EXPONENTIAL SUM ESTIMATES OVER SUBGROUPS AND ALMOST SUBGROUPS OF $\mathbb{Z}_q^*$, WHERE q IS COMPOSITE WITH FEW PRIME FACTORS

Jean Bourgain Mei-Chu Chang

ABSTRACT In this paper we extend the exponential sum results from [B-K] and [B-G-K] for prime moduli to composite moduli q involving a bounded number of prime factors. In particular, we obtain nontrivial bounds on the exponential sums associated to multiplicative subgroups H of size q^δ, for any given $\delta > 0$. The method consists in first establishing a 'sum-product theorem' for general subsets A of $\mathbb{Z}^q$. If q is prime, the statement, proven in [B-K-T], expresses simply that, either the sum-set $A + A$ or the product-set $A.A$ is significantly larger than A, unless $|A|$ is near q. For composite q, the presence of nontrivial subrings requires a more complicated dichotomy, which is established here. With this sum-product theorem at hand,the methods from [B-G-K] may then be adapted to the present context with composite moduli. They rely essentially on harmonic analysis and graph-theoretical results such as Gowers' quantitative version of the Balog-Szemeredi theorem. As a corollary,we do get nontrivial bounds for the 'Heilbronn-type' exponential sums when $q = p^r$ (p prime) for all r. Only the case $r = 2$ had been treated earlier in works of Heath-Brown and Heath-Brown and Konyagin (using Stepanov's method). We also get exponential sum estimates for (possibly incomplete) sums involving exponential functions, as considered for instance in [Konyagin-Shparlinski]

§0. Introduction.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

It was shown in [B-K], [B-G-K] (see also [B1], [B2]) how 'sum-product' theorems in the prime field $\mathbb{F}_p$ imply new exponential sum estimates, for instance for small subgroups H of $\mathbb{F}_p^*$, the multiplicative group of $\mathbb{F}_p$. More precisely, it was proven that if $H < \mathbb{F}_p^*$, $|H| > p^\varepsilon$ then

$$\max_{(a,p)=1} \left| \sum_{x\in H} e_p(ax) \right| < |H| p^{-\delta} \tag{0.1}$$

where $\delta = \delta(\varepsilon) > 0$, $e_q(y) = e^{2\pi i y/q}$ and $(a,p) = \gcd(a,p)$.

Using Stepanov's method, see for instance [K-S], estimate (0.1) was only obtained under the assumption $|H| > p^{\frac{1}{4}+\varepsilon}$.

It is clear that this new method has many more applications to number theoretic and cryptographical problems, as demonstrated in [B-G-K], [B1], [B2]. The purpose of this paper is to explore the case of composite moduli. The initial step consists in establishing a 'sum-product' result in the required context, which is a combinatorial statement.

We first recall the sum-product theorem in the field $\mathbb{F}_p$, p prime. The sumset of A, $\{x + y \,:\, x, y \in A\}$, and productset of A, $\{xy \,:\, x, y \in A\}$, are denoted by $A + A$ and $A.A$, respectively. Let $A \subset \mathbb{F}_p$ be an arbitrary set and

$$p^\varepsilon < |A| < p^{1-\varepsilon} \tag{0.2}$$

for $\varepsilon > 0$. Then,

$$|A + A| + |A.A| > c|A|^{1+\delta} \tag{0.3}$$

where $\delta = \delta(\varepsilon) > 0$. This result was established in [B-K-T]. In fact, as shown in [B-G-K], the assumption $1 < |A| < p^{1-\varepsilon}$ may replace (0.2). The basic idea here is that either the sum or product set of a given set A needs to be substantially larger than A. Recall that in $\mathbb{Z}$ (or $\mathbb{R}$) this 'principle' is expressed by the well-known Erdös-Szemeredi conjecture [E-S], stating that if A is an arbitrary finite subset of $\mathbb{Z}$, then always

$$|A + A| + |A.A| \gg |A|^{2-\varepsilon}. \tag{0.4}$$

The problem is unsolved at this point, the best result here being obtained by J. Solymosi (using the Szemeredi-Trotter theorem)

$$|A + A| + |A.A| \gg |A|^{\frac{14}{11} - \varepsilon}. \tag{0.5}$$

Returning to the finite field case, the research in [B-K-T] was originally motivated by problems around the Kakeya conjecture in $\mathbb{R}^3$ and its discrete versions. But different and very significant applications of the sum-product theorem in $\mathbb{F}_p$ emerged in connection with exponential sums mod p, as mentioned above.

In [B2] the sum-product problem for product of fields, $\mathbb{F}_p \times \mathbb{F}_p$ is explored. For subsets $A \subset \mathbb{F}_p \times \mathbb{F}_p$, it turns out that (0.3) holds, unless $|A| > p^{2-\varepsilon}$ or $p^{1-\varepsilon} < |A| < p^{1+\varepsilon}$ and A has a 'large' intersection with a line.

The motivation of this extension to products was the generalization of the exponential sum estimates from Gauss sum to binomial sums

$$\sum_{x=1}^{p} e_p(ax^k + bx^\ell) \tag{0.6}$$

and, more generally, 'sparse' exponential sums as considered by Mordell [M]

$$\sum_{x=1}^{p} e_p(a, x^{k_1} + a_2 x^{k_2} + \cdots + a_r \alpha^{k_r}) \tag{0.7}$$

where $p-1 > k_1 > k_2 > \cdots > k_r$ and $(a_1, \dots, a_r, p) = 1$. In [B2] we establish nontrivial bounds $p^{1-\delta}$ on (0.7) under the essentially optimal conditions $(k_i, p-1) < p^{1-\varepsilon}$ and $(k_i - k_j, p-1) < p^{1-\varepsilon}$ for $i \neq j$.

In this paper, we start investigating this line of thought in the case of composite moduli $q = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. We assume q has only a bounded number of prime factors $p_1, \dots, p_r$, which are moreover 'large', i.e. $p_i > q^\varepsilon$ for some $\varepsilon > 0$ (hence $\alpha_1 + \cdots + \alpha_r < \frac{1}{\varepsilon}$). In §1 we establish a satisfactory 'sum-product' theorem in the residue classes $\mathbb{Z}_q$, for q as above. Roughly speaking, it states that (0.3) always holds for $A \subset \mathbb{Z}_q$, unless A has a 'large' intersection with a coset of a subring (see Theorem 1.10). The proof uses 'modern' machinery in combinatorial number theory such as the Plűnnecke-Ruzsa inequalities on iterated sum and product sets and also methods from [B-K-T] and [B2].

In the third section of the paper we clarify in greater generality (the case of a finite commutative ring R) the relation between exponential sum estimates and the presence of certain subsets $S \subset R$ for which both $S + S$ and $S.S$ are 'small' (see Theorem 3.2). The argument is basically an abstraction of the proofs of Theorems 5 and 7 from [B-G-K], where Theorem 7 in [B-G-K] is replaced by Proposition 2.1. We use a refinement of the Balog-Szemerédi-Gowers Theorem proven in Appendix (since we could not find this precise statement in the literature).

Though in this paper we only give the proof for the case $R = \prod_j \mathbb{Z}_{q_j}$, the results from sections 2 and 3 do generalize almost verbatim to finite commutative rings R with unit and a 'canonical additive character $e(.)$', which means that the set of characters obtained by considering $e(y.)$ and y varying in R gives all characters. This is equivalent to saying that the ideal $I = \{x \in R : e(xy) = 1 \text{ for all } y \in R\}$ is trivial. We don not know whether there is a more conceptual description of these rings. In fact the existence of such a description is not so important by observing the following: If $e(.)$ is an arbitrary nontrivial character of R, then $e(.)$ factors over R/I, for I defined as above, and is a canonical character for R/I.

Let us briefly explain the heuristics of the argument. Let for simplicity $H < \mathbb{Z}_q^*$ and assume $a \in \mathbb{Z}_q^*$ such that

$$\left| \sum_{x \in H} e_q(ax) \right| > q^{-\varepsilon} |H| \tag{0.8}$$

assuming $\log |H| \sim \log q$ and ε small. (Here $\log |H| \sim \log q$ means $q^{c_1} < |H| < q^{c_2}$ for some $c_1, c_2 > 0$.) Denote $\mu = \mu_H$ the probability measure on $\mathbb{Z}_q$

$$\mu_H = \frac{1}{|H|} \sum_{x \in H} \delta_x. \tag{0.9}$$

Thus (0.8) means that $|\hat{\mu}_H(a)| > q^{-\varepsilon}$. An important point is that μ is obviously H-invariant, in the sense that

$$\hat{\mu}(\xi) = \hat{\mu}(x\xi) \text{ for all } \xi \in \mathbb{Z}_q, x \in H. \tag{0.10}$$

Denote for $\delta > \varepsilon$

$$\Lambda_\delta = \{\xi \in \mathbb{Z}_q | \ |\hat{\mu}(\xi)| > q^{-\delta}\}$$

for which

$$|H| \leq |\Lambda_\delta| < \frac{q^{1+2\delta}}{|H|} \tag{0.11}$$

(the left inequality results from (0.8), (0.10) and the right inequality from Parseval's identity).

Our aim is to give an oversimplified sketch of how we obtain a nontrivial subset S of $\mathbb{Z}_q$ violating the sum-product theorem (this method was also used in [B-G-K]).

Denote $\nu_k = \mu^{(k)}$ the k-fold (additive) convolution of μ, which we assume symmetric. We have

$$\|\nu_k\|_2^2 \equiv \sum_{x \in \mathbb{Z}_q} \nu_k(x)^2 = \frac{1}{q} \sum_{\xi \in \mathbb{Z}_q} \hat{\nu}_k(\xi)^2 > \frac{1}{q} \sum_{\xi \in \Lambda_\delta} \hat{\nu}_k(\xi)^2 > q^{-2\delta k} \frac{|\Lambda_\delta|}{q} \tag{0.12}$$

and also

$$\frac{1}{q} \sum_{\xi \in \mathbb{Z}_q} \hat{\nu}_k(\xi)^2 < \frac{1}{q}(|\Lambda_{\frac{1}{k}}| + 1). \tag{0.13}$$

We will use the notation $\sim$ to indicate factors $q^{\varepsilon'}$ where ε' can be made arbitrary small by taking ε in the assumption (0.8) small enough. Being more explicit about them basically leads to the detailed argument that appears later in the paper.

Based on (0.12), (0.13), we may choose k and $\delta \ll k^{-2}$ suitably, such that

$$\|\nu_k\|_2^2 \sim \frac{1}{q} \sum_{\xi \in \Lambda_\delta} \hat{\nu}_k(\xi)^2. \tag{0.14}$$

The argument is straightforward. Take in (0.12) $\delta = \frac{1}{k_1} < \frac{\varepsilon'}{k^2}$, so that certainly $\sum_{\xi \in \Lambda_\delta} \hat{\nu}_k(\xi)^2 > q^{-\varepsilon'} |\Lambda_\delta|$. Assume $\sum \hat{\nu}_k(\xi)^2 > q^{\varepsilon'} |\Lambda_\delta|$, hence $|\Lambda_{\frac{1}{k}}| > q^{\varepsilon'} |\Lambda_{\frac{1}{k_1}}|$ by (0.13).

Replace k by k_1. After at most $[\frac{4}{\varepsilon'}]$-steps, we obtain the desired result (0.14), where $k < k(\varepsilon')$ and $\delta > \delta(\varepsilon') \gg \varepsilon$.

It follows in particular from (0.14) that

$$\|\nu_k * \nu_k\|_2 \sim \|\nu_k\|_2 \tag{0.15}$$

Indeed, by Cauchy-Schwarz and (0.14)

$$q\|\nu_k\|_2^2 \lesssim |\Lambda_\delta|^{1/2} \Big(\sum \hat{\nu}_k(\xi)^4 \Big)^{1/2} \sim \sqrt{q}\ \ \|\nu_k\|_2 \ \sqrt{q}\ \ \|\nu_k * \nu_k\|_2$$

(while obviously $\|\nu_k * \nu_k\|_2 \leq \|\nu_k\|_2$).

(0.15) roughly means that the support supp ν_k of ν_k is additively stable. The same is true for $\operatorname{supp} \nu_{2k}$.

Next, we invoke the invariance (0.10), implying that for all $\xi \in \mathbb{Z}_q$

$$\sum_x \hat{\nu}_k(x\xi)^2 \mu(x) = \hat{\nu}_k(\xi)^2.$$

Letting $\nu = \nu_k * \nu_k = \nu_{2k}$, write

$$\begin{aligned} \hat{\nu}_k(\xi)^4 = \Big(\sum_x \hat{\nu}(x\xi)\mu(x) \Big)^2 &\leq \sum_{x_1, x_2} \hat{\nu}\big(\xi(x_1 - x_2)\big)\mu(x_1)\mu(x_2) \\ &= \sum_x \hat{\nu}(\xi x)\nu_2(x) \end{aligned}$$

and similarly

$$\hat{\nu}_k(\xi)^{4k} = \Big(\sum_x \hat{\nu}(x\xi)\mu(x)\Big)^{2k} \le \sum_x \hat{\nu}_k(\xi x)^2 \nu_{2k}(x). \tag{0.16}$$

From the choice of δ and k, we also have

$$\sum_{\xi \in \Lambda_\delta} \hat{\nu}_k(\xi)^{4k+2} \sim |\Lambda_\delta|$$

and substituting (0.16)

$$\sum_{x,\xi} \hat{\nu}_k(\xi)^2 \hat{\nu}_k(x\xi)^2 \nu_{2k}(x) \sim |\Lambda_\delta|. \tag{0.17}$$

(The upper bound follows from (0.14), since the left-hand side is at most $\sum_\xi \hat{\nu}_k(\xi)^2$.)

Hence

$$\sum_x \Big[\sum_y \nu_{2k}(xy)\nu_{2k}(y)\Big] \nu_{2k}(x) \sim \sum \nu_{2k}(x)^2. \tag{0.18}$$

Thus we see that ν_{2k} has a large correlation with its multiplicative translates $\nu_{2k}(x.)$ for $x \in \operatorname{supp} \nu_{2k}$. This permits us to obtain multiplicative stability of $\operatorname{supp} \nu_{2k}$.

Thus we have established both additive and multiplicative stability of $\operatorname{supp} \nu_{2k}$ but only in a 'statistical sense'. In order to obtain a set S which satisfies (in a set-theoretical way)

$$|S| \sim |S + S| \sim |S.S| \tag{0.19}$$

and also

$$S \subset \text{supp } \nu_k, \;\; \nu_k(x) \sim \frac{1}{|S|} \sim \big\|\nu_k\big\|_\infty \text{ for some } k, \tag{0.19'}$$

we rely on a key ingredient from graph theory, which is the Balog-Gowers-Szemeredi theorem.

Since $|\Lambda_\delta| \ge |H|$ in (0.12), it follows that

$$\sum \nu_k(x)^2 \gtrsim \frac{|H|}{q} \tag{0.20}$$

and by (0.19') the set S obtained above satisfies $|S| \lesssim \frac{q}{|H|} < q^{1-\delta}$, since $|H| > q^\delta$.

We have therefore contradicted the sum-product theorem.

What we described above is an overview of the proof of Prop. 2.1 in the paper. Let us next indicate another way of deriving the exponential sum estimate over subgroups, which is perhaps conceptually more straightforward (it is a slightly different approach and does not imply immediately the more general Prop. 2.1 which is of an independent interest).

Assume q prime for simplicity.

