac{2\pi a'}{q'}\frac{(x_0 - y)}{2}\right]^2 = 2 - 2\cos\frac{2\pi a'}{q'}(x_0 - y).$$

Together with (6.14) give

$$\sum_{y\in\Omega_{q'}} |e_{q'}(a'x_0)-e_{q'}(a'y)|^2 \le 2|\Omega_{q'}|-2(1-\tau)^2|\Omega_{q'}| < 2\tau|\Omega_{q'}|. \tag{6.15}$$

From (6.15),

$$\left|\left\{y : |e_{q'}(a'x_0)-e_{q'}(a'y)| > 2\sqrt{\tau}\right\}\right| \le \frac{1}{2}|\Omega_{q'}|.$$

So there is a subset $\Omega' \subset \Omega_{q'}$, $|\Omega'| > \frac{1}{2}|\Omega_{q'}|$ such that for all $y \in \Omega'$

$$|e_{q'}(a'x_0)-e_{q'}(a'y)| < 2\sqrt{\tau},$$

hence T1 implies

$$\left\|\frac{a'x_0}{q}-\frac{a'y}{q}\right\| < 2\sqrt{\tau}. \tag{6.16}$$

Therefore

$$|\pi_{q'}(\Omega')| = |\pi_{q'}(a'\Omega')| \le 2\sqrt{\tau}q'+1.$$

Since $\pi_{q'}|\Omega'$ is one-to-one, also

$$\frac{1}{2}q'q^{-\kappa'} < |\Omega'| \le 2\sqrt{\tau}q'+1 \tag{6.17}$$

by (6.8). This gives a lower bound

$$\tau > \frac{1}{16}q^{-2\kappa'}. \qquad \square$$

Take

$$\ell = [q^{3\kappa'}] \tag{6.18}$$

Claim 2. Let $\mu^{(\ell)}$ be the ℓ-fold convolution of μ. Then $\operatorname{supp}\mu^{(\ell)} = \mathbb{Z}_q$.

Proof of Claim 2. For $x \in \mathbb{Z}_q$, write

$$\mu^{(\ell)}(x) = \frac{1}{q}+\frac{1}{q}\sum_{a=1}^{q}\widehat{\mu^{(\ell)}}\left(\frac{a}{q}\right)e_q(ax). \tag{6.19}$$

By Claim 2 and (6.18), the second term in (6.19) is at most

$$\begin{aligned}\max_{1\le a<q}\left|\widehat{\mu^{(\ell)}}\left(\frac{a}{q}\right)\right| &= \max_{1\le a<q}\left|\hat{\mu}\left(\frac{a}{q}\right)\right|^{\ell}\\ &< \left(1-\frac{1}{16q^{2\kappa'}}\right)^{q^{3\kappa'}} < e^{-q^{\kappa'}} < \frac{1}{q}.\end{aligned}$$

Hence $\mu^{(\ell)}(x) > 0$. $\square$

Hence, putting together Claim 2, (6.11), (6.18), (6.5) and (5.2), we have

$$\mathbb{Z}_q = \ell\operatorname{supp}\mu = \ell\,|\mathcal{D}|\,kH^r = k_1H^r$$

with $k_1 \leq q^{3\kappa'} q^{1/\log\log q} q^{\kappa'} < q^{5\kappa'}$. □

Remark 6.1. It is much simpler to prove the following weaker bound

$$\left|\widehat{\mu_{q'}}\left(\frac{a'}{q'}\right)\right| < 1 - \frac{\pi}{2}\frac{1}{(q')^3}.$$

Proof.

Since $|\Omega_{q'}| \geq 2$, there are elements $x_1, x_2 \in \Omega_{q'}$ with $\pi_{q'}(x_1) \neq \pi_{q'}(x_2)$.

