Sum-Product Theorems and Applications

Jean Bourgain

(To M. Nathanson)

Summary This is a brief account of recent developments in the theory of exponential sums and on methods from Arithmetic Combinatorics.

Keywords Exponential sum · Sum-product

Mathematics Subject Classifications (2010). Primary: 11L07, Secondary: 11T23

Introduction

These Notes originate from some lectures given by the author in the Fall of 2007 at IAS during the program on Arithmetic Combinatorics. Their purpose was twofold. The first was to illustrate the interplay between Additive Number Theory and problems on exponential sums, by reviewing various recent contributions in this general area and how they relate to several classical problems. The second was to present a proof of the Gauss sum estimate

$$\max_{a\in\mathbb{F}_p^*}\left|\sum_{x\in H} e_p(ax)\right| < C|H|^{1-\delta}$$

for subgroups $H < \mathbb{F}_p^*$, $|H| > p^\varepsilon$ ($\varepsilon > 0$ fixed and arbitrary), which is a typical sample of those developments. My intent here was to make the argument as elementary and self-contained as possible (which it is, up to the Plunnecke–Ruzsa theory of set addition).

Therefore, what follows is not written in a homogeneous style. The first three sections are indeed presented in great detail, while the remainder is rather a survey with

J. Bourgain
Institute for Advanced Study, Princeton, NJ 08540, USA
e-mail: bourgain@ias.edu

D. Chudnovsky and G. Chudnovsky (eds.), *Additive Number Theory: Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson*,
DOI 10.1007/978-0-387-68361-4_2,

only statements of the results. Note that this presentation is mostly geared toward the author's own research and is certainly far from complete, either from mathematical or historical perspective (the interested reader may wish to consult books such as [K-S] or [T-V] for background material). The reference list only serves this exposé and a more complete bibliography may be found in [K-S] and [T-V].

0 Sum-Product Theorem in $\mathbb{F}_p$

Theorem 1 ([B-K-T] and [B-G-K]).
Given $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset \mathbb{F}_p$ and $1 < |A| < p^{1-\varepsilon}$, then

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

There is the following quantitative statement.

Theorem 2 ([Ga] and [Ka-S]).

$$|A + A| + |A.A| > c \min\left(|A|^{\frac{14}{13}}, p^{\frac{1}{12}}|A|^{\frac{11}{12}}\right).$$

Denote

$$E_+(A, B) = |\{(x_1, x_2, y_1, y_2) \in A^2 \times B^2 | x_1 + y_1 = x_2 + y_2\}|$$

(additive energy)

$$E_\times(A, B) = |\{(x_1, x_2, y_1, y_2) \in A^2 \times B^2 | x_1 y_1 = x_2 y_2\}|$$

(multiplicative energy).

The Sum-Product theorem follows then from:

Proposition 1.

$$E_\times(A, A)^4 \ll |A + A|^9 |A|^2 + \frac{1}{p}|A + A|^8 |A|^5$$

using the inequality

$$|A.A| \geq \frac{|A|^4}{E_\times(A)}.$$

1 Preliminaries from Additive Combinatorics

(Plünnecke–Ruzsa Theory).
We consider subsets of an additive group $G, +$.

Lemma 1 (triangle inequality).

$$|A-B| \le \frac{|A-C|\,|B-C|}{|C|}.$$

Theorem 1 ([P-R]). *Let $X, A_1, \dots, A_k \subset G$ satisfy*

$$|X + A_i| \le \alpha_i |X| \qquad (1 \le i \le k).$$

Then there is $X_1 \subset X$ with

$$|X_1 + A_1 + \cdots + A_k| \le \alpha_1\alpha_2\cdots\alpha_k |X_1|.$$

Corollary 1.

$$|A_1 + \cdots + A_k| \le \frac{|A_1 + X|\cdots|A_k + X|}{|X|^{k-1}}.$$

Corollary 2 ([Ka-S]). *There exists $X' \subset X, |X'| > \frac{1}{2}|X|$ with*

$$|X' + A_1 + \cdots + A_k| \lesssim \frac{|A_1 + X|\cdots|A_k + X|}{|X|^{k-1}}.$$

Proof. If $Y \subset X, |Y| \ge \frac{1}{2}|X|$, then

$$\frac{|A_i + Y|}{|Y|} \le 2\frac{|A_i + X|}{|X|} = 2\alpha_i. \qquad (*)$$

Use [P-R] iteratively.
Construct disjoint set $X_s \subset X$ s.t.

$$|X_s + A_1 + \cdots + A_k| \le 2^k \alpha_1 \cdots \alpha_k |X_s|. \qquad (**)$$

Assume $X_1, \dots, X_s$ obtained. Let $Y = X\backslash(X_1 \cup \dots \cup X_s)$. If $|Y| < \frac{1}{2}|X|$, set $X' = X_1 \cup \dots \cup X_s$. From $(**)$

$$|X' + A_1 + \cdots + A_k| \le \sum_{s' \le s} |X_{s'} + A_1 + \cdots + A_k| \le 2^k \alpha_1 \cdots \alpha_k |X'|.$$

If $|Y| \ge \frac{1}{2}|X|$, then $(*)$. Apply [P-R] to $Y \Rightarrow X_{s+1} \subset Y$ such that

$$|X_{s+1} + A_1 + \cdots + A_k| \le (2\alpha_1)\cdots(2\alpha_k)|X_{s+1}|.$$

□

Proof of Proposition.

$$E_\times(A) = \sum_{a,b\in A} |aA \cap bA|.$$

Hence, there is $b_0 \in A$ and $A_1 \subset A$, $1 \leq N \leq |A|$ with

$$|aA \cap b_0 A| \sim N \text{ if } a \in A_1$$

and

$$|A_1|N \gg \frac{E_\times(A)}{|A|}. \qquad (*)$$

Case 1.

$$\frac{A_1 - A_1}{A_1 - A_1} = \mathbb{F}_p.$$

Then, there is $\xi = \frac{a_1-a_2}{a_3-a_4} (a_i \in A_i)$ s.t.

$$\left| \left\{ (x_1, x_2, x_3, x_4) \in A_1^4 | \xi = \frac{x_1 = x_2}{x_3 - x_4} \right\} \right| \leq \frac{|A_1|^4}{p}.$$

Hence

$$|(a_1 - a_2)A_1 + (a_3 - a_4)A_1| = |\xi A_1 + A_1| \geq \frac{|A_1|^2 |\xi A_1|^2}{E_+(\xi A_1, A_1)} \geq p.$$

Estimate

$$\begin{aligned} |(a_1 - a_2)A_1 + (a_3 - a_4)A_1| &\leq |a_1 A_1 - a_2 A_1 + a_3 A_1 - a_4 A_1| \\ &\overset{[P-R]}{\leq} |A|^{-3} \prod_{i=1}^{4} |a_i A \pm b_0 A|. \end{aligned}$$

From triangle inequality

$$\begin{aligned} |a_i A \pm b_0 A| &\leq \frac{|a_i A + (a_i A \cap b_0 A)| \, |b_0 A + (a_i A \cap b_0 A)|}{|a_i A \cap b_0 A|} \\ &< \frac{|A + A|^2}{N} \text{ (since } a_i \in A_1). \end{aligned}$$

Hence,

$$p \lesssim |A|^{-3} \left(\frac{|A + A|^2}{N} \right)^4 \lesssim |A|^{-3} |A + A|^8 |A|^8 E_\times(A, A)^{-4}$$

since N satisfies $(*)$

$$E_\times(A)^4 \gg \frac{1}{p}|A+A|^8\,|A|^5.$$

Case 2.

$$\frac{A_1-A_1}{A_1-A_1} \neq \mathbb{F}_p.$$

Hence,

$$\frac{A_1-A_1}{A_1-A_1} \not\supset \frac{A_1-A_1}{A_1-A_1}+1$$

and there is $\xi = \frac{a_1-a_2}{a_3-a_4} + 1(a_i \in A_1)$ s.t.

$$\xi \notin \frac{A_1-A_1}{A_1-A_1}.$$

Therefore, for any subset $A' \subset A_1$

$$\begin{aligned}|A'|^2 = |A'+\xi A'| &= |(a_1-a_2)A' + (a_1-a_2+a_3-a_4)A'| \\ &\leq |(a_1-a_2)A' + (a_1-a_2)A_1 + (a_3-a_4)A_1|.\end{aligned}$$

Using the Corollary to [P-R], take A' s.t. $X' = (a_1-a_2)A'$ satisfies $|X'| = |A'| > \frac{1}{2}|A_1|$ and

$$|X' + (a_1-a_2)A_1 + (a_3-a_4)A_1| \lesssim \frac{|(a_1-a_2)A_1+X|\,|(a_3-a_4)A_1+X|}{|X|}$$

where $X = (a_1-a_2)A_1$.