Since the measure $\mu = \mu_H$ in (0.4) is H-invariant, assuming $\hat\mu(a) > q^{-\varepsilon}$ for some $a \in \mathbb{Z}_q^*$ implies

$$\hat\mu(\xi) > q^{-\varepsilon}, \text{ for all } \xi \in aH$$

Starting from aH, one aim is to construct consecutively larger and larger sets $\Lambda \subset \mathbb{Z}_q$ such that $\hat\mu(\xi) > q^{-\varepsilon}$ for $\xi \in \Lambda$. (ε may get larger and larger.)

First, if ν is a probability measure on $\mathbb{Z}_q$, $\hat\nu \in \mathbb{R}$, $\nu = \nu_-$, $\big($notation: $\nu_-(x) = \nu(-x)\big)$ and $\hat\nu(\xi) > q^{-\tau}$ for $\xi \in \Lambda$, then

$$\sum_{\xi_1,\xi_2 \in \Lambda} \hat\nu(\xi_1 - \xi_2) > q^{-2\tau} |\Lambda|^2 \tag{0.21}$$

and hence, denoting

$$G = \left\{ (\xi_1, \xi_2) \in \Lambda \times \Lambda : \hat\nu(\xi_1 - \xi_2) > \frac{q^{-2\tau}}{2} \right\}$$

we have

$$|G| > \frac{q^{-2\tau}}{2} \, |\Lambda|^2.$$

Assume that the set

$$\{\xi_1 - \xi_2 : (\xi_1, \xi_2) \in G\}$$

is not significantly larger then $|\Lambda|$ (otherwise we succeeded in obtaining a larger set). It follows then from the Balog-Szemeredi-Gowers (BSG) theorem that there is $\Lambda' \subset \Lambda$ such that

$$|\Lambda' + \Lambda'| \sim |\Lambda'| \sim |\Lambda|. \tag{0.22}$$

Applying the preceding to $\nu = \mu * \mu_-$ and $\Lambda = aH$, it follows that either we obtained a set Λ_1 such that

$$|\Lambda_1| > q^{\varepsilon'}|H|, \text{ and } \hat{\mu}(\xi) > \frac{1}{2}q^{-4\varepsilon} \text{ for } \xi \in \Lambda_1$$

or there is a set $\Lambda' \subset aH$ with

$$|\Lambda' + \Lambda'| \sim |\Lambda'| \sim |H|. \tag{0.23}$$

Define next the probability measure ν' on $\mathbb{Z}_q$

$$\nu'(x) = \frac{1}{|\Lambda'|}\sum_{\xi\in\Lambda'} \nu(x\xi^{-1}). \tag{0.24}$$

Since ν is H-invariant, so is ν'. Moreover $\hat{\nu}'(1) > q^{-2\varepsilon}$, hence $\hat{\nu}'(\zeta) > q^{-2\varepsilon}$ for all $\zeta \in H$. This means that

$$\sum_{\zeta\in H, \xi\in\Lambda'} \hat{\nu}(\zeta\xi) > q^{-2\varepsilon}|H||\Lambda'|.$$

Denote now

$$G_1 = \{(\zeta,\xi) \in H \times \Lambda' : \hat{\nu}(\zeta\xi) > \frac{q^{-2\varepsilon}}{2}\}$$

for which $|G_1| > \frac{1}{2}q^{-2\varepsilon}|H||\Lambda'|$. Assume again $\{\zeta\xi : (\zeta,\xi) \in G_1\}$ is not substantially larger then $|H|$. Applying now the BSG theorem in multiplicative form, we may then obtain $\Lambda'' \subset \Lambda'$ such that

$$|\Lambda''. \Lambda''| \sim |\Lambda''| \sim |\Lambda'|. \tag{0.25}$$

Hence

$$|\Lambda'' + \Lambda''| \sim |\Lambda'| \sim |\Lambda''\Lambda''| \tag{0.25'}$$

contradicting the sum-product theorem in $\mathbb{Z}_q$.

Summarizing, we proved that $\hat{\mu}(\xi) \sim 1$ for $\xi \in \Lambda$, where $\Lambda \subset \mathbb{Z}_q$ is a set satisfying $|\Lambda| > q^{\varepsilon'}|H|$.

Assume now we established that

(*) if ν is an H-invariant probability measure on $\mathbb{Z}_q$ and $\hat{\nu}(\xi_0) \sim 1$ for some $\xi_0 \in \mathbb{Z}_q^*$, then $\hat{\nu}(\xi) \sim 1$ on a set Λ with $|\Lambda| = q^\gamma$.

Assuming $q^\gamma \lesssim \frac{q}{|H|} = q^{1-\rho}$ (which is the case for $\nu = \mu_H$), our aim is to upgrade the statement (*) by enlarging γ to $\gamma' > \gamma + \delta(\rho)$.

Follow the previous reasoning. If the first attempt based on (0.21) fails to enlarge Λ, we obtain $\Lambda' \subset \Lambda$ satisfying (0.22). Define ν' as in (0.24), hence again an H-invariant measure and satisfying $\hat{\nu}'(1) \sim 1$. Thus $(*)$ applies to ν' and there is $\tilde{\Lambda} \subset \mathbb{Z}_q$ with $\hat{\nu}'(\tilde{\xi}) \sim 1$ for $\tilde{\xi} \in \tilde{\Lambda}$ and $|\tilde{\Lambda}| = q^\gamma$. Write

$$\sum_{\xi \in \Lambda', \tilde{\xi} \in \tilde{\Lambda}} \hat{\nu}(\xi\tilde{\xi}) \sim q^{2\gamma}. \tag{0.26}$$

From (0.26), if

$$G_1 = \{(\xi, \tilde{\xi}) \in \Lambda' \times \tilde{\Lambda} : \hat{\nu}(\xi\tilde{\xi}) \sim 1\}$$

then $|G_1| \sim q^{2\gamma}$. If also $\{\xi\tilde{\xi} : (\xi, \tilde{\xi}) \in G\}$ fails to be significantly larger than q^γ, we obtain $\Lambda'' \subset \Lambda'$ such that (0.25), (0.25$'$) hold. This contradicts the sum-product theorem, since $|\Lambda''| < q^{1-\rho}$. In conclusion, we may conclude to the existence of a larger set $\Lambda_1, |\Lambda_1| > q^{\gamma+\delta(\rho)}$ where $\hat{\nu}(\xi) \sim 1, \xi \in \Lambda_1$. The increment $\delta(\rho) > 0$ depends on the specific statement in the sum-product theorem in $\mathbb{Z}_q$. Eventually we contradict the second inequality in (0.11)

Returning to Proposition 2.1, the main application is the extension of the result from [B-K], [G-G-K] to residue classes $\mathbb{Z}_q$ where q is a composite number $q = p_1^{\nu_1} \cdots p_r^{\nu_r}$ as considered in §1.

The required sum-product theorem for subsets $A \subset \mathbb{Z}_q$ with q as above was obtained in §1. Combining this with Theorem 3.2, it follows in particular that $H < \mathbb{Z}_q^*$, a multiplicative group satisfying

$$|\pi_p(H)| > q^\varepsilon \text{ for all primes } p|q. \tag{0.27}$$

(denoting $\pi_p : \mathbb{Z}_q \to \mathbb{Z}_p$ the quotient map mod p), the estimate

$$\max_{a \in \mathbb{Z}_q \backslash \{0\}} \Big| \sum_{x \in H} e_q(ax) \Big| < |H| q^{-\delta} \text{ with } \delta = \delta(\varepsilon) > 0 \tag{0.28}$$

holds (see Corollary 4.2 and Remark 4.6).

In fact, we show in Theorem 4.7 that if $H < \mathbb{Z}_q^*$ and $|H| > q^\delta$, then

$$\max_{a \in \mathbb{Z}_q^*} \Big| \sum_{x \in H} e_q(ax) \Big| < q^{-\varepsilon} |H|$$

where ε depends only on δ and the number of prime factors of q.

An interesting consequence are nontrivial bounds on the Heilbronn type exponential sums as described in Odoni's paper [O].

Take $q = p^m$ ($m \geq 1$ a fixed integer). Then

$$\max_{(a,p)=1} \Big| \sum_{x=1}^{p} e_{p^{m+1}}(ax^{p^m}) \Big| < C_m p^{1-\delta_m} \qquad (\delta_m > 0) \tag{0.29}$$

(the problem of estimating such sums is attributed in [O] to Davenport).

For $m = 1$, nontrivial bounds were obtained by Heath-Brown [H-B] and Heath-Brown-Konyagin [H-B–K], using Stepanov's method. No results for $m \geq 2$ seem to appear in the literature so far. S. Konyagin informed the first author recently of the work of Malyhin (his student) who obtained the $m = 2$ case (with an explicit bound) independently.

Further applications are given to (possibly incomplete) exponential sums involving exponential functions of the form $\sum_{s=1}^{t} e_q(a\theta^s)$, with $\theta \in \mathbb{Z}_q^+$, as considered in [K-S] (see Theorem 4.5). Finally, in Section 5, we prove exponential sum estimates for a typical modulus q noticing that 'most' q are of the form $q = q_1 q_2$, where q_1 is product of a few prime factors and $q_2 < q^{\varepsilon}$. In this situation, our methods are still applicable.

Notations.

$kA = A + \cdot + A$, $A^k = A. \cdots .A$

$e_N(\theta) = e^{\frac{2\pi i}{N}\theta}$

For a ring R, $R^* = \{r \in R \;:\; r \text{ is invertible}\}$

$A \ll_k B$ means $A < c(k)B$ for a constant $c(k)$

$\pi_p : \mathbb{Z}_q \to \mathbb{Z}_p$ is the quotient map mod p

Let S be a set.

$\mu(S) = \sum_{s\in S} \mu(s)$

$\chi_S(x) = 1$, if $x \in S$, 0 otherwise.

§1. The sum-product theorem in Z^q.

Lemma 1.1. *Let $S \subset \mathbb{Z}_N^*$ and let p be the smallest prime factor of N. If $|S| > p^{-\frac{1}{4}}N + N^{\frac{3}{4}}$, then $\mathbb{Z}_N = 3S^2$.*

Proof. Let $f, g : \mathbb{Z}_N \to \mathbb{R}$ be functions. We define the following terms

(a.) $\hat{f}(m) = \frac{1}{N}\sum_{x\in\mathbb{Z}_N} f(x)e_N(-xm)$,

(b.) $f * g(x) = \frac{1}{N}\sum_{y\in\mathbb{Z}_N} f(x-y)g(y)$.

Then the following are easy to verify:

(c.) $f(x) = \sum_{m \in \mathbb{Z}_N} \hat{f}(m) e_N(xm)$,

(d.) $\widehat{f * g}(m) = \hat{f}(m)\hat{g}(m)$,

(e.) $\sum_{m \in \mathbb{Z}_N} |\hat{f}(m)|^2 = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} |f(x)|^2$,

(f.) $\operatorname{supp}(f * g) \subset$ Supp $f +$ Supp g.

Let

$$f(x) = \frac{1}{|S|} \sum_{y \in S^{-1}} \chi_s(yx), \text{ for } x \in \mathbb{Z}_N. \tag{1.1}$$

(Note that $0 \leq f(x) \leq 1$.)

Then the following properties hold.

(i.) Supp $f \subset S^2$,

(ii.) $\hat{f}(m) = \frac{1}{|S|} \sum_{y \in S^{-1}} \hat{\chi}_s(my^{-1})$,

(iii.) $(f * f * f)(x) = \sum_{m \in \mathbb{Z}_N} \hat{f}(m)^3 e_N(xm)$,

(iv.) $|\hat{f}(m)| \leq |S|^{-1/2} (\sum_{y \in S^{-1}} \hat{\chi}_s(my^{-1})^2)^{\frac{1}{2}}$,

(v.) If $m \in \mathbb{Z}_N^*$, then $|\hat{f}(m)| \leq \frac{1}{\sqrt{N}}$,

(vi.) $\sum_{x \in \mathbb{Z}_N} f(x) = |S|$,

(vii.) $\sum_{m \in \mathbb{Z}_N} |\hat{f}(m)|^2 \leq \frac{|S|}{N}$.

Properties (i) and (ii) are obvious; (iii) follows from (c) and (d); (iv) follows from (ii) and Cauchy-Schwartz, (v) follows from (iv) and (e) (which is applied to $\sum_{\ell \in \mathbb{Z}_N} \hat{\chi}_s(\ell)^2 \geq \sum_{y \in S^{-1}} \hat{\chi}_s(my^{-1})^2$). (vi) follows from the estimate

$$\sum_{x \in \mathbb{Z}_N} f(x) = \frac{1}{|S|} \sum_{y \in S^{-1}} \sum_{x \in \mathbb{Z}_N} \chi_s(yx) = \frac{1}{|S|} |S^{-1}| \, |S| = |S|$$

To see (vii), we observe that, by (e), the left-hand side is

$$\frac{1}{N} \sum_{x \in \mathbb{Z}_N} |f(x)|^2 \leq \frac{1}{N} \sum_{x \in \mathbb{Z}_N} f(x) = \frac{|S|}{N}.$$

This is because $0 \le f(x) \le 1$ and (vi).

Claim. Supp $f * f * f \supset \mathbb{Z}_N$.

Proof of Claim. We rewrite (iii) as

$$(f * f * f)(x) = \hat{f}(0)^3 + \sum_{m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^* \setminus \{0\}} \hat{f}(m)^3 e_N(xm) + \sum_{m \in \mathbb{Z}_N^*} \hat{f}(m)^3 e_N(xm). \tag{1.2}$$

By (a) and (vi), we have

$$\hat{f}(0) = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} f(x) = \frac{|S|}{N}. \tag{1.3}$$

By (v) and (vii), we have

$$\sum_{m \in \mathbb{Z}_N^*} |\hat{f}(m)|^3 \le \frac{1}{\sqrt{N}} \sum_{m \in \mathbb{Z}_N^*} |\hat{f}(m)|^2 \le N^{-\frac{3}{2}} |S|. \tag{1.4}$$

To bound the first summation in (1.2), we use (iv) and observe that when y varies, my^{-1} represents the same element in $\mathbb{Z}_N$ at most $\gcd(N, m)$ many times. Hence (iv) gives

$$|\hat{f}(m)| \le |S|^{-1/2} \left(\frac{N}{p} \sum_{\ell \in \mathbb{Z}_N} \hat{\chi}_s(\ell)^2 \right)^{1/2} = |S|^{-1/2} \left(\frac{N}{p} \frac{|S|}{N} \right)^{1/2} = \frac{1}{\sqrt{p}}, \tag{1.5}$$

where p is the smallest prime factor of N. The first equality follows from (e).

Hence, (1.5) and (vii) imply

$$\sum_{m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^* \setminus \{0\}} |\hat{f}(m)|^3 \le \frac{1}{\sqrt{p}} \sum_{m \in \mathbb{Z}_N} |\hat{f}(m)|^2 \le \frac{|S|}{\sqrt{p} N}. \tag{1.6}$$

Putting (1.2), (1.3), (1.4) and (1.6) together, we have

$$|f * f * f(x)| \ge \frac{|S|^3}{N^3} - \frac{|S|}{N^{\frac{3}{2}}} - \frac{|S|}{\sqrt{p} N},$$

which is positive if $|S|^2 > N^{\frac{3}{2}} + p^{-\frac{1}{2}} N^2$, or if $|S| > N^{\frac{3}{4}} + p^{-\frac{1}{4}} N$. □

Finally, the Claim, Properties (f) and (i) imply

$$\mathbb{Z}_N \subset \text{ Supp } f * f * f \subset 3 \text{ Supp } f \subset 3S^2. \qquad \square$$

Ruzsa's inequality If $|A + B| \le c|A|$, then $|hB - kB| \le c^{h+k} |A|$.

