Van Der Corput's Lemma in Number Theory and Analysis and its Applications to Abelian Varieties with Prescribed Groups

Valentine Chiche-Lapierre

A Thesis
In the Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science (Mathematics) at
Concordia University
Montreal, Quebec, Canada

June, 2014

CONCORDIA UNIVERSITY
SCHOOL OF GRADUATE STUDIES

This is to certify that the thesis prepared

By: **Valentine Chiche-Lapierre**

Entitled: **Van Der Corput's Lemma in Number Theory and Analysis and its Applications to Abelian Varieties with Prescribed Groups**

and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Mathematics)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Approved by _____ Chair
Dr. Chris Cummins

Approved by _____ Examiner
Dr. Hershy Kisilevsky

Approved by _____ Supervisor
Dr. Galia Dafni

Approved by _____ Supervisor
Dr. Chantal David

Approved by _____
Dr. J. Garrido, Graduate Program Director

June 27, 2014 _____

Faculty of Arts and Science

ABSTRACT

Van Der Corput's Lemma in Number Theory and Analysis and its Applications to Abelian Varieties with Prescribed Groups

Valentine Chiche-Lapierre, Master

Concordia University, 2014

Let A be an Abelian variety over a finite field $\mathbb{F}_q$. We are interested in knowing the distribution of the groups $A(\mathbb{F}_q)$ of rational points on A as we run over all varieties defined over $\mathbb{F}_q$. In particular, we want to show that they are in general not too "split". For the case of dimension 1 (elliptic curves) and dimension 2 (Abelian surfaces), there are some theoretical results due to David and her collaborators, but the general case is open.

We are interested in Abelian Varieties of dimension 3. We use Rybakov's criterion, which relates the existence of a given abstract group as the group of points of some Abelian variety to properties of the characteristic polynomial of the variety. We can use it to derive precise properties and then we use the fact that some sequence of monomials of five variables is uniformly distributed modulo one to obtain stronger results that will hold with probability one.

By Weyl's criterion, equidistribution follows by bounding exponential sums, and in order to do so, we will use a combination of different methods. We are particularly interested in Van Der Corput's lemma. It has a continuous version that exhibits the decay of oscillatory integrals and a discrete version that gives a bound for exponential sums. We will see the relation between these two versions and how they apply to the original problem of Abelian varieties.

ACKNOWLEDGEMENTS

I would like to thank my colleagues Nicholas Beck, who read my work and made many valuable suggestions; Alex Cowan, with who I first discussed the idea of generalizing to higher dimension the results known for Abelian surfaces and who found some results that I used; and Patrick Meisner, for his useful remark on Rybakov's Theorem.

I would especially like to thank my supervisors Dr. Galia Dafni and Dr. Chantal David whose guidance and advice lead me to this.

Contents

NOTATION

symbol	meaning
$e(x)$	$e^{2\pi i x}$
$\hat{f}$	the Fourier transform of f, $\int_{-\infty}^{\infty} f(x)e(-x\xi)dx$
$\partial^\alpha f$	directional derivative, that is $\frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{\partial^{\alpha_d}}{\partial x_d^{\alpha_d}} f$ of order $\lvert\alpha\rvert = \alpha_1 + \cdots + \alpha_d$, where $\alpha = (\alpha_1, \ldots, \alpha_d)$
$\mathcal{C}^k$	functions of real variables with continuous derivatives of order k
$\mathcal{C}^\infty$	functions of real variables whose derivatives of any order are continuous
$f = O(g)$	there exists an absolute constant $c > 0$ such that $\lvert f\rvert \leq c\lvert g\rvert$
$f \ll g$	same as $f = o(g)$
$f \ll_\delta g$	$f \ll g$, where the implied constant is allowed to depend on δ
$f = o(g)$	$f/g \to 0$
$f \approx g$	both $f \ll g$ and $f \gg g$
$n \asymp N$	$N \leq n \leq 2N$

List of Figures

Chapter 0

Introduction

Let A be an Abelian variety of dimension 3 over a finite field $\mathbb{F}_q$, for some prime power q. Previous results about the dimension 1 (elliptic curves) and the dimension 2 (Abelian surfaces) will be stated at the beginning of Chapter 4. Let $A(\mathbb{F}_q)$ be the group of rational points on A. It is well known that $A(\mathbb{F}_q)$ form an Abelian group of rank at most 6 i.e.

$$A(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5n_6\mathbb{Z}, \tag{1}$$

for some positive integers $n_1, n_2, n_3, n_4, n_5, n_6$. We are interested in knowing which groups can occur for $A(\mathbb{F}_q)$. In fact, we will show that the group $A(\mathbb{F}_q)$ tends to be not too "split". This is compatible with the general philosophy of the Cohen-Lenstra heuristics, which predict that random Abelian groups naturally occur with probability inversely proportional to the size of their automorphism groups.

Using Rybakov's criterion, we first find the following, which is an analogue of Theorem 1.1 in [DGS+13].

Theorem 0.0.1. *Suppose that*

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5n_6\mathbb{Z}$$

is the group of points of an Abelian variety of dimension 3.

If $15n_2^{2/2}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3} \notin \mathbb{Z}$, *then*

$$n_1 \leq 2800n_2^{7/6}n_3^{10/3}n_4^{5/2}n_5^{5/3}n_6^{5/6}.$$

We want to get a stronger result that will hold with probability one.For some large integers $N_1, N_2, N_3, N_4, N_5, N_6$, let $S(N_1, N_2, N_3, N_4, N_5, N_6)$ be the set of sextuples $(n_1, n_2, n_3, n_4, n_5, n_6)$, for which $N_j \leq n_j \leq 2N_j$ for each $j = 1, 2, 3, 4, 5, 6$, and there exists a prime power q and an Abelian variety $A/\mathbb{F}_q$ of dimension 3 such that (1) holds. Let us now state our main result, which is an analogue of Theorem 1.2 in [DGS+13].

Theorem 0.0.2. *Suppose that*

$$\log N_4 \ll (N_2N_3N_5N_6)^{1/100}.$$

If

$$\frac{N_1N_2^{1/6}}{N_3^{2/3}N_4^{1/2}N_5^{1/3}N_6^{1/6}} \to \infty$$

as $N_2N_3N_5N_6 \to \infty$, *then*

$$\#S(N_1, N_2, N_3, N_4, N_5, N_6) = o(N_1N_2N_3N_4N_5N_6)$$

as $N_2N_3N_5N_6 \to \infty$.

We will give the proof of this theorem in Chapter 4. The main steps of this proof can be considered analogous to the steps provided in [DGS+13]. We will see that an important step of this proof involves the fact that a specific sequence of several variables is uniformly distributed modulo one. By an analogue of Weyl's criterion for higher dimension (that we will prove in Chapter 4), it is enough to find a bound that beats the trivial one in all the variables for a specific family of exponential sums. Chapter 3 is a proof of the existence of such a bound. Let

$$E_k := E_k(N_2, N_3, N_4, N_5, N_6) := \sum_{N_j \leq n_j \leq 2N_j} e(15kn_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3})$$

be the exponential sum that we need to bound in order to prove that the sequence $15n_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}$ is equistributed modulo one. We will show the following:

Proposition 0.0.3. *Suppose that*

$$\log N_4 \ll (N_2N_3N_5N_6)^{1/100}, \tag{2}$$

then for all non zero integer k,

$$E_k = o(N_2N_3N_4N_5N_6) \text{ as } N_2N_3N_5N_6 \to \infty.$$

We will use a combination of methods to bound exponential sums and see that the most important of these is Van Der Corput's lemma.

Van Der Corput's lemma has a discrete version that gives a bound for exponential sums and a continuous version that gives a bound for oscillatory integrals. In general an oscillatory integral is one of the form

$$I(\lambda) = \int_{\mathbb{R}^d} e^{i\lambda\phi(x)}\psi(x)dx,$$

for some variable positive parameter λ, some phase function ϕ and some amplitude function ψ. All the results that we will state and prove rely on the fact that if the phase is smooth then the main contribution of $I(\lambda)$ comes from the points x where the gradient of the phase is vanishing. This is called the stationary phase principle. Note that we will show an interest in the asymptotic behaviour of these integrals for large values of λ because it is important for other applications in analysis.

Reading some of the seminal works that use Van Der Corput's methods, we note that they do not seem to agree on what Van Der Corput's lemma is. To avoid any confusion we will state and give names to the two versions of Van Der Corput's lemma that we will be interested in.

Theorem 0.0.4. (Analytic /Continuous Van Der Corput's lemma)

1) If $|\phi'(x)| \geq \lambda > 0$ *for all* $x \in [a,b]$ *and* $\phi'(x)$ *is monotonic then*

$$\left| \int_a^b e^{i\phi(x)} dx \right| \leq 3\lambda^{-1}.$$

2) If $k \geq 2$ *and* $\left|\phi^{(k)}(x)\right| \geq \lambda > 0$ *for all* $x \in [a,b]$ *then*

$$\left| \int_a^b e^{i\phi(x)} dx \right| \leq 2^k \lambda^{-1/k}.$$

We will prove this in Chapter 1, using the book of Stein and Shakarchi [SS11] as a reference, while also proving several other key results relating to bounds on oscillatory integrals.

Chapter 2 is the important link between bounds on oscillatory integrals and bounds on exponential sums. We now state the result from Chapter 2 that we will need in Chapter 3.

Theorem 0.0.5. (Discrete Van Der Corput's Lemma / kth derivative test) *Let* k *be an integer with* $k \geq 3$. *Suppose* $f \in \mathcal{C}^k$ *and* $\left|f^{(k)}(x)\right| \approx \lambda > 0$ *for all* $x \asymp N$. *Let* $Q = 2^{(k-2)}$, *then*

$$\sum_{n \asymp N} e(f(n)) \ll N\lambda^{-1/(4Q-2)} \quad \textit{provided} \quad \lambda^{-Q/(2Q-1)} \ll N,$$

where the implied constants in each $\ll$ *are allowed to depend on the implied constants in* $\approx$.

Note that we are no longer interested in large values of λ but in large intervals. The main references for this are [Mon94] that makes the link between oscillatory integrals and exponential sums and [Ten95], which gives a property equivalent to the case $k = 3$ for Theorem 0.0.5. Even though the proof of this is original, it is a well known fact that can easily be deduced from a stronger but more complicated theorem that can be found in [GKK91].

When we are looking for bounds on exponential sums, the idea is mainly to use successive kth derivative tests. Using this and Weyl's criterion, we can show the well known fact that for all non-integer positive real numbers α, the sequence n^α is equidistributed modulo one. We also believe that a similar result can be obtained for a multi-variable sequence of monomials. In fact, we were able to show it for bi-variate sequences of monomials.

Proposition 0.0.6. *Let $f(n_1, n_2) = r n_1^{\alpha_1} n_2^{\alpha_2}$, with α_1, α_2 non integer positive real numbers, be a bi-variate sequence, then $f(n_1, n_2)$ is equidistributed modulo one.*

Chapter 1

Oscillatory integrals and stationary phase

Our only reference for this chapter is the book of Stein and Shakarchi [SS11]. We are interested in a special kind of integral called an oscillatory integral that we define by

$$I(\lambda) = \int_{\mathbb{R}^d} e^{i\lambda\phi(x)}\psi(x)dx,$$

where ϕ and ψ are two functions that map $\mathbb{R}^d$ to $\mathbb{R}$ and are called the phase and the amplitude, respectively, and λ is a positive real number that can vary. We are interested in particular in the behaviour of $I(\lambda)$ when λ is large.

We will usually need ϕ and ψ in $\mathcal{C}^k$, for some k. For simplicity we will assume that they are in $\mathcal{C}^\infty$, but the value of k will be clear in each situation. We also assume ψ has compact support so that we do not have to worry about the convergence of the integral.

We will note that if the phase is smooth with non-vanishing gradient then we have a lot of cancellations and the above integral decreases very fast in λ. So we have that if the phase is smooth then the main contribution of $I(\lambda)$ comes from the points x where the gradient of the phase is vanishing; this is called the stationary phase principle.