Hence,

$$|A_1|^2 \sim |A'|^2 \lesssim \frac{|A_1+A_1|.|(a_3-a_4)A_1+(a_1-a_2)A_1|}{|A_1|}$$

and

$$|A_1|^3 \lesssim |A+A|\,|a_1A_1 - a_2A_1 + a_3A_1 - a_4A_1|.$$

As before, since $a_i \in A_1$

$$|a_1A - a_2A + a_3A - a_4A| \ll |A|^{-3}\frac{|A+A|^8}{N^4}.$$

Therefore,

$$|A|^{-3}|A+A|^9 \gtrsim N^4|A_1|^3 \geq \frac{(N.|A_1|)^4}{|A|} \underset{(*)}{\gg} \frac{E_x(A)^4}{|A|^5}$$

and

$$E_\times(A)^4 \gg |A+A|^9|A|^2.$$

□

2 Some Tools from Graph Theory: The Balog–Szemerédi–Gowers Theorem

Statement. *Let $G, +$ be an additive group. There is an absolute constant C such that the following holds. Let $A \subset G$ be a finite set and $K \in \mathbb{R}_+$ such that*

$$E_+(A, A) > \frac{1}{K}|A|^3.$$

Then there is a subset $A' \subset A$ such that

$$|A'| > K^{-C}|A|$$
$$|A' \pm A'| < K^C|A'|.$$

Remark. Underlying Balog–Szemerédi–Gowers is in fact a result from graph theory, which will be implicit in the argument.

Also, Balog–Szemerédi–Gowers is not restricted to an Abelian setting and there are variants for general groups, both in discrete and continuous settings, using similar proofs (see the book [T-V]).

Sketch of the Proof.

Main idea. We construct a large subset $A' \subset A$, such that whenever $x, x' \in A'$, then there are at least $K^{-C}|A|^7$ representations

$$x - x' = x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8 \text{ with } x_i \in A.$$

Hence

$$|A' - A'| \leq \frac{|A|^8}{K^{-C}|A|^7}.$$

The construction.

Let $\omega(x) = |\{(x_1, x_2) \in A^2 | x = x_1 - x_2\}|$ for $x \in G$.
Hence,

$$\sum_{x \in G} \omega(x) = |A|^2$$
$$\sum \omega(x)^2 = E_+(A).$$

Define

$$D = \left\{ z \in G | \omega(z) > \frac{1}{2K}|A| \right\}$$

(the 'popular' differences).

Then

$$\frac{1}{K}|A|^3 < \sum_{z \in D} \omega(z)^2 + \left(\frac{1}{2K}|A|\right)|A|^2$$

and

$$\sum_{z\in D}\omega(z)^2 > \frac{1}{2K}|A|^3.$$

Define the following (directed) graph $R \subset A \times A$

$$(x, y) \in R \Leftrightarrow x - y \in D.$$

Hence,

$$|R| = \sum_{z\in D}\omega(z) > \frac{1}{2K}|A|^2.$$

Denote R_x, R_y the sections of R. Thus,

$$\frac{1}{2K}|A|^2 < \sum_{y\in A}|R_y| \le |A|^{\frac{1}{2}}\left(\sum_{y\in A}|R_y|^2\right)^{\frac{1}{2}}$$

and

$$\sum_{y\in A}|R_y|^2 > \frac{1}{4K^2}|A|^3. \tag{1}$$

Define

$$Y = \{(x, x') \in A \times A|\ |R_x \cap R_{x'}| < \theta|A|\}$$

where we take

$$\theta = 10^{-3}K^{-2}.$$

Then,

$$\sum_{y\in A}|(R_y \times R_y) \cap Y| = \sum_{(x,x')\in Y}|R_x \cap R_{x'}| < \theta|A|^3 \tag{2}$$

and from (1), (2)

$$\sum_{y\in A}|R_y|^2 > \frac{1}{8K^2}|A|^3 + \frac{1}{8K^2\theta}\sum_{y\in A}|(R_y \times R_y) \cap Y|.$$

Therefore, there is $y_0 \in A$ with

$$|R_{y_0}|^2 > \frac{1}{8K^2}|A|^2 + 10|(R_{y_0} \times R_{y_0}) \cap Y|$$
$$\Rightarrow |R_{y_0}| > \frac{1}{3K}|A|.$$

The set A' is defined by

$$A' = \left\{x \in R_{y_0}|\ |(\{x\} \times R_{y_0}) \cap Y| < \frac{1}{3}|R_{y_0}|\right\}.$$

Since

$$\frac{1}{3}|R_{y_0}\setminus A'|\,|R_{y_0}| \le |(R_{y_0}\times R_{y_0})\cap Y| < \frac{1}{10}|R_{y_0}|^2$$

we have

$$|A'| > \frac{1}{2}|R_{y_0}| > \frac{1}{6K}|A|.$$

Take any $x_1, x_2 \in A'$. Then,

$$|\{x \in R_{y_0} | (x_1, x) \notin Y \text{ and } (x_2, x) \notin Y\}| > \left(1 - \frac{2}{3}\right)|R_{y_0}|$$

and

$$|R_{x_1} \cap R_x| > \theta|A|, |R_{x_2} \cap R_x| > \theta|A|$$

for at least $\frac{1}{3}|R_{y_0}|$ elements $x \in R_{y_0}$.

Write

$$\begin{aligned} x_1 - x_2 &= (x_1 - x) - (x_2 - x) \\ &= (x_1 - y_1) - (x - y_1) - (x_2 - y_2) + (x - y_2) \\ &\quad \text{where } y_i \in R_{x_i} \cap R_x \quad (i = 1, 2). \end{aligned}$$

Since $x_1 - y_1, x - y_1, x_2 - y_2, x - y_2 \in D$, each difference has at least $\frac{1}{2K}|A|$ representations in $A - A$. Hence, there are at least

$$\frac{1}{3}|R_{y_0}|.(\theta.|A|)^2.\left(\frac{1}{2K}|A|\right)^4 \gtrsim K^{-9}|A|^7$$

representations

$$x_1 - x_2 = z_1 - z_2 + z_3 - z_4 + z_5 - z_6 + z_7 - z_8$$

with $z_i \in A$, as claimed.

This proves the Balog–Szemerédi–Gowers theorem.

3 Exponential Sum Estimate

We will establish the following estimate on Gauss sums.

Theorem 1. *Let H be a multiplicative subgroup of $\mathbb{F}_p^*$ and $|H| > p^\varepsilon$ for some $\varepsilon > 0$. Then,*

$$\max_{(a,p)=1}\left|\sum_{x\in H} e_p(ax)\right| < C|H|^{1-\delta} \text{ where } \delta = \delta(\varepsilon) > 0.$$

Denote

$$\hat{f}(k) = \sum_{x \in \mathbb{F}_p} e_p(kx) f(x) \qquad (k \in \mathbb{F}_p)$$

the Fourier transform of $f : \mathbb{F}_p \to \mathbb{C}$.

