Mei-Chu Chang

On sum-product representations in $\mathbb{Z}_q$

Received April 15, 2004 and in revised form July 14, 2005

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 (non-trivial 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 $r \sim \log q/\log |A|$ with similar restriction on $k$, something not covered by earlier work of Konyagin and Shparlinski. 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 $\min_{a \in \mathbb{Z}_q^*} \max_{x \in H} \|ax/q\|$ 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 $p | q$, where $\pi_p$ denotes the quotient map $p$. Let $kH$ be the $k$-fold sum set, and $H'$ 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 $\mathbb{Z}_q = kH'$; 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 $\kappa \to 0$ and $M \to \infty$, with the following property. Let $q \in \mathbb{N}$ be odd and $H \subset \mathbb{Z}_q^*$ such that

\begin{align*}
|\pi_p(H)| > 1 & \quad \text{for all prime divisors } p \text{ of } q, \quad (0.1) \\
|\pi_{q'}(H)| > M & \quad \text{for all divisors } q' \text{ of } q \text{ with } q' > q^\kappa. \quad (0.2)
\end{align*}

Then

\[ \mathbb{Z}_q = kH' \with k < q^\kappa' \text{ and } r < \kappa' \log q. \quad (0.3) \]

(This will be proved in §6.)

M. C. Chang: Mathematics Department, University of California, Riverside, CA 92507, USA; e-mail: mcc@math.ucr.edu
The main motivation for this work comes from a recent line of research 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 $|A| > p^\varepsilon$ for some fixed (and arbitrary) $\varepsilon > 0$, then $kA^k = \mathbb{F}_p^*$ provided $k > k(\varepsilon)$ and also

$$\max_{(a,p) = 1} \left| \sum_{x_1, \ldots, x_k \in A} e_p(ax_1 \cdots x_k) \right| < p^{-\delta(\varepsilon)}|A|^k$$

for some $\delta(\varepsilon) > 0$. This and related estimates had very significant applications 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 $\varepsilon = \varepsilon(p)$ be small. The boundary of the assumption here is $\varepsilon > 1/\log \log p$, 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

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

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

It became apparent 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 (0.3) holds, but bring new techniques into play through related and more modest aims.

Our bound in (0.3) is essentially optimal. Consider a composite $q = p_1p_2$, where $p_1$ and $p_2$ are prime. Let $p_1 \approx \frac{1}{2}q^{1/2}$. Define

$$H = \{1, \theta\} + p_1[0, 1, \ldots, p_2 - 1]$$

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

$$kH' = kH \subset \{x + y\theta : x, y \in \mathbb{N}, x + y = k\} + p_1[0, 1, \ldots, p_2 - 1],$$

(0.3) requires $k \geq p_1 \sim \frac{1}{4}q^{1/2}$, 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 $\theta$ 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 $K < |A| < p/K$, we have

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

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

Returning to exponential sums with prime modulus (see (6.20)), 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

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

(0.4)

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

This theorem will be proved in §8.

In the proof, two cases are distinguished. If $H$ contains an element $\theta$ of large multi-
plicative 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, Theorems A and C may be obtained 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 re-
sults 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 Waring
problem and certain partial cases of the 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 solutions 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 $x = (x_1, \ldots, x_d), y = (y_1, \ldots, y_d) \in \mathbb{R}^d$. Then $xy^T = \sum_i x_iy_i$, 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 $\mathbb{Z}_q$. 

1
3. Let $\xi = (\xi_1, \ldots, \xi_d) \in \mathbb{Z}_q^d$. $P = \prod_{i=1}^{d} [A_i, B_i] \subset \mathbb{R}^d$, 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 given, $P$ and $\mathbb{P}$ are used with the above meaning. Sometimes we refer to a progression by $(\xi, P)$, or $(\xi, \mathbb{P})$.

4. A progression $\mathcal{P}$ given by $\xi, P = \prod_{i=1}^{d} [A_i, B_i] \subset \mathbb{R}^d$, 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 given, $P$ and $\mathbb{P}$ are used with the above meaning. Sometimes we refer to a progression by $(\xi, P)$, or $(\xi, \mathbb{P})$.

5. For $A, B \subset \mathbb{Z}_q$, and $k \in \mathbb{N}$,
   
   \[ A + B = \{a + b : a \in A, b \in B\}, \quad kA = (k - 1)A + A, \]
   
   \[ AB = \{ab : a \in A, b \in B\}, \quad A^k = A^{k-1}A, \]
   
   \[ a \cdot B = \{a\}B \pmod{q} \quad \text{for } a \in \mathbb{Z}, \]
   
   \[ aB = \{a\}B \quad \text{for } a \in \mathbb{Z}_q. \]

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

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

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

**Proof.** We do induction on $d$. Let $a = \text{gcd}(y_2, \ldots, y_d)$. The assumption implies that $\text{gcd}(a, y_1) = 1$. Hence there exist $b, c \in \mathbb{Z}$ with $|b| \leq |a|$ and $|c| \leq |y_1|$ such that

\[ y_1b - ac = 1. \]

Let $y_i = ay_i'$ for $i = 2, \ldots, d$, and let $S' = (s_{i,j}) \in \text{SL}_{d-1}(\mathbb{Z})$ be given by induction with $(y_2', \ldots, y_d')$ as the first row. Then

\[
S = \begin{pmatrix}
  y_1 & y_2 & \cdots & y_d \\
  c & y_2' & \cdots & y_d' \\
  0 & s_2,1 & \cdots & s_2,d-1 \\
  0 & \cdots & \cdots & \cdots \\
  0 & s_{d-1,1} & \cdots & s_{d-1,d-1}
\end{pmatrix} \in \text{SL}_d(\mathbb{Z}).
\]

**Remark 1.0.1.** It is clear from our proof that $S(i, j)$, the $(i, j)$-cofactor of $S$, is bounded by $|y_1' \cdots y_j' \cdots y_d'|$.

To prove the next lemma, we need Lemma 6.6 and part of the proof of Theorem 1.2 from Bilu’s work [Bi] on Freiman’s theorem. 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 $e_1, \ldots, e_m$ be a basis of $\mathbb{R}^m$, $W = \langle e_1, \ldots, e_{m-1} \rangle$, and $\pi : \mathbb{R}^m \to W$ be the projection. Let $B$ be a symmetric, convex body. Then
\[
\text{vol}_{m-1}(\pi(B)) \leq \frac{m}{2} \|e_m\|_B \text{vol}(B),
\]
where $\text{vol}(B)$ is the volume of $B \subset \mathbb{R}^m$.