Also note that given $\xi \in \mathbb{R}^d$, if we take $\phi = 2\pi \frac{\xi}{|\xi|} x$ and $\lambda = |\xi|$ we get

$$I(\lambda) = \int_{\mathbb{R}^d} e^{2\pi i x \xi} \psi(x) dx = \hat{\psi}(\xi),$$

which is the Fourier transform of the amplitude, and then the stationary phase principle is in fact the decay of the Fourier transform. We recall that if $\psi \in \mathcal{C}^k$ then $\hat{\psi}^{(k)}(\xi) = (-2\pi i \xi)^k \hat{\psi^{(k)}}(\xi)$ and since $\hat{\psi^{(k)}}(\xi)$ is bounded we have that $\left|\hat{\psi}(\xi)\right| \leq C_k \left|\xi\right|^{-k}$.

Note that we will sometimes give bounds that depends on constants that we do not give explicitly. We will then often rename them from line to line without specifying. As an example we may write $2c \leq c$ by implicitly taking our new c to be half of the old c.

1.1 Dimension one and Van Der Corput's lemma in analysis

Let us first consider the case $d = 1$. The amplitude and the phase are then simply functions that map $\mathbb{R}$ to itself and the gradient of the phase is now just its derivative.

Proposition 1.1.1. *If $|\phi'(x)| \geq 1$ for all $x \in supp(\psi)$, then for each positive integer N, we have that*

$$|I(\lambda)| \leq c_N \lambda^{-N}.$$

Proof. For a function $f \in \mathcal{C}^\infty$, we define the operator

$$L(f) = \frac{1}{i\lambda} a \frac{df}{dx}$$

and its transpose

$$L^T(f) = -\frac{1}{i\lambda} \frac{d}{dx}(af),$$

with

$$a(x) = \frac{1}{\phi'(x)}.$$

So if $f, g \in \mathcal{C}^\infty$ then integration by parts gives

$$\int_{-\infty}^{\infty} L(f)g = \int_{-\infty}^{\infty} fL^T(g) + \left[\frac{a(x)g(x)f(x)}{i\lambda}\right]_{-\infty}^{\infty}$$

$$= \int_{-\infty}^{\infty} fL^T(g) + \left[\frac{g(x)f(x)}{i\lambda\phi'(x)}\right]_{-\infty}^{\infty}.$$

If in addition $g \in \mathcal{C}_0^\infty$, then we have

$$\int_{-\infty}^{\infty} L(f)g = \int_{-\infty}^{\infty} fL^T(g).$$

Also, this operator is useful here because $L(e^{i\lambda\phi}) = e^{i\lambda\phi}$ and then $L^N(e^{i\lambda\phi}) = e^{i\lambda\phi}$ for all $N \in \mathbb{N}$.

Thus

$$I(\lambda) = \int_{\mathbb{R}} L^N(e^{i\lambda\phi(x)})\psi(x)dx$$

$$= \int_{\mathbb{R}} e^{i\lambda\phi(x)}(L^T)^N(\psi(x))dx.$$

Now for each N, $(L^T)^N(\psi(x))$ is $(-\frac{1}{i\lambda})^N$ times a function that is continuous and supported in $supp(\psi)$. This function is then integrable and does not depend on λ.

So we get

$$|I(\lambda)| \leq c_N\lambda^{-N},$$

where for each N the constant C_N depends on the phase and the amplitude but not on λ. Hence as λ goes to infinity, the decay of the integral is very fast and is in fact as fast as the decay of the Fourier transform mentioned above. □

Remark: For each N we said that $(L^T)^N(\psi(x)) = (\frac{1}{i\lambda})^N h_N(x)$, for some function $h_N(x)$ that is integrable and does not depend on λ. In the proof of this proposition we do not need to be more precise about what $h_N(x)$ looks like, but because it will be important later, we decide to describe it now. A simple product rule gives that

$$h_2 = (\frac{da}{dx})^2\psi + \frac{da}{dx}a\frac{d\psi}{dx} + a\frac{d^2a}{dx^2}\psi + a^2\frac{d^2\psi}{dx^2}$$

and by induction, we get that for each N, h_N is a finite sum whose terms are products of N derivatives of a of orders between 0 and N, and a derivative of ψ of order between 0 and N. Now a derivative of a of any order will always be a quotient of continuous functions, and its denominator will have absolute value at least one, since $|\phi'(x)| \geq 1$ for all x in the support of ψ. For x not in the support of ψ, multiplication by $\psi(x)$ makes everything zero. Hence h_N is continuous and supported in $supp(\psi)$.

We will see in Chapter 2 that this proposition can be easily extended to higher dimensions.

Now if we take $\psi(x) = \chi_{[a,b]}(x)$ and define

$$I_1(\lambda) = \int_a^b e^{i\lambda\phi(x)} dx,$$

then ψ has indeed compact support but is not continuous so we cannot use Proposition 1.1.1. In fact, we will no longer be able to get such a fast decay as λ approaches infinity. We will only get a bound of the form

$$|I_1(\lambda)| \leq C\lambda^{-1},$$

for some constant C, which is only the special case $N = 1$ in the Proposition 1.1.1. However, the advantage is that we will be able to make the constant C absolute. We especially insist on the fact that C will not depend on the length of the interval $[a, b]$, which will be important later when we will be interested in large intervals.

Proposition 1.1.2. (Van Der Corput lemma with k=1) *If $|\phi'(x)| \geq 1$ for all $x \in [a, b]$ and $\phi'(x)$ is monotonic, then*

$$|I_1(\lambda)| \leq 3\lambda^{-1}.$$

Proof. We use the same operator as in the proof of Proposition 1.1.1 but now when we

do the integration by parts we get

$$I_1(\lambda) = \int_a^b L(e^{i\lambda\phi(x)})dx$$

$$= \int_a^b e^{i\lambda\phi(x)} L^T(1)dx + \left[\frac{e^{i\lambda\phi(x)}}{i\lambda\phi'(x)}\right]_a^b.$$

The second term is obviously bounded by $\frac{2}{\lambda}$ and the first term is bounded by

$$\int_a^b \left|L^T(1)\right| dx = \frac{1}{\lambda}\int_a^b \left|\frac{d}{dx}\left(\frac{1}{\phi'(x)}\right)\right| dx \tag{1.1}$$

and since $\phi'(x)$ is monotonic and continuous, $\frac{d}{dx}\left(\frac{1}{\phi'(x)}\right)$ does not change sign. Then (1.1) is

$$\frac{1}{\lambda}\left|\int_a^b \frac{d}{dx}\left(\frac{1}{\phi'(x)}\right)dx\right| = \frac{1}{\lambda}\left|\frac{1}{\phi'(b)} - \frac{1}{\phi'(a)}\right| \leq \frac{1}{\lambda}\left|\frac{1}{\phi'(b)}\right|,$$

where the last inequality holds because $\phi'(a)$ and $\phi'(b)$ have the same sign, and this is of course bounded by $\frac{1}{\lambda}$. Putting the two terms together, we get the result. □

Note that if we replace the condition $|\phi'(x)| \geq 1$ by $|\phi'(x)| \geq \mu > 0$ then we can "transfer" a factor of μ to λ in the following way: $\left|\frac{\phi'(x)}{\mu}\right| \geq 1$ so by Proposition 1.1.2 we have that

$$\left|\int_a^b e^{i(\lambda\mu)(\frac{\phi(x)}{\mu})}\right| \leq 3(\lambda\mu)^{-1}.$$

This is a simple trick that we will often use to derive this kind of conclusion from other propositions without re-explaining.

Note that the proof of this proposition involves the evaluation of single integrals and cannot be extended non-trivially to higher dimension.

Now what if $\phi(x)$ is allowed to have a critical point?

Proposition 1.1.3. (Van Der Corput lemma with k=2) *If* $|\phi''(x)| \geq 1$ *for all* $x \in [a,b]$ *then*

$$|I_1(\lambda)| \leq 2\sqrt{3}\lambda^{-1/2}.$$

Proof. By taking the complex conjugate, we may assume that $\phi''(x) \geq 1$, so $\phi'(x)$ is monotone increasing. Now suppose that ϕ has a critical point and note that the fact that ϕ' is monotone increasing forces this point to be unique; we call it x_0.

For any $\delta > 0$ we can break $[a, b]$ into three subintervals. Two of them that are δ away from x_0, for which we will be able to use the Proposition 1.1.2, and one that contains x_0 but whose length is bounded by 2δ.

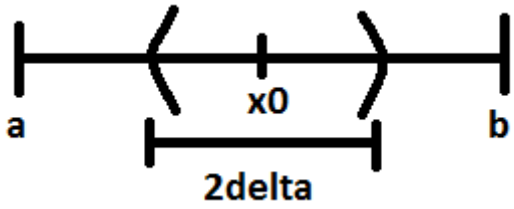

Figure 1.1: break $[a, b]$ into three subintervals

Then for all $x > x_0 + \delta$ we have $\phi'(x) > \phi'(x_0 + \delta)$ since ϕ' is increasing, and by the Mean Value Theorem, there is some $\xi \in (x_0, x_0 + \delta)$ such that

$$\frac{\phi'(x_0 + \delta) - \phi'(x_0)}{\delta} = \phi''(\xi) \geq 1.$$

Using the fact that $\phi'(x_0) = 0$ and rearranging this we obtain

$$\phi'(x_0 + \delta) \geq \delta.$$

So we have $\phi'(x) \geq \delta$ on $[x_0 + \delta, b]$, which allows us to use the Proposition 1.1.2 to get

$$\left| \int_{x_0+\delta}^{b} e^{i\lambda\phi(x)} dx \right| \leq 3(\delta\lambda)^{-1},$$

and similarly $\phi'(x) \leq -\delta$ on $[a, x_0 - \delta]$, so

$$\left| \int_{a}^{x_0-\delta} e^{i\lambda\phi(x)} dx \right| \leq 3(\delta\lambda)^{-1}.$$

Now by talking the trivial bound on the interval containing x_0 we get

$$\left| \int_{x_0-\delta}^{x_0+\delta} e^{i\lambda\phi(x)} dx \right| \leq 2\delta,$$

and putting everything together gives

$$|I_1(\lambda)| \leq 6(\delta\lambda)^{-1} + 2\delta.$$

To optimize this bound, we want to choose δ such that

$$6(\delta\lambda)^{-1} = 2\delta,$$

or equivalently

$$\delta = \sqrt{\frac{3}{\lambda}},$$

and taking this δ we get

$$|I_1(\lambda)| \leq 2\sqrt{3}\lambda^{-1/2}.$$

To complete the proof, if ϕ has no critical point we can take x_0 to be any point and the rest of the proof still works. □

In fact, using induction this proof extends to the general Van Der Corput lemma.

Proposition 1.1.4. (Van Der Corput Lemma for $k \geq 2$) *If $\left|\phi^{(k)}(x)\right| \geq 1$ for all $x \in [a, b]$ then*

$$|I_1(\lambda)| \leq 2^k \lambda^{-1/k}. \tag{1.2}$$

Proof. Let $k = 2$. By Proposition 1.1.3 we have

$$|I_1(\lambda)| \leq 2\sqrt{3}\lambda^{-1/2} \leq 2^2\lambda^{-1/2},$$

which is (1.2) for $k = 2$.

Now let $k \geq 3$ and suppose (1.2) holds for $k - 1$. Take $\delta > 0$ and follow the same

steps as the case $k = 2$. We get

$$|I_1(\lambda)| \leq 2(2^{k-1})(\delta\lambda)^{-\frac{1}{k-1}} + 2\delta$$

The optimal choice of δ being $2^{\frac{(k-1)^2}{k}}\lambda^{-1/k}$, which is less that $2^{k-1}\lambda^{-1/k}$, we get the desired result. □

Note that one could probably improve the constant 2^k but the point is that it only depends on k and not on the length of the interval $[a, b]$.

These last three propositions were with no amplitude, and they are the ones we will be interested in for an application to number theory that has to do with uniform distribution modulo 1, for which by Weyl's theorem we need to bound an exponential sum, as we will see in the next chapter.

The Proposition 1.1.1 was with amplitude in the case $k = 1$; now let us consider the case $k = 2$.

Proposition 1.1.5. *If $|\phi''(x)| \geq 1$ for all $x \in supp(\psi)$ then*

$$|I(\lambda)| \leq c_\psi \lambda^{-1/2},$$

where $c_\psi = 4\int |\psi'(x)|\, dx$.