Lemma 2 (harmonic analysis). *Let $\mu : \mathbb{F}_p \to [0,1]$ be a probability measure ($\sum \mu(x) = 1$).*

Denote for $\delta > 0$

$$\Lambda_\delta = \{k \in \mathbb{F}_p | \, |\hat{\mu}(k)| > p^{-\delta}\}.$$

Then,

$$|\{(k_1, k_2) \in \Lambda_\delta | k_1 - k_2 \in \Lambda_{2\delta}\}| > p^{-2\delta} |\Lambda_\delta|^2.$$

Proof. Let $|\hat{\mu}(k)| = c_k \hat{\mu}(k)$ with $c_k \in \mathbb{C}, |c_k| = 1$. We have

$$|\Lambda_\delta| . p^{-\delta} < \sum_{k \in \Lambda_\delta} c_k \hat{\mu}(k) = \sum_{x \in \mathbb{F}_p} \left[\sum_{k \in \Lambda_\delta} c_k e_p(kx) \right] \mu(x)$$

and

$$|\Lambda_\delta|^2 p^{-2\delta} < \sum_{x \in \mathbb{F}_p} \left| \sum_{k \in \Lambda_\delta} c_k e_p(kx) \right|^2 \mu(x) \leq \sum_{k_1, k_2 \in \Lambda_\delta} |\hat{\mu}(k_1 - k_2)|.$$

□

Corollary 3.

$$E_+(\Lambda_\delta, \Lambda_\delta) > p^{-4\delta} \frac{|\Lambda_\delta|^4}{|\Lambda_{2\delta}|}.$$

Corollary 4. *There is the following dichotomy. Let $\kappa > \delta > 0$.*

Either

$$|\Lambda_{2\delta}| > p^\kappa |\Lambda_\delta|$$

or there is $\Lambda \subset \Lambda_\delta$ such that

$$|\Lambda| > p^{-C\kappa} |\Lambda_\delta|$$
$$|\Lambda + \Lambda| < p^{C\kappa} |\Lambda|.$$

Proof. Corollary 1+ Balog–Szemerédi–Gowers. □

Let $H < \mathbb{F}_p^*, |H| = p^\alpha$ for some $\alpha > 0$.

Definition. A probability measure μ on $\mathbb{F}_p$ is H-invariant provided

$$\hat{\mu}(k) = \hat{\mu}(hk) \text{ for all } k \in \mathbb{F}_p, h \in H.$$

Example.

$$\mu(x) = \begin{cases} \frac{1}{|H|} \text{ if } x \in H \\ 0 \text{ if } x \notin H. \end{cases} .$$

Main Proposition.

For all $\rho < 1$ and $\delta > 0$, there is $\delta' = \delta'(\alpha, \rho, \delta) > 0$ such that

$$\Lambda_{\delta'} \neq \{0\} \Rightarrow |\Lambda_\delta| > p^\rho.$$

Here, $\Lambda_\delta = \Lambda_\delta(\mu)$, where μ is an arbitrary H-invariant measure.

The argument gives $\delta'(\alpha, \rho, \delta) = \frac{\delta}{\exp(\frac{1}{\alpha(1-\rho)})^C}$.

The limitation of the method: $|H| = p^\alpha$ with $\alpha \sim \frac{1}{\log\log p}$ (see [B1]).

Proof of Theorem using Proposition.

Take $\rho = 1 - \frac{\alpha}{3}, \delta = \frac{\alpha}{4} \Rightarrow \delta'$, according to the Proposition.

Apply the Proposition with $\mu = \frac{1}{|H|} 1_H$.

Assume $|\hat{\mu}(a)| > p^{-\delta'}$ for some $a \in \mathbb{F}_p^* \Rightarrow \Lambda_{\delta'} \neq \{0\}$.

Hence, $|\Lambda_\delta| > p^\rho \Rightarrow$

$$p^{\rho-2\delta} < \sum_{k \in \mathbb{F}_p} |\hat{\mu}(k)|^2 = p \sum_{x \in \mathbb{F}_p} \mu(x)^2 = \frac{p}{|H|} = p^{1-\alpha}$$

(contradiction).

Proof of the Main Proposition.

By H-invariance: $\Lambda_\delta = H.\Lambda_\delta$.

Hence,

$$\Lambda_\delta \neq \{0\} \Rightarrow |\Lambda_\delta| \geq p^\alpha.$$

Thus, the statement certainly holds for $\rho = \alpha$.

Assume now we established the statement for some $\rho < 1$. Thus

$$(*)\ \forall \delta > 0, \exists \delta' > 0 \text{ such that } \Lambda_{\delta'} \neq \{0\} \Rightarrow |\Lambda_\delta| > p^\rho$$

for arbitrary H-invariant μ.

We will then derive the statement for $\rho_1 = \rho + c \min(\rho, 1 - \rho)$.

Take $\delta > 0$ (small enough) $\underset{(*)}{\Rightarrow} \delta' < \delta$ and $\frac{1}{2}\delta' \underset{(*)}{\Rightarrow} \delta''$.

Assume $\Lambda_{\delta''} \neq \{0\} \Rightarrow |\Lambda_{\frac{1}{2}\delta'}| > p^\rho$.

Apply dichotomy from Corollary 2. Fix $\delta < \kappa < \rho$ to be specified. There are 2 cases

$$|\Lambda_{\delta'}| > p^{\kappa}|\Lambda_{\frac{1}{2}\delta'}| \Rightarrow |\Lambda_{\delta}| > p^{\rho+\kappa} \text{ and we are done}$$

$$\nearrow$$

$$\searrow$$

$$\exists \Lambda \subset \Lambda_{\frac{1}{2}\delta'} \cap \mathbb{F}_p^* \text{ with } \begin{cases} |\Lambda| > p^{-C\kappa}|\Lambda_{\frac{1}{2}\delta'}| > p^{\rho - C\kappa} \\ |\Lambda + \Lambda| < p^{C\kappa}|\Lambda| \end{cases}$$

where C is the constant from Corollary 2.

Since $|\Lambda + \Lambda| < p^{C\kappa}|\Lambda|$, the sum-product proposition implies

$$E_{\times}(\Lambda)^4 \ll |\Lambda + \Lambda|^9|\Lambda|^2 + \frac{1}{p}|\Lambda + \Lambda|^8|\Lambda|^5$$

hence,

$$E_{\times}(\Lambda) \ll p^{3C\kappa}\left(|\Lambda|^{\frac{11}{4}} + p^{-\frac{1}{4}}|\Lambda|^{\frac{13}{4}}\right). \qquad (**)$$

Denote $\mu_-(x) = \mu(-x)$ and

$$(\mu * \mu_-)(x) = \sum_{y \in \mathbb{F}_p} \mu(x-y)\mu_-(y)$$

the (additive) convolution of μ and μ_-. Hence,

$$\widehat{\mu * \mu_-}(k) = |\hat{\mu}(k)|^2.$$

Define a new probability measure η on $\mathbb{F}_p$ by

$$\eta(x) = \frac{1}{|\Lambda|}\sum_{y \in \Lambda}(\mu * \mu_-)\left(\frac{x}{y}\right).$$

Hence,

$$\hat{\eta}(k) = \frac{1}{|\Lambda|}\sum_{y \in \Lambda}|\hat{\mu}(yk)|^2.$$

Since $\Lambda \subset \Lambda_{\frac{\delta'}{2}}$, it follows

$$\begin{aligned} \hat{\eta}(1) = \frac{1}{|\Lambda|}\sum_{y \in \Lambda}|\hat{\mu}(y)|^2 &> p^{-\delta'} \\ &\Rightarrow \Lambda_{\delta'}(\eta) \neq \{0\} \\ &\underset{(*)}{\Rightarrow} |\Lambda_{\delta}(\eta)| > p^{\rho}. \end{aligned}$$

Denote

$$\tilde{\Lambda} = \Lambda_\delta(\eta), \text{ hence } |\tilde{\Lambda}| > p^\rho.$$

Then,

$$\sum_{k\in\tilde{\Lambda}} \hat{\eta}(k) > p^{-\delta}|\tilde{\Lambda}|$$
$$\Rightarrow \sum_{y\in\Lambda, k\in\tilde{\Lambda}} |\hat{\mu}(yk)|^2 > p^{-\delta}|\Lambda|.|\tilde{\Lambda}|.$$