Since $(a', q') = 1$, also $\pi_{q'}(a'x_1) \neq \pi_{q'}(a'x_2)$. Therefore, by T2,

$$|e_{q'}(a'x_1) + e_{q'}(a'x_2)| \leq |e_{q'}(1) + 1| < 2 - \frac{\pi}{2}\frac{1}{(q')^2}$$

Write

$$\begin{aligned}\left|\sum_{x\in\Omega_{q'}} e_{q'}(a'x)\right| &\leq (|\Omega_{q'}| - 2) + |e_{q'}(a'x_1) + e_{q'}(a'x_2)| \\ &< |\Omega_{q'}| - \frac{\pi}{2}\frac{1}{(q')^2}.\end{aligned}$$

Therefore

$$\left|\widehat{\mu_{q'}}\left(\frac{a'}{q'}\right)\right| < 1 - \frac{\pi}{2}\frac{1}{(q')^3}.$$ □

Remark 6.2. For q prime, Theorem A has a simpler proof, which gives a slightly weaker bound on r. In this case, $\mathbb{Z}_q^*$ is a cyclic group. The condition on $H \subset \mathbb{Z}_q^*$ is simply $|H| > M$ with M large. It follows that H contains an element $\theta \in H$ of multiplicative order $t > \sqrt{M}$. Assuming (as we may) that $1 \in H$, it follows that

$$\{1, \theta, \cdots, \theta^r\} \subset H^r.$$

We distinguish 2 cases.

Case 1. $t \geq \frac{\log q}{(\log\log q)^{1/2}}$.

Take $r_0 \gtrsim \log q (\log\log q)^4$.

Using the inequality

$$\max_{(a,q)=1}\left|\sum_{x=1}^{r_0} e_q(a\theta^x)\right| < r_0\left(1 - \frac{c}{(\log q)^2}\right)$$

due to Konyagin (see [KS], p. 26), simple application of the circle method implies

$$kH^{r_0} = \mathbb{Z}_q \text{ with } k < C(\log q)^3.$$

Case 2. $t < \frac{\log q}{(\log\log q)^{1/2}}$.

Denote $\varphi(t) = |\mathbb{Z}_t^*|$. Use then Theorem 4.2 from [KS]

$$\max_{(a,q)=1} \left| \sum_{x-1}^{t} e_q(a\theta^x) \right| < t - c(\rho) q^{-2/\rho} \text{ for } 2 \leq \rho \leq \varphi(t). \tag{6.20}$$

Hence

$$kH^t = \mathbb{Z}_q \text{ with } k < \frac{1}{c(\rho)} (\log q)^2 q^{2/\rho}.$$

Since $\varphi(t) \to \infty$ for $M \to \infty$, we may achieve $k < c(\kappa') q^{\kappa'}$ with $\kappa'(M) \to 0$ as $M \to \infty$.

§**7.**

Corollary 3.

1. Let $H \subset \mathbb{Z}_q^*$ satisfy the assumption (5.1) of Proposition 1 and κ' be as in Proposition 1. Let $q'|q$, $q' > q^{\kappa'}$ and $(a, q') = 1$.

Let $r \in \mathbb{N}, r > \kappa' \log q$.

Then

$$\max_{x,y \in H^r} \left\| \frac{a}{q'}(x-y) \right\| > q^{-2\kappa'}. \tag{7.1}$$

2. Let $H < \mathbb{Z}_q^*$ be a multiplicative subgroup satisfying assumption (5.1) of Proposition 1.

Let $q'|q, q' > q^{\kappa'}$ and $(a, q') = 1$.

Then

$$\max_{x,y \in H} \left\| \frac{a}{q'}(x-y) \right\| > q^{-2\kappa'}. \tag{7.2}$$

Proof.