Proof. Since ψ has compact support we can find a and b so that ψ is supported in the interval $[a, b]$. Let $J(x) = \int_a^x e^{i\lambda\phi(u)}du$, so that $J(a) = 0$. Then integration by parts gives

$$\int_a^b J(x)\psi'(x)dx = [J(x)\psi(x)]_a^b - \int_a^b e^{i\lambda\phi(x)}\psi(x)dx,$$

and then

$$I(\lambda) = -\int_a^b J(x)\psi'(x)dx + J(b)\psi(b),$$

since the first term vanishes since $supp(\psi) \subseteq [a, b]$. By Proposition 1.1.4 we know that

$|J(x)| \leq 4\lambda^{-1/2}$ for all $x \geq a$, so

$$|I(\lambda)| \leq 4\lambda^{-1/2} \int_a^b |\psi'(x)|\, dx.$$

□

1.2 Higher dimensions

Now we want to bound integrals of the form

$$I(\lambda) = \int_{\mathbb{R}^d} \psi(x) e^{i\lambda\phi(x)} dx,$$

where d can be greater than one. The nice results of Van Der Corput that give a bound with an absolute constant is not extendible to higher dimensions, but we see that we can still bound these integrals in some way.

The following theorem is an extension of Proposition 1.1.1 in the previous section.

Theorem 1.2.1. *Suppose ϕ and ψ are two $\mathcal{C}^\infty$ functions and ψ has compact support. If $|\nabla\phi| \geq 1$ for all $x \in supp(\psi)$ then for any integer $N \geq 0$,*

$$|I(\lambda)| \leq c_N \lambda^{-N}.$$

Proof. The proof here is quite similar to the proof of Proposition 1.1.1, which is actually just the special case $d = 1$ of what we are about to do. Consider the vector field L defined on $f \in C^\infty$ by

$$\begin{aligned} L(f) &= \frac{1}{i\lambda} \sum_{k=1}^{d} a_k \frac{\partial}{\partial x_k}(f) \\ &= \frac{1}{i\lambda} a \cdot \nabla f, \end{aligned}$$

with

$$a = (a_1, ..., a_d) = \frac{\nabla\phi}{|\nabla\phi|^2}.$$

Note that for each k and for all $x \in supp(\psi)$,

$$|a_k(x)| \leq \frac{\left|\frac{\partial \phi}{\partial x_k}\right|}{|\nabla \phi|^2} \leq \left|\frac{\partial \phi}{\partial x_k}\right|,$$

which is uniformly bounded since $supp(\psi)$ is compact and $\phi \in \mathcal{C}^\infty$. In fact, we can see that all the a_k's and all their partial derivatives are bounded on $supp(\psi)$, and these bounds depend on partial derivatives of ϕ.

We know L has a transpose

$$L^T(f) = -\frac{1}{i\lambda} \sum_k \frac{\partial}{\partial x_k}(a_k f) = -\frac{1}{i\lambda} \nabla \cdot (af),$$

and that $L(e^{i\lambda\phi}) = e^{i\lambda\phi}$. So for all integers $N > 0$, we have

$$I(\lambda) = \int \psi(x) L^N(e^{i\lambda\phi(x)}) = \int (L^T)^N(\psi(x)) e^{i\lambda\phi(x)}.$$

Now as it was explained in the remark after Proposition 1.1.1, extended to higher dimensions we have that

$$(L^T)^N(\psi(x)) = (-\frac{1}{i\lambda})^N \sum_{finite} (D_{\alpha_1} a)...(D_{\alpha_N} a)(D_\alpha \psi)$$

where each $(D_{\alpha_i} a)$ corresponds to a partial derivative of a of order between 0 and N and $(D_\alpha \psi)$ corresponds to a partial derivative of ψ of order between 0 and N. Therefore, this sum is bounded by $\frac{C_N}{\lambda^N}$ and supported in $supp(\psi)$, and

$$|I(\lambda)| \leq \frac{C_N}{\lambda^N},$$

as desired. □

Note that the constant C_N depends on the support of ψ and on partial derivatives of ϕ and ψ.

The following is now an extension of Proposition 1.1.5 in the previous section.

Theorem 1.2.2. *Suppose ψ has compact support. Let $\nabla^2\phi = \left\{\frac{\partial^2\phi}{\partial x_j \partial x_k}\right\}$ be the $d \times d$ Hessian matrix of ϕ. If $\det\{\nabla^2\phi\} \neq 0$ on $supp(\psi)$ then*

$$|I(\lambda)| \leq C\lambda^{-d/2}.$$

Proof. Take $\epsilon > 0$ to be arbitrary for now. We need to control the support of ψ but since it is compact we can cover it by finitely many ϵ-balls. We will see that the choice of ϵ eventually depends on ϕ and not on the support of ψ, so that we will be able to do this. We write

$$supp(\psi) \subseteq \bigcup_{j=1}^{J} B_j =: B,$$

so there exists a smooth partition of unity $\{\eta_j\}_{j=1}^J$ with, η_j smooth, $supp(\eta_j) \subseteq B_j$ for each j and $\sum_{j=1}^J \eta_j = 1$ on $supp(\psi)$.

We can then write ψ as finitely many $\mathcal{C}^\infty$ functions supported in ϵ-balls in the following way:

$$\psi(x) = \sum_{j=1}^{J} \psi(x)\eta_j(x).$$

So it is enough to prove the theorem replacing $\psi(x)$ by $\psi(x)\eta_j(x)$ for any of these j. Then without loss of generality we may assume that the support of ψ is included in an ϵ-ball.

We use the fact that $|I(\lambda)|^2 = I(\lambda)\overline{I(\lambda)}$ to write

$$|I(\lambda)|^2 = \int_{\mathbb{R}^d}\int_{\mathbb{R}^d} e^{i\lambda[\phi(y)-\phi(x)]}\psi(y)\overline{\psi(x)}dydx.$$

Fix x and change the variable in the inner integral: $u = y - x$, and then swap the two integrals. Then the above becomes

$$|I(\lambda)|^2 = \int_{\mathbb{R}^d} J_\lambda(u)du,$$

where

$$J_\lambda(u) = \int_{\mathbb{R}^d} e^{i\lambda[\phi(u+x)-\phi(x)]}\psi(x,u)dx$$

and $\psi(x,u) = \psi(x+u)\overline{\psi(x)}$ is $\mathcal{C}^\infty$ and has compact support. In particular it is supported in $|u| \leq 2\epsilon$.

We will show that

$$|J_\lambda(u)| \leq C_N(\lambda\,|u|)^{-N} \text{ for all } N \geq 0, \tag{1.3}$$

and then by taking simultaneously $N = 0$ and $N = d+1$, this will imply that

$$\begin{aligned}
\int_{\mathbb{R}^d} |J_\lambda(u)|\,du \int_{\mathbb{R}^d} &\leq \min\{C_0, C_{d+1}(|u|\,\lambda)^{-(d+1)}\}du \\
&\leq C\int_{\mathbb{R}^d}\left(\frac{1}{1+|u|\,\lambda}\right)^{d+1}du \\
&\leq C\int_0^\infty \frac{r^{d-1}}{(1+r\lambda)^{d+1}}dr \\
&= \frac{C}{\lambda^d}\int_0^\infty \frac{t^{d-1}}{(1+t)^{d+1}}dt.
\end{aligned}$$

The second to last integral is obtained by passing from Cartesian to spherical coordinates, and the last integral is obtained by the change of variable $t = r\lambda$ and is known to converge. This implies that

$$|I(\lambda)|^2 \leq C\lambda^{-d},$$

which proves the theorem.

To see that (1.3) is true, we fix u and use the usual vector field $L(f) = \frac{1}{i\lambda}(a\cdot\nabla f)$ and its transpose $L^T(f) = -\frac{1}{i\lambda}\nabla\cdot(af)$, where

$$a = \frac{b}{|b|^2}$$

with

$$b = \nabla_x[\phi(x+u) - \phi(x)],$$

and all the derivatives are taken with respect to the variable x. As usual we want use the fact that $L^N(e^{i\lambda[\phi(u+x)-\phi(x)]}) = e^{i\lambda[\phi(u+x)-\phi(x)]}$, which gives that

$$J_\lambda(u) = \int_{\mathbb{R}^d} \int e^{i\lambda[\phi(u+x)-\phi(x)]} (L^T)^N(\psi(x,u))dx,$$

for all integer $N \geq 0$. So we are looking for an upper bound on $\left|(L^T)^N(\psi(x,u))\right|$. Now as it was explained in the remark after Proposition 1.1.1 and already extended to higher dimensions in the proof of Theorem 1.2.1, we have that

$$(L^T)^N(\psi(x)) = (-\frac{1}{i\lambda})^N \sum_{finite} (D_{\alpha_1}a)...(D_{\alpha_N}a)(D_\alpha\psi) \tag{1.4}$$

where each $(D_{\alpha_i}a)$ corresponds to a partial derivative of a of order between 0 and N and $(D_\alpha\psi)$ corresponds to a partial derivative of ψ of order between 0 and N. We know that ψ is smooth so all its partial derivatives are bounded on its support, which is compact, so we are actually looking for a bound of the partial derivatives of the a_k's. In fact, we want to show that for each multi-index α,

$$|\partial^\alpha a| \leq C_\alpha |u|^{-1}, \tag{1.5}$$

for some constant C_α.

We claim that $|b| = |\nabla_x[\phi(x+u) - \phi(x)]| \approx |u|$.

To see that $|b| \leq c|u|$ we simply use the fact that ϕ is smooth so $\nabla_x\phi(x)$ is differentiable and then $\frac{\nabla_x\phi(x+u)-\nabla_x\phi(x)}{|u|}$ has a limit as $|u| \to 0$. Then for $|u|$ small enough, we have $\frac{|b|}{|u|} < C$, for some $C > 0$ and then $|b| < C|u|$. Now we need to pick ϵ small enough to control $|u|$ and this choice only depends on the function ϕ and not on ψ or its support.

On the other hand, to see that $|b| \geq c|u|$ we fix x and use the Taylor expansion of ϕ as a function of u about $u = 0$. We get

$$\nabla_x[\phi(x+u) - \phi(x)] = 0 + \nabla^2\phi(x) \cdot u + O(|u|^2) \tag{1.6}$$

We will need the following simple lemma from linear algebra.

Lemma 1.2.3. *Let A be an invertible matrix; then there exists a constant $C > 0$ such that for all vectors x we have that*

$$|Ax| \geq C\,|x|\,.$$

Proof. Suppose for contradiction that for all $C > 0$ there exists a vector x such that

$$|Ax| < C\,|x|\,.$$

By dividing both sides by $|x|$ we can take x such that $|x| = 1$. Then we can construct a sequence $\{x_n\}$ with the property that for each n, $|x_n| = 1$ and

$$|Ax_n| < 1/n,$$

which tells us that

$$\lim_{n\to\infty} Ax_n = 0.$$

Since A is invertible we have that

$$\lim_{n\to\infty} x_n = 0,$$

which contradicts the fact that $|x_n| = 1$ for all n. □

In our situation we have that $\nabla^2\phi(x)$ has a non-vanishing determinant, so it is invertible, and by Lemma 1.2.3

$$\left|\nabla^2\phi(x)\cdot u\right| \geq C\,|u|\,,$$

for some $C > 0$. Using this and (1.6) we get that, for $|u|$ small enough so that the term $O(|u|^2)$ is negligible (and again we need to choose ϵ small enough depending on the function ϕ), $|b| \approx |u|$.

In order to complete the proof of (1.5), note that in showing that $|b| \leq c\,|u|$ we used

the fact that ϕ is smooth but in the same way we can use the fact that $\partial^\alpha \phi$ is smooth for each multi-index α and get that $\nabla[\partial^\alpha \phi(x+u) - \partial^\alpha \phi(x)] \leq C_\alpha |u|$, and then by swapping ∂ and ∇ we get that $|\partial^\alpha b| \leq C_\alpha |u|$. Now using this with the fact that $|b| \approx |u|$ we obtain (1.5), that we now recall:

$$|\partial^\alpha a| \leq C_\alpha |u|^{-1}.$$

Plugging this in (1.4) we get that

$$\left|(L^T)^N(\psi(x,u))\right| \leq C_N(|u|\,\lambda)^{-N}$$

and then

$$\begin{aligned} |J_\lambda(u)| &\leq \int_{\mathbb{R}^d} C_N(|u|^N \lambda)^{-N} \chi_{supp(\psi(x,u))}(x)dx \\ &\leq C_N(|u|\,\lambda)^{-N}, \end{aligned}$$

which completes the proof of (1.3) and then the proof of the theorem. □

The next theorem is what we can get if allow the Hessian to be vanishing.