Denote

$$\omega(z) = |\{(y,k) \in \Lambda \times \tilde{\Lambda} | yk = z\}|.$$

Thus,

$$\sum \omega(z)|\hat{\mu}(z)|^2 > p^{-\delta}|\Lambda|.|\tilde{\Lambda}|$$
$$\Rightarrow \omega(\Lambda_\delta) > \frac{1}{2}p^{-\delta}|\Lambda|.|\tilde{\Lambda}|.$$

Also

$$\begin{aligned}\omega(\Lambda_\delta) &= |\{(y,k) \in \Lambda \times \tilde{\Lambda} | yk \in \Lambda_\delta\}| \\ &\le |\Lambda_\delta|^{\frac{1}{2}} E_\times(\Lambda, \tilde{\Lambda})^{\frac{1}{2}} \\ &\le |\Lambda_\delta|^{\frac{1}{2}} E_\times(\tilde{\Lambda})^{\frac{1}{4}} E_\times(\Lambda)^{\frac{1}{4}} \\ &\le |\Lambda_\delta|^{\frac{1}{2}} |\tilde{\Lambda}|^{\frac{3}{4}} E_\times(\Lambda)^{\frac{1}{4}}.\end{aligned}$$

We use here the inequalities

$$E(A,B) \le E(A,A)^{\frac{1}{2}}.E(B,B)^{\frac{1}{2}}$$

and

$$E(A,A) \le |A|^3.$$

Therefore,

$$p^{-\delta}|\Lambda|\,|\tilde{\Lambda}|^{\frac{1}{4}} \le |\Lambda_\delta|^{\frac{1}{2}} E_\times(\Lambda)^{\frac{1}{4}}$$

and bounding $E_\times(\Lambda)$ using $(**)$ gives

$$p^{-\delta}|\Lambda|\,|\tilde{\Lambda}|^{\frac{1}{4}} \le p^{C\kappa}|\Lambda_\delta|^{\frac{1}{2}}(|\Lambda|^{\frac{11}{16}} + p^{-\frac{1}{16}}|\Lambda|^{\frac{13}{16}}).$$

Recalling that

$$|\Lambda| > p^{\rho - C\kappa}$$
$$|\tilde{\Lambda}| > p^\rho$$

it follows that either

$$|\Lambda_\delta| > p^{\frac{9}{8}\rho - 8C\kappa} > p^{\frac{10}{9}\rho}$$

or

$$|\Lambda_\delta| > p^{\frac{1}{8}(1+7\rho)-8C\kappa} > p^{\frac{1+9\delta}{10}}$$

(letting $\kappa \sim \min(\rho, 1-\rho)$ be small enough).

This completes the proof. □

4 Additive Relations in Multiplicative Groups

Obtaining nontrivial bounds on Gauss sums is essentially equivalent with estimates on the number of additive relations.

For $A \subset \mathbb{F}_p$ and $k \in \mathbb{Z}_+$, define

$$E_{(k)}(A) = |\{(x_1, \dots, x_{2k}) \in A^{2k} | x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k}\}|.$$

Thus,

$$E_{(2)}(A) = E_+(A, A).$$

Lemma 1. *Assume A satisfies an exponential sum bound*

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in A} e_p(ax) \right| < p^{-\varepsilon}|A| \text{ for some } \varepsilon > 0.$$

Then

$$E_{(k)}(A) = \left(\frac{1}{p} + 0(p^{-2k\varepsilon}) \right) |A|^{2k}.$$

In particular,

$$E_{(k)}(A) < \frac{2}{p}|A|^{2k} \quad \text{for } k > \frac{1}{2\varepsilon}.$$

Proof. Use the circle method. Thus

$$E_{(k)}(A) = \frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{x \in A} e_p(ax) \right|^{2k}$$

and isolating the contribution of $a = 0$, we get

$$\left| E_{(k)}(A) - \frac{|A|^{2k}}{p} \right| < \max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in A} e_p(ax) \right|^{2k} < p^{-2k\varepsilon}|A|^{2k}.$$

□

Conversely, we have the following:

Lemma 2. *Let $H < \mathbb{F}_p^*$ and assume*

$$E_{(2k)}(H) < p^{-\frac{1}{2}-\delta}|H|^{4k}$$

for some $k \in \mathbb{Z}_+$ and $\delta > 0$. Then,

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in H} e_p(ax) \right| \leq p^{-\frac{\delta}{4k^2}} |H|.$$

Proof. Write

$$\left| \sum_{x \in H} e_p(ax) \right|^{2k} = \sum_{x \in \mathbb{F}_p} \omega(z) e_p(az)$$

with

$$\omega(z) = |\{(x_1, \ldots, x_{2k}) \in H^{2k} | x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{2k} = z\}|.$$

Since H is a multiplicative group

$$\omega(z) = \omega(xz) \text{ if } x \in H, z \in \mathbb{F}_p.$$

Also

$$\sum_z \omega(z)^2 = \|\omega\|_2^2 = E_{2k}(H).$$

□

Next

$$\begin{aligned}
\left| \sum_{x \in H} e_p(ax) \right|^{4k^2} &= \left| \frac{1}{|H|} \left[\sum_{\substack{z \in \mathbb{F}_p \\ x \in H}} \omega(z) e_p(axz) \right] \right|^{2k} \\
&\leq \frac{1}{|H|^{2k}} \left(\sum_{z \in \mathbb{F}_p} \omega(z) \left| \sum_{x \in H} e_p(axz) \right| \right)^{2k} \\
&\overset{\text{(Hölder)}}{\leq} \frac{1}{|H|^{2k}} \left(\sum \omega(z) \right)^{2k-1} \left[\sum_z \omega(z) \left| \sum_{x \in H} e_p(axz) \right|^{2k} \right] \\
&= |H|^{4k(k-1)} \left| \sum_{z,z'} \omega(z) \omega(z') e_p(azz') \right| \\
&\overset{\text{(Hadamard)}}{\leq} |H|^{4k(k-1)} \|\omega\|_2^2 \sqrt{p} < |H|^{4k^2 - \delta}
\end{aligned}$$

proving Lemma 2.

Recall the classical bound

$$\max_{a\in\mathbb{F}_p^*}\left|\sum_{x\in H} e_p(ax)\right| \le \sqrt{p}|H|,$$

which is nontrivial for $|H| > \sqrt{p}$.

Prior to [B-G-K], completely explicit Gauss-sum estimates (with power-saving) for smaller groups (up to $|H| > p^{\frac{1}{4}+\varepsilon}$) had been obtained using variants of Stepanov's method (Garcia–Voloch, Shparlinski, Heath–Brown, Heath-Brown-Konyagin, Konyagin). In particular, one has

Proposition 1. *Let $H < \mathbb{F}_p^*$ and $|H| < p^{2/3}$. Then,*

$$E_{(2)}(H) \ll |H|^{\frac{5}{2}}$$

(see [K-S]). The proof is a variant of Stepanov's method.

Corollary 1. *If $H < \mathbb{F}_p^*$ and $|H| > p^{\frac{1}{3}+\varepsilon}$. Then*

$$\max_{a\in\mathbb{F}_p^*}\left|\sum_{x\in H} e_p(ax)\right| \ll p^{-\frac{3}{8}\varepsilon}|H|.$$

Proof. By Proposition 1

$$E_{(2)}(H) \ll |H|^4 p^{-\frac{3}{2}(\frac{1}{3}+\varepsilon)}$$

and Lemma 2 applies with $k = 1, \delta = \frac{3}{2}\varepsilon$. □

Proposition 2 ([Kon]). *Let $H < \mathbb{F}_p^*$, $|H| < p^{\frac{1}{2}}$. Then for $k \in \mathbb{Z}_+$*

$$E_{(k)}(H) \ll |H|^{2k-2+2^{1-k}}.$$

This allows us to replace the $\frac{1}{3}$-exponent by $\frac{1}{4}$.