In Particular, $|L - L|\ |L| \le |2L|^2$.

Lemma 1.2. *Let F be a finite abelian group, and let $L \subset F$. If*

$$|L| > \frac{|F|}{m^{\alpha}} \text{ for some } m \in \mathbb{N} \text{ and } \alpha > \frac{1}{5}, \tag{1.7}$$

and

$$L - L = F \tag{1.8}$$

then for some $\ell < 10\alpha$, $|2^{\ell} L| > \frac{|F|}{m^{\frac{1}{5}}}$.

Proof. First, we prove

Claim. For any nonnegative ℓ, one of the following cases hold

(a) $|2^{\ell+1} L| \geq m^{\frac{\ell+1}{10}} |L|$,

(b) $|2^{\ell} L| > \frac{|F|}{m^{\frac{1}{5}}}$.

Proof of Claim. We will use induction on ℓ. For $\ell = 0$, if $|L + L| \geq m^{\frac{1}{10}} |L|$, then (a) holds. Otherwise Ruzsa's inequality (see [N] Theorem 7.8) and (1.8) imply that

$$|F| = |L - L| < m^{\frac{1}{5}} |L|.$$

This is Case (b).

Now we assume either $|2^{\ell} L| \geq m^{\frac{\ell}{10}} |L|$ or $|2^{\ell-1} L| > |F| \ m^{-\frac{1}{5}}$. The latter in particular implies $|2^{\ell} L| > |F| \ m^{-\frac{1}{5}}$. For the former, we repeat the initial case. If $|2^{\ell} L + 2^{\ell} L| \geq m^{\frac{1}{10}} |2^{\ell} L|$, then

$$|2^{\ell+1} L| \geq m^{\frac{1}{10}} m^{\frac{\ell}{10}} |L| = m^{\frac{\ell+1}{10}} |L|.$$

If $|2^{\ell} L + 2^{\ell} L| < m^{\frac{1}{10}} |2^{\ell} L|$, then Ruzsa's inequality and (1.8) give $|F| = |2^{\ell} L - 2^{\ell} L| < m^{\frac{1}{5}} |2^{\ell} L|$, which is Case (b). □

To see that the Claim implies the lemma, we use (1.7) on Case (a)

$$|F| \geq |2^{\ell+1} L| \geq m^{\frac{\ell+1}{10}} |L| > m^{\frac{\ell+1}{10} - \alpha} |F|.$$

Therefore, the process has to stop for some $\ell < 10\alpha$. □

The next sum-product theorem for $\mathbb{Z}_p$ is a combination of a theorem in [BKT] and a theorem in [BGK].

Theorem. *$[BKT - BGK]$ Given $\varepsilon > 0$, there is $\delta = \delta(\varepsilon) > 0$ such that if $A \subset \mathbb{Z}_p$ and*

$$1 < |A| < p^{1-\varepsilon}. \tag{1.9}$$

Then

$$|2A| + |A^2| > c(\varepsilon)|A|^{1+\delta}. \tag{1.10}$$

Remark. Instead of(1.10), a more convenient conclusion is

$$|2A^2| = |A(A+A)| \gg |A|^{1+\delta}.$$

Lemma 1.3. *Given $\varepsilon > 0$ and $\alpha < 1$, there is $k = k(\varepsilon, \alpha) \in \mathbb{N}$ such that if $A \subset \mathbb{Z}_p$ with $|A| > p^\varepsilon$ then $|kA^k| > p^\alpha$.*

Proof. We may assume $|A| \leq p^\alpha$ and take $\varepsilon = 1 - \alpha$ in(1.9). Then as in the Remark above, $|2A^2| \gg |A|^{1+\delta}$ for some $\delta = \delta(\alpha)$. If $|2A^2| \leq p^\alpha$, we apply Theorem BKT-BGK again and obtain $|2(2A^2)^2| \gg |2A^2|^{1+\delta} \gg |A|^{(1+\delta)^2}$. After ℓ steps, we get

$$|2^{2^\ell - 1} A^{2^\ell}| > |A|^{(1+\delta)^\ell}.$$

The process stops for some ℓ such that $|A|^{(1+\delta)^\ell} > p^{\varepsilon(1+\delta)^\ell} > p^\alpha$ with $k \leq 2^{2^\ell - 1}$. □

Proposition 1.4. *Let $A \subset \mathbb{Z}_N^*$ and $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. If there is $\varepsilon > 0$ such that*

$$|\pi_p(A)| > p^\varepsilon \textit{ for all } p|N, \tag{1.11}$$

then $kA^k = \mathbb{Z}_N$ for all $k \geq k(\varepsilon, m)$, where $m = \alpha_1 + \cdots + \alpha_r$.

Proof. We do induction on the number of prime factors. For the initial case when $N = p$, a prime, the proposition follows from Lemma 1.3 (with $\alpha > \frac{3}{4}$) and Lemma 1.1.

Let p be the smallest prime factor of N, and let $N' = \frac{N}{p}$.

Since prime factors of N' are prime factors of N,(1.11) holds for $\pi_{N'}(A) \subset \mathbb{Z}^*_{N'}$. The induction hypothesis implies $\pi_{N'}(kA^k) = k\big(\pi_{N'}(A)\big)^k = \mathbb{Z}_{N'}$ for $k \geq k_0 = k_0(\varepsilon)$. In particular, $|kA^k| \geq N'$.

Claim 1. $|kA^k| > N'$ for some $k \leq 2k_0$.

Proof of Claim 1. Assume $|kA^k| = N'$ for all $k \leq 2k_0$.

Take $z_0 \in k_0A^{k_0}$ and let $P = k_0A^{k_0} - z_0$. Then $0 \in P \subset P + P$. Since $N' = |P| \leq |P+P| \leq |2k_0A^{2k_0}| = N'$, we have $|P| = |P+P|$ and P is closed under addition. Hence $P = (p)$, the subring generated by p. Therefore, $k_0A^{k_0} = z_0 + (p)$ and $|\pi_p(k_0A^{k_0})| = 1$ contradicting to assumption (1.11). $\square$

Let $k \leq 2k_0$ be given by the Claim such that $|kA^k| > N'$. So $\pi_{N'}$ is not one-to-one on kA^k and there exists $nN' \in kA^k - kA^k$ such that $nN' \neq 0$ in $\mathbb{Z}_N$, i.e., $0 < n < p$.

Claim 2. $n(kA^k)N' + kA^{2k} = \mathbb{Z}_N$.

Proof of Claim 2. Since $N = pN'$, every element in $\mathbb{Z}_N$ is represented as $a + bN'$, where $1 \leq a \leq N'$ and $1 \leq b \leq p$. From the earlier steps of induction, we have $\pi_{N'}(kA^{2k}) = \mathbb{Z}_{N'}$ and $\pi_p(kA^k) = \mathbb{Z}_p$. The former implies that for $1 \leq a \leq N'$, there exists $\ell \in \mathbb{Z}$ such that

$$a + \ell N' \in kA^{2k}. \tag{1.12}$$

Since $n \neq 0$ in $\mathbb{Z}_p$, for any $b = 1, \cdots, p$, there exists $1 \leq c \leq p$ such that

$$\ell + cn \equiv b \pmod{p}. \tag{1.13}$$

Also, $\pi_p(kA^k) = \mathbb{Z}_p$ implies that there exists m such that

$$c + mp \in kA^k. \tag{1.14}$$

Combining (1.12), (1.13) and (1.14), we see that in $n(kA^k)N' + kA^{2k}$ there exists

$$n(c + mp)N' + a + \ell N' \equiv a + (\ell + cn)N' \equiv a + bN' \pmod{pN'}. \qquad \square$$

Claim 2 implies $(kA^k - kA^k)kA^k + kA^{2k} = \mathbb{Z}_N$. Let $L = k_1 A^{k_1}$, where $k_1 = 2k^2$. Then $L - L = \mathbb{Z}_N$. Using Ruzsa's inequality, we have

$$|2L| \geq (N\,|L|)^{1/2} \geq \left(N\,\frac{N}{p}\right)^{1/2} = p^{-\frac{1}{2}} N.$$

Since $L - L = \mathbb{Z}_N$ implies $2L - 2L = \mathbb{Z}_N$, we can apply Lemma 1.2 to $2L$ to obtain $|32L| \geq p^{-\frac{1}{5}} N$. Now Lemma 1.1 gives $\mathbb{Z}_N = 3(32L)^2$. □

Let A, B, A_1, A_2, A_3 be subsets of a finite commutative ring F. The following facts will be used to prove Proposition 1.9.

Fact 1.5. Let $S \subset A \times B$ with $|S| > \frac{|A|\,|B|}{K}$ for some $K > 0$. Let

$$T = \{a \in A : |(\{a\} \times B) \cap S| > \frac{|B|}{2K}\}.$$

Then

$$|T| > \frac{|A|}{2K}.$$

Fact 1.6. $\chi_B \leq \frac{1}{|A|} \sum_{x \in A+B} \chi_{x-A}$.

Fact 1.7. (Ruzsa's triangle inequality)

Let $A_i \subset F$ for $i = 1, \cdots, 4$. Then

$$|A_1 + A_2| \leq \frac{|A_1 + A_3|\,|A_2 + A_4|\,|A_3 + A_4|}{|A_3|\,|A_4|}$$

Fact 1.8. Let $A \subset F^*$. Then $|A|^2 \leq |A^2|^{\frac{1}{2}} (\sum_{x,x' \in A} |xA \cap x'A|)^{1/2}$.

Facts 1.5 and 1.6 are obvious. Fact 1.7 can be seen by restricting the map $\rho : (A_1 + A_3) \times (A_2 + A_4) \times (A_3 + A_4) \to F$, defined by $\rho(x, y, z) = x + y - z$, to $S = \{(a_1 + a_3, a_2 + a_4, a_3 + a_4) : a_i \in A_i\}$, and noticing that the fibers of ρ contains $A_3 \times A_4$ and $\rho(S) = A_1 + A_2$.

To see Fact 1.8, we notice that $\operatorname{supp} \sum_{x\in A} \chi_{xA} = A^2$ and use Cauchy-Schwartz inequality for the following series

$$|A|^2 = \sum_{x\in A} |xA| = \sum_{x\in A} \sum_{y\in A^2} \chi_{xA}(y) = \sum_{y\in A^2} \Big(\sum_{x\in A} \chi_{xA}(y) \Big).$$

Proposition 1.9. Let F be a commutative ring and let $A \subset F^*$ with

$$|2A| + |A^2| < K\,|A| \tag{1.15}$$

for some $K > 0$. Then for $k \in \mathbb{N}$, there is $A_1 \subset A$ with

$$|A_1| > \frac{1}{2K}|A| \text{ and } |kA_1^k| \ll_k K^C|A|, \tag{1.16}$$

where $C = (8k+9)(k+1)+k$.

Proof. Fact 1.8 and the assumption that $|A^2| < K|A|$ imply

$$\sum_{x,x'\in A} |xA \cap x'A| > K^{-1}|A|^3.$$

Hence there is $\bar{x} \in A$ such that

$$\sum_{x\in A} |xA \cap \bar{x}A| > K^{-1}|A|^2.$$

Let

$$A_1 = \{x \in A : |xA \cap \bar{x}A| > \frac{|A|}{2K}\}. \tag{1.17}$$

Then Fact 1.5 implies

$$|A_1| > \frac{|A|}{2K}. \tag{1.18}$$

Claim. For all $k \geq 1$, for $y_1, y_2 \in A_1^k A_1^{-1}$,

$$|y_1A + y_2A| \ll_k K^c|A|,$$

where $c = 4k + 5$.

Proof of Claim. First, we do induction on k to show

$$|y_1A + y_2A| < 2^{2k}K^{4k+1}|A| \ , \text{ for all } y_1, y_2 \in A_1^k. \tag{1.19}$$

For $k = 1$. In Fact 1.7 we take $A_i = y_iA$ and $A_{i+2} = y_iA \cap \bar{x}A$ for $i = 1, 2$. Then

$$|A_i + A_{i+2}| \le |y_iA + y_iA| = |A + A| < K|A| \ , \quad \text{and} \quad |A_{i+2}| > \frac{|A|}{2K} \quad \text{for } i = 1, 2.$$

The last inequality is by (1.17). On the other hand,

$$|A_3 + A_4| \le |\bar{x}A + \bar{x}A| < K|A|.$$

Therefore, Fact 1.7 gives

$$|y_1A + y_2A| < 2^2K^5|A|.$$

For the general case, for $i = 1, 2$, let $y_i = x_ix_{i+2} \in A_1^k$ with $x_i \in A_1^{k-1}$ and $x_{i+2} \in A_1$. We use Fact 1.7 again by taking

$$A_i = y_iA = x_ix_{i+2}A, \quad \text{and} \quad A_{i+2} = y_iA \cap x_i\bar{x}A = x_i(x_{i+2}A \cap \bar{x}A).$$

Then similarly,

$$|A_i + A_{i+2}| < K|A| \ , \quad \text{and} \quad |A_{i+2}| = |x_{i+2}A \cap \bar{x}A| > \frac{|A|}{2K}.$$

On the other hand, by the induction hypothesis,

$$|A_3 + A_4| < |\bar{x}(x_1A + x_2A)| < 2^{2(k-1)}K^{4k-3}|A|.$$

Now, (1.19) follows from Fact 1.7.

To conclude the proof of the Claim, for $y_i \in A_1^kA_1^{-1}$, we write $y_i = x_ix_{i+2}^{-1}$ with $x_i \in A_1^k$ and $x_{i+2} \in A_1$, and observe that $|y_1A + y_2A| = |x_1x_4A + x_2x_3A|$ and use (1.19) for $x_1x_4, x_2x_3 \in A_1^{k+1}$. $\square$

Using Fact 1.6 for $B = A_1^k, A = A_1^{-1}$, we have

$$\chi_{A_1^k + A_1^k} \leq \frac{1}{|A_1|^2} \sum_{y_i \in A_1^{-1} A_1^k} \chi_{y_1 A_1 + y_2 A_1}.$$

(For any $a + b \in A_1^k + A_1^k$, there are $|A_1|^2$ many representations $(c^{-1}a)c + (d^{-1}b)d$ in $y_1 A_1 + y_2 A_1$.)

Hence

$$|A_1^k + A_1^k| \leq \frac{|A_1^{-1} A_1^k|^2}{|A_1|^2} |y_1 A_1 + y_2 A_1| < 2^{4k+14} K^{4k+4} K^{4k+5} |A|. \tag{1.20}$$

For the second inequality, we use Ruzsa's inequality and the bounds (1.15), (1.18) to see that

$$|A_1^{-1} A_1^k| \leq \left(\frac{|A_1^2|}{|A_1|} \right)^{k+1} |A_1| \leq \left(\frac{|A^2|}{|A_1|} \right)^{k+1} |A_1| \leq \left(\frac{K \cdot 2K |A_1|}{|A_1|} \right)^{k+1} |A_1|.$$

To see the second inequality in (1.16), again we apply Ruzsa's inequality (see the version stated before Lemma 1.2) to (1.20).

$$\begin{aligned} |kA_1^k| \leq |kA_1^k - A_1^k| &\leq \left(2^{4k+14} K^{8k+9} \frac{|A|}{|A_1^k|} \right)^{k+1} |A_1^k| \\ &\leq (2^{4k+14} K^{8k+9})^{k+1} (2K)^k |A|. \end{aligned}$$

In the last inequality, we use that $\frac{|A|}{|A_1^k|} < \frac{|A|}{|A_1|} < 2K$. □

Theorem 1.10. *Let $A \subset \mathbb{Z}_N$ with $|A| > N^{\varepsilon_0}$, $\varepsilon_0 > 0$, and $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Let $\varepsilon < \delta < \varepsilon_0$. Assume*

$$|2A| + |A^2| < N^{\varepsilon} |A|, \ \varepsilon > 0. \tag{1.21}$$

Let $m = \alpha_1 + \cdots + \alpha_r$. Then one of the following holds.