B3. Let $\lambda_1, \ldots, \lambda_m$ be consecutive minima related to $\| \cdot \|_B$. Then there exists $L > 0$ such that the progression $f_1, \ldots, f_m \in \mathbb{Z}$ (called a Mahler basis) such that
\[
\|f_1\|_B \leq \lambda_1, \quad \|f_i\|_B \leq \frac{i}{2} \lambda_i \quad \text{for } i = 2, \ldots, m.
\]

B4. Let $f_1, \ldots, f_m \in \mathbb{Z}$ be the Mahler basis as given in B3 and $\rho_i = \|f_i\|_B$. Then for $x = \sum x_i f_i$,
\[
\|x\|_\rho := \max_i \rho_i |x_i|.
\]

B5. For $x \in \mathbb{R}^m$, we have
\[
m^{-1} \|x\|_B \leq \|x\|_\rho \leq \frac{m^2}{2m-1} \|x\|_B.
\]

Lemma 1.1. Let a progression $\mathcal{P}$ be given by $\xi \in \mathbb{Z}_q^d$ and $P = \prod_{i=1}^d \mathbb{Z}[-J_i, \bar{J}_i]$. Assume there exists $L > 0$ such that the progression $(\xi, \prod_{i=1}^d \mathbb{Z}[1, L\bar{J}_i])$ is not proper. Then there exist $\nu \in \mathbb{N}$ and a progression $\mathcal{P}'$ given by $\xi' \in \mathbb{Z}_q^{d-1}$, $P' = \prod_{i=1}^{d-1} \mathbb{Z}[-J_i', \bar{J}_i']$ satisfying
(i) $\nu < L \min J_i$ and $\nu \mid q$,
(ii) $\prod_{i=1}^{d-1} J_i' < C_d L^{1 \nu} \prod_{i=1}^d J_i$, where $C_d = d \left( \frac{(d-1)^2}{2d-2} (d-1) \right)^{d-1}$,
(iii) $\nu \cdot \{x \xi^T : x \in \mathbb{P}\} \subset \{x' \xi'^T : x' \in \mathbb{P}'\}$.

Proof. Let $\nu = \gcd(y_1, \ldots, y_d)$. We may clearly assume that $\nu \mid q$. Let $y' = (y_1', \ldots, y_d') = (y_1/\nu, \ldots, y_d/\nu)$. Hence $\gcd(y_1', \ldots, y_d') = 1$. Let $e_1, \ldots, e_d$ be the standard basis of $\mathbb{R}^d$, and let $S' \in \text{SL}_d(\mathbb{Z})$ with $e_d S = y'$ be given by Lemma 1.0. For $x \in \mathbb{P}$, let $\bar{x} \in \mathbb{Z}_q^{d-1}$ and $\bar{\xi} \in \mathbb{Z}_q^{d-1}$ be defined by
\[
xS^{-1} = (\bar{x}, \ast), \quad (1.1)
\]
\[
vS\bar{\xi}^T = (\bar{\xi}, 0)^T. \quad (1.2)
\]
Hence
\[
vS\bar{\xi}^T = (xS^{T^{-1}})(vS\bar{\xi}^T) = \bar{x}\bar{\xi}^T. \quad (1.3)
\]
Let
\[
B = PS^{-1}. \quad (1.4)
\]
Then
\[ \text{vol}(B) = 2^d \prod_{i=1}^{d} J_i. \]  
(1.5)
Denote by \( \pi \) the orthonormal projection on \([e_1, \ldots, e_{d-1}]\). Let \( f_1, \ldots, f_{d-1} \) be a Mahler basis for \( \pi(B) \subset [e_1, \ldots, e_{d-1}] \). For \( \bar{x} = \sum_{i=1}^{d-1} x'_i f_i \in \pi(B) \), the second inequality in B5 implies
\[ |x'_i| \leq \frac{\rho_i^{-1}}{d} \langle \bar{x}, \rho_i \rangle \leq c_d \rho_i^{-1}, \quad \forall i, \]  
(1.6)
where \( c_d = (d-1)^2/2^{d-2} \). Let
\[ J'_i = c_d \rho_i^{-1}, \quad P' = \prod_{i=1}^{d-1} [-J'_i, J'_i]. \]  
(1.7)
(1.8)
Define
\[ x' = (x'_1, \ldots, x'_{d-1}), \quad F = \begin{pmatrix} f_1 & \cdots & f_{d-1} \end{pmatrix} \in \text{GL}_{d-1}(\mathbb{Z}), \quad \xi'^T = F \xi^T. \]
Then
\[ \bar{x} \xi^T = (x' F) \xi'^T = x' \xi'^T. \]
(1.9)
This is property (iii) in our conclusion.

From the choice of \( S \), we have
\[ e_d = y' S^{-1} = \frac{y}{v} S^{-1} \in \frac{L}{v} P S^{-1} = \frac{L}{v} B. \]  
(1.10)
Hence (cf. B1)
\[ \|e_d\|_B \leq L/v. \]  
(1.11)
Combining (1.11), B2, and (1.5) we have
\[ \text{vol}(\pi(B)) < \frac{dL}{2v} \text{vol}(B) = 2^d \frac{dL}{2v} \prod_{i=1}^{d} J_i. \]  
(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
\[ 2^{d-1} \prod_{i=1}^{d-1} \rho_i^{-1} \leq (d-1)^{d-1} \text{vol}(\pi(B)). \]  
(1.13)
Putting (1.7), (1.13) and (1.12) together, we have
\[
\prod_{i=1}^{d-1} J'_i = c_d^{-1} \prod J_i^{-1} \leq c_d^{-1} 2^{-(d-1)(d-1)} |\text{vol}(\pi(B))| \leq c_d^{-1} 2^{d-1} dL \prod_{i=1}^{d} J_i.
\] (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 \(P = (\xi, P)\) with \(P = \prod_{i=1}^{d} [1, J_i]\). Then \(P'\) is given by \((\xi', \prod_{i=1}^{d} [1, J'_i])\).

## 2

**Lemma 2.1.** Let \(\mathcal{P} = (\xi, P)\) be the progression with \(\xi = (\xi_1, \ldots, \xi_d) \in \mathbb{Z}_q^d\) and \(P = \prod_{i=1}^{d} [1, J_i] \subset \mathbb{R}^d\), where the integers \(J_i\) satisfy \(J_1 \geq \cdots \geq J_d > 0\). Assume there exist \(\varepsilon > 0\) 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) \(J_i < 2/\varepsilon\),

(ii) \(\mathcal{P}\) is not proper with respect to \(9/\varepsilon\),

(iii) there exist \(k_i \in \mathbb{Z}\) and \(k' = (k'_1, \ldots, k'_d) \in \mathbb{Z}^d\) such that
\[
0 < k_i < 1/\varepsilon, \quad |k'_s| < 8/\varepsilon^2 \quad \text{for all } s \leq d, \quad ak_i \xi_i = k'\xi^T.
\]

**Proof.** Define \(\Omega = \{x \in \mathcal{P} : ax\xi^T \in \mathcal{P} \cap a\mathcal{P}\}\). \(\tag{2.2}\)

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 \(x_1, \ldots, \hat{x}_i, \ldots, x_d \in \mathbb{Z}\) such that
\[
|[x_i : x = (x_1, \ldots, x_d) \in \Omega]| > \varepsilon J_i.
\]

Assume (i) fails as well. Then \(\varepsilon J_i \geq 2\) and there is \(k_i \in \mathbb{Z}\) with
\[
0 < k_i < 1/\varepsilon \tag{2.4}
\]
and \(ak_i\xi_i \in \mathcal{P} - \mathcal{P}\). Hence
\[
 ak_i\xi_i = k'\xi^T \quad \text{with} \quad k' = (k'_1, \ldots, k'_d) \in \prod_{s=1}^{d} [-J_s, J_s] \cap \mathbb{Z}^d. \tag{2.5}
\]

To show assumption (iii) holds, we need to show \(|k'_i| < 8/\varepsilon^2\) for \(i \leq s \leq d\). We assume
\[
 |k'_t| \geq 8/\varepsilon^2 \quad \text{for some } t \in \{i, \ldots, d\}. \tag{2.6}
\]

Let
\[
 R = [4/\varepsilon], \tag{2.7}
\]
\[
 \ell = 2 \min_s J_s / |k'_s| = 2 J_i / k'_i, \tag{2.8}
\]
\[
 S = \{x\xi^T + r\ell k_i \xi_i : x \in \Omega, r = 1, \ldots, R\}, \tag{2.9}
\]
\[
 \bar{S} = \{x + r\ell k_i e_i : x \in \Omega, r = 1, \ldots, R\}. \tag{2.10}
\]