Corollary 2 ([Kon]). *Let $H < \mathbb{F}_p^*$ and $p^{\frac{1}{4}+\varepsilon} < |H| < p^{\frac{1}{2}}$. Then*

$$\max_{a\in\mathbb{F}_p^*}\left|\sum_{x\in H} e_p(ax)\right| < p^{-\varepsilon_1}|H|$$

with

$$\varepsilon_1 = \max_{k\in\mathbb{Z}_+} \frac{1}{4k^2}\left(2\varepsilon - \left(\frac{1}{2}+2\varepsilon\right)4^{-k}\right).$$

The [B-G-K] exponents are still explicit but rather poor.

Combining Proposition 2 with the sum-product techniques, one gets for instance.

Proposition 3 ([B-G]). *Let $H < \mathbb{F}_p^*$ and $|H| > p^{\frac{1}{4}}$. Then,*

$$\max_{a\in\mathbb{F}_p^*}\left|\sum_{x\in H} e_p(ax)\right| < |H|^{0,999984073+o(1)}.$$

For even smaller groups, one has:

Proposition 4. *Let $H < \mathbb{F}_p^*$ and $|H| > p^{\alpha}$. Then*

$$\max_{a\in\mathbb{F}_p^*}\left|\sum_{x\in H} e_p(ax)\right| \ll p^{-e^{-5k}}|H|$$

if $k \geq 4$ is a power of 2 satisfying

$$\alpha k > \left(\frac{k}{2}\right)^{0,968}.$$

Present technology requires

$$\frac{\log|H|}{\log p} > \frac{C}{(\log\log p)}$$

for some constant C. See [B1].

On the other hand, there is the following conjecture due to Montgomery, Vaughan, and Wooley (partly based on numerics).

Conjecture ([M-V-W]).

$$\max_{(a,p)=1}\left|\sum_{x\in H} e_p(ax)\right| < \min\left(p^{\frac{1}{2}}, C(\log p)^{\frac{1}{2}}|H|^{\frac{1}{2}}\right).$$

According to this conjecture, $\frac{|H|}{\log p} \to \infty$ would imply equidistribution of H (mod p).

Problem. (related to Furstenberg's conjecture $\times 2, \times 3$).

Let G_p be the group generated by 2 and 3 in $\mathbb{F}_p^*$, thus,

$$G_p = \langle 2, 3\rangle < \mathbb{F}_p^*.$$

Does G_p become equidistributed for $p \to \infty$?

Remark.

$$\frac{\mathrm{ord}_p(2) + \mathrm{ord}_p(3)}{\log p} \to \infty \text{ for } p \to \infty$$

(Corvaja–Zannier, based on the subspace theorem).

See also [B-L-M-V] for recent developments.

5 Multilinear Exponential Sums

The [B-G-K] argument provides in fact more general results for products of arbitrary sets $A_j \subset \mathbb{F}_p^*$.

Theorem 1 ([B-G-K], [B-G]). *Let $k \geq 4$ be a power of 2 and $A_1, \ldots, A_k \subset \mathbb{F}_p^*$ satisfy*

$$|A_1| \ldots |A_k| > p^{(\frac{k}{2})^{0,968}}.$$

Then

$$\left| \sum_{x_1 \in A_1, \ldots, x_k \in A_k} e_p(x_1 \ldots x_k) \right| \ll p^{-e^{-5k}} |A_1| \cdots |A_k|.$$

Recall the classical (Hadamard) inequality for $k = 2$

$$\left| \sum_{x \in A, y \in B} e_p(xy) \right| \leq |A|^{\frac{1}{2}} |B|^{\frac{1}{2}} p^{\frac{1}{2}}.$$

This inequality is nontrivial provided $|A|.|B| > p$.

A multilinear analogue with sharp entropy requirement on the sources is given by the following:

Theorem 2 ([B1]). *Assume $0 < \delta < \delta_0 < \frac{1}{4}$ and $k \geq 3$.*

There is

$$\delta' > \left(\frac{\delta}{k} e^{-1/\delta_0} \right)^{Ck}$$

such that if $A_1, \ldots, A_k \subset \mathbb{F}_p$ satisfy

(i) $|A_i| > p^{\delta_0}$ *for* $i = 1, \ldots, k$

(ii) $|A_1| \cdots |A_k| > p^{1+\delta}$.

Then

$$\left| \sum_{x_1 \in A_1, \ldots, x_k \in A_k} e_p(x_1 \ldots x_k) \right| < p^{-\delta'} |A_1| \cdots |A_k|.$$

6 Extensions to 'Almost Groups'

New estimates on exponential sums involving exponential functions may be obtained as well.

Theorem 1. *For all $\delta > 0$, there is $\delta' > 0$ such that if $\theta \in \mathbb{Z}_+$ satisfies*

$(\theta, p) = 1$ *and* $O_p(\theta) \geq t > p^\delta$
$(O_p(\theta) =$ *multiplicative order of* θ *mod* $p)$

then

$$\max_{(a,p)=1} \left| \sum_{s=1}^{t} e_p(a\theta^s) \right| < tp^{-\delta'}$$

Thus the sum may be incomplete. This result has many applications (see [K-S]), in particular.

Number fields.
Minimum norm representatives in residue classes and the Euclidean division algorithm in algebraic number fields (Egami's problem).

Coding theory.
The Odlyzko–Stanley enumeration problem.

Hyperelliptic curves.
Supersingularity of mod p reduction (Kodama's problem).
See [K-S] for details.

7 Sum-Product Theorem and Gauss Sums in Arbitrary Finite Fields

The results for prime fields generalize as follows.

Theorem 1 ([B-K-T], explicit exponents in [K-S]). *Assume $S \subset \mathbb{F}_q, |S| > q^\delta$ ($\delta > 0$ arbitrary) and*

$$|S + S| + |S.S| < K|S|.$$

Then there is a subfield G of $\mathbb{F}_q$ and $\xi \in \mathbb{F}_q^*$ such that

$$|G| < K^C|S|$$

and

$$|S \backslash \xi G| < K^C$$

where $C = C(\delta)$.

Exponential sum bounds in $\mathbb{F}_q$.

$$q = p^m \qquad Tr(x) = x + x^p + \cdots + p^{m-1}$$
$$\psi(x) = e_p(Tr(x)) \qquad \text{additive character.}$$

Theorem 2 ([B-C]). *Let $g \in \mathbb{F}_q^*$ of order t and*

$$t \geq t_1 > q^{\varepsilon}$$
$$\max_{\substack{1 \leq \nu < m \\ \nu | m}} gcd\,(p^\nu - 1, t) < q^{-\varepsilon} t$$

($\varepsilon > 0$ arbitrary).
Then

$$\max_{a \in \mathbb{F}_q^*} \left| \sum_{j \leq t_1} \psi(a g^j) \right| < C q^{-\delta} t_1$$

where $\delta = \delta(\varepsilon) > 0$.

8 The Case of General Polynomial (mod p)

We first recall Weil's estimate.

Theorem 1 (Weil). *Let $f(x) \in \mathbb{F}_p[X]$ of degree d. Then*

$$\left| \sum_{1 \leq x \leq p} e_p(f(x)) \right| \leq d\sqrt{p}.$$

Problem. Obtain non-trivial estimates for $d \geq \sqrt{p}$.

Sum-product technology enables one to obtain such results for special (sparse) polynomials (as considered by Mordell, cf. [Mor]).

Theorem 2 ([B2]). *Let*

$$f(x) = \sum_{i=1}^{r} a_i x^{k_i} \in \mathbb{Z}[X] \text{ and } (a_i, p) = 1$$

such that

$$(k_i, p-1) < p^{1-\delta} \qquad (1 \leq i \leq r)$$
$$(k_i - k_j, p-1) < p^{1-\delta} \qquad (1 \leq i \neq j < r).$$

Then

$$\left| \sum_{x=1}^{p} e_p\left(f(x)\right) \right| < Cp^{1-\delta'}$$

where $\delta' = \delta'(r, \delta) > 0 \quad (\delta > 0$ *arbitrary).*

The following example shows that the second condition is necessary.