(a.) $|A| > N^{1 - c(\delta)\varepsilon}$, where $c(\delta)$ also depends on m.

(b.) $|A \cap a + (p)| > (2^3 N^{\varepsilon} p^{\delta})^{-1} |A|$ for some $a \in A$, and some prime $p|N$.

(c.) $|A \cap (p)| > (2r)^{-1}|A|$*, for some prime* $p|N$*.*

Proof of the Theorem.

Case 1. $|A \cap \mathbb{Z}_N^*| > \frac{1}{2}|A|$.

Proposition 1.9 provides $A_1 \subset (A \cap \mathbb{Z}_N^*)$ with

$$|A_1| > \frac{1}{2^3 N^\varepsilon}|A| \tag{1.22}$$

and

$$|kA_1^k| < N^{c\varepsilon}|A|, \text{ for all } k \tag{1.23}$$

where $c = c(k)$.

Case 1(a). $|\pi_p(A_1)| > p^\delta$ for all $p|N$.

Proposition 1.4 implies $kA_1^k = \mathbb{Z}_N$ for all $k \geq k(\delta, m)$. This together with (1.23), we have

$$N^{c\varepsilon}|A| > |kA_1^k| = N, \text{ for } k \geq k(\delta, m),$$

hence $|A| > N^{1-c(\delta)\varepsilon}$.

This is Case (a).

Case 1(b). $|\pi_p(A_1)| \leq p^\delta$ for some $p|N$.

Then there is $a \in \mathbb{Z}_p$ such that $|A_1 \cap \pi_p^{-1}(a)| \geq \frac{|A_1|}{p^\delta} > \frac{|A|}{2^3 N^\varepsilon p^\delta}$.

This is Case (b).

Case 2. $|A \cap \mathbb{Z}_N^*| \leq \frac{1}{2}|A|$.

Since more than half of the elements of A are zero divisors, we have $|\pi_p^{-1}(0)| \geq \frac{|A|}{2r}$ for some $p|N$. This is Case (c). □

Remark 1.11. Under assumption (1.21), Case (b) is equivalent to the following statement.

(b') there is $p|N$ such that

$$|\pi_p(A)| < N^d, \quad \text{for some } d = d(\delta) > 0.$$

It is clear that (b') implies (b) without additional assumptions. To see (b) and (1.21) imply (b'), first, we note that $|\pi_p(A)|\ |A \cap \pi_p^{-1}(a)| \leq |2A|$. Indeed, $2A$ contains $\{b_1 + y_1 P, \cdots, b_m + y_m p\} + \{a + x_1 p, \cdots, a + x_n p\}$, where $m = |\pi_p(A)|, n = |A \cap \pi_p^{-1}(a)|$, and b_j's are all distinct. Therefore $(b_j + y_j p) + (a + x_i p) = (b_m + y_m p) + (a + x_\ell p)$ implies that $b_j + a = b_m + a$. Hence $j = m$ and $i = \ell$.

By (1.21), $|\pi_p(A)|\ |A \cap \pi_p^{-1}(a)| < N^\varepsilon |A|$, which implies

$$|\pi_p(A)| < 2^3 N^{2\varepsilon} p^\delta < 2^3 N^{3\delta}. \tag{1.24}$$

Similarly for Case (c), under assumption (1.21), we have

$$|\pi_p(A)| < 2rN^\varepsilon < N^d, \tag{1.25}$$

if d satisfies $\frac{1}{2} N^{d-\varepsilon} > r$. Hence, in the statement of the Theorem, (b) and (c) can be replaced by (b').

Theorem 1.12. *Let $A \subset \mathbb{Z}_N$ with $|A| > N^{\varepsilon_0}$, $\varepsilon_0 > 0$, and $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Let $\varepsilon < \delta < \varepsilon_0$. Assume*

$$|2A| + |A^2| < N^\varepsilon |A|,\ \varepsilon > 0.$$

Let $m = \alpha_1 + \cdots + \alpha_r$ be bounded by a constant $\frac{1}{\alpha}$. Then one of the following holds.

(a.) $|A| > N^{1-c(\delta)\varepsilon}$, where $c = c(\delta)$ also depends on m.

(b'.) $|\pi_p(A)| < N^{c'(\delta)}$, for some prime $p|N$.

§2. A general estimate for mixed additive and multiplicative convolutions.

The goal of this section is to prove Proposition 2.1. (See also Remark 2.2.) For convenience, we will use the following notions which are different by a constant multiple from those in Section 1.

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

(2a.) $\hat{\mu}(\xi) = \sum_x \mu(x) e_q(x\xi)$,

(2b.) $\mu * \nu(x) = \sum_y \mu(x-y)\nu(y)$.

Then the following are easy to verify:

(2c.) $\mu(x) = \frac{1}{q}\sum_\xi \hat{\mu}(\xi) e_q(-x\xi)$,

(2d.) $\sum_\xi |\hat{\mu}(\xi)|^2 = q \sum_x |\mu(x)|^2$,

(2e.) If $\sum \mu(x) = 1$ and $\mu(x) \geq 0$, then $|\hat{\mu}(\xi)| \leq 1$ and $(\mu * \nu)(S) \leq \max_x \nu(x+S)$.

Let $R = \prod_j \mathbb{Z}_{q_j}$. Denote for $x \in R$,

$$e(x) = \prod_j e_{q_j}(x_j),$$

where $e_{q_j}(x_j) = \exp(\frac{2\pi i}{q_j} x_j)$. Then the above notions and properties still make sense.

Fact 2.1.1. Let $T = \{x \ : \ \phi(x) > \lambda\}$. Then $|T| < \frac{1}{\lambda}\phi(T) = \frac{1}{\lambda}\sum_{x \in T}\phi(x)$.

Proposition 2.1. *Let $R = \prod_j \mathbb{Z}_{q_j}$ be a commutative ring with $|R| = q$. Let μ be a probability measure on R. (i.e. $\sum \mu(x) = 1$ and $\mu \geq 0$.) Let $\varepsilon > 0$. Then one of the following alternatives hold:*

(i.) $\sum\limits_{\xi, y \in R} |\hat{\mu}(\xi)|^2 |\hat{\mu}(y\xi)|^2 \mu(y) < q^{-\varepsilon} \sum\limits_{\xi \in R} |\hat{\mu}(\xi)|^2$

(ii.) $\max\limits_{x \in R} \mu\big(x + (R \backslash R^*)\big) > cq^{-2\varepsilon}$

(iii.) *There is a subset $\bar{S}$ of R^* such that*

$$|\bar{S}|.\left(\sum |\hat{\mu}(\xi)|^2\right) < 10q^{1+\varepsilon}, \tag{2.2}$$

$$|\bar{S}+\bar{S}|+|\bar{S}.\bar{S}|<q^{C\varepsilon}|\bar{S}|, \tag{2.3}$$

$$\max_{x\in R}\mu(x+\bar{S})>q^{-C\varepsilon}, \tag{2.4}$$

where c, C are some constants $\big(cf.(2.15)\big)$.

Proof. We adapt the argument from [B-G-K]. We will use Balog-Szemeredi-Gowers Theorem in both multiplicative and additive forms to find a set $\bar{S}$ satisfying (iii) by assuming (i) and (ii) fail. Namely, we assume

$$\sum_{\xi,y}|\hat{\mu}(\xi)|^2|\hat{\mu}(y\xi)|^2\mu(y)>q^{-\varepsilon}\sum_{\xi}|\hat{\mu}(\xi)|^2, \tag{2.5}$$

and

$$\mu(R\backslash R^*)<\frac{1}{2}q^{-\varepsilon}. \tag{2.6}$$

Defining $\mu^-(x)=\mu(-x)$, we denote $\big($cf. (2c)$\big)$

$$\phi(x)=q(\mu*\mu^-)(x)=\sum_{\xi}|\hat{\mu}(\xi)|^2e(x\xi),\quad \phi(x)\geq 0. \tag{2.7}$$

Then

$$\sum_{x\in R}\phi(x)=q,\quad \text{and}\quad \phi(0)=\sum_{\xi}|\hat{\mu}(\xi)|^2=\max\phi(x) \tag{2.8}$$

Claim 1.

$$\sum_{\substack{x\in R\\ y\in R^*}}\phi(x)\phi(xy)\mu(y)>\frac{1}{2}q^{1-\varepsilon}\phi(0). \tag{2.9}$$

Proof of Claim 1. For y fixed, (2.7) gives

$$\sum_x\phi(x)\phi(xy)=\sum_{\xi,\eta}|\hat{\mu}(\xi)|^2|\hat{\mu}(\eta)|^2\sum_x e(x\eta+xy\xi)=q\sum_{\xi}|\hat{\mu}(\xi)|^2|\hat{\mu}(-y\xi)|^2.$$

Therefore, multiplying the above expression by $\mu(y)$ and summing over y, by (2.5) and (2e), the left-hand side of (2.9) is

$$\begin{aligned}\sum_y-\sum_{y\in R\backslash R^*}&>q\Big(q^{-\varepsilon}\sum_{\xi}|\hat{\mu}(\xi)|^2-\sum_{\xi}|\hat{\mu}(\xi)|^2\sum_{y\in R\backslash R^*}|\hat{\mu}(-y\xi)|^2\mu(y)\Big)\\ &>q\Big(q^{-\varepsilon}-\mu(R\backslash R^*)\Big)\sum|\hat{\mu}(\xi)|^2.\end{aligned}$$

Now Claim 1 follows from (2.6) and (2.8). □

Define the set

$$S = \{x \in R \ : \ \phi(x) > \frac{1}{10} q^{-\varepsilon} \phi(0)\}. \tag{2.10}$$

We have

$$\sum_{x \in S,\ y \in \mathbb{R}^*,\ xy \in S} \phi(x)\phi(xy)\mu(y) > \frac{1}{4} q^{1-\varepsilon} \phi(0). \tag{2.11}$$

Indeed, by (2.8)

$$\sum_{x \notin S} \phi(x)\phi(xy)\mu(y) \leq \frac{1}{10} q^{-\varepsilon}\phi(0) \sum_{x,y} \phi(xy)\mu(y) \leq \frac{1}{10} q^{1-\varepsilon}\phi(0).$$

Similarly,

$$\sum_{xy \notin S} \phi(x)\phi(xy)\mu(y) \leq \frac{1}{10} q^{1-\varepsilon}\phi(0).$$

Hence Claim 1 implies (2.11).

Claim 2.

$$\frac{1}{4} q^{1-\varepsilon}\phi(0)^{-1} < |S| < 10 q^{1+\varepsilon}\phi(0)^{-1}. \tag{2.12}$$

Proof of Claim 2.

$$|S| = \sum |S| \ \mu(y) \geq \sum_{y \in R^*} |S \cap y^{-1} S| \ \mu(y) > \frac{1}{4} q^{1-\varepsilon}\phi(0)^{-1}. \tag{2.13}$$

The last inequality is because of (2.11) and that, by (2.8), the left-hand-side of (2.11) is bounded above by $\phi(0)^2 \sum |S \cap y^{-1} S| \ \mu(y)$. On the other hand, Fact 2.1.1, (2.8) and (2.7) imply

$$|S| < 10 q^{\varepsilon} \phi(0)^{-1} \left[\sum_{x \in S} \phi(x) \right] \leq 10 q^{1+\varepsilon} \phi(0)^{-1}, \tag{2.14}$$

which is the upper bound on $|S|$ in Claim 2. □

Assuming moreover

$$\max_x \mu\big(x + (R \backslash R^*)\big) < \frac{1}{10^3} q^{-2\varepsilon}, \tag{2.15}$$

Claim 3.

$$|S\backslash R^*| < 10^{-2}q^{1-\varepsilon}\phi(0)^{-1}. \tag{2.16}$$

Proof of Claim 3. By (2.10), Fact 2.1.1, (2.7), (2e) and (2.15),

$$\begin{aligned}|S\backslash R^*| &\le 10q^{\varepsilon}\phi(0)^{-1}\Big[\sum_{x\in S\backslash R^*}\phi(x)\Big]\\ &= 10q^{1+\varepsilon}\phi(0)^{-1}(\mu*\mu^-)(S\backslash R^*)\\ &\le 10q^{1+\varepsilon}\phi(0)^{-1}\max_x \mu\big(x+(S\backslash R^*)\big)\\ &\le 10q^{1+\varepsilon}\phi(0)^{-1}\max_x \mu\big(x+(R\backslash R^*)\big) < 10^{-2}q^{1-\varepsilon}\phi(0)^{-1}. \quad \square\end{aligned}$$

Let

$$S^* = S\cap R^*$$

Then Claims 2 and 3 imply

$$|S^*| > 10^{-1}q^{1-\varepsilon}\phi(0)^{-1} > 10^{-2}q^{-2\varepsilon}|S|. \tag{2.17}$$

Write

$$S\cap y^{-1}S = (S^*\cap y^{-1}S^*)\cup\big(S^*\cap y^{-1}(S\backslash S^*)\big)\cup\big((S\backslash S^*)\cap y^{-1}S\big),$$

and note that, by Claim 3,

$$\sum_y |(S\backslash S^*)\cap y^{-1}S|\,\mu(y) \le |S\backslash R^*|\sum \mu(y) \le 10^{-2}q^{1-\varepsilon}\phi(0)^{-1}.$$

Similarly,

$$\sum_y |S^*\cap y^{-1}(S\backslash S^*)|\,\mu(y) \le 10^{-2}q^{1-\varepsilon}\phi(0)^{-1}.$$

Putting together with the second inequality of (2.13), we have

$$\sum_{y\in R^*}|S^*\cap y^{-1}S^*|\,\mu(y) > \frac{1}{20}q^{1-\varepsilon}\phi(0)^{-1}. \tag{2.18}$$

Defining

$$\Lambda = \{y \in R^* \ : \ |S^* \cap y^{-1} S^*| > \frac{1}{40} q^{1-\varepsilon} \phi(0)^{-1}\}. \tag{2.19}$$

Claim 4.

$$|\Lambda| > 10^{-7} q^{-5\varepsilon} |S|. \tag{2.20}$$

Proof of Claim 4. Claim 2 imply

$$|S^*| \ \mu(\Lambda) = |S^*| \sum_{y\in\Lambda} \mu(y) \geq \sum_{y\in\Lambda} |S^* \cap y^{-1}S^*| \ \mu(y) > \frac{1}{40} q^{1-\varepsilon}\phi(0)^{-1} > 10^{-3} q^{-2\varepsilon} |S|.$$

The second inequality is because of (2.18) and that, by (2.19), $\sum_{y\notin\Lambda} < \frac{1}{40} q^{1-\varepsilon}\phi(0)^{-1}$. Therefore, Cauchy-Schwartz, (2d) and (2.8) give

$$\begin{aligned} 10^{-3} q^{-2\varepsilon} < \mu(\Lambda) &\leq |\Lambda|^{1/2} \Big(\sum \mu(x)^2 \Big)^{1/2} \\ &= \Big(\frac{|\Lambda|}{q} \Big)^{1/2} \Big(\sum |\hat{\mu}(\xi)|^2 \Big)^{1/2} = \Big(\frac{|\Lambda| \ \phi(0)}{q} \Big)^{1/2}. \end{aligned} \tag{2.21}$$

Namely,

$$|\Lambda| \ \phi(0) > 10^{-6} q^{1-4\varepsilon}. \tag{2.22}$$

The Claim follows from (2.12). □

Consequently, (by shrinking Λ, if necessary) there is $\Lambda \subset R^*$, with $|S^*| \geq |\Lambda| > 10^{-7} q^{-5\varepsilon} |S^*|$ such that for any $y \in \Lambda$,

$$|S^* \cap y^{-1} S^*| > 10^{-3} q^{-2\varepsilon} |S^*|.$$

We will use the multiplicative form of the following refinement of Balog-Szemerédi-Gowers Theorem. (See [T-V].)