By (5.4)

$$|\pi_{q'}(kaH^r)| = |\pi_{q'}(kH^r)| > \frac{q^{1-\kappa'}}{q/q'} = q' q^{-\kappa'} > 1. \tag{7.3}$$

Hence there are elements $z, w \in kH^r$ s.t.

$$\left\| \frac{a}{q'}(z-w) \right\| \geq q^{-\kappa'}. \tag{7.4}$$

Writing $z = x_1 + \cdots + x_k, w = y_1 + \cdots + y_k$ with $x_i, y_i \in H^r$, it follows that

$$\max_{x,y \in H^r} \left\| \frac{a}{q'}(x-y) \right\| \geq \frac{1}{k} q^{-\kappa'} > q^{-2\kappa'}.$$

by (5.2).

Corollary 4.

1. Let $H \subset \mathbb{Z}_q^*$ satisfy conditions (6.1), (6.2) and κ' be as in Theorem A.

Let $1 \leq a < q$. Then for $r > \kappa' \log q$

$$\max_{x,y \in H^r} \left\| \frac{a}{q}(x-y) \right\| \gtrsim q^{-5\kappa'}. \tag{7.5}$$

2. If moreover $H < \mathbb{Z}_q^*$ is a group, we get

$$\max_{x,y \in H} \left\| \frac{a}{q}(x-y) \right\| \gtrsim q^{-5\kappa'} \tag{7.6}$$

Proof.

Write $\frac{a}{q} = \frac{a'}{q'}, (a', q') = 1$. Since $\pi_{q'}(k_1 H^r) = \mathbb{Z}_{q'}$,

$$\max_{z,w \in k_1 H^r} \left\| \frac{a'}{q'}(z-w) \right\| \geq \frac{1}{2} \tag{7.7}$$

hence

$$\max_{x,y \in H^r} \left\| \frac{a'}{q'}(x-y) \right\| \gtrsim \frac{1}{k_1} > q^{-5\kappa'}. \tag{7.8}$$

§8. The case of subgroups

The main result of this section is the following (for q prime this issue was considered in [P])

Theorem 5. *Let $H < \mathbb{Z}_q^*, |H| > M > 1$. Then*

$$\min_{a \in \mathbb{Z}_q^*} \max_{x,y \in H} \left\| \frac{a}{q}(x-y) \right\| > q^{-\delta} \tag{8.1}$$

where $\delta = \delta(M) \to 0$ for $M \to \infty$ (independently of q).

We first treat the case when H contains an element of large multiplicative order. The next result has a simple proof obtained by a straightforward modification of an argument in [KS] (see §4) for prime modulus.

Lemma 8.1.

Let $\theta \in \mathbb{Z}_q^*$ be of order t (large). Then

$$\min_{(a,q)=1} \max_{j,k} \left\| \frac{a}{q}(\theta^j - \theta^k) \right\| > c(r) q^{-\frac{1}{r-1}} \tag{8.2}$$

for $1 < r < \varphi(t)$.

Proof. For $j = 1, \dots, t$, let $b_j \in \mathbb{Z}$ such that

$$b_j = a\theta^j \pmod q \tag{8.3}$$

and extend periodically with period t for $j \in \mathbb{Z}$.

Claim. Let $c \in \mathbb{Z}$ and $2 \le r < \varphi(t)$. Then $\max_j |b_j - c| > c(r)q^{\frac{r-2}{r-1}}$.

proof of Claim. Let

$$B = \max_{1\le j\le t} |b_j - c|. \tag{8.4}$$

Denote $b = (b_1, \cdots, b_r)$, and $\mathbf{1} = (1, \cdots, 1)$. We consider the lattice

$$\begin{aligned} L =& \big\{\ell = (\ell_1, \dots, \ell_r) \in \mathbb{Z}^r : b\,\ell^T = 0,\ \ \mathbf{1}\,\ell^T = 0\big\} \\ =& \big\{\ell = (\ell_1, \dots, \ell_r) \in \mathbb{Z}^r : (b - c\mathbf{1})\,\ell^T = 0,\ \ \mathbf{1}\,\ell^T = 0\big\} \end{aligned} \tag{8.5}$$