Theorem 1.2.4. *Suppose ψ has compact support. If rank $\{\nabla^2\phi(x)\} \geq m$ for all $x \in supp(\phi)$ then*

$$|I(\lambda)| \leq C\lambda^{-m/2}.$$

Proof. Taking $x_0 \in supp(\phi)$, we have that $\nabla^2\phi(x)$ has rank at least m, so we can introduce a new coordinate system $x = (x', x'') \in \mathbb{R}^m \times \mathbb{R}^{d-m}$ such that H', the Hessian restricted to $\mathbb{R}^m$, is non-vanishing at x_0', where $x_0 = (x_0', x_0'')$. Now since $\phi \in \mathcal{C}^\infty$, H' is also non-vanishing on a small ball around x_0'. More precisely, there exists $\epsilon > 0$ (that depends only on ϕ) such that H' is non-vanishing on $B := B(x_0', \epsilon)$. For the same reasons as in the previous theorem, we may assume that the support of ψ restricted to the first coordinate, $supp_{\mathbb{R}_m}(\psi)$ is contained in B. This allow us to use Theorem 1.2.2 to get that

$$\left|\int_{\mathbb{R}^m} e^{i\lambda\phi(x')}\psi dx'\right| \leq C\lambda^{-m/2}.$$

Then we have

$$\begin{aligned}
|I(\lambda)| &\leq C \int_{\mathbb{R}^{d-m}} \left| \int_{\mathbb{R}^m} \psi(x) e^{i\lambda\phi(x)} dx' \right| dx'' \\
&\leq C \int_{\mathbb{R}^{d-m}} \chi_{supp(\psi)} \lambda^{-m/2} dx'' \\
&\leq C\lambda^{-m/2},
\end{aligned}$$

where the constant C, that we rename at each step, eventually depends on the implied constant from Theorem 1.2.2, the number of ϵ-balls needed to approximate ψ, which depends on $supp(\psi)$, and on ϕ (more precisely on the Hessian of ϕ). □

Chapter 2

Van Der Corput's methods to bound exponential sums

2.1 Process B

Let f be a real valued function. We are interested in sums of the form

$$S := \sum_n e(f(n)),$$

where n varies in some range that we will specify later. We will be particularly interested in ranges such as $N \leq n \leq 2N$ as N gets very big.

We will use results from Chapter 1, Section 1 from a different point of view. We used to fix the phase ϕ and have the variable parameter λ that multiplied ϕ and we were interested in the behaviour of the integral for large values of λ. This was the analytic point of view of this. Now λ will no longer be a varying parameter but will be included in the phase in the following way. Let us call θ our new phase and suppose that $|\theta'| \geq \lambda > 0$. Then if we let $\phi = \theta/\lambda$ we get that $|\phi'| \geq 1$ and the phase is our usual $\lambda\phi$. Then we can write the Analytic Van Der Corput's lemma (Propositions 1.1.2 and 1.1.4) in a slightly different way:

Theorem 2.1.1. (Analytic /Continuous Van Der Corput's lemma)

1) If $|\phi'(x)| \geq \lambda > 0$ for all $x \in [a,b]$ and $\phi'(x)$ is monotonic then

$$\left| \int_a^b e^{i\phi(x)} dx \right| \leq 3\lambda^{-1}.$$

2) If $k \geq 2$ and $\left|\phi^{(k)}(x)\right| \geq \lambda > 0$ for all $x \in [a,b]$ then

$$\left| \int_a^b e^{i\phi(x)} dx \right| \leq 2^k \lambda^{-1/k}.$$

The following theorem can be found in the book [Mon94] by Montgomery.

Theorem 2.1.2. ***Strong analytic Van Der Corput's lemma for k=1***
Let $\psi(x)$ and $\theta(x)$ be real-valued functions on $[a,b]$ such that $\psi(x)$ and $\theta'(x)$ are continuous. Suppose that $\theta'(x)/\psi(x)$ is positive and monotonically increasing on this interval. If $0 < \lambda_1 \leq \theta'(x)/\psi(x)$ then

$$\left| \int_a^b \psi(x) e(\theta(x)) dx \right| \leq \frac{2}{\pi \lambda_1}. \tag{2.1}$$

Proof. The proof of this is very similar to the regular analytic Van Der Corput's lemma for $k = 1$, which is Proposition 1.1.2 above. We use the operator $L(f) = \frac{1}{2\pi i} \cdot \frac{f'}{\theta'}$ and its transpose $L^T(f) = -\frac{1}{2\pi i} \cdot \frac{d}{dx}\left(\frac{f}{\theta'}\right)$ then

$$\int_a^b \psi(x) L(e(\theta(x))) dx = \frac{1}{2\pi i} \left[\frac{\psi(x) e(\theta(x))}{\theta'(x)} \right]_a^b + \int_a^b L^T(\psi(x)) e(\theta(x)) dx,$$

where the first term is bounded by $\frac{1}{\lambda_1 \pi}$, and the second term is bounded by

$$\frac{1}{2\pi i} \int_a^b \left| \frac{d}{dx} \left(\frac{\psi(x)}{\theta'(x)} \right) \right| dx,$$

which, using the conditions on $\theta'(x)/\psi(x)$, is bounded by $\frac{1}{\pi \lambda_1}$ in the same way as in the proof of Proposition 1.1.2. Note that the conditions on $\theta'(x)/\psi(x)$ force its reciprocal to be continuous, which allows us to use the Fundamental Theorem of Calculus. □

The next corollaries are not in [Mon94] but we believe they are necessary to make the details work in the next theorem.

Corollary 2.1.3. *Let $\psi(x)$ and $\theta(x)$ be real-valued functions on $[a,b]$ such that $\psi(x)$ and $\theta'(x)$ are continuous. Suppose that $\theta'(x)/\psi(x)$ does not change sign and is monotone on this interval. If $0 < \lambda_1 \leq \mid \theta'(x)/\psi(x) \mid$ then*

$$\left| \int_a^b \psi(x) e(\theta(x)) dx \right| \leq \frac{1}{\pi \lambda_1}. \tag{2.2}$$

Proof. Replacing θ by $-\theta$ changes the sign of $\theta'(x)/\psi(x)$ and is taking the complex conjugate of the integral, which does not change its norm. So without loss of generality we may assume $\theta'(x)/\psi(x) > 0$.

Now if $\theta'(x)/\psi(x)$ is monotone decreasing, we can do the change of variable $u = -x$ and

$$\left| \int_a^b \psi(x) e(\theta(x)) dx \right| = \left| \int_{-b}^{-a} \psi(-u) e(\theta(-u)) du \right|, \tag{2.3}$$

for which we can get a bound that does not depend on the interval of integration. So by replacing $\theta'(x)/\psi(x)$ by $\theta'(-x)/\psi(-x)$ without loss of generality we may assume $\theta'(x)/\psi(x)$ is monotone increasing. □

Corollary 2.1.4. *Let $\psi(x)$ and $\theta(x)$ be real-valued functions on $[a,b]$ such that $\psi(x)$ and $\theta'(x)$ are continuous. Suppose that $\theta'(x)/\psi(x)$ is monotone on the intervals whose endpoints are a, b and the possible m points of discontinuities (of any type) of $\theta'(x)/\psi(x)$. If $0 < \lambda_1 \leq \mid \theta'(x)/\psi(x) \mid$ then*

$$\left| \int_a^b \psi(x) e(\theta(x)) dx \right| \leq \frac{m+1}{\pi \lambda_1}. \tag{2.4}$$

Proof. We prove the case $m = 1$ and the general case will follow similarly. Suppose there is a unique point $x_0 \in [a,b]$ such that $\theta'(x)/\psi(x)$ has a discontinuity at $x = x_0$. Since θ' and ψ are continuous, we must have $\psi(x_0) = 0$.

For any ϵ positive and small enough so that $|\psi(x)| < 1$ for all $x \in [x_0 - \epsilon, x_0 + \epsilon]$, we have that the conditions of the previous corollary are satisfied on the intervals $[a, x_0 - \epsilon]$ and $[x_0 + \epsilon, b]$, thus

$$\begin{aligned}\left|\int_a^b \psi(x)e(\theta(x))dx\right| &\leq \left|\int_a^{x_0-\epsilon} \psi(x)e(\theta(x))dx\right| + \left|\int_{x_0-\epsilon}^{x_0+\epsilon} \psi(x)e(\theta(x))dx\right| + \left|\int_{x_0+\epsilon}^b \psi(x)e(\theta(x))dx\right| \\ &\leq \frac{2}{\pi\lambda_1} + 2\epsilon\end{aligned}$$

and the result follows by letting $\epsilon \to 0$. □

The next theorem can also be found in [Mon94] but we added some details in the proof and believe they are necessary. To avoid keeping track of constants while they are not really important we use the notation $f = O(g)$ or equivalently $f \ll g$ to say that there exists an absolute constant $C > 0$ such that $|f| \leq C|g|$. We insist on the fact that the constant cannot depend on anything, it is just a number that we could compute but we avoid to do so only for convenience.

Theorem 2.1.5. ***(Truncated Poisson Theorem)*** *Let f be a real-valued function, and suppose that f' is continuous and increasing on $[a, b]$. Write $\alpha = f'(a)$ and $\beta = f'(b)$. Then*

$$\sum_a^b e(f(n)) = \sum_{\alpha-1\leq\nu\leq\beta+1} \int_a^b e(f(x) - \nu x)dx + O(\log(2 + \beta - \alpha)). \tag{2.5}$$

Proof. Let N be an integer such that such that $\left|N - \frac{\alpha+\beta}{2}\right| \leq \frac{1}{2}$. If we replace $f(x)$ by $f_0(x) = f(x) - Nx$ then (2.5) does not change and f_0' is still continuous and increasing but then $f_0'(a) = \alpha - N$ and $f_0'(b) = \beta - N$ so $|f_0'(a) + f_0'(b)| = |\alpha + \beta - 2N| \leq 1$. Therefore without loss of generality we may assume that $|\alpha + \beta| \leq 1$. Note that since $\alpha < \beta$ this forces $\beta > -1/2$ and $\alpha < 1/2$.

Define $r(x) = e(f(x))\chi_{[a,b]}$ Then r has bounded variation, since it is continuous except for a possible jump-discontinuity at a and b, and is obviously integrable, so we can use

the Poisson summation formula. This is explained in [Hel95]. We then have

$$\begin{aligned}\sum_a^b e(f(n)) &= \sum_n \frac{r(n^+)+r(n^-)}{2} + O(1)\\ &= \sum_\nu \hat{r}(\nu) + O(1),\end{aligned}$$

where $\hat{r}(\nu) = \int_a^b e(f(x)-\nu x)dx$ is the Fourier transform of r. Note that the implied constant is absolute (at most 2). The idea is that when ν is away from the interval $[\alpha,\beta]$, the integral that defines $\hat{r}(\nu)$ has no stationary phase, so it will be small. So the main contribution of the sum $\sum_\nu \hat{r}(\nu)$ comes from the ν's that belong to $[\alpha,\beta]$. In fact, we will show that $\sum_{\nu\notin[\alpha-1,\beta+1]} \hat{r}(\nu) \ll \log(2+\beta-\alpha)$, which proves of the theorem.

Take $\nu \notin [\alpha-1,\beta+1]$. By integrating by parts we can express $\hat{r}(\nu)$ as

$$\int_a^b e(f(x))e(-\nu x)dx = \frac{e(f(a)-\nu a)}{2\pi i\nu} - \frac{e(f(b)-\nu b)}{2\pi i\nu} + \frac{1}{\nu}\int_a^b f'(x)e(f(x)-\nu x)dx. \quad (2.6)$$

Note that $0 \in (\alpha-1,\beta+1)$ since $|\,\alpha+\beta\,| \leq 1$, so ν cannot be zero and then

$$\hat{r}(\nu) = \frac{1}{\nu}\int_a^b f'(x)e(f(x)-\nu x)dx + O(1),$$

where the implied constant is absolute (at most $\frac{1}{\pi}$).

We want to show that

$$\sum_{\nu\notin[\alpha-1,\beta+1]} \frac{1}{\nu}\int_a^b f'(x)e(f(x)-\nu x)dx \ll log(2+\beta-\alpha).$$

Take $\nu > \beta+1$. We want to use Theorem 2.1.2 with $\psi = f'$ and $\phi(x) = f(x)-x\nu$. We know that

$$\left(\frac{f'-\nu}{f'}\right)' = \frac{\nu f''}{(f')^2} > 0, \quad (2.7)$$

so $\frac{f'-\nu}{f'}$ has no more than one point of discontinuity, is monotone increasing and

$$\begin{aligned}\left|\frac{f'-\nu}{f'}\right| &\geq min\left\{\left|\frac{\alpha-\nu}{\alpha}\right|, \left|\frac{\beta-\nu}{\beta}\right|\right\} \\ &\geq min\left\{\left|\frac{\beta-\nu}{\beta+1}\right|, \left|\frac{\beta-\nu}{\beta}\right|\right\} \\ &= \frac{\nu-\beta}{\beta+1} > 0\end{aligned}$$

since ν is closer to β than is it to α and $\beta \geq -1/2$.