Theorem BSG'. *Let A, B be finite sets with $|A| \geq |B|$ and let $G \subset A \times B$ with $|G| > K^{-1}|A|^2$. Denote*

$$A \overset{G}{+} B = \{a + b \ : \ (a,b) \in G\}.$$

If $|A \overset{G}{+} B| < K|A|$, *then there are subsets* $A' \subset A$, *and* $B' \subset B$ *such that*

$$|A' + A'| + |B' + B'| + |A' + B'| < K^c|B|$$

and

$$|(A' \times B') \cap \mathcal{G}| > K^{-c}|A|^2,$$

where c *is an absolute constant.*

For the convenience of the readers, we give the deduction of Theorem BSG' from the usual statement of the Balog-Szemerédi-Gowers Theorem in the Appendix.

We take $G = \{(x, y) \ : \ y \in \Lambda, x \in S^* \cap y^{-1}S^*\} \subset \Lambda \times S^*$ in Theorem BSG'. Keeping in mind that $|G| > 10^{-7}q^{-5\varepsilon}|S^*| \cdot 10^{-3}q^{-2\varepsilon}|S^*|$, and $|A \overset{G}{.} A| \leq |S^*|$, we obtain from Theorem BSG' a subset $S_1 \subset S^* \subset S$ satisfying

$$|S_1| > q^{-C_1\varepsilon}|S^*| > q^{-(C_1+2)\varepsilon}|S| \tag{2.23}$$

$$|S_1.S_1| < q^{C_1\varepsilon}|S_1|. \tag{2.24}$$

Next, we pass to the additive property.

Claim 5.

$$\sum_{x_1, x_2 \in S_1} \phi(x_1 - x_2) > 10^{-2}q^{-2\varepsilon}\phi(0)|S_1|^2. \tag{2.25}$$

Proof of Claim 5. Since $S_1 \subset S$, from (2.10), (2.7), and (2b),

$$q \sum_{x \in S_1} \sum_y \mu(x + y)\mu(y) > \frac{1}{10}q^{-\varepsilon}\phi(0)|S_1|$$

and hence Cauchy-Schwartz, (2d) and (2.8) imply

$$\begin{aligned} \sum_y \big[\sum_{x \in S_1} \mu(x + y)\big]^2 &> \frac{\big(10^{-1}q^{-1-\varepsilon}\phi(0)|S_1|\big)^2}{\sum \mu(y)^2} \\ &= 10^{-2}q^{-1-2\varepsilon}\phi(0)|S_1|^2. \end{aligned} \tag{2.26}$$

The left-hand-side of (2.26) is $\sum_{x_1,x_2\in S_1}\sum_y \mu(x_1+y)\mu(x_2+y)$, which by (2.7), is $q^{-1}\sum_{x_1,x_2\in S_1}\phi(x_1-x_2)$. □

Define

$$S' = \{x \in R\ : \phi(x) > 10^{-3}q^{-2\varepsilon}\phi(0)\}. \tag{2.27}$$

Then Fact 2.1.1, (2.8), (2.12) and (2.23) imply

$$|S'| < 10^3 q^{1+2\varepsilon}\phi(0)^{-1} < 10^4 q^{3\varepsilon}|S| < 10^4 q^{(5+C_1)\varepsilon}|S_1|.$$

Let

$$G = \{(x_1,-x_2) \in S_1 \times (-S_1)\ :\ x_1 - x_2 \in S'\}.$$

Then (2.8), Claim 5 and (2.27) imply

$$\begin{aligned}|G|\ \phi(0) &\geq \sum_{(x_1,-x_2)\in G}\phi(x_1-x_2)\\ &\geq \sum_{x_1,x_2\in S_1}\phi(x_1-x_2) - \sum_{(x_1,-x_2)\notin G}\phi(x_1-x_2)\\ &> (10^{-2}-10^{-3})q^{-2\varepsilon}\phi(0)|S_1|^2.\end{aligned}$$

Hence

$$|G| > 10^{-3}q^{-2\varepsilon}|S_1|^2. \tag{2.28}$$

Another application of Theorem BSG' (in additive form) yields $\bar{S} \subset S_1$ satisfying

$$|\bar{S}| > q^{-C_2\varepsilon}|S_1| \tag{2.29}$$

$$|\bar{S}+\bar{S}| < q^{C_2\varepsilon}|\bar{S}|. \tag{2.30}$$

Recalling also (2.23), (2.24), the set $\bar{S} \subset R^*$ satisfies thus

$$|\bar{S}| > q^{-(C_1+C_2+2)\varepsilon}|S| \tag{2.31}$$

$$|\bar{S}+\bar{S}| < q^{C_2\varepsilon|}\bar{S}| \tag{2.32}$$

$$|\bar{S}.\bar{S}| < q^{(C_1+C_2)\varepsilon}|\bar{S}|. \tag{2.33}$$

Note that (2.32) and (2.33) are (2.3). $\bar{S}$ satisfies (2.2), because $\bar{S} \subset S$, and (2.12) and (2.8) give

$$|\bar{S}| \leq |S| < 10 \frac{q^{1+\varepsilon}}{\sum |\hat{\mu}(\xi)|^2} \, . \tag{2.34}$$

For (2.4), by (2e), it suffices to see $(\mu * \mu^-)(\bar{S}) > q^{-C\varepsilon}$. By (2.7), this is the same as $\phi(\bar{S}) > q^{1-C\varepsilon}$. Fact 2.1.1, (2.10), (2.31), and (2.12) give

$$\phi(\bar{S}) > \frac{1}{10} q^{-\varepsilon} \phi(0) \, |\bar{S}| > \frac{1}{10} q^{-\varepsilon} \phi(0) \cdot q^{-(C_1+C_2+2)\varepsilon} |S| > q^{1-(C_1+C_2+5)\varepsilon}.$$

Summarizing, recall assumptions (2.6), (2.15), we showed that if (i) fails, then there exists $\bar{S}$ satisfying (2.2)-(2.4). This proves the proposition. □

Remark 2.2. The statement of Proposition 2.1 is still true for a commutative ring R such that (2a)-(2e) hold.

§3. Estimation of the Fourier transform of measures associated to iterated product sets.

In this section we will prove a technical theorem which relates sum-product theorem and the exponential sum estimates.

Fact 3.1.1. If $\sum a_i = 1$, then $(\sum A_i a_i)^r \leq \sum A_i^r a_i$. A special case is $(\frac{\sum_{i=1}^n A_i}{n})^2 \leq \frac{\sum A_i^2}{n}$, for $A_1, \cdots, A_n \in \mathbb{R}$.

Proof. Use Hőlder inequality on $\sum (A_i a_i^{\frac{1}{r}}) \, a_i^{\frac{r-1}{r}}$.

Theorem 3.1. *Let $R = \prod_j \mathbb{Z}_{q_j}$ be a commutative ring with $|R| = q$ and let $A \subset R^*$ with $|A| = q^\delta$ for $0 < \delta \leq 1$. Assume there exist $0 < \kappa_0, \kappa_1 < \frac{\delta}{20}$ such that the following properties hold*

(i.) $\max_x \left|A \cap \left(x + (R \backslash R^*)\right)\right| < q^{-\kappa_0}|A|$.

(ii.) $\max_x \left|A \cap (x + S)\right| < q^{-\kappa_0}|A|$, *whenever $S \subset R^*$ satisfies*

(a.) $|S| < q^{1-\kappa_1}$,

(b.) $|S+S| + |S.S| < q^{\kappa_0}|S|$.

Denote μ_k *the probability measure on* R

$$\mu_k = |A|^{-k} \sum_{x_1,\dots,x_k \in A} \delta_{x_1 \dots x_k}, \tag{3.2}$$

where δ_z *is the Dirac measure at* $z \in R$.

Then there is $k = k(\kappa_0)$ *and* $\varepsilon = \varepsilon(\kappa_0)$ *such that*

$$\max_{\xi \in R^*} |\hat{\mu}_k(\xi)| < q^{-\varepsilon}. \tag{3.3}$$

Proof. We again follow essentially [B-G-K].

The following can be checked straightforwardly from (3.2). $\big($Use (3a) and Fact 3.1.1 for (3b).$\big)$

(3a.) $\hat{\mu}_{k+\ell}(\xi) = \sum_y \hat{\mu}_k(y\xi)\mu_\ell(y)$.

(3b.) $\sum_\xi |\hat{\mu}_{k+l}(\xi)|^s \le \sum_\xi |\hat{\mu}_k(\xi)|^s$, and $|\hat{\mu}_k(\xi)| \le 1$.

We denote $\nu^-(x) = \nu(-x)$ and $\nu^{(r)}$ the r-fold convolution of ν. Then

(3c.) $(\nu * \nu^-)^{(r)}(z) = \sum_{y_1 - y_2 + \dots - y_{2r} = z} \nu(y_1)\nu(y_2)\cdots\nu(y_{2r})$.

Define for $k \in \mathbb{Z}_+$, and $\varepsilon > 0$ the set

$$\Omega_{k,\varepsilon} = \{\xi \in R \ : \ |\hat{\mu}_k(\xi)| > q^{-\varepsilon}\}. \tag{3.4}$$

Claim 1. If $\xi \in \Omega_{2k,\varepsilon}$, then

$$\sum_{z,\xi} |\hat{\mu}_{2k}(\xi)|^{4r} |\hat{\mu}_k(z\xi)|^{4r} (\mu_k * \mu_k^-)^{(r)}(z) > q^{-12\varepsilon r^2} |\Omega_{2k,\varepsilon}|. \tag{3.5}$$

Proof of Claim 1. For $\xi \in \Omega_{2k,\varepsilon}$, (2a) and (3a) imply

$$\sum\nolimits_x \big| \sum\nolimits_y e_q(xy\xi)\mu_k(y) \big| \mu_k(x) > q^{-\varepsilon}$$

and hence for $r \in \mathbb{Z}_+$, by Fact 3.1.1,

$$\sum\nolimits_x \big| \sum\nolimits_y e_q(xy\xi)\mu_k(y) \big|^{2r} \mu_k(x) > q^{-2\varepsilon r}. \tag{3.6}$$

By (2a) and (3c), the left-hand side of (3.6) equals

$$\sum_{y_1,\cdots,y_{2r}} \hat{\mu}_k\big((y_1 - y_2 + \cdots - y_{2r})\xi\big)\mu_k(y_1)\cdots\mu_k(y_{2r}) = \sum_z \hat{\mu}_k(z\xi)(\mu_k * \mu_k^-)^{(r)}(z).$$

Therefore, by Fact 3.1.1 again,

$$\sum_z |\hat{\mu}_k(z\xi)|^{4r} (\mu_k * \mu_k^-)^{(r)}(z) > q^{-8\varepsilon r^2}. \tag{3.7}$$

The Claim follows from multiplying (3.7) with

$$|\hat{\mu}_{2k}(\xi)|^{4r} > (q^{-\varepsilon})^{4r} > q^{-4\varepsilon r^2},$$

and summing over $\xi \in \Omega_{2k,\varepsilon}$. □

Define $\delta_{k,r}$ such that

$$\sum\nolimits_\xi |\hat{\mu}_k(\xi)|^{4r} = q^{1-\delta_{k,r}}. \tag{3.8}$$

Then

(3*d*.) $\delta_{1,1} > \delta$,

(3*e*.) $\delta_{k,r}$ is an increasing function in both k and r.

In fact, (3d) follows from the following observation

$$q^{1-\delta_{1,1}} = \sum |\hat{\mu}_1(\xi)|^4 \leq \sum |\hat{\mu}_1(\xi)|^2 = q \sum \mu_1(x)^2 = \frac{q}{|A|} = q^{1-\delta},$$

while (3e) follows from (3b).

We want to apply Proposition 2.1 with

$$\mu = \frac{1}{2}[(\mu_k * \mu_k^-)^{(r)} + (\mu_{2k} * \mu_{2k}^-)^{(r)}]. \tag{3.9}$$

By Fact 3.1.1,

$$\textstyle\sum_\xi |\hat{\mu}(\xi)|^2 = \displaystyle\sum_\xi \left(\frac{|\hat{\mu}_k(\xi)|^{2r} + |\hat{\mu}_{2k}(\xi)|^{2r})}{2}\right)^2 \leq \frac{1}{2}\textstyle\sum_\xi (|\hat{\mu}_k(\xi)|^{4r} + |\hat{\mu}_{2k}(\xi)|^{4r}). \tag{3.10}$$

Hence, together with (3b) and (3.8), we have

$$\frac{1}{4}q^{1-\delta_{k,r}} < \sum |\hat{\mu}(\xi)|^2 \leq q^{1-\delta_{k,r}}. \tag{3.11}$$

Claim 2. Alternatives 2.1.(ii) and 2.1.(iii) in Proposition 2.1 cannot hold under assumptions 3.1.(i) and 3.1.(ii), if

$$C\kappa = \kappa_0. \tag{3.12}$$

and

$$\delta_{k,r} < 1 - \frac{\delta}{10} \tag{3.13}$$

Proof of Claim 2. First, it is clear that (3.13) and the assumption that $\kappa_0, \kappa_1 < \frac{\delta}{20}$ imply

$$\kappa_0 < 1 - \kappa_1 - \delta_{k,r}. \tag{3.14}$$

Then (3.14) and (3.12) imply

$$\kappa < \kappa_0 < 1 - \kappa_1 - \delta_{k,r}. \tag{3.15}$$

Next we observe that by (2e), if $S \subset R$, and μ is introduced as in (3.9), then

$$\begin{aligned} \mu(S) &\leq \frac{1}{2}\max_{x\in R}(\mu_k + \mu_{2k})(x + S) \\ &\leq \max_{x\in R, y\in R^*} \mu_1(x + yS). \end{aligned} \tag{3.16}$$

Note that $y(R\backslash R^*) = R\backslash R^*$. Also, if S satisfies (2.2) and (2.3), so does yS. In order to rule out 2.1.(ii), and (2.4) in 2.1.(iii), we need thus to assume

$$\max_{x\in R} \mu_1\big(x + (R\backslash R^*)\big) = \max_{x\in R} \frac{A\cap (x + (R\backslash R^*)|}{|A|} < cq^{-2\kappa} \tag{3.17}$$

and

$$\max_{x\in R} \mu_1(x + S) = \max_{x\in R} \frac{A\cap (x + S)|}{|A|} < q^{-C\kappa} \tag{3.18}$$

whenever $S \subset R^*$ satisfies

$$|S| < \Big(\sum |\hat{\mu}(\xi)|^2\Big)^{-1} 10q^{1+\varepsilon} < \big(\frac{1}{4}q^{1-\delta_{k,r}}\big)^{-1} 10q^{1+\kappa} < q^{\kappa+\delta_{k,r}} \tag{3.19}$$

and

$$|S + S| + |S.S| < q^{C\kappa}|S|. \tag{3.20}$$

(The equalities in (3.17) and (3.18) are by the definition of μ_1.)