For \(r \in \mathbb{N}, 1 \leq r \leq R\), by (2.7), (2.8), (2.4) and (2.6), we have
\[
 r\ell k_i < \frac{4}{\varepsilon} \frac{J_i}{|k'_i|} \leq J_i \leq J_i. \tag{2.11}
\]

Hence \(\bar{S} \subset \mathcal{P} + [0, J_i] e_i\). This inclusion and the assumption that \(\mathcal{P}\) is proper with respect to \(9/\varepsilon\) imply
\[
 |aS| = |S| \leq 2J_1 \cdots J_d. \tag{2.12}
\]

On the other hand, for any \(x \in \Omega\), by (2.2) we have
\[
 ax\xi^T = \tilde{x}\xi^T \in \mathcal{P} \tag{2.13}
\]

for some \(\tilde{x} = \tilde{x}(x) \in \mathcal{P}\). Let \(\tilde{\Omega} \subset \mathcal{P}\) be the set of all such \(\tilde{x}\). Then there is a one-to-one correspondence between \(\Omega\) and \(\tilde{\Omega}\). Putting (2.5) and (2.12) together, we have (as any element in \(a \cdot S\) (cf. (2.9))
\[
 ax\xi^T + ar\ell k_i \xi_i = (\tilde{x} + r\ell k')\xi^T. \tag{2.14}
\]

Since for \(s \in \{1, \ldots, d\},
\[
 |r\ell k'_s| < \frac{4}{\varepsilon} \frac{J_s}{|k'_s|} < \frac{8}{\varepsilon} J_s, \tag{2.15}
\]
we have
\[
 \tilde{x} + r\ell k' \in \prod_{s=1}^{d} \left[-\left(1 + \frac{8}{\varepsilon}\right) J_s, \left(1 + \frac{8}{\varepsilon}\right) J_s\right].
\]

The failure of assumption (ii) and (2.15) imply that \(a \cdot S\) is proper.
Let $\sigma$ be such that $J_\sigma / |k_\sigma'| = \min_i J_i / |k_i'|$. Then $\ell k_\sigma' = 2J_\sigma$ and the sets $\mathbb{P} + \ell k'$, $\mathbb{P} + 2\ell k'$, $\ldots$, $\mathbb{P} + R\ell k'$ are disjoint. Hence the sets $\Omega + \ell k'$, $\Omega + 2\ell k'$, $\ldots$, $\Omega + R\ell k'$ are all disjoint. Therefore,$$
abla |S| = \left| \bigcup_{r=1}^R (\Omega + r\ell k')^T \right| = |\Omega| R > \varepsilon J_1 \cdots J_d R > 3J_1 \cdots J_d,$$which contradicts (2.11).

**Proof of Theorem B.** We will use the notation $c(K')$ for various (maybe different) constants depending on $K'$.

Assume $A \subset \mathbb{Z}_p$ is such that $K < |A| < p/K$ and $|A + \theta A| < K'|A|$, where $\theta \in \mathbb{Z}_p^*$ satisfies the assumption of Theorem B. By Ruzsa’s inequality$$(|A - A| \leq |A + B|^2 / |B|),$$for $|A| = |B|$ we have$$(|A - A| < (K')^2 |A|).$$Identifying $\mathbb{Z}_q \cong \{0, 1, \ldots, q - 1\}$, we apply Freiman’s theorem to $A$, first considered as a subset of $\mathbb{Z}$ with doubling constant $\leq 2K'^2$ and $A = -A$. It follows from Freiman’s theorem that $A \subset \mathcal{P}$, where $\mathcal{P}$ is a generalized $d$-dimensional progression with $d < c(K')$ and $|\mathcal{P}|/|A| < c(K')$. 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 $\hat{P} = \mathcal{P} - \mathcal{P}$. Then $|\hat{P}| = c(K')|\mathcal{P}|$. We get$$|\hat{P} \cap \theta \hat{P}| > c(K')|\hat{P}|.$$Our aim is to apply Lemma 2.1 with $\epsilon = c(K')$ and $a = \theta$. Some simplifications occur because $q$ is prime. We want to rule out alternatives (i) and (ii). If (i) holds for some $i = 1, \ldots, d$, we may clearly replace $\hat{P}$ by a progression $\mathcal{P}_1 \subset \hat{P}$ of dimension $d - 1$ with $(c(K')/2)|\mathcal{P}_1| \leq |\mathcal{P}_1|$ and still satisfying$$|\mathcal{P}_1 \cap \theta \mathcal{P}_1| > c_1(K')|\mathcal{P}_1| \geq c_1(K')|\mathcal{P}_1|.$$If (ii) holds, apply Lemma 1.1 to obtain a reduction from $d$ to $d - 1$. Observe that since the integer $v$ in Lemma 1.1 satisfies $v | p$ and$$v < c(K') \min_i J_i < c(K')|A| < c(K') \frac{p}{K} < p,$$
necessarily \( v = 1 \) (assuming \( K \) is large enough). Thus by Lemma 1.1 \( \mathcal{P} \subset \mathcal{P}_1 \), where \( |\mathcal{P}_1| < c(K')|\mathcal{P}| \) and \( \mathcal{P}_1 \) is 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 \( i = 1, \ldots, d_1 \), where \( d_1 \) is the dimension of \( \bar{\mathcal{P}} \) and \( \epsilon = \epsilon(K') \). Thus
\[
\bar{\mathcal{P}} = \left\{ \sum_{i=1}^{d_1} x_i \xi_i : 0 \leq x_i \leq J_i, x_i \in \mathbb{Z} \right\}
\]
and for all \( i = 1, \ldots, d_1 \) there are \( k_i \in \mathbb{Z} \) and \( k'_{i,s} \in \mathbb{Z} \) (\( 1 \leq s \leq d_1 \)) satisfying
\[
\begin{align*}
\theta k_i \xi_i &= \sum_{s=1}^{d_1} k'_{i,s} \xi_s, \\
0 < k_i < c(K'), \\
|k'_{i,s}| < c(K') \frac{J_s}{J_i} & \quad \text{for all} \ s = 1, \ldots, d_1.
\end{align*}
\]
For (2.20), we use (2.10) (cf. (2.8)) which is valid for all \( s = 1, \ldots, d_1 \) (rather than (2.6) which is a consequence).

Returning to (2.18), it follows that the polynomial
\[
p(x) = \det \left[ (xk_i - k'_{i,j})e_{i,j} - \sum_{j \neq i} k'_{i,j} e_{i,j} \right] \in \mathbb{Z}_p[x]
\]
has \( \theta \) 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
\[
\sum_{\pi \in \text{Sym}(d_1)} \prod_{i=1}^{d_1} (|k_i| + |k'_{i,\pi(i)}|) < c(K') \sum_{\pi \in \text{Sym}(d)} \prod_{i=1}^{d_1} \frac{J_{\pi(i)}}{J_i} < c'(K').
\]
This contradicts the assumption on \( \theta \) for \( K \) sufficiently large.