Example (Cochrane–Pinner). Let

$$f(x) = x^{\frac{p-1}{2}+1} - x.$$

Then

$$\begin{aligned} \sum e_p(f(x)) &= \frac{p-1}{2} + \sum_{(\frac{x}{p})=-1} e_p(-2x) \\ &= \frac{p-1}{2} + 0(\sqrt{p}). \end{aligned}$$

Theorem 3. *Let* $\theta_1, \ldots, \theta_r \in \mathbb{F}_p^*$ *satisfy* ($\delta > 0$ *arbitrary)*

$$\begin{aligned} 0(\theta_i) &> p^{\delta} \qquad (1 \le i \le r) \\ 0(\theta_i \theta_j^{-1}) &> p^{\delta} \qquad (1 \le i \ne j \le r). \end{aligned}$$

Then, for $t > p^{\delta}$

$$\max_{a_i \in \mathbb{F}_p^*} \left| \sum_{s=1}^{t} e_p \left(\sum_{i=1}^{r} a_i \theta_i^s \right) \right| < Cp^{-\delta'} t$$

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

Applications to cryptography and distributional properties of Diffie–Hellman triples $\{\theta^x, \theta^y, \theta^{xy}\}$.

Power generators $u_{n+1} = u_n^e$.

Blum-Blum-Shub generator ($e = 2$).

Theorems 2 and 3 rely on an extension of the sum-product theorem to Cartesian products.

Theorem 4. *Fix* $\varepsilon > 0$. *There is* $\delta'(\delta) \overset{\delta \to 0}{\longrightarrow} 0$ *such that if*

$$A \subset \mathbb{F}_p \times \mathbb{F}_p \quad (p^{\epsilon} < |A| < p^{2-\varepsilon})$$

and

$$|A + A| + |A.A| < p^{\delta}|A|$$

then

$$p^{1-\delta'} < |A| < p^{1+\delta'}$$

and there is a line $L \subset \mathbb{F}_p \times \mathbb{F}_p$ *of the form*

$$L = \{a\} \times \mathbb{F}_p, L = \mathbb{F}_p \times \{a\},$$

$$L = \{(x, ax) | x \in \mathbb{F}_p\}$$

such that

$$|A \cap L| > p^{1-\delta'}.$$

9 The Sum-Product in $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$

Because of the presence of subrings when q is composite, additional restrictions on $A \subset \mathbb{Z}_q$ are needed.

The following gives a uniform statement in the modulus q.

Theorem 1 ([B3]). *Given* $0 < \delta_1 < 1$, $0 < \delta_2 < 1$, *there are* $\varepsilon = \varepsilon(\delta_1, \delta_2) > 0$ *and* $\gamma = \gamma(\delta_1, \delta_2) > 0$ *such that the following holds.*

Let $A \subset \mathbb{Z}_q$ *(q arbitrary and large enough) satisfy:*

(i) $|A| < q^{1-\delta_1}$

(ii) $|\pi_{q_1}(A)| > q_1^{\delta_2}$ *for all* $q_1 | q$ *with* $q_1 > q^{\varepsilon}$ *where* $\pi_{q_1} : \mathbb{Z}_q \to \mathbb{Z}_{q_1}$ *is the quotient map.*

Then

$$|A + A| + |A.A| > q^{\gamma}|A|.$$

Remark. Let $q = p_1^{m_1} p_2^{m_2} \ldots$ be the prime factorization. Then

$$\mathbb{Z}_q \simeq \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \ldots$$

We first establish the theorem for $q = p^m$ a prime power (with uniformity in p and m) and then recombine the factors.

Gauss sums (mod q).

Theorem 2 ([B4]). *For all* $\varepsilon > 0$, *there is* $\delta = \delta(\varepsilon)$ *such that if* $H < \mathbb{Z}_q^*$ *(q arbitrary) satisfies*

$$|H| > q^{\varepsilon}.$$

Then

$$\max_{\xi \in \mathbb{Z}_q^*} \left| \sum_{x \in H} e_q(\xi x) \right| < q^{-\delta}|H|.$$

Corresponding statement for incomplete sums is more restrictive.

Example. $q = p^2$.

Take $g = 1 + p$. Then

$$g^s \equiv 1 + sp \pmod{q}.$$

Hence

$$\left| \sum_{1 \le s < \frac{p}{5}} e_q(g^s) \right| \sim p.$$

Theorem 3 ([B3]). *Given $\varepsilon > 0$, there is $\delta = \delta(\varepsilon) > 0$ such that the following holds.*

Let $q \in \mathbb{Z}_+$ be large enough and $g \in \mathbb{Z}_q^*$ satisfy

$$ord_{q_1}(g) > q_1^{\varepsilon} \text{ whenever } q_1 | q, q_1 > q^{\delta}.$$

Then for $t > q^{\varepsilon}$

$$\max_{\xi \in \mathbb{Z}_q^*} \left| \sum_{1 \le s \le t} e_q(\xi g^s) \right| < t^{1-\delta}.$$

Special Case. $q = p^m$ (p fixed) and g fixed ($m \to \infty$).

Remark. $\operatorname{ord}_{p^m}(g) \sim p^m$.

There is the following more precise result due to Korobov.

Theorem 4 ([Kor]). *Given p and $g \in \mathbb{Z}_+, g \ge 2$, there is a constant $\rho = \rho(p, g)$ such that for $m \to \infty$, $t < q = p^m$*

$$\max_{(\xi, p)=1} \left| \sum_{s=1}^{t} e_{p^m}(\xi g^s) \right| \ll t . \exp\left(-\rho \frac{(\log t)^3}{(\log q)^2} \right).$$

This estimate is non-trivial for $\log t \gg (\log q)^{\frac{2}{3}}$.

Sketch of the Proof.

Fix d and take $m_1 \in \mathbb{Z}_+$ with $d m_1 < m \le (d+1) m_1$.

Take $s_1 < p^{m_1}$ such that $g^{s_1} \equiv 1 (\operatorname{mod} p^{m_1})$. Hence $g^{s_1} = 1 + b p^{m_1}$.

Apply the binomial formula

$$g^{k s_1} = (1 + b p^{m_1})^k \equiv \sum_{j \le d} \binom{k}{j} b^j p^{j m_1} \pmod{p^m}.$$

This is a polynomial in k of degree $d < \frac{m}{m_1}$.

Take m_1 with $p^{m_1} < t^{\frac{1}{4}}$ and $N \sim t^{\frac{1}{4}}$. Write

$$\sum_{1\le x,y\le N} e_{p^m}(\xi g^{s_1 xy}) = \sum_{1\le x,y\le N} e\left(F(x,y)\right)$$

where

$$F(x,y) = \sum_{j\le d} \binom{xy}{j} b^j \frac{1}{p^{m-jm_1}}.$$

Apply then Vinogradov exponential sum bound.
$\Rightarrow$ nontrivial estimate provided $d^2 = o(\log N)$, hence for

$$m^2 = o\left((\log t)^3\right).$$

There is the following general multilinear bound for composite modulus.

Theorem 5 ([B3]). *Given $\varepsilon > 0$, there are $\delta > 0$ and $k \in \mathbb{Z}_+$ such that if $A_1, \dots, A_k \subset \mathbb{Z}_q$ (q arbitrary) satisfy*

$$|A_i| > q^{\varepsilon} \qquad (1 \le i \le k)$$

and also

$$\max_{\xi\in\mathbb{Z}_{q_1}} \left|A_i \cap \pi_{q_1}^{-1}(\xi)\right| < q_1^{-\varepsilon}|A_i| \text{ whenever } q_1|q, q_1 > q^{\delta}.$$

Then

$$\left|\sum_{x_1\in A_1,\dots,x_k\in A_k} e_q(x_1\dots x_k)\right| < q^{-\delta}|A_1|\cdots|A_k|.$$

10 Exponential Sums in Finite Commutative Rings

Let R be a finite commutative ring with unit and assume

$$|R| = q \text{ with no small prime divisors.}$$

Denote $R^* =$ invertible elements.