Then by Theorem 2.1.2 with $\lambda_1 = \frac{\nu-\beta}{\beta+1}$,

$$\int_a^b f'(x)e(f(x)-\nu x)dx \ll \frac{\beta+1}{\nu-\beta}, \tag{2.8}$$

where the implied constant is absolute.

Now if $\beta \geq 1$ then $(\beta+1) \leq 2\beta$, so

$$\int_a^b f'(x)e(f(x)-\nu x)dx \ll \frac{\beta}{\nu-\beta}$$

and

$$\begin{aligned}\sum_{\nu>\beta+1} \frac{1}{\nu}\frac{\beta}{\nu-\beta} &= \sum_{\nu>\beta+1}\left(\frac{1}{\nu-\beta}-\frac{1}{\nu}\right) \\ &\leq \sum_{\nu=\lceil\beta\rceil+1}^{\infty}\left(\frac{1}{\nu-\lceil\beta\rceil}-\frac{1}{\nu}\right) \\ &= \lim_{N\to\infty}\left(\sum_{\nu=\lceil\beta\rceil+1}^{N}\frac{1}{\nu-\lceil\beta\rceil}-\sum_{\nu=\lceil\beta\rceil+1}^{N}\frac{1}{\nu}\right) \\ &= \sum_{\nu=1}^{\lceil\beta\rceil}\frac{1}{\nu} \\ &\leq 1+\log(\lceil\beta\rceil) \\ &\leq 3\log(\beta+2),\end{aligned}$$

and if $-1/2 < \beta < 1$ then using 2.8, we have

$$\int_a^b f'(x)e(f(x) - \nu x)dx \ll \frac{1}{\nu + 1/2}$$

and

$$\sum_{\nu > \beta+1} \frac{1}{\nu} \frac{1}{\nu + 1/2} \leq \sum_{\nu=1}^{\infty} \frac{1}{\nu^2} = \frac{\pi^2}{6} \leq 5 \log(3/2) \ll \log(\beta + 2).$$

We treat the case $\nu < \alpha - 1$ in the same way. But now $\frac{f'-\nu}{f'}$ is monotone decreasing and ν is closer to α than it is to β so

$$\left| \frac{f' - \nu}{f'} \right| \geq \frac{\nu - \alpha}{\alpha + 1} > 0,$$

which, using the strong analytic Van der Corput's lemma, that is Theorem 2.1.2 with $\lambda_1 = \frac{\nu-\alpha}{\alpha+1}$, gives

$$\int_a^b f'(x)e(f(x) - \nu x)dx \ll \frac{\alpha + 1}{\nu - \alpha}$$

and

$$\sum_{\nu \leq \alpha - 1} \frac{1}{\nu} \frac{\alpha + 1}{\nu - \alpha} \ll \log(-\alpha + 2).$$

Putting everything together, we get

$$\begin{aligned} \sum_{\nu \notin [\alpha-1, \beta+1]} \frac{1}{\nu} \int_a^b f'(x)e(f(x) - \nu x)dx &\ll \log(\beta + 2) + \log(-\alpha + 2) \\ &\ll \log(\max\{\beta + 2, \alpha + 2\}) \\ &\ll \log(\beta - \alpha + 2), \end{aligned}$$

where the last inequality is clear for $\alpha \leq 0$ and $\beta \geq 0$. If $-1/2 < \beta < 0$ then using $|\alpha + \beta| \leq 1$ and $\alpha < \beta$, we get $-1 < \alpha < 0$ and then $\max\{\beta + 2, \alpha + 2\} < 3$. Then

$$\log(\max\{\beta + 2, \alpha + 2\}) < \log 3 < 3 \log 3/2 < 3 \log(\beta - \alpha + 2),$$

since $\beta - \alpha + 2 > 3/2$. □

The following result can be found in the book [Ten95] of Tenenbaum.

Theorem 2.1.6. (2nd derivative test) *Let $f \in \mathcal{C}^2[a,b]$ and suppose there exists $c > 1$ such that for all $t \in (a,b)$ we have*

$$0 < \lambda \leq |f''(t)| \leq c\lambda;$$

then

$$\sum_{a<n\leq b} e(f(n)) \ll_c (b-a)\lambda^{1/2} + \lambda^{-1/2}.$$

Here we use the notation $\ll_c$ to indicate that the implied constant depends on c.

Proof. The condition on f'' forces f' to be monotone (increasing or decreasing). By taking complex conjugates on both sides, we may assume f' is monotone increasing. So we can use the Truncated Poisson Theorem to get that

$$\sum_{a}^{b} e(f(n)) = \sum_{\alpha-1\leq\nu\leq\beta+1} \int_a^b e(f(x)-\nu x)dx + O(\log(2+\beta-\alpha)), \tag{2.9}$$

where $\alpha = f'(a)$ and $\beta = f'(b)$. Now for each $\nu \in [\alpha-1, \beta+1]$, let $g(t) = f(t) - \nu t$; then $g'(t) = f'(t) - \nu$ and $g''(t) = f''(t)$. So we have

$$0 < \lambda \leq |g''(t)| \leq c\lambda$$

and we can use Van der Corput's lemma for $k = 2$ to get that

$$\int_a^b e(g(x))dx \ll \lambda^{-1/2}.$$

So the sum over ν is bounded by this times the length of the interval $[\alpha-1, \beta+1]$, and using the Mean Value Theorem,

$$\beta - \alpha = f'(b) - f'(a) = (b-a)f''(\xi) \leq (b-a)c\lambda \ll_c (b-a)\lambda. \tag{2.10}$$

The length of the interval $[\alpha-1, \beta+1]$ is then bounded by a constant times $(b-a)\lambda + 1$

(the $+1$ is necessary to ensure that the implied constant does not depend on λ). The sum on the right hand side of (2.9) is then, up to a constant that depends only on c, bounded by

$$[(b-a)\lambda+1]\lambda^{-1/2} = (b-a)\lambda^{1/2} + \lambda^{-1/2},$$

and whenever $a \neq b$, we use (2.10) to see that

$$\log(2+\beta-\alpha) \ll_c \log(2+(b-a)\lambda) \ll (b-a)\lambda^{1/2},$$

so we do not need to consider $\log(2+\beta-\alpha)$ in (2.9). □

2.2 Combining process A and process B

We want to get bounds using higher derivatives. The following lemma is a classical trick that will enable us to deduce information about the kth derivative of a function from information about its $(k+1)$st derivative. The next result can also be found in [Ten95].

Lemma 2.2.1. (Process A) *Let $f_h(x) = f(x+h) - f(x)$ be a discrete derivative of f where f is a real-valued function on $[a,b]$. Let H be an integer such that $1 \leq H \leq b-a$, then*

$$|S| := \left|\sum_{n=a}^{b} e(f(n))\right| \leq \frac{2(b-a)}{H^{1/2}} + 2\left(\frac{b-a}{H}\sum_{h=1}^{H}\left|\sum_{n=a}^{b-h} e(f_h(n))\right|\right)^{1/2}.$$

Proof. Let $F(n) = e(f(n)) \cdot \chi_{[a,b]}$. Then we can write

$$\begin{aligned}
S &= \sum_{n=-\infty}^{\infty} F(n) \\
&= \frac{1}{H}\sum_{m=1}^{H}\sum_{n=-\infty}^{\infty} F(n) \\
&= \frac{1}{H}\sum_{m=1}^{H}\sum_{n=-\infty}^{\infty} F(n+m) \text{ by changing the variable } n \to n+m \text{ for each } m \\
&= \frac{1}{H}\sum_{n=-\infty}^{\infty}\left(\sum_{m=1}^{H} F(n+m)\right)
\end{aligned}$$

Note that what is inside the parenthesis is only non-zero when n is such that there exist

at least one m such that $1 \le m \le H$ and $a \le n+m \le b$, which is only the case for $(a-H-1) \le n \le (b-1)$. So we can restrict the sum over n and write

$$S = \frac{1}{H} \sum_{n=a-H-1}^{b-1} \left(\sum_{m=1}^{H} F(n+m) \right),$$

and use the Cauchy-Schwartz inequality to get

$$|S|^2 \le \frac{1}{H^2} \left(\sum_{n=a-H-1}^{b-1} 1 \right) \left(\sum_{n=a-H-1}^{b-1} \sum_{m,m'=1}^{H} F(n+m)\overline{F(n+m')} \right). \tag{2.11}$$

Now the first factor here is at most $b-a+H \le 2(b-a)$. Let us look at the inner sum in the second factor. When $m = m'$ we have $F(n+m)\overline{F(n+m')} = 1$ so we can isolate this case that happens exactly H times. Now since we do not change the terms by exchanging m and m' and we know this sum is real, we can write it as

$$H + 2\mathfrak{Re} \sum_{1 \le m < m' \le H} F(n+m)\overline{F(n+m')}.$$

So we see that the second factor in (2.11) is at most

$$2H(b-a) + 2 \left| \sum_{1 \le m < m' \le H} \sum_{n \in \mathbb{Z}} F(n+m)\overline{F(n+m')} \right|. \tag{2.12}$$

Then we perform the change of variables $\nu = n+m$ and $r = m-m'$ then ν runs over $\mathbb{Z}$ and r takes the values $1, ..., H-1$. Moreover, for each fixed ν and r there are exactly $H-r$ solutions for $\{n, m, m'\}$, namely $\{\nu - j - r, j+r, j\}$, where $1 \le j \le H-r$, so (2.12) becomes

$$\begin{aligned} &2H(b-a) + 2 \left| \sum_{r=1}^{H-1} (H-r) \sum_{\nu \in \mathbb{Z}} F(\nu)\overline{F(\nu-r)} \right| \\ &\le 2H(b-a) + 2H \sum_{r=1}^{H-1} \left| \sum_{\nu \in \mathbb{Z}} F(\nu)\overline{F(\nu-r)} \right|. \end{aligned}$$

Pugging our upper bound for the first and the second product in (2.11) we obtain

$$|S|^2 \leq \frac{1}{H^2} \cdot 2(b-a) \cdot 2H \left((b-a) + \sum_{r=1}^{H-1} \left| \sum_{\nu \in \mathbb{Z}} F(\nu)\overline{F(\nu - r)} \right| \right)$$
$$= \left(\frac{2(b-a)}{\sqrt{H}} \right)^2 + 4 \left(\frac{b-a}{H} \sum_{r=1}^{H-1} \left| \sum_{\nu \in \mathbb{Z}} F(\nu)\overline{F(\nu - r)} \right| \right).$$

Now we know that for all $x, y \geq 0$, $x + y \geq \sqrt{x^2 + y^2)}$ and thus $|S|$ is at most the sum of the square root of each term, which gives the result, noting that $F(\nu)F(\nu - r) \neq 0$ only if $a \leq \nu \leq b - r$. □

Remark 2.2.2. *Process A (Lemma 2.2.1) implies the following that will be useful later. Let $f_h(x) = f(x+h) - f(x)$ be a discrete derivative of f where f is a real-valued function on $[a, b]$. Let H be an integer such that $1 \leq H \leq b - a$ and*

$$\sum_{h=1}^{H} \left| \sum_{n=a}^{b-h} e(f_h(n)) \right| \ll b - a.$$

Then

$$\sum_{n=a}^{b} e(f(n)) \ll \frac{b-a}{H^{1/2}}.$$

For simplicity and because this is what we will eventually be interested in, we will take the special case $[a, b] = [N, 2N]$, for some big integer N. So we redefine

$$S := \sum_{n \asymp N} e(f(n)).$$

Also, we want to weaken a little bit the condition $0 < \lambda \leq |f''(t)| \leq c\lambda$ in Theorem 2.1.6 to $f(t) \approx g(t)$. Following the proof of the 2nd derivative test, it is not hard to see that we can extend it in the following way.