**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 how large the quantity
\[
\min_{p^\epsilon < |A| < p^{1-\epsilon}} |A + \theta A|/|A|
\]
can be made for some \( \theta \in \mathbb{F}_p \). Considering sets \( A \) of the form \( A = \{ \sum_{i=1}^{d} x_i \theta^i : 0 \leq x_i \leq M \} \), it is easily seen that (2.22) is less than \( \exp(\sqrt{\log p}) \).
Lemma 3.1. Let $\mathcal{P} = (\xi, P)$ be a progression with $\xi = (\xi_1, \ldots, \xi_d) \in \mathbb{Z}_q^d$ and $P = \prod_{i=1}^d [1, J_i] \subset \mathbb{R}^d$, where the integers $J_i$ satisfy $J_1 \geq \cdots \geq J_d > 0$. Assume

$$\delta_0 \prod_{i=1}^d J_i < |P| < q^{1-3\gamma}$$

with $\gamma > 0$ a constant. Let $\varepsilon, M > 0$ ($\varepsilon$ small, $M$ large) satisfy

$$\delta_0^{-1} \varepsilon^{d+10} < M < q^{\gamma/2}.$$  

Assume

$$|\pi_{q'}(\mathcal{P})| > M \quad \text{for all } q' \mid q, q' > q^\gamma.$$  

Let $B \subset \mathbb{Z}^d_q$ be such that

$$|\pi_{q'}(B)| > M \quad \text{for all } q' \mid q, q' > q^{\gamma/10d}.$$  

Here $\pi_{q'} : \mathbb{Z}_q \to \mathbb{Z}_{q'}$ denotes the quotient map mod $q'$. Then there is $a \in B$ such that

$$|aP \cap P| < \varepsilon|P|.$$  

Lemma 3.1 will be proved by assuming $|aP \cap P| > \varepsilon|P|$ 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

$$\varepsilon_0 = \varepsilon.$$  

Assume

$$\delta_0 |P| \leq |P|,$$  

and $\mathcal{P}$ is not proper with respect to $9/\varepsilon_0$. Lemma 1.1 then allows a reduction of the dimension of the progression $\mathcal{P}$ in the following sense: there are $v_0 \in \mathbb{N}$ and $\xi^{(1)} \in \mathbb{Z}_{q}^{d-1}$, $\mathcal{P}_1 = \prod_{i=1}^{d-1} [1, J_i] \cap \mathbb{Z}^{d-1}$ satisfying

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

$$|\mathcal{P}_1| < \frac{C}{\delta_0 v_0} |P|,$$  

$$v_0 \mathcal{P} \subset \mathcal{P}_1.$$  

By (3.7)–(3.9),

$$|\mathcal{P}_1| \geq |\mathcal{P}_1| \geq \frac{|P|}{v_0} > \frac{\delta_0 v_0 |P|}{\delta_1 |\mathcal{P}_1|}$$

with

$$\delta_1 = c \varepsilon_0 \delta_0.$$
Take \( \varepsilon_1 = \varepsilon \delta_1 \). (3.12)

and repeat the preceding.

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

\[
v_1 < \frac{9}{\varepsilon_1} \min J_{1,j}, \quad v_1 | q, \quad |\mathcal{P}_2| < \frac{C}{\varepsilon_1 v_1} |\mathcal{P}_1|, \quad v_1 \cdot \mathcal{P}_1 \subset \mathcal{P}_2.
\] (3.13)

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

\[
|\mathcal{P}_2| \geq |\mathcal{P}_2| > \frac{|\mathcal{P}_1|}{v_1} > \frac{\delta_1}{v_1} |\mathcal{P}_1| > \delta_2 |\mathcal{P}_2|,
\] (3.15)

with

\[
\delta_2 = c \varepsilon_1 \delta_1.
\] (3.16)

Notice that

\[
\mathcal{P}_2 \supset v_0 v_1 \mathcal{P}.
\] (3.17)

Take

\[
\varepsilon_{r-1} = \varepsilon \delta_{r-1}.
\] (3.18)

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

\[
v_{r-1} < \frac{9}{\varepsilon_{r-1}} \min J_{r-1,i}, \quad v_{r-1} | q, \quad |\mathcal{P}_r| < \frac{C}{\varepsilon_{r-1} v_{r-1}} |\mathcal{P}_{r-1}|, \quad v_{r-1} \cdot \mathcal{P}_{r-1} \subset \mathcal{P}_r.
\] (3.19)

Same reasoning as before yields

\[
|\mathcal{P}_r| \geq |\mathcal{P}_r| > \delta_r |\mathcal{P}_r|
\] (3.22)

with

\[
\delta_r = c \varepsilon_{r-1} \delta_{r-1}.
\] (3.23)

Also,

\[
v_0 v_1 \cdots v_{r-1} \mathcal{P} \subset \mathcal{P}_r.
\] (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'') \( \varepsilon_0\varepsilon_1 \cdots \varepsilon_{r-1} > c\varepsilon\varepsilon^{2^{d+1}} > c\varepsilon^{2^{d+1}} \).

(4) \( |P| > c\varepsilon_0\varepsilon_1 \cdots \varepsilon_{r-1}v_0v_1 \cdots v_{r-1}|P_r| \).

(4') \( \left(\frac{C}{\varepsilon}\right)^{2^{d+1}}|P| > v_0v_1 \cdots v_{r-1} \).

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

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 \( |P \cap aP| > \varepsilon|P| \).

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

\[
|P_r \cap aP_r| \geq \left|(v_0v_1 \cdots v_{r-1}P) \cap a(v_0v_1 \cdots v_{r-1}P)\right| \\
\geq (v_0v_1 \cdots v_{r-1})^{-1}|P \cap aP| > (v_0v_1 \cdots v_{r-1})^{-1}c\varepsilon_0|P| \\
\geq c\varepsilon_0\varepsilon_1 \cdots \varepsilon_{r-1}\delta_0|P_r| = c\varepsilon_0|P_r| = c\varepsilon_r|P_r|, \tag{3.25}
\]

where

\( \varepsilon_r = \varepsilon\delta_r \). \tag{3.26}

We need the following little fact from algebra to prove Lemma 3.1.

**Fact A.** Let \( A \subset \mathbb{Z}_q \), \( k \in \mathbb{Z}_q \), and \( q' = q/gcd(k, q) \). Then \( |\pi_q(A)| = |kA| \).

**Proof of Lemma 3.1.** We assume after \( r \) reductions \( P_r \) is proper with respect to \( 9/\varepsilon_r \). (If \( P \) is already proper with respect to \( 9/\varepsilon_r \), then \( r = 0 \) and \( P_0 = P \).) We apply Lemma 2.1 to \( P' = P_r \), replacing \( \varepsilon \) by \( \varepsilon_r \). By our construction, alternative (ii) in Lemma 2.1 is ruled out.

Assume \( J_i' := J_i \) are ordered decreasingly, \( J_1' \geq \cdots \geq J_{d'} \).

Let \( \xi_i' = \xi_i^{(r)} \in \{1, \ldots, q - 1\} \subset \mathbb{Z}_q \setminus \{0\} \) and define

\[
q_1 = gcd(\xi_1', q), \\
q_2 = gcd(\xi_1', \xi_2', q), \\
\vdots \\
q_{d'} = gcd(\xi_1', \ldots, \xi_{d'}', q).
\]

**Claim.** \( q_{d'} \leq q^{1-\gamma} \).

**Proof of Claim.** Assume \( q_{d'} > q^{1-\gamma} \). Let \( w = q/q_{d'} < q^{\gamma} \). Then (5), (3.1) and (3.2) imply

\[
v_0v_1 \cdots v_{r-1}w \leq (C/\varepsilon)^{2^{d+1}}|P| \cdot q^{\gamma} \leq (C/\varepsilon)^{2^{d+1}} \frac{1}{\delta_0}q^{-2\gamma} < q^{1-\gamma}. \tag{3.27}
\]
Also,
\[ w_ξ' = \cdots = w_ξ'_{d'} = 0 \pmod{q}, \]
hence, from (3.24),
\[ v_0 v_1 \cdots v_{r-1} w P = 0 \pmod{q}. \]
By Fact A,
\[ \pi_{q'}(P) = 0 \quad (3.28) \]
with (by (3.27))
\[ q' = q / \gcd(q, v_0 \cdots v_{r-1} w) > q^\gamma. \]
This contradicts (3.3), proving the Claim.