Theorem 1 ([B5]). *Let $H < R^*, |H| > q^{\delta}$ (δ arbitrary).*

For all $\varepsilon > 0$, there is $\varepsilon' = \varepsilon'(\varepsilon) \to 0$ such that one of the following alternatives holds

(1) $\max_{\mathcal{X}\neq\mathcal{X}_0} \left|\sum_{x\in H} \mathcal{X}(x)\right| < |H|^{1-\varepsilon}$

($\mathcal{X} =$ *additive character of* R).

(2) There is nontrivial ideal I in R with

$$|H \cap (1+I)| > |H|^{1-\varepsilon'}.$$

(3) There is a nontrivial subring R_1 of R, such that $1 \in R_1$ and

$$|H \cap R_1| > |H|^{1-\varepsilon'}.$$

Application to Heilbronn sums (dv. [Od]).

Theorem 2 ([B4]). *For given $m \in \mathbb{Z}_+, m \geq 2$ and $r \geq 1$, there is $\delta = \delta(m,r) > 0$ such that*

$$\left| \sum_{x=1}^{p} e_{p^m} \left(\sum_{s=1}^{r} a_s x^{sp^{m-1}} \right) \right| < p^{1-\delta}$$

for p (prime) sufficiently large and $(a_1, \ldots, a_r) \in \mathbb{Z}_{p^m}^r \setminus \{0\}$.

Remark. Since $(x+py)^{p^{m-1}} \equiv x^{p^{m-1}} \pmod{p^m}$, the sum is complete.

Earlier results.

Heath–Brown,(1995), $\delta(2,1) = \frac{1}{12}$ ([H-B]).
Heath–Brown, Konyagin, (2000), $\delta(2,1) = \frac{1}{8}$ ([H-K]).
Malykhin-Bourgain-Chang, (2005), $\delta(m,1)$ for general m. (see [B-C3]).

11 Euclidean Algorithm in Algebraic Number Fields

Let K be a given algebraic number field and O its maximal order.
Let I be an integral ideal and $\alpha \in O/I$. Define

$$N_I(\alpha) = \min_{x \in \alpha} |N(x)|$$

(the minimal norm (taken in $\mathbb{Q}$) of all elements of α.)
Define further

$$L(K,I) = \max_{\alpha \in (O/I)^*} N_I(\alpha).$$

One has always the inequality

$$L(K,I) \leq N(I) = |O/I|.$$

K is an Euclidean field if

$$L(K,I) < N(I)$$

for all principal ideals I.

Only a few examples are known. For instance (cf. [K-S]), the only Euclidean quadratic fields $\mathbb{Q}(\sqrt{d})$ are obtained for

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

However, if K has an infinite group $U(K)$ of units or equivalently, if

$$r_1 + r_2 - 1 > 0$$

where $[K : \mathbb{Q}] = n = r_1 + 2r_2$, with r_1 (resp. r_2) the number of real (resp. complex) embeddings of K in $\mathbb{C}$, then K is 'almost Euclidean' in the sense that

$$L(K, I) = o(N(I))$$

for almost all ideals I (Egami's problem).
(results by Konyagin–Shparlinski, Bourgain–Chang, ...).
More precise statements obtained in [B-C2].

Prime ideal case.

Denote $\pi_K(T)$ the number of prime ideals of norm $\leq T$. Then

$$\pi_K(T) = (1 + o(1)) \frac{T}{\log T}.$$

Theorem 1 ([B-C2]). *For all $\varepsilon > 0$, there is $\delta = \delta(\varepsilon, K) > 0$ such that for $T \to \infty$*

$$|\{\mathcal{P} | \mathcal{P} \text{ prime ideal with } N(\mathcal{P}) \leq T, L(K, \mathcal{P}) > N(\mathcal{P})^{1-\delta}\}| < T^{\varepsilon}.$$

General integral ideals.

Denote $M(T)$ the number of ideals I in O of norm $N(I) \leq T$. Then

$$M(T) = (h(K)\kappa + o(1))\, T$$

where

$$\begin{aligned} h(K) &= \text{ class number} \\ \kappa = \kappa(K) &= 2^{r_1}(2\pi)^{r_2} R(K) |d\,(K)|^{-\frac{1}{2}}\, w(K)^{-1} \\ R(K) &= \text{ regulator} \\ d(K) &= \text{discriminant} \\ w(K) &= |E(K)|. \end{aligned}$$

Theorem 2 ([B-C2]). *There is $\delta' = \delta'(\delta) \to 0$ with $\delta \to 0$ such that*

$$L(K, I) < N(I)^{1-\delta}$$

for ideals I outside a sequence of asymptotic density at most δ'.

Main idea.

Consider the quotient map $\varphi : O \to O/I$.
If

$$I = \prod \mathcal{P}^{a(\mathcal{P})} \quad \text{(prime ideal factorization)}$$

then

$$O/I = \prod O/\mathcal{P}^{a(\mathcal{P})}.$$

Let $U = U(K)$ be the group of units and consider

$$G = \varphi(U) < (O/I)^*.$$

The main issue is to establish equidistribution results of G in O/I.

12 Application to QUE

We refer the reader to [K-R] for background material.

The Quantum Cat Map.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and consider the toral automorphism $\mathbb{T}^2 \to \mathbb{T}^2$: $x \mapsto Ax$.

The classical evolution on $\mathcal{C}^\infty(\mathbb{T}^2)$ is defined by

$$f \to f \circ A.$$

We describe next the quantization of Hannay and Berry. Assume

$$ab \equiv cd \equiv 0 \pmod 2.$$

Let $N \in \mathbb{Z}_+$ and consider the Hilbert space

$$\mathcal{H}_N = L^2(\mathbb{Z}_N) \qquad \mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$$

with inner product

$$\langle \phi, \psi \rangle = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} \phi(x)\, \overline{\psi(x)}.$$

We associate to $f = \sum_{n \in \mathbb{Z}^2} \hat{f}(n) e^{2\pi i n x}$ in $C^\infty(\mathbb{T}^2)$ its 'quantization' $Op_N(f)$ acting on $\mathcal{H}_N$ and defined by

$$Op_N(f) = \sum_{n \in \mathbb{Z}^2} \hat{f}(n) T_N(n)$$

where

$$T_N(n)\phi(x) = e^{i\pi\frac{n_1 n_2}{N}} e^{2\pi i \frac{n_2 x}{N}} \phi(x + n_1).$$

One may then assign to A a unitary operator $U_N(A)$ called 'quantum propagator' satisfying the 'exact' Egorov theorem

$$U_N(A)^* Op_N(f) U_N(A) = Op_N(f \circ A).$$

We are concerned with the eigenfunctions ψ of $U_N(A)$.

In the context of cat maps, Schnirelman's general theorem takes the following form.

Let $f \in \mathcal{C}^\infty(\mathbb{T}^2)$ and let for each $N \in \mathbb{Z}_+$, $\{\psi_j\}_{1 \le j \le N}$ be an orthonormal basis of $\mathcal{H}_N$ of eigenfunctions of $U_N(A)$. Then there is a subset $J(N) \subset \{1, \dots, N\}$ such that

$$\frac{\#J(N)}{N} \to 1 \text{ for } N \to \infty$$

and

$$\langle Op_N(f)\psi_j, \psi_j \rangle \to \int_{\mathbb{T}^2} f$$

when $j \in J(N), N \to \infty$.

The result of Kurlberg and Rudnick [K-R] goes beyond this, showing that there is $\mathcal{N} \subset \mathbb{Z}_+$ of asymptotic density 1, such that

$$\max_j \left| \langle Op_N(f)\psi_j, \psi_j \rangle - \int_{\mathbb{T}^2} f \right| \xrightarrow{N \to \infty, N \in \mathcal{N}} 0.$$

More precisely they obtain the inequality

$$\sum_{j=1}^{N} \left| < O_{p_N}(f)\psi_j, \psi_j \rangle - \int_{\mathbb{T}^2} f \right|^4 \ll \frac{N(\log N)^{14}}{\mathrm{ord}(A, N)^2}$$

where $\mathrm{ord}(A, N)$ denotes the order of $A \pmod N$.