(3.17) holds because of (3.12) and 3.1.(i). For $S \subset R^*$ satisfies (3.19) and (3.20), (3.15) and (3.12) imply that S satisfies 3.1.(ii)(a) and 3.1.(ii)(b). Therefore, (3.18) holds because of assumption 3.1.(ii). □

Claim 3. Assuming (3.12) and (3.13), we take $\varepsilon = \frac{\kappa}{100r^2}$, and let

$$\bar{r} = \left[\frac{1}{\varepsilon}\right]. \tag{3.21}$$

Then

$$\delta_{2k,\bar{r}} > \delta_{k,r} + \frac{\kappa}{4}. \tag{3.22}$$

Proof of Claim 3. Under the assumptions, Claims 1, 2, Proposition 2.1 and (3.10) imply

$$q^{-\kappa} \sum |\hat{\mu}(\xi)|^2 > \sum |\hat{\mu}(\xi)|^2 |\hat{\mu}(y\xi)|^2 \mu(y) > 2^{-5} q^{-12\varepsilon r^2} |\Omega_{2k,\varepsilon}|. \tag{3.23}$$

By (3.11), this is

$$|\Omega_{2k,\varepsilon}| < 2^5 q^{1-\delta_{k,r}-\kappa+12\varepsilon r^2}. \tag{3.24}$$

With ε as chosen, for q large, we have

$$|\Omega_{2k,\varepsilon}| < q^{1-\delta_{k,r}-\frac{\kappa}{2}} \tag{3.25}$$

Let $\bar{r}$ be as in (3.21). Then

$$\begin{aligned} q^{1-\delta_{2k,\bar{r}}} = \sum_{\xi} |\hat{\mu}_{2k}(\xi)|^{4\bar{r}} &\leq \sum_{\xi} |\hat{\mu}_{2k}(\xi)|^{2\bar{r}} \\ &= \sum_{\xi\in\Omega_{2k,\varepsilon}} + \sum_{\xi\notin\Omega_{2k,\varepsilon}} \\ &\leq |\Omega_{2k,\varepsilon}| + q\cdot q^{-\varepsilon\cdot 2\bar{r}} < q^{1-\delta_{k,r}-\frac{\kappa}{4}}. \qquad \square \end{aligned}$$

Returning to conditions (3.12), (3.13) and assumptions 3.1.(i), 3.1.(ii) assume thus

$$\delta_{2k,\bar{r}} > \delta_{k,r} + \bar{c}\kappa_0 \tag{3.26}$$

with

$$\bar{r} < \bar{C}\frac{r^2}{\kappa_0}. \tag{3.27}$$

Starting from $k = 1, r = 1$, assuming $\delta_{1,1} < 1 - \frac{\delta}{10}$, we perform an iteration based on (3.26), (3.27), until

$$\delta_{2^{s'},r_{s'}} > 1 - \frac{\delta}{10}. \tag{3.28}$$

We obtain

$$\delta_{2^s,r_s} > \delta_{2^{s-1},r_{s-1}} + \bar{c}\kappa_0 \tag{3.29}$$

$$r_s < \bar{C}\,\frac{r_{s-1}^2}{\kappa_0}. \tag{3.30}$$

Hence,

$$\delta_{2^s,r_s} > \delta_{2^{s-1},r_{s-1}} + \bar{c}\kappa_0 > \bar{c}s\kappa_0 \tag{3.31}$$

$$r_s < \bar{C}\frac{r_{s-1}^2}{\kappa_0} < \left(\frac{\bar{C}}{\kappa_0}\right)^{2^s} \tag{3.32}$$

$$s' < \bar{C}\kappa_0^{-1} \tag{3.33}$$

$$r_{s'} < \exp\exp\frac{\bar{C}}{\kappa_0}. \tag{3.34}$$

Denoting $k' = 2^{s'}, r' = r_{s'}$, we obtained that

$$\sum_\xi |\hat{\mu}_{k'}(\xi)|^{4r'} < q^{\delta/10}. \tag{3.35}$$

It follows from (3a), Fact 3.1.1, and (3b), that for all $\xi_0 \in R^*$ and $k > k'$,

$$\begin{aligned} |\hat{\mu}_k(\xi_0)|^{4r'} &\leq \frac{1}{|A|} \sum_{x\in A} |\hat{\mu}_{k-1}(x\xi_0)|^{4r'} \\ &\leq \frac{1}{|A|} \sum_\xi |\hat{\mu}_{k-1}(\xi)|^{4r'} \\ &\leq q^{-\delta} \sum_\xi |\hat{\mu}_{k'}(\xi)|^{4r'} < q^{-\frac{9}{10}\delta}. \end{aligned} \tag{3.36}$$

Hence

$$|\hat{\mu}_k(\xi_0)| < q^{-\varepsilon}.$$

with

$$k < \exp \bar{C}/\kappa_0 \tag{3.37}$$

$$\varepsilon = \frac{\delta}{5r'} > \left(\exp\exp\frac{\bar{C}}{\kappa_0}\right)^{-1}. \tag{3.38}$$

This proves the theorem. □

Define for $k \in \mathbb{Z}_+$

$$S_k(\xi, A) = \sum_{x_1,\dots,x_k\in A} e_q(x_1\dots x_k\xi). \tag{3.39}$$

Thus

$$|A|^{-k}\, S_k(\xi, A) = \hat{\mu}_k(\xi)$$

We conclude

Theorem 3.2. *Let* $R = \prod_j \mathbb{Z}_{q_j}$ *be a commutative ring with* $|R| = q$ *and let* $A \subset R^*$ *with* $|A| = q^\delta$ *for* $0 < \delta \leq 1$. *Assume there exist* $0 < \kappa_0, \kappa_1 < \frac{\delta}{20}$ *such that the following properties hold*

$(i.)$ $\max_x \big|A \cap \big(x + (R\backslash R^*)\big)\big| < q^{-\kappa_0}|A|$.

$(ii.)$ $\max_x \big|A \cap (x + S)\big| < q^{-\kappa_0}|A|$, *whenever* $S \subset R^*$ *satisfies*

$(a.)$ $|S| < q^{1-\kappa_1}$,

$(b.)$ $|S + S| + |S.S| < q^{\kappa_0}|S|$.

Then there is $k = k(\kappa_0)$ *and* $\varepsilon = \varepsilon(\kappa_0)$ *such that*

$$\max_{\xi \in R^*} |S_k(\xi, A)| < |A|^k q^{-\varepsilon}. \tag{3.40}$$

§4. Exponential sum estimates on $\mathbb{Z}^q$ and Heilbronn type sums.

Let $q = \prod_{\alpha=1}^{\beta} p_\alpha^{\nu_\alpha} \in \mathbb{Z}^+$. We say q has *few prime factors*, if $\sum_{\alpha \leq \beta} \nu_\alpha < C_0$ for some constant C_0.

We will use Theorem 1.12 which characterize subsets of $\mathbb{Z}_q$ with small sum product set.

Observe also that $\mathbb{Z}_q\backslash\mathbb{Z}_q^* = \bigcup_\alpha \pi_{p_\alpha}^{-1}(0)$.

Theorem 4.1. *Let* $q \in \mathbb{Z}_+$ *have few prime factors and* $A \subset \mathbb{Z}_q$, $|A| = q^\delta$. *Assume*

$$\max_{p|q, t \in \mathbb{Z}_p} |A \cap \pi_p^{-1}(t)| < q^{-\gamma}|A| \tag{4.1}$$

with $0 < \gamma < \frac{\delta}{25}$.

Then for $k > k(\gamma), \varepsilon = \varepsilon(\gamma)$

$$\max_{\xi \in \mathbb{Z}_q^*} |S_k(\xi, A)| < |A|^k q^{-\varepsilon}. \tag{4.2}$$

Proof. We will use Theorem 3.2. Assume 3.2.(i) fails. Since the number of prime factors is bounded by C_0, there is $p|q$ such that (4.1) fails. Assume 3.2.(ii) fails. Namely, there exists $S \subset R^*$ satisfying 3.2.(ii) (a) and (b), and

$$\max_x \big|A \cap (x+S)\big| > q^{-\kappa_0}|A|. \tag{4.3}$$

Theorem 1.12 and 3.2.(ii)(a), (b) imply that

$$|\pi_{p_\alpha}(S)| < q^{\kappa_0'} \text{ for some } \alpha, \tag{4.4}$$

and $\kappa_0' = \kappa_0'(\kappa_0)$.

Hence (4.3) and (4.4) give

$$\max_{t,\alpha} |A \cap \pi_{p_\alpha}^{-1}(t)| > q^{-\kappa_0 - \kappa_0'}|A|. \tag{4.5}$$

Take κ_0 such that

$$\kappa_0 + \kappa_0' < \gamma \tag{4.6}$$

and $\kappa_1 = \kappa_0' < \frac{\delta}{50}$. Then, by (4.1), Theorem 3.2(ii) will hold and Theorem 3.2 applies.

□

The following Corollary is immediate.

Corollary 4.2. *Let $q \in \mathbb{Z}_+$ have few prime factors, and let $H < \mathbb{Z}_q^*$ be a subgroup with $|H| = q^\delta$ and*

$$\min_{p|q} |\pi_p(H)| > q^{\delta'}. \tag{4.7}$$

Then

$$\max_{\xi \in \mathbb{Z}_q^*} \Big|\sum_{x\in H} e_q(\xi x)\Big| < |H|q^{-\varepsilon} \tag{4.8}$$

with $\varepsilon = \varepsilon(\delta')$.

Indeed, if $p|q$ and $H_p := \pi_p(H) < \mathbb{Z}_p^*$, then

$$|(\pi_p|_H)^{-1}(t)| = \frac{|H|}{|H_p|} \tag{4.9}$$

for all $t \in H_p$ and we may take $\gamma = \delta'$ in (4.1). Also,

$$S_k(\xi, H) = |H|^{k-1} \sum_{x \in H} e_q(x\xi).$$

Of course, (4.7) already presumes that $\log p \sim \log q$, if $p|q$.

Considering in particular Gauss sums, we get:

Corollary 4.3. *Let $q = \prod_\alpha p_\alpha^{\nu_\alpha}$ have few prime factors and $k \in \mathbb{Z}_q$ satisfy*

$$(k, p_\alpha - 1) < (p_\alpha - 1)q^{-\delta} \text{ for all } \alpha, \text{ for some } \delta. \tag{4.10}$$

Then

$$\max_{\xi \in \mathbb{Z}_q^*} \left| \sum_{x=0}^{q-1} e_q(\xi x^k) \right| < q^{1-\delta'} \tag{4.11}$$

where $\delta' = \delta'(\delta, C_0)$.

Proof. First we note that (4.10) implies $p_\alpha > q^\delta$ for all α.

Consider first $x \in \mathbb{Z}_q \backslash \mathbb{Z}_q^*$. Thus the contribution to the exponential sum is at most

$$|\mathbb{Z}_q \backslash \mathbb{Z}_q^*| = \prod_{\alpha=1}^{\beta} p_\alpha^{\nu_\alpha} - \prod_{\alpha=1}^{\beta} (p_\alpha - 1) p_\alpha^{\nu_\alpha - 1} < q\Big(\sum_{\alpha=1}^{\beta} \frac{1}{p_\alpha}\Big) < \beta q^{1-\delta}. \tag{4.12}$$

The last inequality is because of (4.10).

For $p|q$, let

$$H = \{x^k \ : \ x \in \mathbb{Z}_q^*\} < \mathbb{Z}_q^*.$$

Since $\pi_p(H) = \{x^k \ : \ x \in \mathbb{Z}_p^*\}$, (4.10) implies

$$|\pi_p(H)| = \frac{p-1}{(k, p-1)} > q^\delta.$$

Corollary 4.2 gives

$$\Big|\sum_{y\in H} e_q(\xi y)\Big| < |H| q^{-\varepsilon(\delta)}. \tag{4.13}$$

Hence

$$\big|\sum_{x\in\mathbb{Z}_q^*} e_q(\xi x^k)\big| = \frac{|\mathbb{Z}_q^*|}{|H|}\,\big|\sum_{y\in H} e_q(\xi y)\big| < \frac{q}{|H|}\,|H| q^{-\varepsilon(\delta)} = q^{1-\varepsilon(\delta)} \tag{4.14}$$

Putting together (4.12) and (4.14), we see that the left-hand side of (4.11) is bounded by $\beta q^{1-\delta} + q^{1-\varepsilon(\delta)}$. □

A particular application of Corollary 4.3 with $q = p^2$ is Heilbronn's exponential sum

$$\sum_{x=1}^{p} e_{p^2}(\xi x^p). \tag{4.15}$$

A nontrivial bound on (4.15) was first established in [H-B] and later improved in [H-B-K] (both arguments are based on Stepanov's method). We apply Corollary 4.3 with $k = p$ and observe that for $x, y \in \mathbb{Z}$

$$(x + py)^p \equiv x^p \pmod{p^2}$$

and hence it suffices in (4.11) to consider the restricted sum (4.15).

More generally, we may take $k = p^{m-1}, q = p^m$ (where $m < C_0$), and note that

$$\sum_{x=1}^{p^m} e_{p^m}(\xi x^{p^{m-1}}) = p^{m-1}\sum_{x=1}^{p} e_{p^m}(\xi x^{p^{m-1}})$$

Applying Corollary 4.3, we get (cf. [O]):

Corollary 4.4.

$$\max_{(\xi,p)=1}\big|\sum_{x=1}^{p} e_{p^m}(\xi x^{p^{m-1}})\big| < p^{1-\delta_m} \tag{4.16}$$

for some $\delta_m > 0$ and p large enough.

Theorem 4.1 applies to more general structures and we get in particular bounds on sums of the form

$$\sum_{s=1}^{t} e_q(a\theta^s)$$

with $\theta \in \mathbb{Z}_q^*$ (cf. [B-G-K], [B]). Considering condition (4.1) with

$$A = \{\theta^s \ : \ s = 1, \dots, t\} \subset \mathbb{Z}_q^*.$$

Clearly for $p|q$,

$$\pi_p(\theta^s) = \pi_p(\theta^{s'})$$

if and only if

$$\mathrm{o}rd_p(\theta)|\ (s - s'),$$

where $\mathrm{o}rd_p(\theta)$ denotes the multiplicative order of θ mod p. Therefore,

$$|\pi_p(A)| \geq \min\{t, \mathrm{o}rd_p(\theta)\}, \tag{4.17}$$

and we have

Corollary 4.5. *Let $q = \prod_\alpha p_\alpha^{\nu_\alpha}$ have few prime factors, and $\theta \in \mathbb{Z}_q^*$ such that*

$$\mathrm{o}rd_p(\theta) > q^\delta \text{ for all } p|q. \tag{4.18}$$

Then, for $t > q^\delta$

$$\max_{\xi \in \mathbb{Z}_q^*} \left| \sum_{s=1}^{t} e_q(\xi\theta^s) \right| < t^{1-\varepsilon}. \tag{4.19}$$

Proof. The assumptions and (4.17) imply

$$|\pi_p(A)| > q^\delta. \tag{4.20}$$

Since the elements of A are distributed evenly among the fibers of π_p, (4.20) implies inequality (4.1). The corollary follows from Theorem 4.1. □

Remark 4.6. In (4.8) (see Corollary 4.2) and (4.11) (see Corollary 4.3), one may take $\xi \in \mathbb{Z}_q \setminus \{0\}$. In fact, the assumption in Corollary 4.2 obviously carries over to $\pi_{q'}(H) < \mathbb{Z}_{q'}^*$ for any nontrivial divisor q' of q.