Therefore, there is \( i \in \{1, \ldots, d'\} \) such that
\[ \frac{q_{i-1}}{q_i} > q^\gamma / d', \quad (3.29) \]
\[ \frac{q}{q_1}, \frac{q_1}{q_2}, \ldots, \frac{q_{i-2}}{q_{i-1}} \leq q^\gamma / d. \quad (3.30) \]
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
\[ (C/\varepsilon)^{2d+1} > 2/\varepsilon, \quad J_i' \geq J_{i+1}' \geq \cdots \geq J_{d'}'. \quad (3.31) \]
Let
\[ v = v_0 \cdots v_{r-1} q / q_{i-1}. \]
By (3.30), (5), (3.1) and (3.2),
\[ v \leq v_0 \cdots v_{r-1} q^\gamma < (C/\varepsilon)^{2d+1} |P| q^\gamma < cq^{1-3\gamma + \gamma / 2} q^\gamma < q^{1-\gamma}. \]
Hence, from the definition of \( q_{i-1} \),
\[ vP = v_0 v_1 \cdots v_{r-1} q / q_{i-1} P \subset \frac{q}{q_{i-1}} P = \frac{q}{q_{i-1}} \left\{ \sum_{s \geq i} x_s \xi_s' : x_s \leq J_i' \right\}. \quad (3.32) \]
(3.31), (3.32) imply
\[ |vP| \leq J_i' J_{i+1}' \cdots J_{d'}' < (C/\varepsilon)^{2d+1} < M. \]
Hence Fact A implies \( |\pi_{q'}(P)| = |vP| < M \) with \( q' = q / \gcd(q, v) > q^\gamma \), again contradicting (3.3).
So alternative (iii) holds and there are $k_i, (k'_s)_{1 \leq s \leq d'} \in \mathbb{Z}$ such that

\begin{align}
0 < k_i < 1/\varepsilon_r, \\
|k'_s| < 8/\varepsilon_r^2 \quad \text{for } i \leq s \leq d', \tag{3.33} \\
\text{ak}_i \xi'_i = \sum_{s=1}^{d'} k'_s \xi'_s \pmod{q}. \tag{3.35}
\end{align}

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

\begin{equation}
\text{ak}_i \xi'_i = \sum_{s \geq i} k'_s \xi'_s \pmod{q_{i-1}}. \tag{3.36}
\end{equation}

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

Recalling (3.29) and (3.4) we have

\begin{equation}
|\pi_{q_{i-1}/q_i}(B)| > M \tag{3.37}
\end{equation}

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

\begin{equation}
|P' \cap aP'| > \varepsilon_r |P'| \tag{3.38}
\end{equation}

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 $B' \subset \tilde{B}$ with $|B'| > M^{1/2}$ such that for all $a \in B'$, (3.36) holds with the same coefficients $k_i, k'_i$ ($s \geq i$). Taking any $a_1, a_2$ in $B'$ we obtain

\begin{align}
(a_1 - a_2)k_i \xi'_i &= 0 \pmod{q_{i-1}}, \\
(a_1 - a_2)k_i &= 0 \pmod{q_{i-1}/q_i}, \tag{3.39}
\end{align}

implying

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

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 exist elements $a_1, \ldots, a_R$ in $B$ with $R \sim M^{1/10}$ such that

\begin{equation}
|a_s P \cap a_s' P| < \varepsilon |P| \quad \text{for } s \neq s'. \tag{3.40}
\end{equation}
Proof. Let $\tilde{B} \subset B$ be the set constructed in the proof of Lemma 3.1. Assume $a_1, \ldots, a_r \in \tilde{B}$ are already obtained satisfying (3.40) and suppose
$$\max_{1 \leq s \leq r} |a_s P \cap a P| > \varepsilon |P| \quad \text{for all } a \in \tilde{B}.$$Hence, there is some $s = 1, \ldots, r$ and $B_1 \subset \tilde{B}$ with
$$|B_1| > \frac{1}{r} |\tilde{B}| > \frac{M}{R} > M^{9/10}$$and such that
$$|P \cap \frac{a}{a_s} P| > \varepsilon |P| \quad \text{for all } a \in B_1. \quad (3.41)$$It follows that all elements $a/a_s$, $a \in B_1$, have a representation (3.36). Passing again to a subset $B'_1$ with $|B'_1| > \frac{M}{R} > \frac{M}{10}$, we may ensure the same coefficients $k_i, (k'_i), \gamma \geq i$ and get a contradiction as before.

4

Let $A \subset Z_q$ be such that
$$|A + A| < K|A|, \quad (4.1)$$
$$1 \ll |A| < q^{3-4y}. \quad (4.2)$$Identifying $Z_q \simeq \{0, 1, \ldots, q - 1\}$, we apply Freiman’s theorem to $A$, first considered as a subset of $Z$ (with doubling constant $\leq 2K$).

From [C], we obtain
$$d \leq 2K$$and a progression $P$ given by $\xi = (\xi_1, \ldots, \xi_d) \in Z^d$ and $P = \prod_{i=1}^d [0, J_i]$, with $J_1 \geq \cdots \geq J_d$ in $\mathbb{N}$, such that
$$A \subset P = \{x \xi^T : x \in \mathbb{P} \}, \quad (4.3)$$
$$|P| < C^d |A|. \quad (4.4)$$Applying $\pi_q : \mathbb{Z} \to Z_q$, $P$ becomes a progression in $Z_q$ containing $A \subset Z_q$. Assuming
$$C^d < q^{\gamma/2}, \quad (4.5)$$by (4.2)–(4.5), we have
$$q^{1-3y} > C^{d} q^{1-4y} > |P| \geq |P| \geq |A| > C^{-K^3} |P|. \quad (4.6)$$Thus assumption (3.1) in Lemma 3.1 holds with $\delta_0 = C^{-K^3}$.

Let $\varepsilon, M$ satisfy (3.2), i.e.
$$C^d (1/\varepsilon)^{10K^5} < M < q^{\gamma/2} \quad (4.7)$$
Assume $B \subset \mathbb{Z}_q^*$ is such that $|\pi_{q'}(B)| \leq |\pi_{q'}(A)|$ (e.g. $B$ contained in a translate of $A$) for all $q' | q$ and $q' > q'$. Furthermore, assume $B$ satisfies

$$|\pi_{q'}(B)| > M \quad \text{if} \quad q' | q \text{ and } q' > q'',$

(4.8)

Since by assumption also

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

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

Apply Lemma 3.1'.