Theorem 2.2.3. (2nd derivative test) *Let $f \in \mathcal{C}^2([a, b])$ and suppose that $|f''(x)| \approx \lambda > 0$ for all $x \asymp N$; then*

$$S \ll N\lambda^{1/2} + \lambda^{-1/2},$$

where the implied constant in $\ll$ is allowed to depend on the implied constants in $\approx$.

As we will see in Chapter 3, we are interested in getting a bound that beats the trivial one for exponential sums where the phase f is a monomial like n^α. In this case, we have that the kth derivative of f, $f^{(k)}(x) \approx x^{\alpha-k}$, so the main term in the 2nd derivative test, which is $N\lambda^{1/2}$, beats the trivial bound if and only if $\frac{\alpha-2}{2} + 1 < 1$, which is only true for α small. For bigger α, we need a bigger k to decrease the exponent of N in λ. We are then looking for a higher derivative test. In order to do so, we will combine processes A and B and see that an induction process is possible. The following result can be found in [Ten95], page 94.

Theorem 2.2.4. (3rd derivative test version 1) *Suppose $|f'''(x)| \approx \lambda > 0$ for all $x \asymp N$; then*

$$S \ll N\lambda^{1/6} + N^{1/2}\lambda^{-1/6},$$

where the implied constant in $\ll$ is allowed to depend on the implied constants in $\approx$.

Proof. Let H be an arbitrary (for now) integer such that $1 \leq H \leq N$. By Lemma 2.2.1 (Process A), we know that

$$|S| \leq \frac{2N}{H^{1/2}} + 2\left(\frac{N}{H}\sum_{h=1}^{H}\left|\sum_{n=N}^{2N-h} e(f_h(n))\right|\right)^{1/2}. \tag{2.13}$$

It follows from Taylor's Theorem and the fact that $|f'''(x)| \approx \lambda$ that $|f_h''(x)| \approx h\lambda$. So we can use the 2nd derivative test on f_h for each h from 1 to H to get that

$$\begin{aligned}\sum_{n=N}^{2N-h} e(f_h(n)) &\ll (h\lambda)^{1/2}(N-h) + (h\lambda)^{-1/2} \\ &\leq (h\lambda)^{1/2}N + (h\lambda)^{-1/2}.\end{aligned}$$

Plugging this into (2.13) and using, as in the proof of Lemma 2.2.1, the fact that $x + y \geq \sqrt{x^2+y^2}$, we obtain

$$|S| \ll NH^{-1/2} + NH^{1/4}\lambda^{1/4} + N^{1/2}H^{-1/4}\lambda^{-1/4}.$$

Now we need to choose H optimally. The choice $H = \lfloor \lambda^{-1/3} \rfloor$ makes the first two terms of the same order of magnitude and gives

$$|S| \ll N\lambda^{1/6} + N^{1/2}\lambda^{-1/6}. \tag{2.14}$$

Note that this choice of H is only possible if $1 \leq \lambda^{-1/3} \leq N$, but if $\lambda > 1$ then the first term in (2.14) is greater than N and if $\lambda^{-1/3} > N$ then the second term in (2.14) is greater than N. In both cases, the theorem is trivially true. □

Remark 2.2.5. *An important step in the proof of Theorem 2.2.4 is the choice of H. We saw that choosing H such that the first two terms have the same order of magnitude works perfectly. If instead we want the first and last terms or the second and last term to have the same order of magnitude, we need $H \approx N^2\lambda$ and $H \approx (N\lambda)^{-1}$, respectively, which is possible when N and λ are such that $1 \leq H \leq N$, but this time there is nothing we can do with the other cases.*

In the application of this that we will interested in, the first term in the bound of Theorem 2.2.4 usually has a bigger order of magnitude that the second term. We will then call the first and second terms the main and error terms respectively. To make the induction process easier and get higher derivative test, we will state the following, which is a consequence of Theorem 2.2.4, and prove it in a different way.

Theorem 2.2.6. (3rd derivative test version 2) *Suppose $|f'''(x)| \approx \lambda > 0$ for all $x \asymp N$; then*

$$S \ll N\lambda^{1/6} \quad \textit{provided} \quad \lambda^{-2/3} \ll N,$$

where the implied constants in each $\ll$ are allowed to depend on the implied constants in $\approx$.

Proof. We saw in the proof of Theorem 2.2.4 that we may assume that $\lambda \leq 1$.

Suppose that $\lambda^{-2/3} \ll N$. This, together with the fact that $\lambda \leq 1$, immediately gives us that $\lambda^{-1/3} \ll N$, which allow us to pick H to be a positive integer with $H \approx \lambda^{1/3}$ and $H \leq N$.

Just like in the proof of Theorem 2.2.4, it follows from Taylor's Theorem that if $|f'''(x)| \approx \lambda$ then $|f_h''(x)| \approx h\lambda$. So we can use the 2nd derivative test on f_h for each h from 1 to H to get that

$$\begin{aligned}\sum_{n=N}^{2N-h} e(f_h(n)) &\ll (h\lambda)^{1/2}(N-h) + (h\lambda)^{-1/2} \\ &\leq (h\lambda)^{1/2}N + (h\lambda)^{-1/2},\end{aligned}$$

which gives

$$\begin{aligned}\sum_{h=1}^{H}\left|\sum_{n=N}^{2N-h} e(f_h(n))\right| &\ll \lambda^{1/2}N\sum_{h=1}^{H} h^{1/2} + \lambda^{-1/2}\sum_{h=1}^{H} h^{-1/2} \\ &\ll N + \lambda^{-2/3},\end{aligned}$$

since $H \approx \lambda^{1/3}$. Now the fact that $\lambda^{-2/3} \ll N$ gives

$$\sum_{h=1}^{H}\left|\sum_{n=N}^{2N-h} e(f_h(n))\right| \ll N,$$

so we can use Remark 2.2.2 to get that

$$S \ll \frac{N}{H^{1/2}} \ll N\lambda^{1/6}.$$

□

Theorem 2.2.6 will be the starting point of our induction process and we will proceed in a similar way. Graham gives an explicit but somewhat complicated bound in [GKK91], from which we can deduce the following theorems that we will prove in an easier way.

Theorem 2.2.7. (kth derivative test) *Let k be an integer with $k \geq 3$. Suppose $f \in \mathcal{C}^k$ and $\left|f^{(k)}(x)\right| \approx \lambda > 0$ for all $x \asymp N$. Let $Q = 2^{(k-2)}$. Then*

$$S \ll N\lambda^{1/(4Q-2)} \quad \textit{provided} \quad \lambda^{-Q/(2Q-1)} \ll N,$$

where the implied constants in each $\ll$ are allowed to depend on the implied constants in $\approx$.

Proof. We proceed by induction on k, the case $k = 3$ being covered by Theorem 2.2.6. We suppose that $k > 3$ and that the theorem holds for $(k-1)$. We may again assume that $\lambda < 1$.

Let H be an arbitrary (for now) integer such that $1 \leq H \leq N$. It follows from Taylor's Theorem that $\left|f_h^{(k-1)}(x)\right| \asymp h\lambda$ since $\left|f^{(k)}(x)\right| \asymp \lambda$, so we can use the (k-1)st derivative test on f_h for each h from 1 to H with $\lambda_h = h\lambda$ then the condition for the kth derivative with the fact that $h \geq 1$ implies that

$$\lambda_h^{-(Q/2)/(2(Q/2)-1)} \leq \lambda^{-Q/(2Q-1)} \ll N,$$

which is the condition for the $(k-1)$st derivative test, so we can use it to get that

$$\sum_{n=N}^{2N-h} e(f_h(n)) \ll N(\lambda h)^{1/(2Q-2)}.$$

We would like to pick $H \approx \lambda^{-1/(2Q-1)}$ and we can do so because the condition $\lambda^{-Q/(2Q-1)} \ll N$ implies that $\lambda^{-1/(2Q-1)} \ll N^{1/Q} \leq N$, which also gives that

$$\begin{aligned}\sum_{h=1}^{H}\left|\sum_{n=a}^{b-h} e(f_h(n))\right| &\ll \lambda^{1/(2Q-2)} N \sum_{h=1}^{H} h^{1/(2Q-2)} \\ &\ll N\lambda^{1/(Q-2)} H^{(2Q-1)/(2Q-2)} \\ &\ll N.\end{aligned}$$

So by Remark 2.2.2 (Process A),

$$S \ll \frac{N}{H^{1/2}} \leq N\lambda^{1/(4Q-2)}.$$

□

2.3 Application: uniform distribution of sequences of monomials

Now we can use this to get a bound on an exponential sum where the phase is a single variable monomial. By Weyl's criterion, a sequence $f(n)$ is equidistributed modulo one if and only if for each integer $m \neq 0$,

$$S := \sum_{n \asymp N} e(mf(n)) = o(N) \text{ as } N \to \infty$$

Proposition 2.3.1. *Suppose $\alpha > 0$ and $\alpha \notin \mathbb{Z}$. Then for all non zero real numbers r, the sequence $\{rn^\alpha\}$ is equidistributed modulo 1.*

Proof. Take an integer $m \neq 0$ and let $f(x) = mrx^\alpha$. By Weyl's criterion, we need to show that $S = o(N)$ as $N \to \infty$.

Take $k = \lfloor \alpha \rfloor + 1$. Then for all $x \asymp N$, we have

$$| \, mf^{(k)}(x) \, | = mr(\alpha)(\alpha - 1)...(\alpha - k + 1)x^{(\alpha' - 1)} \approx N^{(\alpha' - 1)},$$

where α' is the fractional part of α.

So taking $\lambda = N^{(\alpha' - 1)}$ and $Q = 2^{k-2}$, we see that the condition $\lambda^{-\frac{Q}{2Q-1}} \ll N$ is always satisfied since $-(\alpha' - 1)$ and $\frac{Q}{2Q-1}$ are both less than 1. So we can use the kth derivative test to get that

$$S \ll N\lambda^{\frac{1}{4Q-2}},$$

and since $\lambda = o(1)$ as $N \to \infty$ we conclude that $S = o(N)$ and then the sequence is equidistributed modulo one. □

We now consider the case of two variables. Let $f(x_1, x_2) = rx_1^{\alpha_1}x_2^{\alpha_2}$ with α_1 α_2 non integer positive real numbers and some non-zero real number s. We say that the sequence

$f(n_1, n_2)$ is equidistributed modulo one if

$$\lim_{N_1,N_2\to\infty} \frac{\#Z_f(N_1, N_2; \alpha, \beta)}{N_1 N_2} = \beta - \alpha,$$

where $Z_f(N_1, N_2; \alpha, \beta)) = \{(n_1, n_2) : n_1 \asymp N_1, n_2 \asymp N_2, \alpha \leq \{f(n_1, n_2)\} \leq \beta\}$. In fact, the method that we use gives us this limit by only letting the product $N_1 N_2$ go to infinity, that is

$$\lim_{N_1 N_2\to\infty} \frac{\#Z_f(N_1, N_2; \alpha, \beta)}{N_1 N_2} = \beta - \alpha. \tag{2.15}$$

To avoid re-writing (2.15) every time, we decide, in this chapter, to say that the sequence $f(n_1, n_2)$ is equidistributed if (2.15) holds.

In Chapter 4, we will see that there is some Weyl's criterion for higher dimension, see Theorem 4.0.36 and Corollary 4.0.37, for the case of five variables, but in fact the same proof can easily be adapted to any number of variables.

Theorem 2.3.2. (Weyl's criterion for two variables) *Let $f(n_1, n_2)$ be a sequence of real numbers. If for each integer $m \neq 0$ we have that*

$$S := \sum_{n_1\asymp N_1} \sum_{n_2\asymp N_2} e(mf(n_1, n_2)) = o(N_1 N_2) \text{ as } N_1 N_2 \to \infty$$

then $f(n_1, n_2)$ is equidistributed modulo one.