Corollary 4.2 may actually be formulated in the stronger form.

Theorem 4.7. *Let $q \in \mathbb{Z}_+$ have few prime factors and let $H < \mathbb{Z}_q^*$ satisfy $|H| = q^\delta$. Then*

$$\max_{\xi \in \mathbb{Z}_q^*} \Big| \sum_{x \in H} e_q(\xi x) \Big| < q^{-\varepsilon} |H|. \tag{4.21}$$

where $\varepsilon > 0$ depends on the numbers of prime factors of q and $\delta > 0$ only.

Similarly in Corollary 4.3, it suffices to assume that

$$\big(k, \phi(q)\big) < q^{-\delta} \phi(q), \tag{4.22}$$

where $\phi(q) = \prod_\alpha p_\alpha^{\nu_\alpha - 1}(p_\alpha - 1)$, and in Corollary 4.5 that $\mathrm{ord}_q(\theta) > q^\delta$, provided we take $t = \mathrm{ord}_q(\theta)$ in (4.19).

Note that for incomplete sums, i.e. $t < \mathrm{ord}_q(\theta)$ in Corollary 4.5, the stronger assumption (4.18) is still necessary. As an example, take

$$q = p^2, \text{ and } \theta = 1 + p.$$

Then $\mathrm{ord}_q(\theta) = p$ but letting $t = [\frac{p}{10}]$,

$$\Big| \sum_{s=1}^t e_{p^2}(\theta^s) \Big| = \Big| \sum_{s=1}^t e_p(s) \Big| \sim t. \tag{4.23}$$

Proof of Theorem 4.7.

Let $q = \prod_{\alpha \in I} p_\alpha^{\nu_\alpha}$ with $\nu_\alpha \geq 1$ and denote $q' = \prod_{\alpha \in I} p_\alpha$.

Claim. If $\pi_{q'}|_H$ is not one-to-one. then

$$\sum_{x\in H} e_q(\xi x) = 0 \text{ for all } \xi \in \mathbb{Z}_q^*. \tag{4.24}$$

Proof of Claim. Under the assumption, there is a nontrivial subgroup H' of H such that $\pi_{q'}(H') = \{1\}$. Since $\mathbb{Z}_q^* \simeq \prod(\mathbb{Z}_{p_\alpha^{\nu_\alpha - 1}} \times \mathbb{Z}_{p_\alpha - 1})$, H' has to be a subgroup of $\prod_{\nu_\alpha \geq 2} \mathbb{Z}_{p_\alpha^{\nu_\alpha - 1}}$. Therefore there is a further nontrivial subgroup H'' of H' of order p_α for some $\alpha \in I$, with $\nu_\alpha \geq 2$. Hence H'' is of the form

$$H'' = \left\{1 + y\,\frac{q}{p_\alpha}\ :\ y = 0, 1, \cdots, p_\alpha - 1\right\} \tag{4.25}$$

and for $\xi \in \mathbb{Z}_q^*$, we have

$$\left|\sum_{x\in H''} e_q(\xi x)\right| = \left|\sum_{y=0}^{p_\alpha - 1} e_{p_\alpha}(y\xi)\right| = 0.$$

Now the claim follows from partitioning H in H''-cosets.

Therefore, we may assume that $\pi_{q'}|_H$ is one-to-one.

Suppose thus $|H| = |\pi_{q'}(H)|$. Define

$$\tau = \frac{\delta}{10\,|I|}. \tag{4.26}$$

We make the following construction.

If $|\pi_{p_\alpha}(H)| > q^\tau$ for all $\alpha \in I$, we apply Corollary 4.2 with $\delta' = \tau$.

Therefore, we further assume that there exists $\alpha_1 \in I$ with $|\pi_{p_{\alpha_1}}(H)| \leq q^\tau$ and define

$$H_1 = \{x \in H : \pi_{p_{\alpha_1}}(x) = 1\} < H$$

for which

$$|H_1| \geq q^{-\tau}|H| > q^{\delta - \tau} > q^{\frac{\delta}{2}}. \tag{4.27}$$

Assume further that

$$|\pi_{p_\alpha}(H_1)| > q^\tau \text{ for all } \alpha \in I \setminus \{\alpha_1\}. \tag{4.28}$$

At this stage, application of Corollary 4.2 is not immediate and requires some extra work. For $\xi \in \mathbb{Z}_q^*$, assume

$$\Big| \sum_{x_1 \in H_1} e_q(\xi x_1) \Big| > q^{-\kappa}\, |H_1|. \tag{4.29}$$

Squaring (4.29) gives

$$\Big| \sum_{x_1, y_1 \in H_1} e_q\big(\xi(x_1 - y_1)\big) \Big| > q^{-2\kappa}\, |H_1|^2. \tag{4.30}$$

Since H_1 is a group, the sum remains preserved if we replace ξ by ξz, with $z \in H_1$. Therefore,

$$\sum_{x_1, y_1 \in H_1} e_q\big(\xi(x_1 - y_1)\big) = \frac{1}{|H_1|} \sum_{x_1, x_2, y_1 \in H_1} e_q\big(\xi(x_1 - y_1)x_2\big),$$

and from (4.30)

$$\sum_{x_1, y_1 \in H_1} \big| \sum_{x_2 \in H_1} e_q\big(\xi(x_1 - y_1)x_2\big) \big| > q^{-2\kappa}\, |H_1|^3. \tag{4.31}$$

By Cauchy-Schwartz inequality,

$$\sum_{x_1, y_1, x_2, y_2 \in H_1} e_q\big(\xi(x_1 - y_1)(x_2 - y_2)\big) = \sum_{x_1, y_1 \in H_1} \big| \sum_{x_2 \in H_1} e_q\big(\xi(x_1 - y_1)x_2\big) \big| > q^{-4\kappa} |H_1|^4. \tag{4.32}$$

Iterating, we see that

$$\Big| \sum_{x_i, y_i, z \in H_1} e_q\big(\xi \prod_{i-1}^{\nu} (x_i - y_i) z\big) \Big| > q^{-2\nu\kappa} |H_1|^{2\nu + 1}, \tag{4.33}$$

where we take $\nu = \nu_{\alpha_1}$.

For any choice of $x_i, y_i \in H_1$, let $x = (x_1, \cdots, x_\nu), y = (y_1, \cdots, y_\nu)$, and let

$$\xi_{x,y} = \xi \prod_{i=1}^{\nu} (x_i - y_i), \tag{4.34}$$

Note that since $x_i - y_i = 0 \pmod{p_{\alpha_1}}$, necessarily

$$\xi_{x,y} = 0 \pmod{p_{\alpha_1}^{\nu_{\alpha_1}}}.$$

Fixing $x_i, y_i \in H_1$, we denote

$$q_1 = \frac{q}{p_{\alpha_1}^{\nu_{\alpha_1}}}, \text{ and } \xi'_{x,y} = \frac{\xi_{x,y}}{p_{\alpha_1}^{\nu_{\alpha_1}}}.$$

The x-sum in (4.33) becomes

$$\sum_{z \in H_1} e_q(\xi_{x,y}\, z) = \sum_{z \in H_1} e_{q_1}(\xi'_{x,y}\, z) = \frac{|H_1|}{|\pi_{q_1}(H_1)|} \sum_{z \in \pi_{q_1}(H_1)} e_{q_1}(\xi'_{x,y}\, z). \tag{4.35}$$

Since by assumption $\pi_{q_1}(H_1) < \mathbb{Z}^*_{q_1}$ satisfies the conditions of Corollary 4.2 (with $\delta' = \tau$), we get for some $\varepsilon = \varepsilon(\tau)$ and for those $\xi'_{x,y} \in \mathbb{Z}^*_{q_1}$,

$$\Big| \sum_{z \in \pi_{q_1}(H_1)} e_{q_1}(\xi'_{x,y}\, z) \Big| < q_1^{-\varepsilon}\, |\pi_{q_1}(H_1)|.$$

Hence, by (4.35)

$$\Big| \sum_{z \in H_1} e_q(\xi_{x,y} z) \Big| < q_1^{-\varepsilon} |H_1|. \tag{4.36}$$

For those $x = (x_1, \cdots, x_\nu), y = (y_1, \cdots, y_\nu)$ such that $\xi'_{x,y} = 0 \notin \mathbb{Z}^*_{q_1}$, necessarily $x_i = y_i \pmod{p_\alpha}$ for some $i = 1, \cdots, \nu$ and some $\alpha \in I \setminus \{\alpha_1\}$. Therefore, by (4.27) and (4.28), the left-hand-side of (4.33) is clearly bounded by

$$q_1^{-\varepsilon} |H_1|^{2\nu+1} + c\, q^{-\tau}\, |H_1|^{2\nu+1} < |H_1|^{2\nu+1-\varepsilon} < q^{-\frac{\varepsilon\delta}{2}}\, |H_1|^{2\nu+1}. \tag{4.37}$$

By (4.33), this shows that in (4.33)

$$\kappa > \frac{\varepsilon\delta}{4\nu_{\alpha_1}}. \tag{4.38}$$

Namely, if we choose $\kappa \le \frac{\varepsilon\delta}{4\nu_{\alpha_1}}$, then $|\sum_{z\in H_1} e_q(\xi z)| < q^{-\kappa}|H_1|$.

Again, partitioning H in H_1-cosets shows that

$$\Big|\sum_{z\in H} e_q(\xi z)\Big| < q^{-\kappa}|H| \tag{4.39}$$

under the assumption (4.28).

If (4.28) fails, there is again $\alpha_2 \in I\setminus\{\alpha_1\}$ such that $|\pi_{p_{\alpha_2}}(H_1)| < q^\tau$.

Define

$$H_2 = \{x\in H : \pi_{p_{\alpha_1}}(x) = \pi_{p_{\alpha_2}}(x) = 1\} < H_1$$

for which

$$|H_2| \ge q^{-\tau}|H_1| \ge q^{-2\tau}|H|. \tag{4.40}$$

If $|\pi_{p_\alpha}(H_2)| > q^\tau$ for all $\alpha \in I\setminus\{\alpha_1,\alpha_2\}$, the previous considerations permit again to establish (4.39). Otherwise, we repeat the process, and obtain subgroups

$$H > H_1 > \cdots > H_s \ \ (\text{with } s \le |I|)$$

satisfying

$$|H_s| > q^{-s\tau}|H| > q^{\delta-|I|\tau} > q^{\frac{\delta}{2}} \tag{4.41}$$

and $\pi_{p_{\alpha_1}}(H_s) = \cdots = \pi_{p_{\alpha_s}}(H_s) = \{1\}$.

If the process only terminates at $s = |I|$, necessarily $\pi_{q'}(H_s) = \{1\}$. Therefore, by (4.41) $\pi_{q'}|_{H_s}$ and $\pi_{q'}|_H$ are not one-to-one and (4.24) holds.

Remark 4.8. It is shown in [B3] that Theorem 4.7 holds for $H < \mathbb{Z}_q^*$, $|H| > q^\delta$ and q arbitrary, with ε in (4.21) only dependent on δ. This argument is considerably more complicated.

§5. The case of a typical modulus.

The results from §3 do allow us to treat more general moduli. For instance, the following extension holds

There following two facts will be used in the proof of Theorem 5.1 and are easy to check.

Fact 5.1.1. If $\sum_x f(x) = 1$, then $\big(\sum_\xi \hat{f}(\xi)\big)^2 \leq \sum_{\xi_1,\xi_2} \hat{f}(\xi_1 - \xi_2)$.

Fact 5.1.2. $|H|^{-2r} \sum_{x_i \in H} f(x_1 - x_2 + \cdots - x_{2r}) = \sum_y f(y)(\mu * \mu_-)^{(r)}(y)$.

Theorem 5.1. *Let $q \in \mathbb{Z}_+$ and $H < \mathbb{Z}_q^*$ be a subgroup. Assume q factorizes as $q = q_1 \cdot q_2$, where q_1 is a product of a bounded number of large prime factors (as in §4), thus*

$$q_1 = p_1^{\nu_1} \cdots p_r^{\nu_r} \text{ with } p_s > q^{\varepsilon_0} \text{ for all } 1 \leq s \leq r \tag{5.1}$$

and

$$q_2 < q^{\frac{1}{2} - \varepsilon_0}. \tag{5.2}$$

Assume further that

$$|\pi_p(H)| > q^{\varepsilon_1} \text{ for all primes } p | q_1. \tag{5.3}$$

Then

$$\max_{\xi \in \mathbb{Z}_q^*} \Big| \sum_{x \in H} e_q(\xi x) \Big| < C|H|q^{-\delta} \text{ with } \delta = \delta(\varepsilon_1) > 0. \tag{5.4}$$

Proof. Recall that, as in (3.39), $\sum_{x \in H} e_q(\xi x) = S_1(\xi, H) = |H| \ \hat{\mu}_1(\xi)$. Hence we denote

$$\mu = \mu_1 = \frac{1}{|H|} \sum_{z \in H} \delta_z$$

and assume on the contrary that there exists $\xi \in \mathbb{Z}_q^*$ such that

$$|\hat{\mu}(\xi)| > q^{-\delta} \tag{5.5}$$

We repeat an argument from [B2].

Fix a positive integer $r \in \mathbb{Z}_+$ to be specified later.

Let

$$\phi = (\mu * \mu_-)^{(r)} \tag{5.6}$$

Claim. $\phi(0) > q^{-\frac{1}{2}-4r^2\delta}$.