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

$$\left| \bigcup_{r \leq R} a_r A \right| \geq R|A| - \sum_{r \neq s} |a_r A \cap a_s A| \geq R|A| - \sum_{r \neq s} |a_r P \cap a_s P|$$

$$> R|A| - R^2 \varepsilon C K^3 |A|.$$  

(4.9)

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

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

(4.10)

Assume

$$M > C^{50 K+10}$$  

(4.11)

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

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

From (4.10) and (4.11),

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

(4.12)

Replacing $4 \gamma$ by $\gamma$ and summarizing, we have proved the following:

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

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

(4.13)

$$|A + A| < K|A|.$$  

(4.14)

Let $M$ satisfy

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

(4.15)

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

$$|\pi_{q'}(B)| \leq |\pi_{q'}(A)| \quad \text{if} \quad q' | q \text{ and } q' > q',$$

$$|\pi_{q'}(B)| > M \quad \text{if} \quad q' | q \text{ and } q' > q'/80K.$$  

(4.16)

Then

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

(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

$$|\pi_q(H)| > M \quad \text{whenever } q' \mid q, q' > q^\kappa. \quad (5.1)$$

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

$$k < q^\kappa', \quad (5.2)$$

$$r < \log_2 q^\kappa', \quad (5.3)$$

$$|kH^r| > q^{1-\kappa'}, \quad (5.4)$$

where $\kappa' = \kappa'(\kappa, M) \to 0$ as $\kappa \to 0, M \to \infty$ (independently of $q$).

Proof. We describe the construction. Given any $\kappa_1 > \kappa_1/2$, (5.5)

set

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

Let $A_0 = H$ and $A_\alpha = k\alpha H^{r\alpha}$ be the set obtained at stage $\alpha$. 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 $M < q^{7/10}$. 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

$$|A_{\alpha+1}| > K|A_\alpha|, \quad (5.7)$$

with

$$k_{\alpha+1} \leq 2k_\alpha, \quad r_{\alpha+1} \leq r_\alpha + 1. \quad (5.8)$$

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

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

By (5.8), in (5.2) we have

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

Hence

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

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 \( \nu \) is a probability measure, i.e. \( 0 \leq \nu(x) \leq 1 \), then \( |\hat{\nu}(\xi)| \leq 1 \).

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

F3. \( \text{supp}(\nu \ast \nu') \subset \text{supp} \nu + \text{supp} \nu' \).

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

F5. \( \hat{\nu} \ast \nu'(\xi) = \hat{\nu}(\xi) \hat{\nu}'(\xi) \).

Let \( 0 \leq x \leq 5\pi/6 \). Then

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

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

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

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

\[
|\pi_p(H)| \geq 2 \quad \text{for all primes } p | q, \quad (6.1)
|\pi_{q'}(H)| > M \quad \text{for all } q' | q, q' > q^\kappa. \quad (6.2)
\]

We want to show that \( k_1 H' = \mathbb{Z}_q \) for some \( k_1, r \in \mathbb{N} \) satisfying

\[
r < \log q^\kappa, \quad (6.3)
\]
\[
k_1 < q^{5\kappa}. \quad (6.4)
\]

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

Define

\[ D = \{ q' \in \mathbb{N} : q' \neq 1 \text{ and } q' | q \}, \]

hence

\[ |D| < q^{1/\log \log q}. \quad (6.5) \]

For \( q' \in D \), we have

\[ |\pi_{q'}(k H')| \geq |k H'| \frac{q'}{q} \frac{q'}{q'} \geq q' q^\kappa q^\kappa, \quad (6.6) \]

while by (6.1), also

\[ |\pi_{q'}(k H')| \geq |\pi_{q'}(H)| \geq 2. \quad (6.7) \]

Take a subset \( \Omega_{q'} \subset k H' \) such that \( \pi_{q'}|\Omega_{q'} \) is one-to-one and

\[ |\Omega_{q'}| \geq \max \{ 2, q' q^\kappa \}. \quad (6.8) \]
Define the probability measures
\[ \mu_{q'} = \frac{1}{|\Omega_{q'}|} \sum_{x \in \Omega_{q'}} \delta_x, \tag{6.9} \]
\( \delta_x \) being the indicator function, and their convolution
\[ \mu(x) = \ast_{q' \in D} \mu_{q'}(x) = \sum_{y_1, \ldots, y_{|D|-1}} \mu_{q'|D'}(x - y_1 - \cdots - y_{|D|-1}) \cdots \mu_{q_2}(y_2) \mu_{q_1}(y_1). \tag{6.10} \]
Then by F3,
\[ \text{supp } \mu \subset \sum_{q' \in D} \text{supp } \mu_{q'} \subset \sum_{q' \in D} |\Omega_{q'}| \subset |D|kH'. \tag{6.11} \]
We estimate the Fourier coefficients
\[ \hat{\mu}(a/q) = \sum_{x \in \mathbb{Z}_q} e_q(-ax) \mu(x) \]
for \( 0 < a < q \). Let \( a/q = a'/q' \) where \( q'|q \) and \( (a', q') = 1 \). From (6.10) and F5,
\[ \left| \hat{\mu}(a/q) \right| \leq \left| \hat{\mu}_{q'}(a'/q') \right| = \frac{1}{|\Omega_{q'}|} \sum_{x \in \Omega_{q'}} e_{q'}(a'x). \tag{6.12} \]

**Claim 1.** \( |\hat{\mu}(a/q)| < 1 - \frac{1}{16}q^{-2k'} \).

**Proof of Claim 1.** Assume \( \hat{\mu}(a/q) > 1 - \tau \). We want to find a lower bound on \( \tau \).

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
\[ |e_{q'}(a'x_0) - e_{q'}(a'y)|^2 = \left[ 2 \sin \frac{2\pi a'}{q'} (x_0 - y) \right]^2 = 2 - 2 \cos \frac{2\pi a'}{q'} (x_0 - y). \]
Together with (6.14) this gives
\[ \sum_{y \in \Omega_{q'}} |e_{q'}(a'x_0) - e_{q'}(a'y)|^2 \leq 2|\Omega_{q'}| - 2(1 - \tau)^2 |\Omega_{q'}| < 2\tau |\Omega_{q'}|. \tag{6.15} \]
From (6.15),
\[ |\{ y : |e_{q'}(a'x_0) - e_q(a'y)| > 2\sqrt{\tau} \}| \leq \frac{1}{2} |\Omega_q'|. \]
So there is a subset \( \Omega' \subset \Omega_q' \) with \( |\Omega'| > \frac{1}{2} |\Omega_q'| \) such that for all \( y \in \Omega' \),
\[ |e_{q'}(a'x_0) - e_q(a'y)| < 2\sqrt{\tau}, \]
hence T1 implies
\[ \|a'x_0/q - a'y/q\| < 2\sqrt{\tau}. \] (6.16)
Therefore
\[ |\pi_{q'}(\Omega')| = |\pi_{q'}(a'\Omega')| \leq 2\sqrt{\tau}q' + 1. \]

Since \( \pi_{q'}|\Omega' \) is one-to-one, also
\[ \frac{1}{2} q' q^{-\kappa'} < |\Omega'| \leq 2\sqrt{\tau}q' + 1 \] (6.17)
by (6.8). This gives a lower bound \( \tau > \frac{1}{16} q^{-2\kappa'} \), proving Claim 1.

Take
\[ \ell = [q^{3\kappa'}]. \] (6.18)

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

**Proof of Claim 2.** For \( x \in \mathbb{Z}_q \), write
\[ \mu^{(\ell)}(x) = \frac{1}{q} + \frac{1}{q} \sum_{a=1}^{q} \hat{\mu}(\ell)\left( \frac{a}{q} \right) e_q(ax). \] (6.19)

By Claim 2 and (6.18), the second term in (6.19) is at most
\[ \max_{1 \leq a < q} \left| \hat{\mu}(\ell)\left( \frac{a}{q} \right) \right| \leq \max_{1 \leq a < q} \left| \hat{\mu}(\ell)\left( \frac{a}{q} \right) \right| < \left( 1 - \frac{1}{16q^{2\kappa'}} \right) q^{3\kappa'} e^{-q^{2\kappa'}} < \frac{1}{q}. \]
Hence \( \mu^{(\ell)}(x) > 0 \), proving Claim 2.