We considering all expressions $\sum (b_i - c)\ell_i$, with $\sum \ell_i = 0$ and $|b_i - c| \le B$. From the pigeonhole principle and (8.4), there is $(\ell_1, \dots, \ell_r) \in L \backslash \{0\}$ such that

$$\max_{1\le j\le r} |\ell_j| < c(r)B^{\frac{1}{r-2}}. \tag{8.6}$$

For this vector $\ell = (\ell_1, \dots, \ell_r)$,

$$b_1\ell_1 + \cdots + b_r\ell_r = 0.$$

Hence, multiplying with θ^j,

$$b_{j+1}\ell_1 + \cdots + b_{j+r}\ell_r = 0 \pmod q$$

for all j. Since also $\ell_1 + \cdots + \ell_r = 0$

$$(b_{j+1} - c)\ell_1 + \cdots + (b_{j+r} - c)\ell_r = 0 \pmod q. \tag{8.7}$$

The left side is bounded by

$$rBc(r)B^{\frac{1}{r-2}} < c(r)B^{\frac{r-1}{r-2}}$$

by (8.4), (8.6).

Assume $c(r)B^{\frac{r-1}{r-2}} < q$, hence

$$B < c(r)q^{\frac{r-2}{r-1}}. \tag{8.8}$$

It follows then from (8.7) that

$$\begin{aligned} &(b_{j+1} - c)\ell_1 + \cdots + (b_{j+r} - c)\ell_r = 0 \\ &b_{j+1}\ell_1 + \cdots + b_{j+r}\ell_r = 0 \end{aligned} \tag{8.9}$$

for all j.

Hence (b_j) is a periodic linearly recurrent sequence of order at most r and smallest period t.

Let $\psi(x)$ be the minimal polynomial of (b_j). (See [KS].) Then form (8.9)

$$\psi(x)|(\ell_1+\ell_2x+\cdots+\ell_rx^{r-1})$$

implying $\deg\psi\le r-1$.

Obviously $\psi(x)|(x^t-1)$. Assume

$$\psi(x)|\prod_{1\le r<t}(1-x^\tau).$$

Since $\psi(\theta)=0 \pmod q$, it would follow that $\theta^\tau\equiv 1 \ (\bmod q)$ for some $\tau<t$, contradicting $\operatorname{ord}_q(\theta)=t$.

Therefore one of the roots of ψ is a primitive t^{th}-root and ψ is divisible by the t-cyclotomic polynomial.

Hence

$$\phi(t)\le\deg\psi<r$$

a contradiction.

Hence (8.8) fails. □

Suppose (8.2) fails. Letting $c=a\theta^k\in\mathbb{Z}_q=\{0,1,\dots,q-1\}$,

$$\max_j\left\|\frac{a\theta^j-c}{q}\right\|<c(r)q^{-\frac{1}{r-1}}.$$

Hence

$$\max_j \operatorname{dist}(a\theta^j-c,q\mathbb{Z})<c(r)q^{\frac{r-2}{r-1}}. \tag{8.10}$$

From (8.10), we may for each $j=1,\dots,t$ take $b_j\in\mathbb{Z}$ such that

$$b_j=a\theta^j \ (\bmod q), \ \text{ and } \ |b_j-c|<c(r)q^{\frac{r-2}{r-1}}.$$

This contradicts the Claim and proves the lemma.

Proof of Theorem 5

Let $H<\mathbb{Z}_q^*, |H|>M$.

Fix $\kappa>0$ (small) and $1\ll M_1<M^{\frac{\kappa}{2}}$.

By Lemma 8.2, we may assume

$$\operatorname{ord}_q(x)<M_1 \ \text{ for all } \ x\in H. \tag{8.11}$$

If $|\pi_{q_1}(H)|>M_1$ for all $q_1|q$, with $q_1>q^\kappa$, then (8.1) holds for $\delta=\delta(\kappa,M_1)\to 0$ for $\kappa\to 0, M_1\to\infty$ $\big($by Corollary 3(2)$\big)$.