Proof of Claim. Since $\mu(x^{-1}z) = \mu(z)$ for $x \in H$, we have $\hat{\mu}(\xi) = \hat{\mu}(x\xi)$. Hence, by (5.5)

$$\sum_{x\in H} \widehat{(\phi * \phi)}(x\xi) = \sum_{x\in H} |\hat{\mu}(x\xi)|^{4r} > |H|\, q^{-4r\delta}.$$

Fact 5.1.1 implies

$$\sum_{x_1,x_2\in H} \widehat{\phi * \phi}\,\big((x_1 - x_2)\xi\big) > |H|^2 q^{-8r\delta}.$$

Repeating Fact 5.1.1 $\frac{\log r}{\log 2}$ times (assuming r a power of 2), we have

$$\sum_{x_1,x_2,\dots,x_{2r}\in H} \widehat{\phi * \phi}\,\big((x_1 - x_2 + \cdots - x_{2r})\xi\big) > |H|^{2r} q^{-8r^2\delta}.$$

By Fact 5.1.2, after being divided by $|H|^{2r}$, this is

$$\sum_y \widehat{\phi * \phi}\,(y\xi)\ (\mu * \mu^-)^{(r)}(y) > q^{-8r^2\delta}. \tag{5.7}$$

Since $\phi(y) \le \phi(0)$, the left size of (5.7) is clearly bounded above by

$$\phi(0) \sum_{\zeta\in\mathbb{Z}_q} |\hat{\phi}(\zeta)|^2 = q\ \phi(0) \sum_{x\in\mathbb{Z}_q} \phi(x)^2 \le q\ \phi(0)^2 \sum_x \phi(x) = q\ \phi(0)^2. \quad \square \tag{5.8}$$

From (5.6) and (3c), we have

$$\phi(0) = |H|^{-2r} |\{x_1, x_2, \dots, x_{2r}) \in H^{2r}\ :\ x_1 - x_2 \cdots - x_{2r} = 0 \pmod q)\}|. \tag{5.9}$$

Let $\pi_1 : \mathbb{Z}_q \to \mathbb{Z}_{q_1}$ be the quotient map to the residues mod q_1 and $H_1 = \pi_1(H) < \mathbb{Z}^*_{q_1}$. (5.9) gives

$$\begin{aligned}\phi(0) &\leq |H_1|^{-2r} |\{(x_1, \dots, x_{2r}) \in H_1^{2r} \ : \ x_1 - x_2 \cdots - x_{2r} = 0 \ (\text{ mod } q_1)\}| \\ &= \frac{|H_1|^{-2r}}{q_1} \sum_{\eta \in \mathbb{Z}_{q_1}} \Big| \sum_{x \in H_1} e_{q_1}(\eta x) \Big|^{2r} \\ &= \frac{1}{q_1} + \frac{1}{q_1} \sum_{\eta \in \mathbb{Z}_{q_1} \setminus \{0\}} \Big| \frac{1}{|H_1|} \sum_{x \in H_1} e_{q_1}(\eta x) \Big|^{2r}. \end{aligned} \tag{5.10}$$

To estimate the second term in (5.10), we apply Corollary 4.2 to the subgroup $H_1 \lhd \mathbb{Z}^*_{q_1}$. The required assumptions hold by (5.1), (5.3). Hence, by (4.8),

$$\max_{(\eta, q_1) = 1} \Big| \sum_{x \in H_1} e_{q_1}(\eta x) \Big| < |H_1| . q_1^{-\delta_1} \tag{5.11}$$

for some $\delta_1 > 0$.

Since obviously (5.1), (5.3) still hold for any divisor $q_1' > 1$ of q_1, also

$$\max_{\eta \in \mathbb{Z}_{q_1} \setminus \{0\}} \Big| \sum_{x \in H_1} e_{q_1}(\eta x) \Big| < |H_1| q_1^{-\delta_1}. \tag{5.12}$$

Substitution in (5.10) implies

$$q^{-\frac{1}{2} - 4r^2\delta} < \frac{1}{q_1} + \frac{1}{q_1}(q_1 - 1) q^{-r\delta_1} < \frac{2}{q_1} < 2q^{-\frac{1}{2} - \varepsilon_0} \tag{5.13}$$

by (6.9), (5.2) and choosing $r = [\frac{2}{\delta_1}]$.

Taking δ small enough in (5.4), a contradiction follows. This proves Theorem 5.1.□

It is a well known elementary fact (see e.g. [H-Ro], Lemma 7, p264) that if we denote

$$\mathcal{Z}_\varepsilon = \{q \in \mathbb{Z}_+ \ : \ q = q_1 . q_2 \text{ with } q_1 > q^{3/4} \text{ and } p > q^\varepsilon \text{ for any factor } p \text{ of } q_1\}, \tag{5.14}$$

then density $\mathcal{Z}_\varepsilon \overset{\varepsilon \to 0}{\to} 1$.

The precise statement of the result in [H-Ro] will be recalled at the end of this section.

In particular, Theorem 5.1 applies to ‘most’ moduli q.

Corollary 5.2. *Fix $\theta \in \mathbb{Z}, \theta > 1$. For $q \in \mathbb{Z}_+, (\theta, q) = 1$, denote $t = 0_q(\theta)$ the multiplicative order of $\theta \in \mathbb{Z}_q^*$. Then the estimate*

$$\max_{a \in \mathbb{Z}_q^*} \left| \sum_{s=1}^{t} e_q(a\theta^s) \right| < t^{1-\delta} \tag{5.15}$$

holds for 'most' moduli q, when $\delta \to 0$.

Proof. Condition (5.3) amounts to $\text{ord}_p(\theta) > p^\tau > q^{\varepsilon\tau}$ for all $p|q_1$ with $q = q_1q_2$ as in (5.14). Here $\tau > 0$ may be taken an arbitrary constant and in (5.3) we let then $\varepsilon_1 = \varepsilon\tau$. First, recall that θ is fixed. We have

$$|\{p \leq \mathcal{P}\colon ord_p(\theta) \leq p^\tau\} \leq \sum_{n \leq \mathcal{P}^\tau} |\{p : p|(\theta^n - 1) \text{ and } p \text{ is prime }\}| < c(\theta) \sum_{n \leq \mathcal{P}^\tau} n < c(\theta)\mathcal{P}^{2\tau}.$$

Fix $\tau < \frac{1}{2}$ and estimate

$$|\{q\colon Q < q < 2Q, q \text{ has a prime divisor } p > Q^\varepsilon \text{ such that } \text{ord}_p(\theta) < p^\tau\}|,$$

which is

$$\leq \sum_{Q^\varepsilon < 2^k < Q} \quad \sum_{p \sim 2^k, ord_p(\theta) < p^\tau} \frac{Q}{p} < c \sum_{Q^\varepsilon < 2^k < Q} \frac{Q}{2^k} 4^{\tau k} < Q^{1-(1-2\tau)\varepsilon}$$

implying in particular that the set of residues q with a prime divisor $p > q^\varepsilon$ such that $\text{ord}_p(\theta) < p^\tau$ has density 0.

A similar statement may be formulated for incomplete sums in the spirit of Corollary 4.5.

For the convenience of the readers, let us formulate Lemma 7, p264 in [H-Ro].

Lemma 5.3. *Fix $\tau > 0$ a small number and decompose every integer $0 < n \leq T$ as product $n = n^{(1)}.n^{(2)}$ where $n^{(1)}$ (respectively, $n^{(2)}$) is composed only of prime factors $p \leq T^{\tau^2}$ (resp. $p > T^{\tau^2}$). Then*

$$k = |\{0 < n \leq T : n^{(1)} > T^\tau\}| < C\tau T. \tag{5.15}$$

It is easily derived that the set $\mathcal{Z}_\varepsilon$ defined in (5.14) has asymptotic density at most $\sqrt{2}$.

Acknowledgement. The authors would like to thank the referee for many helpful comments.

Appendix: On the Balog-Szemerédi-Gowers Theorem

In this appendix we will prove Theorem BSG' as stated after the proof of Claim 4 in Section 2.

(1). Let us first recall the usual Balog-Szemerédi-Gowers theorem

There is a constant C_1 such that for any finite set A, if $|A| \leq N$, and $\mathcal{G} \subset A \times A$ with

$$|\mathcal{G}| > \frac{1}{K} N^2 \tag{1.1}$$

$$|A \underset{\mathcal{G}}{+} A| < KN. \tag{1.2}$$

Then there is $A' \subset A$ with

$$|A'| > K^{-C_1} N \tag{1.3}$$

$$|A' + A'| < K^{C_1} N. \tag{1.4}$$

(2). *Proof of Theorem BSG'.*

Assume $|A|, |B| \leq N$, $\mathcal{G} \subset A \times B$ with

$$|\mathcal{G}| > \frac{4}{K} N^2 \tag{2.1}$$

$$|A \underset{\mathcal{G}}{+} B|^{<} 2KN. \tag{2.2}$$

Apply (1) considering $\mathcal{G} \subset (A \cup B) \times (A \cup B)$. We obtain either a subset $A_0' \subset A$ satisfying (1.3), (1.4) or a subset $B_0' \subset B$ satisfying (1.3), (1.4). Assume first alternative.

Write

$$\mathcal{G} = \big(\mathcal{G} \cap (A_0' \times B)\big) \cup \big(\mathcal{G} \cap \big((A \backslash A_0') \times B\big)\big) = \mathcal{G}' \cup \mathcal{G}_1.$$

Either $|\mathcal{G}'| > \delta|\mathcal{G}|$ or $|\mathcal{G}_1| > (1-\delta)|\mathcal{G}|$ (δ to be specified).

Assume $|\mathcal{G}_1| > (1-\delta)|\mathcal{G}|$. Apply again (1) with $\mathcal{G}_1 \subset \big((A\backslash A') \cup B\big) \times \big((A\backslash A') \cup B\big)$. Denote $A_1 = A\backslash A_0', B_1 = B$. We obtain either $A_1' \subset A_1$ or $B_1' \subset B_1$ satisfying (1.3), (1.4) with K replaced by $\frac{K}{1-\delta}$ and a decomposition of $\mathcal{G}_1 = \mathcal{G}_1' \cup \mathcal{G}_2$. Assuming again $|\mathcal{G}_2| > (1-\delta)|\mathcal{G}_1|$, repeat with $\mathcal{G}_2$, etc. Observe that $|A_1|\ |B_1| < (1-K^{-C_1})N^2, |A_2|\ |B_2| < (1-(\frac{K}{1-\delta})^{-C_1})|A_1|\ |B_1|$ and after s steps

$$\begin{aligned}|A_s|\ |B_s| &< \Big(1 - \Big(\frac{(1-\delta)^s}{K}\Big)^{C_1}\Big) \cdots \Big(1 - \Big(\frac{1-\delta}{K}\Big)^{C_1}\Big)\Big(1 - \frac{1}{K^{C_1}}\Big)N^2 \\ &< \Big[1 - \Big(\frac{(1-\delta)^s}{K}\Big)^{C_1}\Big]^s N^2.\end{aligned}$$

Also, $|\mathcal{G}_s| > (1-\delta)|\mathcal{G}_{s-1}| > (1-\delta)^s|\mathcal{G}| > (1-\delta)^s\frac{1}{K}N^2$ and since $\mathcal{G}_s \subset A_s \times B_s$

$$(1-\delta)^s\frac{1}{K} < \Big[1 - \Big(\frac{(1-\delta)^s}{K}\Big)^{C_1}\Big]^s. \tag{2.3}$$

Take

$$\delta = K^{-2C_1} \tag{2.4}$$

so that for $s < K^{2C_1}$, (2.3) gives that

$$\frac{1}{10K} < \Big(1 - \frac{1}{(10K)^{C_1}}\Big)^s$$

or

$$-\log K - \log 10 < s \log\Big(1 - \frac{1}{(10K)^{C_1}}\Big) < -s\frac{1}{(10K)^{C_1}}$$

and in fact s is restricted to

$$s < (\log K)(10K)^{C_1} < (10K)^{C_1+1} \tag{2.5}$$

We have therefore shown that there is $s < (10K)^{C_1+1}$ such that $|\mathcal{G}'_s| > \delta|\mathcal{G}_s|$, hence either $A' = A_s \subset A$ satisfying

$$|A' + A'| < 2K^{C_1}N \tag{2.6}$$

and

$$|\mathcal{G} \cap (A' \times B)| > \delta(1-\delta)^s|\mathcal{G}| \overset{(2.4),(2.5)}{>} 2K^{-2C_1-1}N^2 \tag{2.7}$$

or $B' \subset B$ such that

$$|B' + B'| < 2K^{C_1}N \tag{2.8}$$

and

$$|\mathcal{G} \cap (A \times B')| > 2K^{-2C_1}N^2. \tag{2.9}$$

Assume (2.6), (2.7). From (2.7), notice that obviously

$$|A'| > 2K^{-2C_1-1}N. \tag{2.10}$$

Next, for $z \in A \underset{\mathcal{G}}{+} B$, denote

$$O_z = \{(x,y) \in \mathcal{G} \cap (A' \times B) | x + y = z\}$$

so that

$$|\mathcal{G} \cap (A \times B')| \le \sum_{z \in A' \underset{\mathcal{G}}{+} B} |O_z|$$

$$\le |A' \underset{\mathcal{G}}{+} B|^{1/2}\Big(\sum_{z \in A' \underset{\mathcal{G}}{+} B} |O_z|^2\Big)^{1/2}$$

and by (2.7), (1.2)

$$\sum_{z \in A' \underset{\mathcal{G}}{+} B} |O_z|^2 > 4K^{-4C_1-2}N^4K^{-1}N^{-1} > K^{-5C_1}N^3. \tag{2.11}$$

Recalling the definition of O_z, (2.11) means that

$$|\{(x_1, y_1, x_2, y_2) \in A' \times B \times A' \times B | (x_1, y_1) \in \mathcal{G}, (x_2, y_2) \in \mathcal{G} \text{ and } x_1 + y_1 = x_2 + y_2\}| > K^{-5C_1} N^3. \tag{2.11}$$

By Fubini, we may therefore find some $y_2 = b \in B$ such that

$$|\{(x_1, y_1) \in (A' \times B) \cap \mathcal{G} | x_1 + y_1 \in A' + b\}| > K^{-5C_1} N^2. \tag{2.12}$$

Denote $B' \subset B$ the projection of this set to the y_1-coordinate. Then

$$|(A' \times B') \cap \mathcal{G}| > K^{-5C_1} N^2 \tag{2.13}$$

and also

$$B \subset A' - A' + b. \tag{2.14}$$

From (2.6) and Ruzsa's inequality

$$|A' + B'| \leq |A' + A' - A'| < K^{3C_1} N. \tag{2.15}$$

References

[B1]. J. Bourgain, *Estimates on exponential sums related to the Diffie-Hellman distributions*, to appear in GAFA.

[B2]. J. Bourgain, *Mordell's exponential sum estimate revisited, (preprint 2004, submitted to JAMS).*

[B3]. J. Bourgain, *Exponential sum estimates on subgroups of $\mathbb{Z}_q^*, q$ arbitrary*, J. Analysi (to appear).

[B-Ch]. J. Bourgain, M. Chang, *Sum-product theorem and exponential sum estimates in residue classes with moduli involving few prime factors*, preprint 2004.

[B-K]. J. Bourgain, S. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, CR Acad. Sci., Paris 337 (2003), no 2, 75–80.

[B-G-K]. 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.

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

[E-S]. P. Erdős, E. Szemerédi, *On sums and products of integers*, In P. Erdös, L. Alpár, G. Halász (editors), Studies in Pure Mathematics; to the memory of P. Turán, p. 213–218.

[H-B]. R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, Analytic Number Theory, Proc. Conf. in honor of H. Halberstam, Birkhäuser, Boston MA (1996), 451–463.

[H-B–K]. R. Heath-Brown, S. Konyagin, *New bounds for Gauss sums derived from k^{th} powers, and for Heilbronn's exponential sums*, Quat. J. Math. 51 (2000), 221–235.

[H-R]. H. Halberstam, Richert, *Sieve methods.*

[H-Ro]. H. Halberstam, K. Roth, *Sequences*, Oxford Press, Vol 1 (1966).

[K-S]. S. Konyagin, I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Tracts in Mathematics, 136, Cambridge UP, Cambridge 1999.

[L-R]. Laczkovich, I. Ruzsa, *The number of homothetic subsets,*, in 'The mathemattics of P. Erdős, II. (R.L. Grham, J. Nesetril, eds.), Springer, Algorithms Combin. 14 (1997), 294-302.

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

[O]. R. Odoni, *Trigonometric sums of Heilbronn's type*, Math. Proc. Comb. Phil. Soc. (1985), 98, 389–396.

[S]. J. Solymosi, *On the number of sums and products,*, (preprint) (2003).

[T-V]. T. Tao, V. Vu, *Additive Combinatorics (preprint).*