Putting together Claim 2, (6.11), (6.18), (6.5) and (5.2), we have
\[ \mathbb{Z}_q = \ell \ \text{supp} \ \mu = \ell|D|kH' = k_1 H' \]
with \( k_1 \leq q^{3\kappa'} q^{1/\log q} q^{\kappa'} < q^{5\kappa'} \), which completes the proof of Theorem A.

**Remark 6.1.** It is much simpler to prove the weaker bound
\[ \left| \hat{\mu}_{q'}\left( \frac{a'}{q'} \right) \right| < 1 - \frac{\pi}{2} \left( \frac{1}{q'} \right)^2. \]
Indeed, since \( |\Omega_{q'}| \geq 2 \), there are \( x_1, x_2 \in \Omega_{q'} \) with \( \pi_{q'}(x_1) \neq \pi_{q'}(x_2) \). As \( (a', q') = 1 \), also \( \pi_{q'}(a'x_1) \neq \pi_{q'}(a'x_2) \). Therefore, by T2,
\[ |e_{q'}(a'x_1) + e_{q'}(a'x_2)| \leq |e_{q'}(1) + 1| < 2 - \frac{\pi}{2} \left( \frac{1}{q'} \right)^2 \]
Write
\[
\left| \sum_{x \in \Omega_q} e_q(a' x) \right| \leq (|\Omega_q| - 2) + |e_q(a' x_1) + e_q(a' x_2)| < |\Omega_q| - \pi \frac{1}{2 (q')^2}.
\]
This yields the stated bound.

**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
\[
\{1, \theta, \ldots, \theta^r\} \subset H^r.
\]

We distinguish 2 cases.

**Case 1:** \( t \geq \log q / (\log \log q)^{1/2} \). Take \( r_0 \geq \log q(\log \log q)^4 \). 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 \( kH^{r_0} = \mathbb{Z}_q \) with \( k < C(\log q)^3 \).

**Case 2:** \( t < \log q / (\log \log q)^{1/2} \). Define \( \varphi(t) = |\mathbb{Z}_q^*| \). Use Theorem 4.2 from [KS] to get
\[
\max_{(a,q)=1} \left| \sum_{x=1}^{t} e_q(a \theta^x) \right| < t - c(\rho)q^{-2/\rho} \quad \text{for } 2 \leq \rho \leq \varphi(t). \tag{6.20}
\]

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

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 assumption (5.1) of Proposition 1 and \( \kappa' \) be as in that proposition. Let \( q' \mid q, q' > q^{\kappa'} \) and \( (a, q') = 1 \). Let \( r \in \mathbb{N} \) with \( r > \kappa' \log q \). Then
\[
\max_{x,y \in H^r} \left\| \frac{a}{q'} (x - y) \right\| > q^{-2\kappa'} \tag{7.1}
\]
(2) Let \( H \subset \mathbb{Z}_q^* \) be a multiplicative subgroup satisfying assumption (5.1) of Proposition 1. Let \( q' \mid q, q' > q^{\kappa'} \) and \( (a, q') = 1 \). Then

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

(7.2)

**Proof.** By (5.4),

\[
|\pi_{q'}(kaH^r)| = |\pi_{q'}(kH^r)| > q^{1-\kappa'} = q' q^{-\kappa'} > 1.
\]  

(7.3)

Hence there are \( z, w \in kH' \) such that

\[
\left\| \frac{a}{q'} (z - w) \right\| \geq q^{-\kappa'}.
\]  

(7.4)

Writing \( z = x_1 + \cdots + x_k \) and \( w = y_1 + \cdots + y_k \) with \( x_i, y_i \in H' \), it follows that

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

by (5.2).

**Corollary 4.**

(1) Let \( H \subset \mathbb{Z}_q^* \) satisfy conditions (6.1), (6.2) and \( \kappa' \) be as in Theorem A. Let \( 1 \leq a < q \). Then for \( r > \kappa' \log q \),

\[
\max_{x,y \in H} \left\| \frac{a}{q} (x - y) \right\| \geq q^{-5\kappa'}.
\]  

(7.5)

(2) If moreover \( H \subset \mathbb{Z}_q^* \) is a group, we get

\[
\max_{x,y \in H} \left\| \frac{a}{q} (x - y) \right\| \geq q^{-5\kappa'}.
\]  

(7.6)

**Proof.** Write \( a/q = a'/q' \), \( (a', q') = 1 \). Since \( \pi_{q'}(k_1H') = \mathbb{Z}_q^* \), we have

\[
\max_{z,w \in k_1H'} \left\| \frac{a'}{q'} (z - w) \right\| \geq \frac{1}{2^k},
\]  

hence

\[
\max_{x,y \in H'} \left\| \frac{a'}{q} (x - y) \right\| \geq \frac{1}{k_1} > q^{-5\kappa'}.
\]
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 $H < \mathbb{Z}_q^*$ with $|H| > M > 1$. Then

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

(8.1)

where $\delta = \delta(M) \to 0$ as $M \to \infty$ (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

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

(8.2)

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

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

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

(8.3)

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

**Claim.** Let $c \in \mathbb{Z}$ and $2 \leq r < \varphi(t)$. Then

$$\max_{1 \leq j \leq t} |b_j - c| > c(r)q^{(r-2)/(r-1)}.$$

**Proof of Claim.** Let

$$B = \max_{1 \leq j \leq t} |b_j - c|. \quad (8.4)$$

Set $b = (b_1, \ldots, b_t)$, and $1 = (1, \ldots, 1)$. We consider the lattice

$$L = \{ \ell = (\ell_1, \ldots, \ell_r) \in \mathbb{Z}^r : b\ell^T = 0, 1\ell^T = 0 \} = \{ \ell = (\ell_1, \ldots, \ell_r) \in \mathbb{Z}^r : (b - c)\ell^T = 0, 1\ell^T = 0 \}. \quad (8.5)$$

We consider all expressions $\sum (b_i - c)\ell_i$ with $\sum \ell_i = 0$ and $|b_i - c| \leq B$. From the pigeonhole principle and (3.4), there is $(\ell_1, \ldots, \ell_r) \in L \setminus \{0\}$ such that

$$\max_{1 \leq j \leq t} |\ell_j| < c(r)B^{1/(r-2)}. \quad (8.6)$$

For this vector $\ell = (\ell_1, \ldots, \ell_r)$ we have $b_1\ell_1 + \cdots + b_t\ell_r = 0$. Hence, multiplying with $\theta^j$ gives

$$b_j + 1 \ell_1 + \cdots + b_j + r \ell_r = 0 \pmod{q}$$
for all $j$. Since also $\ell_1 + \cdots + \ell_r = 0$,

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

The left side is bounded by

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

by (8.4) and (8.6).

Assume $c(r)B^{(r-1)/(r-2)} < q$; hence

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

It then follows from (8.7) that

$$(b_{j+1} - c)\ell_1 + \cdots + (b_{j+r} - c)\ell_r = 0,
\quad b_{j+1}\ell_1 + \cdots + b_{j+r}\ell_r = 0 \pmod{q} \quad (8.9)$$

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 from (8.9),

$$\psi(x) | (\ell_1 + \ell_2 x + \cdots + \ell_r x^{r-1})$$

implying $\deg \psi \leq r - 1$. Obviously $\psi(x) | (x^t - 1)$.

Assume

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

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

Therefore one of the roots of $\psi$ is a primitive $t$th root and $\psi$ is divisible by the $t$-cyclotomic polynomial. Hence $\varphi(t) \leq \deg \psi < r$, a contradiction. Hence (8.8) fails, proving the Claim.