Assume thus there exists $q_1|q$, with $q_1 > q^\kappa$ and $|\pi_{q_1}(H)| \leq M_1$. Hence

$$H_1 = H \cap \pi_{q_1}^{-1}(1) < \mathbb{Z}_q^*$$

satisfies

$$|H_1| > \frac{M}{M_1}.$$

Consider the set

$$\mathcal{H}_1 = \{x \in \mathbb{Z}_{\frac{q}{q_1}} : 1 + q_1 x \in H_1\} = \frac{H_1 - 1}{q_1}.$$

Assume there is $q_2\Big|\frac{q}{q_1}$, with $q_2 > q^\kappa$ and $|\pi_{q_2}(\mathcal{H}_1)| < M_1$. Hence $|\pi_{q_1 q_2}(H_1)| < M_1$ and defining $H_2 = H_1 \cap \pi_{q_1 q_2}^{-1}(1)$, we have

$$|H_2| > \frac{|H_1|}{M_1} > \frac{M}{M_1^2}.$$

Considering the set

$$\mathcal{H}_2 = \Big\{x \in \mathbb{Z}_{\frac{q}{q_1 q_2}} : 1 + q_1 q_2 x \in H_2\Big\} = \frac{H_2 - 1}{q_1 q_2},$$

we repeat the process.

At some stage $s \leq \frac{1}{\kappa}$, the process has to stop.

Thus

$$H_s = H \cap \pi_{q_1 \cdots q_s}^{-1}(1), \tag{8.12}$$

$$\mathcal{H}_s = \{x \in \mathbb{Z}_{\frac{q}{q_1 \cdots q_s}} : 1 + q_1 \cdots q_s x \in H_s\} = \frac{H_s - 1}{q_1 \cdots q_s}, \tag{8.13}$$

$$|H_s| = |\mathcal{H}_s| > \frac{M}{M_1^{1/\kappa}} > M^{1/2}, \tag{8.14}$$

and

$$|\pi_{q'}(\mathcal{H}_s)| > M_1 \text{ for all } q'|\frac{q}{q_1 \cdots q_s}, \text{ with } q' > q^\kappa. \tag{8.15}$$

Define

$$Q_1 = q_1 \dots q_s \text{ and } Q_2 = \frac{q}{Q_1}.$$

Case 1. $Q_2 < q^{\sqrt{\kappa}}$.

Since $|H_s| \geq 2$, there are elements $x \neq y$ in $\mathcal{H}_s \subset \mathbb{Z}_{Q_2}$. Hence

$$ax \neq ay \pmod{Q_2}$$

and

$$\left\|\frac{a(x-y)}{Q_2}\right\| > \frac{1}{Q_2} > q^{-\sqrt{\kappa}}.$$

Let $\bar{x} = 1 + Q_1 x, \bar{y} = 1 + Q_1 y \in H_s < H$. Writing

$$\frac{a(x-y)}{Q_2} = \frac{a(Q_1 x - Q_1 y)}{q} = \frac{a(\bar{x} - \bar{y})}{q},$$

we obtain

$$\left\| \frac{a(\bar{x}-\bar{y})}{q} \right\| > q^{-\sqrt{\kappa}}$$

and hence (8.1) holds.

Case 2. $Q_2 \geq q^{\sqrt{\kappa}}$.

First, note that if there is no ambiguity, we use the

notation $(A, B) = \gcd(A, B)$.

Claim 1. $(Q_1, Q_2) \leq q^\kappa$.