Next they show that

$$\mathrm{ord}(A, N) \gg N^{\frac{1}{2}} \exp\left((\log N)^\delta\right) \qquad (*)$$

for some $\delta > 0$ and N restricted to $\mathcal{N} \subset \mathbb{Z}_+$ of asymptotic density 1.

Problem ([K-R]). What if $\mathrm{ord}(A, N) < N^{\frac{1}{2}}$?

It turns out one may now deal with the case $\mathrm{ord}(A, N) > N^\varepsilon$ for any $\varepsilon > 0$. The following results are obtained in [B5].

Proposition 1. *[B6] For all $\varepsilon > 0$, there is $\delta > 0$ such that if N is prime and $\mathrm{ord}(A, N) > N^{\varepsilon}$, then*

$$\max_{\psi} |\langle T_N(n)\psi, \psi\rangle| < N^{-\delta}$$

with ψ a normalized eigenfunction of $U_N(A)$.

Theorem 2. *[B6] (N prime).*

For all $\varepsilon > 0$, there is $\delta > 0$ and a sequence $\mathcal{S}_\varepsilon$ of primes such that

$$\#\{N \in \mathcal{S}_\varepsilon | N < T\} \ll T^{\varepsilon}$$

and for given $f \in \mathcal{C}^\infty(\mathbb{T}^2)$

$$\max_{\psi} \left| \langle Op_N(f)\psi, \psi\rangle - \int_{\mathbb{T}^2} f \right| < N^{-\delta}$$

for N a sufficiently large prime outside $\mathcal{S}_\varepsilon$.

Theorem 3. *[B6] (N general).*

There is a density 1 sequence $\mathcal{N} \subset \mathbb{Z}_+$ and $\delta > 0$ such that for all observables $f \in \mathcal{C}^\infty(\mathbb{T}^2)$

$$\max_{\psi} \left| \langle Op_N(f)\psi, \psi\rangle - \int_{\mathbb{T}^2} f \right| < C_f N^{-\delta}$$

for $N \in \mathcal{N}$.

Sketch of the Proof of Proposition 1.

$N = p$ (prime).
$K =$ real quadratic field containing eigenvalues of A (units).
$O =$ maximal order of K.
$\mathcal{P} =$ prime of K lying above p.
Denote

$$K_p = O/\mathcal{P} \simeq \begin{cases} \mathbb{F}_p \text{ if } p \text{ splits} \\ \mathbb{F}_{p^2} \text{ if } p \text{ is inert.} \end{cases}$$

Diagonalize A over K_p. Thus

$$A' = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} \qquad \varepsilon \in K_p^*.$$

Problem reduces then to an estimate on the number of solutions of the following system in K_p.

$$\begin{cases} \sum_{s=1}^{4\ell} (-1)^s \varepsilon^{j_s} = 0 \\ \sum_{s=1}^{4\ell} (-1)^s \varepsilon^{-j_s} = 0 \end{cases}$$

with $(j_1, \ldots, j_{4\ell}) \in \{1, \ldots, t\}^{4\ell}$ and $t = \mathrm{ord}_{K_p}(\varepsilon)$.

Use of exponential sum bounds with ℓ taken large enough. We distinguish 2 cases.

Split Case. $K_p = \mathbb{F}_p$.

Bounds on $\sum_{j=1}^{t} e_p(a_1\varepsilon^j + a_2\varepsilon^{-j})$. Apply theorems 3 from Sect.Ṡ8.

Inert Case. $K_p = \mathbb{F}_{p^2}$.

Bounds on $\sum_{j=1}^{t} e_p\left(Tr(a_1\varepsilon^j) + Tr(a_2\varepsilon^{-j})\right)$.

Apply Theorem 2 from Sect. 7 and Theorem 3 from Sect. 8. (2 further cases must be distinguished in view of the condition in Theorem 2, Sect. 7.)

References

[B1] J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, GAFA 18 (2009), no 5, 1477–1502.

[B2] J. Bourgain, *Mordell's exponential sum estimate revisited*, JAMS 18(2) (2005), 477–499.

[B3] J. Bourgain, The *Sum-product theorem in $\mathbb{Z}_q$, with q arbitrary*, J. Analyse 106 (2008), 1–93.

[B4] J. Bourgain, *Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary*, J. Analyse 97 (2005), 317–356.

[B5] J. Bourgain, *Exponential sum estimates in finite commutative rings and applications*, J. Analyse Math., 101 (2007), 325–355.

[B6] J. Bourgain, *A remark on quantum ergodicity for cat maps*, Springer, Berlin, lMN, 1910 (2007), 89–98.

[B-C1] J. Bourgain, M. Chang, *A Gauss sum estimate in arbitrary finite fields*, C.R. Math. Acad. Sci. Paris 342(9) (2006), 643–646.

[B-C2] J. Bourgain, M. Chang, *On the minimum norm of representatives of residue classes in number fields*, Duke Math. J. 138(2) (2007), 263–280.

[B-C3] J. Bourgain, M. Chang, *Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors*, GAFA 16(2) (2006), 327–366.

[B-G] J. Bourgain, M.Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Camb. Phil. Soc. (2008).

[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*, J. London Math. Soc. 73 (2006), 380–398.

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

[B-L-M-V] J. Bourgain, E. Lindenstrauss, P. Michel, A. Venkatesh, *Some effective results for a, b*, ETDS, vol 29, 06 (2009), 1705–1722.

[Ga] M. Garaev, *An explicit sum-product estimate in $\mathbb{F}_p$*, IMRN (2007), no 11.

[H-B] D.R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, Analytic Number Theory: The Halberstam Festschrift (B.C. Berndt, H.G. Diamond, A.J. Hildebrand, eds.), 451–463 (Progress in Mathematics 138/139, Birkhäuser-Verlag, Boston 1996).

[H-K] D.R. Heath-Brown, S.V. Konyagin, *New bounds for Gauss sum derived from k-th powers and for Heilbronn's exponential sum*, Q. J. Math. 51 (2003), 221–335.

[Ka-S] N. Katz, C.-Y. Shen, *A slight improvement to Garaev sum-product estimate*, Proc. AMS 136(7) (2008), 2499–2504.

[Kon] S.V. Konyagin, *Estimates for trigonometric sums over subgroups and for Gauss sums*, International Conference on Modern Problems of Number Theory and its Applications: Current Problems, Part III, 86–114 (Moscow State University, 2002) (in Russian).

[Kor] N. Korobov, *The distribution of digits in periodic fractions*, Math. Sb. (N.S) 89(131) (1972), 654–670.

[K-S] S.V. Konyagin, I.E. Shparlinski, *Character Sums with Exponential Functions and their Applications* (Cambridge Tracts in Mathematics 136, Cambridge University Press, Cambridge 1999).

[K-R] P. Kurlberg, Z. Rudnick, *On quantum ergodicity for linear maps of the torus*, Comm. Math. Phys. 222 (201), 201–227.

[M-V-W] H. Montgomery, R. Vaughan, T. Wooley, *Some remarks on Gauss sums associated with kth powers*, Math. Proc. Cambridge Philos. Soc. 118(1) (1995), 21–22.

[Mor] L.J. Mordell, *On a sum analogous to a Gauss sum*, Q.J. Math. 3 (1932), 161–162.

[Od] R.W.K. Odoni, *Trigonometric sums of Heilbronn's type*, Math. Proc. Cambridge Philos. Soc. 98 (1985), 389–396.

[T-V] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced mathematics, vol. 105, Cambridge University Press, Cambridge (2006).

http://www.springer.com/978-0-387-37029-3

Additive Number Theory
Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson
Chudnovsky, D.; Chudnovsky, G. (Eds.)
2010, XI, 361 p., Hardcover
ISBN: 978-0-387-37029-3