Suppose (8.2) fails. Letting $c = a^t \in \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$, we get

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

Hence

$$\max_j \text{dist}(a^j - c, q\mathbb{Z}) < c(r)q^{(r-2)/(r-1)}. \quad (8.10)$$

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

$$b_j = a^j \pmod{q} \quad \text{and} \quad |b_j - c| < c(r)q^{(r-2)/(r-1)}.$$

This contradicts the Claim and proves the lemma.
Proof of Theorem 5. Let $H < \mathbb{Z}_q^*$, $|H| > M$. Fix $\kappa > 0$ (small) and $1 \ll M_1 < M^{\kappa/2}$.

By Lemma 8.1, we may assume

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

If $|\pi_{q_1}(H)| > M_1$ for all $q_1 | q$ with $q_1 > q^\kappa$, then (8.11) holds, since $\delta = \delta(\kappa, M_1) \to 0$ as $\kappa \to 0, M_1 \to \infty$ (by Corollary 3(2)).

Assume 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 $|H_1| > M/M_1$. Consider the set

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

Assume there is $q_2 \mid q_1$ with $q_2 > q^\kappa$ and $|\pi_{q_2}(\mathcal{H}_1)| < M_1$. Hence $|\pi_{q_1q_2}(H_1)| < M_1$ and defining $H_2 = H_1 \cap \pi_{q_1q_2}^{-1}(1)$, we have

$$|H_2| > \frac{|H_1|}{M_1} > \frac{M}{M_1^2}. \hfill (8.12)$$

Considering the set

$$\mathcal{H}_2 = \{x \in \mathbb{Z}_{q/q_1q_2} : 1 + q_1q_2 x \in H_2\} = \frac{H_2 - 1}{q_1q_2},$$

we repeat the process. At some stage $s \leq 1/\kappa$, the process has to stop. Thus

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

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

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

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

Define

$$Q_1 = q_1 \cdots q_s \quad \text{and} \quad Q_2 = q/Q_1.$$

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 $\bar{x} = 1 + Q_1x$, $\bar{y} = 1 + Q_1y \in H_s < H$. Writing

$$\frac{a(x - y)}{Q_2} = \frac{a(Q_1x - Q_1y)}{q} = \frac{a(\bar{x} - \bar{y})}{q},$$
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 \((1 + Q_1x)(1 + Q_1y) = 1 + Q_1(x + y) \pmod{Q_1^2}.\)

Consider \(\pi_{Q_1, Q_2}(H_\kappa) < Z_{Q_1, Q_2}^*\). It follows from the preceding that
\[ \pi_{Q_1, Q_2}(H_\kappa) = 1 + Q_1S \]
where \(S\) is an additive subgroup of \(Z_{Q_1, Q_2}\). Hence
\[ (1 + Q_1x)(1 + Q_1y) = 1 + Q_1(x + y) \pmod{Q_1(Q_1, Q_2)} \]
are cyclic. By assumption (8.14), all elements of \(H_\kappa < H\) are of order \(\leq M_1\), implying
\[ |\pi_{Q_1, Q_2}(H_\kappa)| \leq M_1. \]
Therefore
\[ |\pi_{Q_1, Q_2}(H_\kappa)| \leq M_1. \tag{8.16} \]
By construction of \(H_\kappa\), (8.16) implies
\[ (Q_1, Q_2) \leq q^\kappa, \tag{8.17} \]
and Claim 1 is proved.

Let \(Q'_1 = Q_1/(Q_1, Q_2)\) and \(Q'_2 = Q_2/(Q_1, Q_2)\). 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 \(\pi_{Q'_2}(H_\kappa) \leq Z_{Q'_2}^*\) with \(4\sqrt{\kappa}\) and \(M_1\). Let \(q' | Q'_2\)
with \(q' > (Q'_2)^{4\sqrt{\kappa}} > q^{\kappa}\), and let \(q'' = q'/(q', Q_1, Q_2)\). Thus by (8.17), \(q'' > q^\kappa\).

**Claim 2.** \(|\pi_{q''}(H_\kappa)| > M_1.\)**

**Proof of Claim 2.** It follows from (8.13) that \(|\pi_{q''}(H_\kappa)| > M_1\). Let \(x_1, \ldots, x_n \in H_\kappa, n > M_1\), be such that \(x_i - x_j \neq 0 \pmod{q''}\). Since \((q'', Q'_1) = (q', Q'_1) = 1\) and
\[ \begin{pmatrix} q'' & (Q_1, Q_2) \\ (q', Q_1, Q_2) \end{pmatrix} = 1, \]
we also have
\[ \frac{Q_1}{(q', Q_1, Q_2)}(x_i - x_j) \neq 0 \pmod{q''}. \]
Hence \( Q_1(x_i - x_j) \neq 0 \pmod{q'} \). Since \( 1 + Q_1x_i \in H_s \), it follows that \( |\pi_{q'}(H_s)| > M_1 \), proving Claim 2.

Apply Corollary 3(2) to the group \( \pi_{Q'_2}(H_s) \subset \mathbb{Z}_{q'_2}^* \). Claim 2 implies that

\[
|\pi_{q'}(\pi_{Q'_2}(H_s))| = |\pi_{q'}(H_s)| > M_1
\]

for all \( q' \mid Q'_2 \) with \( q' > (Q'_2)^{4\sqrt{k}} \). Hence for any \( a' \) with \( (a', Q'_2) = 1 \), there are \( \bar{x}, \bar{y} \in H_s \) such that

\[
\left\| \frac{a'}{Q'_2}(\bar{x} - \bar{y}) \right\| > (Q'_2)^{-\kappa'} > q^{-\kappa'} \tag{8.18}
\]

where \( \kappa' = \kappa'(4\sqrt{k}, M_1) \to 0 \) as \( \kappa \to 0 \) and \( M_1 \to \infty \).

Write \( \bar{x} = 1 + Q_1x \) and \( \bar{y} = 1 + Q_1y \) with \( x, y \in H_s \). 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 \( a'Q'_1 \equiv a \pmod{Q'_2} \). Then (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

\[
\left\| \frac{a}{q}(\bar{x} - \bar{y}) \right\| = \left\| \frac{a}{q}(Q_1x - Q_1y) \right\| > q^{-\kappa'-2\kappa}.
\]

Therefore

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

where \( \kappa, \kappa' \) may be made arbitrarily 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 \( \{x_1, \ldots, x_{|H|}\} = aH \), and let \( ax = x_1 \) and \( ay = x_2 \) be given in Theorem 5 such that

\[
\left\| \frac{x_1 - x_2}{q} \right\| > q^{-\kappa}
\]
where \( \kappa = \kappa(M) \). Let

\[
S = \sum_{i=1}^{\lfloor H \rfloor} e_q(x_i).
\]

Then

\[
S^2 = |H| + 2 \sum_{i \neq j} \cos \left( \frac{2\pi (x_i - x_j)}{q} \right)
\]

\[
\leq |H| + 2 \left( \frac{|H|}{2} - 1 \right) + 2 \cos \left( \frac{2\pi (x_1 - x_2)}{q} \right)
\]

\[
\leq |H|^2 - 2 + 2 \left( 1 - \pi \left\| \frac{x_1 - x_2}{q} \right\|^2 \right) < |H|^2 - 2\pi q^{-2\kappa}.
\]

References


[R] Robinson, R.: Numbers having \( m \) small \( m \)th roots mod \( p \). Math. Comp. 61, 393–413 (1993) Zbl 0785.11003 MR 1189522