Proof of Claim 1. Observe that $(1 + Q_1 x)(1 + Q_1 y) = 1 + Q_1(x + y) \pmod{Q_1^2}$. Hence

$$(1 + Q_1 x)(1 + Q_1 y) = 1 + Q_1(x + y) \pmod{Q_1(Q_1, Q_2)}.$$

Consider $\pi_{Q_1(Q_1,Q_2)}(H_s) < \mathbb{Z}^*_{Q_1(Q_1,Q_2)}$. It follows from the preceding that

$$\pi_{Q_1(Q_1,Q_2)}(H_s) = 1 + Q_1 S$$

where S is an additive subgroup of $\mathbb{Z}_{(Q_1,Q_2)}$. Hence

$$S < \langle \mathbb{Z}_{(Q_1,Q_2)}, + \rangle \text{ and } \pi_{Q_1(Q_1,Q_2)}(H_s) < \mathbb{Z}^*_{Q_1 \cdot (Q_1,Q_2)}$$

are cyclic. By assumption (8.11), all elements of $H_s < H$ are of order $\leq M_1$, implying

$$|\pi_{Q_1(Q_1,Q_2)}(H_s)| \leq M_1.$$

Therefore

$$|\pi_{(Q_1,Q_2)}(\mathcal{H}_s)| \leq M_1. \tag{8.16}$$

By construction of $\mathcal{H}_s$, (8.16) implies

$$(Q_1, Q_2) \leq q^\kappa. \qquad \square \tag{8.17}$$

Let $Q_1' = \frac{Q_1}{(Q_1,Q_2)}, Q_2' = \frac{Q_2}{(Q_1,Q_2)}$. Hence $(Q_1', Q_2') = 1$ and $Q_2' > q^{\sqrt{\kappa}-\kappa}$ by case assumption and (8.17).

We want to apply Corollary 3(2) to $\pi_{Q_2'}(H_s) < \mathbb{Z}^*_{Q_2'}$ with $4\sqrt{\kappa}$ and M_1.

Let $q' | Q_2'$ with $q' > (Q_2')^{4\sqrt{\kappa}} > q^{2\kappa}$, and let $q'' = \frac{q'}{(q', Q_1, Q_2)}$. Thus by (8.17),

$$q'' > q^\kappa.$$

Claim 2. $|\pi_{q'}(H_s)| > M_1$.

Proof of Claim 2. It follows from (8.15) that $|\pi_{q''}(\mathcal{H}_s)| > M_1$.

Let $x_1, \dots, x_n \in \mathcal{H}_s, n > M_1$ such that

$$x_i - x_j \not\equiv 0 \pmod{q''}.$$

Since $(q'', Q_1') = (q', Q_1') = 1$ and

$$\left(q'', \frac{(Q_1, Q_2)}{(q', Q_1, Q_2)}\right) = 1,$$

we also have

$$\frac{Q_1}{(q', Q_1, Q_2)}(x_i - x_j) \not\equiv 0 \pmod{q''}.$$

Hence

$$Q_1(x_i - x_j) \not\equiv 0 \pmod{q'}.$$

Since $1 + Q_1 x_i \in H_s$, it follows that

$$|\pi_{q'}(H_s)| > M_1. \qquad \square$$

Apply Corollary 3 (2) to the group $\pi_{Q_2'}(H_s) < \mathbb{Z}^*_{Q_2'}$. Claim 2 implies that

$$\left|\pi_{q'}\left(\pi_{Q_2'}(H_s)\right)\right| = |\pi_{q'}(H_s)| > M_1$$

for all $q' | Q_2'$ with $q' > (Q_2')^{4\sqrt{\kappa}}$. Hence for any $a', (a', Q_2') = 1$, there are thus $\bar{x}, \bar{y} \in H_s$ such that

$$\left\| \frac{a'}{Q_2'}(\bar{x} - \bar{y}) \right\| > (Q_2')^{-\kappa'} > q^{-\kappa'} \tag{8.18}$$

where $\kappa' = \kappa'(4\sqrt{\kappa}, M_1) \to 0$ for $\kappa \to 0, M_1 \to \infty$.