Proposition 2.3.3. *Suppose $\alpha_1, \alpha_2 > 0$ and $\notin \mathbb{Z}$. If $\alpha_1 + \alpha_2 < 2$ then the sequence $\{f(n_1, n_2)\}$ is equidistributed modulo 1.*

Proof. By the 2nd derivative test we have

$$S \ll (\lambda_1^{1/2} N_1 + \lambda_1^{-1/2}) N_2$$
$$S \ll (\lambda_2^{1/2} N_2 + \lambda_2^{-1/2}) N_1,$$

where $\lambda_1 = N_1^{\alpha_1-2}N_2^{\alpha_2}$ and $\lambda_2 = N_1^{\alpha_1}N_2^{\alpha_2-2}$. So we have

$$S \ll N_1^{\alpha_1/2}N_2^{1+\alpha_2/2} + N_1^{1-\alpha_1}N_2^{1-\alpha_2/2}$$
$$S \ll N_1^{1+\alpha_1/2}N_2^{\alpha_2/2} + N_1^{1-\alpha_1}N_2^{1-\alpha_2/2}$$

and by averaging these inequalities with respective weights t and $(1-t)$, we get

$$\begin{aligned} S &\ll N_1^{1-\alpha_1/2}N_2^{1-\alpha_2/2} + \min\{N_1^{\alpha_1/2}N_2^{1+\alpha_2/2}, N_1^{1+\alpha_1/2}N_2^{\alpha_2/2}\} \\ &\ll N_1^{1-\alpha_1/2}N_2^{1-\alpha_2/2} + N_1^{t\alpha_1/2+(1-t)(1+\alpha_1/2)}N_2^{t(1+\alpha_2/2)+(1-t)\alpha_2/2}. \end{aligned}$$

Now the first term is obviously $o(N_1N_2)$, and the average of the exponents in the second term is $\frac{2+\alpha_1+\alpha_2}{4}$, which is smaller that 1, since $\alpha_1+\alpha_2 < 2$. So by choosing the optimal t, we can make the second term beat the trivial bound in all the variables. □

Using the same technique as for single variable monomials, there should be a way to extend this to bigger α_1 and α_2.

Proposition 2.3.4. *Let k be an integer with $k \geq 3$ and let $Q = 2^{k-2}$. If*

$$N_1^{(k-\alpha_1)\frac{Q}{2Q-1}-1} \ll N_2^{\alpha_2\frac{Q}{2Q-1}} \tag{2.16}$$

and

$$N_2^{(k-\alpha_2)\frac{Q}{2Q-1}-1} \ll N_1^{\alpha_1\frac{Q}{2Q-1}} \tag{2.17}$$

then

$$S \ll N_1^{1+(\alpha_1-tk)/(4Q-2)}N_2^{1+(\alpha_2-(1-t)k)/(4Q-2)}$$

for all $t \in [0,1]$.

Proof. Conditions (2.16) and (2.17) are precisely the conditions for the kth derivative test with variables N_1 and N_2, respectively, for which the value of λ is $N_1^{\alpha_1-k}N_2^{\alpha_2}$ and

$N_1^{\alpha_1} N_2^{\alpha_2 - k}$, respectively. Applying these two kth derivative tests simultaneously, we get

$$\sum_{n_1 \asymp N_1} e(mf(n_1, n_2)) \ll N_1^{1+\frac{\alpha_1 - k}{4Q-2}} N_2^{\frac{\alpha_2}{4Q-2}}$$
$$\sum_{n_2 \asymp N_2} e(mf(n_1, n_2)) \ll N_1^{\frac{\alpha_1}{4Q-2}} N_2^{1+\frac{\alpha_2 - k}{4Q-2}},$$

which trivially gives

$$S \ll N_1^{1+\frac{\alpha_1 - k}{4Q-2}} N_2^{1+\frac{\alpha_2}{4Q-2}}$$
$$S \ll N_1^{1+\frac{\alpha_1}{4Q-2}} N_2^{1+\frac{\alpha_2 - k}{4Q-2}}.$$

Now, as it is will be explained in Chapter 3 (Lemma 3.0.11), for all $t \in [0, 1]$, we can average these two inequalities with respective weights t and $1 - t$ to get the result. □

Proposition 2.3.5. *Let $k = \lfloor \alpha_1 + \alpha_2 + 1 \rfloor$ and $Q = 2^{k-2}$. Suppose that $k \geq 3$. If*

$$N_1^{(k-\alpha_1)\frac{Q}{2Q-1}-1} \ll N_2^{\alpha_2 \frac{Q}{2Q-1}}$$

and

$$N_2^{(k-\alpha_2)\frac{Q}{2Q-1}-1} \ll N_1^{\alpha_1 \frac{Q}{2Q-1}}$$

then the sequence is equidistributed modulo 1.

Proof. Follows directly from Proposition 2.3.4 since the average of the exponents is $\frac{2+\alpha_1+\alpha_2-k}{2}$ which is strictly less that one since $k > \alpha_1 + \alpha_2$. So by choosing the optimal $t \in [0, 1]$, we get a bound that beats the trivial one in all the variables. □

Note that the two conditions in Proposition 2.3.5 are not very restrictive since the power on the left hand side is less than the power in the right hand side. In particular they are satisfied if $N_1 \approx N_2$.

Proposition 2.3.6. *For all integers $k \geq 3$, if the condition for the $(k+1)$st derivative test with N_1 as a variable fails, then the kth derivative test with N_1 as a variable, under*

its weaker condition, can be re-arranged get

$$S = o(N_1 N_2) \text{ as } N_1 N_2 \to \infty.,$$

Proof. Fix $k \geq 3$ and let $Q = 2^{k-2}$. Suppose that the condition for the $(k+1)$st derivative test with N_1 as a variable fails. Then we have that

$$N_1^{(k+1-\alpha_1)\frac{2Q}{4Q-1}-1} \gg N_2^{\alpha_2 \frac{2Q}{4Q-1}}. \tag{2.18}$$

Note that the exponent on the right hand side is positive, so (2.18) is only possible if the exponent in the left hand side is also positive:

$$(k+1-\alpha_1)\frac{2Q}{4Q-1} - 1 > 0. \tag{2.19}$$

Now, under its condition which is weaker, the kth derivative test with respect to N_1 gives

$$S \ll N_1^{1+\frac{\alpha_1-k}{4Q-2}} N_2^{1+\frac{\alpha_2}{4Q-2}}, \tag{2.20}$$

which for all $t > 0$, we can re-arrange using (2.18) to obtain

$$S \ll N_1^{1+\frac{\alpha_1-k}{4Q-2}+t[(k+1-\alpha_1)\frac{2Q}{4Q-1}-1]} N_2^{1+\frac{\alpha_2}{4Q-2}-t[\alpha_2\frac{2Q}{4Q-1}]}. \tag{2.21}$$

If possible, the optimal choice for t is such that both exponents are the same, that is

$$t = \frac{k+\alpha_2-\alpha_1}{4Q-2}\frac{1}{(k+1-\alpha_1+\alpha_2)\frac{2Q}{4Q-1}-1}. \tag{2.22}$$

Now using (2.19), we see that the right hand side in (2.22) is positive and then we can

choose this t, for which both exponents in (2.21) are

$$\begin{aligned}\gamma &= 1 + \frac{\alpha_2}{4Q-2} - \frac{k+\alpha_2-\alpha_1}{4Q-2}\frac{1}{(k+1-\alpha_1+\alpha_2)\frac{2Q}{4Q-1}-1}\alpha_2\frac{2Q}{4Q-1} \\ &= 1 + \frac{\alpha_2}{4Q-2}\left(1 - \frac{(k+\alpha_2-\alpha_1)2Q}{(k+1-\alpha_1+\alpha_2)2Q-(4Q-1)}\right) \\ &= 1 + \frac{\alpha_2}{4Q-2}\left(1 - \frac{(k+\alpha_2-\alpha_1)2Q}{(k-\alpha_1+\alpha_2)2Q-(2Q-1)}\right) \\ &< 1\end{aligned}$$

□

Now we state our result about bi-variate sequences of monomials.

Proposition 2.3.7. *Let $f(x_1, x_2) = rx_1^{\alpha_1}x_2^{\alpha_2}$ with α_1, α_2 non integer positive real numbers and some non-zero real number r, then the sequence is equidistributed modulo one.*

Proof. If $\alpha_1 + \alpha_2 < 2$ then we can use Proposition 2.3.3 to get the result. Now assume $\alpha_1+\alpha_2 \geq 2$. Let $k = \lceil \alpha_1+\alpha_2+1 \rceil$, then $k \geq 3$. If the two conditions of Proposition 2.3.5 holds then we're done. If the first condition, that is the condition of the kth derivative test with respect to the variable N_2, fails, then we can use Proposition 2.3.6 to use lower derivative tests to get the result under weaker and weaker conditions, until we use the 3rd derivative test.

Suppose that the condition of the 3rd derivative test fails. Recall the 2nd derivative test gives without any condition that

$$S \ll N_1N_2\lambda^{1/2} + N_2\lambda^{-1/2}, \tag{2.23}$$

where $\lambda = N_1^{\alpha_1-2}N_2^{\alpha_2}$. Note that the first term in (2.23) is precisely what we get if we plug $k = 2$ in the bounds that we usually get in the higher derivative tests, so the proof of Proposition 2.3.6 gives us that the first term in (2.23) is $o(N_1N_2)$ as $N_1N_2 \to \infty$. Now the second term in (2.23) can be written as $N_1^{1-\alpha_1/2}N_2^{1-\alpha_2/2}$, which is also $o(N_1N_2)$ as $N_1N_2 \to \infty$.

Similarly if the second inequality in Proposition 2.3.5 fails, then we can go through the same process swapping N_1 and N_2 to complete the proof. □

Note that this gives an algorithm that we can apply similarly to sequences of monomials with more than two variables, and even though we do not show it, we suspect that it would be successful most of the time. We will see in Chapter 4 a particular case with five variables.

Chapter 3

Application: Finding a bound that beats the trivial one for a specific family of exponential sums

In this chapter we consider the sequence $f(n_2, n_3, n_4, n_5, n_6) = 3n_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}$ of five variables. The choice of this specific sequence and notation (no variable n_1) will be motivated in Chapter 4. Our goal is to show that this sequence is uniformly distributed modulo one with the most general possible range of the variables and, as we will explain in Chapter 4 (Theorem 4.0.36 and Corollary 4.0.37), it is enough to find a bound for a family of exponential sums that beat the trivial one in all of the variables. We now define the family of exponential sums that we are interested in: for some non zero integer k, let

$$E_k := E_k(N_2, N_3, N_4, N_5, N_6) := \sum_{n_j \asymp N_j} e(3kn_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}).$$

Let us state the main result of this chapter;

Proposition 3.0.8. *Suppose that*

$$\log N_4 \ll (N_2N_3N_5N_6)^{1/100}, \tag{3.1}$$

then for all non zero integer k,

$$E_k = o(N_2N_3N_4N_5N_6) \text{ as } N_2N_3N_5N_6 \to \infty.$$

The rest of this chapter is the proof of this proposition.

Consider the following 5 conditions:

$$\begin{aligned}
(1) \quad & N_2^{59} \ll (N_3^4N_4^3N_5^2N_6)^8 \\
(2) \quad & N_3^{43} \ll (N_2^2N_4^3N_5^2N_6)^8 \\
(3) \quad & N_5^{59} \ll (N_2^2N_3^4N_4^3N_6)^8 \\
(4) \quad & N_6^{67} \ll (N_2^2N_3^4N_4^3N_5^2)^8 \\
(5) \quad & N_4^5 \ll (N_2N_3N_5N_6)^2
\end{aligned}$$

Let us first assume that (1)-(4) hold.

The following is just a special case Theorem 2.2.7 and it also stated as such in the introduction of [Sar00].

Theorem 3.0.9. (5th derivative test) *If $f^{(5)}(x) \approx \lambda$ and $M \gg \lambda^{-8/15}$ then*

$$\sum_{m \asymp M} e(f(m)) \ll M\lambda^{1/30}.$$

where the implied constant in $\ll$ is allowed to depend on the implied constant in $\approx$.

Corollary 3.0.10. *If (1)-(4) holds, then*

$$(1) \implies E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{77}N_3^{94}N_4^{93}N_5^{92}N_6^{91})^{1/90} \tag{3.2}$$

$$(2) \implies E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{92}N_3^{79}N_4^{93}N_5^{92}N_6^{91})^{1/90} \tag{3.3}$$

$$(3) \implies E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{92}N_3^{94}N_4^{93}N_5^{77}N_6^{91})^{1/90} \tag{3.4}$$

$$(4) \implies E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{92}N_3^{94}N_4^{93}N_5^{92}N_6^{76})^{1/90}. \tag{3.5}$$

Proof. To get (3.2), we fix n_3, n_4, n_5, n_6 and use Theorem 3.0.9 with $m = n_2$ and $M = N_2$ that is $f(x) = 15kx^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}$ and $\lambda = N_2^{-13/3}N_3^{4/3}N_4N_5^{2/3}N_6^{1/3}$. Condition (1) being equivalent to $M \gg \lambda^{-8/15}$, we get that

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{77}N_3^4N_4^3N_5^2N_6)^{1/90}.$$

Now taking the trivial bound for all the remaining variables, we obtain the first inequality of the corollary.