Write $\bar{x} = 1 + Q_1 x, \bar{y} = 1 + Q_1 y$ with $x, y \in \mathcal{H}_s$. From (8.18)

$$\left\| \frac{a' Q_1}{Q_2'}(x - y) \right\| > q^{-\kappa'}. \tag{8.19}$$

Recalling that $(Q_1', Q_2') = 1$, we may choose a' satisfying

$$a' Q_1' \equiv a \pmod{Q_2'}.$$

Therefore (8.19) gives

$$\left\| \frac{a(Q_1, Q_2)^2}{Q_2}(x - y) \right\| > q^{-\kappa'}.$$

Hence, by Claim 1,

$$\left\| \frac{a}{Q_2}(x - y) \right\| > \frac{q^{-\kappa'}}{(Q_1, Q_2)^2} > q^{-\kappa' - 2\kappa},$$

and

$$\left\| \frac{a}{q}(\bar{x} - \bar{y}) \right\| = \left\| \frac{a}{q}(Q_1 x - Q_1 y) \right\| > q^{-\kappa' - 2\kappa}.$$

Therefore

$$\max_{x,y\in H}\left\|\frac{a}{q}(x-y)\right\| > q^{-\kappa'-2\kappa},$$

where κ, κ' may be made arbitrary small by taking M large enough. This proves Theorem 5.

Theorem C is an extension of Theorem 4.2 in [KS] for composite modules and is an immediate consequence of Theorem 5.

Proof of Theorem C. For $a \in \mathbb{Z}_q^*$, let $\{x_1, \cdots, x_{|H|}\} = aH$, and let $x_1 = ax, x_2 = ay$ be given in Theorem 5 such that

$$\left\| \frac{x_1 - x_2}{q} \right\| > q^{-\kappa}$$

where $\kappa = \kappa(M)$.

Let

$$S = \left|\sum_{i=1}^{|H|} e_q(x_i)\right|.$$

Then

$$\begin{aligned}
S^2 =&|H| + 2\sum_{i\neq j}\cos\left(\frac{2\pi(x_i - x_j)}{q}\right)\\
\leq&|H| + 2\left[\binom{|H|}{2} - 1\right] + 2\cos\left(\frac{2\pi(x_1 - x_2)}{q}\right)\\
\leq&|H|^2 - 2 + 2\left(1 - \pi\left\|\frac{x_1 - x_2}{q}\right\|^2\right)\\
<&|H|^2 - 2\pi q^{-2\kappa}.
\end{aligned}$$

References

[BIW]. B. Barak, R. Impagliazzo, A. Wigderson, *Extracting randomness using few independent sources*, Proc of the 45th FOCS (2004), 384-393.

[BKSSW]. B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, A. Wigderson, *Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers, and Extractors*, STOC (to appear).

[B]. J. Bourgain, *Mordell's exponential sum estimate revisited, (preprint 2004, submitted to JAMS).*

[BC]. J. Bourgain, M. Chang, *Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_q^*$, where q is composite with few prime factors*, submitted to GAFA.

[BGK]. J. Bourgain, A. Glibichuk, S. Konyagin, *Estimate for the number of sums and products and for exponential sums in fields of prime order*, submitted to J. London MS.

[BKT]. J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields and their applications*, GAFA 14 (2004), n1, 27–57.

[C]. M. Chang, *A polynomial bound in Freiman's theorem*, Duke Math. J. 113 (2002), no 3, 399–419.

[Bi]. Y. Bilu, *'Structure of sets with small sumset'*, in 'Structure theory of et additions', Asterisque 258, SMF (1999), 77–108.

[KL]. S. Konyagin, I. Laba, *Distance sets of well-distributed planar sets for polygonal norms*, Israel J. Math (to appear).

[KS]. S. Konyagin, I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Tracts in Math., 136 (1999).

[N]. M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer (1996)..*

[P]. C. Powell, *Bounds for multiplicative cosets over fields of prime order*, Math. Comp. 66 (1997), no 218, 807–822.

[R]. R. Robinson, *Number having m small mth roots mod p*, Mathematics of Computation Vol 61, no 203, (1993), 393-413.

Mathematics Department, University of California, Riverside CA 92507

E-mail address: mcc@math.ucr.edu