Inequalities (3.3), (3.4), (3.5) are obtained in the same way using Theorem 3.0.9 simultaneously with $m = n_3, m = n_5, m = n_6$ respectively and $\lambda = N_2^{2/3}N_3^{-11/3}N_4N_5^{2/3}N_6^{1/3}$, $\lambda = N_2^{2/3}N_3^{4/3}N_4N_5^{-13/3}N_6^{1/3}, \lambda = N_2^{2/3}N_3^{4/3}N_4N_5^{2/3}N_6^{-14/3}$ respectively. Then the condition (2),(2) and (4) are equivalent to $M \gg \lambda^{-8/15}$ for each case. □

Inequalities (3.2),(3.3),(3.4),(3.5) are bounds on E_k that beat the trivial bound for the variable N_2, N_3, N_5, N_6, respectively. The idea now is to combine these four bounds to get only one that beats the trivial bound in the variables N_2, N_3, N_5, N_6 together.

Lemma 3.0.11. *Let $f(x_1, \dots, x_d)$ be a function that maps $\mathbb{R}^d$ to $\mathbb{R}$. Suppose we have a finite set of functions $\{A_m\}$ with*

$$f \ll A_m,$$

for each m, then

$$f \ll \prod_m A_m^{\gamma_m}$$

for all sets $\{\gamma_m\}$ of positive real numbers, with $\sum_m \gamma_m = 1$.

Proof. Fix $x \in \mathbb{R}^d$ and evaluate the functions at this point. Without loss of generality we may assume that $A_1 \leq A_k$ for each k. Then

$$f \ll A_1 = \prod_m A_1^{\gamma_m} \leq \prod_m A_m^{\gamma_m}.$$

□

We will refer to this process as "averaging the inequalities with respective weights $\gamma_1, \ldots, \gamma_s$".

Now by averaging the four inequalities in Corollary 3.0.10 with respective weights 7/30,11/30,7/30 and 5/30, we obtain

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{177} N_3^{177} N_4^{186} N_5^{177} N_6^{177})^{1/180}, \tag{3.6}$$

and these weight are optimal in the sense that they give a bound that is equally strict in all the variables that we are working with.

Here we specify the optimal weights but in fact we can simply note that the average of the exponents of N_2, N_3, N_5, N_6 in the right hand side of the inequalities in Corollary 3.0.10 is always $\frac{177}{180}$. It is then clear that (3.6) is the optimal bound that we get by averaging these inequalities and the weights are not important. In the future, we will directly deduce the optimal bound from the inequalities.

In addition, if (5) holds, then N_4 is small relative to the other variables. The bound given by (3.6) is then less than another bound that we can obtain by "transferring" powers of N_4 to the other variables. We will often say that we "re-arrange" a bound to refer to this process. So we can re-arrange (3.6) to get

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2 N_3 N_4 N_5 N_6)^{179.8/180},$$

which beats the trivial bound in all the variables.

Else, if (5) fails, then we have

$$N_4^5 \gg (N_2 N_3 N_5 N_6)^2,$$

which implies that

$$N_4^{0.5} \gg (N_2 N_3 N_5 N_6)^{0.2}.$$

In order to use this, we want a bound for which the exponent of N_4 is small. For this, we

need Lemma 5.2 in [DGS$^+$13], that we now state.

Lemma 3.0.12. *Let $g(t)$ be a real, continuously differentiable function on the interval $[a,b]$, with $\mid g'(t) \mid \geq \lambda > 0$, and let $N > 0$. Then*

$$\sum_{a \leq n \leq b} min\{N, 1/ \mid\mid g(n) \mid\mid\} \ll (\mid g(b) - g(a) \mid +1)(N + \frac{1}{\lambda} log(b-a+2)).$$

Proof. See page 77 of [Krä89]. □

We also need the following, that is an analogue of Lemma 5.3 in [DGS$^+$13].

Lemma 3.0.13. *For every $\delta > 0$,*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll_\delta N_2^{2+2\delta} N_3^{4+4\delta} N_4^0 N_5^{2+2\delta} N_6^{1+\delta}$$

$$+ N_2^{2/3+2\delta} N_3^{4/3+4\delta} N_4^1 N_5^{2/3+2\delta} N_6^{1/3+\delta}$$

Proof. Fix $\delta > 0$. For some positive integer n, let

$$b_n = \sum_{n_2 \asymp N_2} \sum_{n_3 \asymp N_3} \sum_{n_5 \asymp N_5} \sum_{\substack{n_6 \asymp N_6 \\ n_2^2 n_3^4 n_5^2 n_6 = n}} 1$$

and note that $b_n \leq d(n)^3$, where $d(n)$ is the number of divisors of n. Now it is well known that $d(n) \ll_\delta n^\delta$, refer to page 296 of [Apo76] for a proof. We then have that $b_n \ll_\delta n^{\delta/2}$.

We recall the well-known bound

$$\sum_{n \asymp N} e(\alpha n) \ll min\{N, 1/ \mid\mid \alpha \mid\mid\},$$

that can be found in [IK04] page 199.

Applying Lemma 3.0.12 with $N = N_4$, $g(t) = 3kt^{1/3}$, which is continuously differen-

tiable on the interval $[N_2^2N_3^4N_5^2N_6, 512N_2^2N_3^4N_5^2N_6]$ so $\lambda = (N_2^2N_3^4N_5^2N_6)^{-2/3}$, we have

$$\begin{aligned} E_k(N_2,N_3,N_4,N_5,N_6) &= \textstyle\sum_{N_2^2N_3^4N_5^2N_6\le n\le 512N_2^2N_3^4N_5^2N_6} b_n \sum_{n_4\asymp N_4} e(3kn^{1/3}n_4) \\ &\ll_\delta (N_2^2N_3^4N_5^2N_6)^{\delta/2} \textstyle\sum_{N_2^2N_3^4N_5^2N_6\le n\le 512N_2^2N_3^4N_5^2N_6} \min\{N_4, \frac{1}{||3kn^{1/3}||}\} \\ &\ll (N_2^2N_3^4N_5^2N_6)^{\delta/2}(N_2^2N_3^4N_5^2N_6)^{1/3}(N_4 \\ &\quad +(N_2^2N_3^4N_5^2N_6)^{2/3}\log(511N_2^2N_3^4N_5^2N_6+2)) \\ &\ll (N_2^2N_3^4N_5^2N_6)^{\delta}[(N_2^2N_3^4N_4^3N_5^2N_6)^{1/3} + (N_2^2N_3^4N_5^2N_6)]. \end{aligned}$$

□

Taking (3.3) from Corollary 3.0.10 and Lemma 3.0.13 with respective weights 10/11 and 1/11, we get

$$\begin{aligned} E_k &\ll_\delta N_2^{2/3+2\delta}N_3^{4/3+4\delta}N_4N_5^{2/3+2\delta}N_6^{1/3+\delta} \\ &\quad +\min\{(N_2^{92}N_3^{79}N_4^{93}N_5^{92}N_6^{91})^{1/90}, N_2^{1.12+2\delta}N_3^{1.17+4\delta}N_4^{0.94}N_5^{1.12+2\delta}N_6^{1.02+\delta}\} \\ &\ll N_2^{2/3+2\delta}N_3^{4/3+4\delta}N_4N_5^{2/3+2\delta}N_6^{1/3+\delta} + N_2^{1.12+2\delta}N_3^{1.17+4\delta}N_4^{0.94}N_5^{1.12+2\delta}N_6^{1.02+\delta}, \end{aligned}$$

and using the fact that (5) fails, that is N_4 is large relative to the other variables, we can re-arrange the second term of the bound above to get

$$E_k(N_2,N_3,N_4,N_5,N_6) \ll_\delta N_2^{2/3+2\delta}N_3^{4/3+4\delta}N_4N_5^{2/3+2\delta}N_6^{1/3+\delta} + (N_2N_3N_4N_5N_6)^{0.99+4\delta}. \tag{3.7}$$

The exponent of N_3 is still greater than one. In order to fix this, we want to combine this with a bound that is "good" for the variable N_3 and whose exponent for N_4 is not more that one. We will need the following theorem by Fouvry and Iwaniec that can be found in [FI89], Theorem 3, for which we will omit the proof.

Theorem 3.0.14. *Let α, α_1, α_2 be real constants such that $\alpha \neq 1$ and $\alpha\alpha_1\alpha_2 \neq 0$. Let M, M_1, M_2, $x > 1$. We then have*

$$\sum_{m\asymp M}\sum_{m_1\asymp M_1}\sum_{m_2\asymp M_2} e(x\frac{m^\alpha m_1^{\alpha_1}m_2^{\alpha_2}}{M^\alpha M_1^{\alpha_1}M_2^{\alpha_2}}) \ll$$

$$[x^{1/4}M^{1/2}(M_1M_2)^{3/4}$$

$$+M^{7/10}M_1M_2 + M(M_1M_2)^{3/4}$$

$$+x^{-1/4}M^{11/10}M_1M_2)](\log 2MM_1M_2)^2.$$

Corollary 3.0.15. *Without any assumption on the variables, we have that*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{11/12}N_3^{5/6}N_4N_5^{7/6}N_6^{13/12}$$

$$+N_2N_3^{7/10}N_4N_5N_6 + N_2^{3/4}N_3N_4^{3/4}N_5N_6$$

$$+N_2^{5/6}N_3^{23/30}N_4^{3/4}N_5^{5/6}N_6^{11/12})(\log N_4)^2.$$

Proof. Applying Theorem 3.0.14 with $x = 15kM^{\alpha}M_1^{\alpha_1}M_2^{\alpha_2}n_5n_6$, $m = n_3$, $m_1 = n_2$, $m_2 = n_4$, and of course $M = N_3, M_1 = N_2, M_2 = N_4$, with their corresponding exponent in the sequence i.e. $\alpha = 4/3$, $\alpha_1 = 2/3$, $\alpha_2 = 1$ and the trivial bound on the two remaining variables n_5 and n_6, we get

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{11/12}N_3^{5/6}N_4N_5^{7/6}N_6^{13/12}$$

$$+N_2N_3^{7/10}N_4N_5N_6 + N_2^{3/4}N_3N_4^{3/4}N_5N_6$$

$$+N_2^{5/6}N_3^{23/30}N_4^{3/4}N_5^{5/6}N_6^{11/12})(\log 2N_2N_3N_4)^2.$$

Now note that

$$(\log 2N_2N_3N_4)^2 \ll (\log N_2 + \log N_3 + \log N_4)^2 \ll (\max\{\log N_2, \log N_3, \log N_4\})^2, \quad (3.8)$$

and since we are in the case where (5) fails, we have

$$N_4^4 \gg (N_2N_3N_5N_6)^2 \gg N_2^2,$$

which implies that

$$\log N_4 \gg \log N_2, \quad (3.9)$$

and similarly, we have

$$\log N_4 \gg \log N_3. \tag{3.10}$$

Now plugging (3.9) and (3.10) in (3.8), we obtain

$$(\log 2N_2N_3N_4)^2 \ll (\log N_4)^2.$$

□

Corollary 3.0.16. *Without any assumption on the variables, we have that*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{7/6}N_3^{5/6}N_4N_5^{11/12}N_6^{13/12}$$

$$+N_2N_3^{7/10}N_4N_5N_6 + N_2N_3N_4^{3/4}N_5^{3/4}N_6$$

$$+N_2^{5/6}N_3^{23/30}N_4^{3/4}N_5^{5/6}N_6^{11/12})(\log N_4)^2.$$

Proof. Since n_2 and n_5 have the same exponent, we can just swap them from Corollary 3.0.15. □

Now note that if $N_3 \ll (N_2N_5N_6)^{1/3}$ then we can re-arrange (3.7) to get a bound of the form $(N_2N_3N_5N_6)^{1-\epsilon}N_4$ as desired. Otherwise, we have that $N_3 \gg (N_2N_5N_6)^{1/3}$ that we can use to re-arrange the second terms in Corollary 3.0.15 and 3.0.16 to get $N_2^{1/15}N_3^{9/10}N_4N_5^{1/15}N_6^{1/15}(\log N_4)^2$. Now recall we initially assumed (see (3.1)) that $\log N_4 \ll (N_2N_3N_5N_6)^{1/100}$. so the second terms in each corollaries are actually bounded by $(N_2N_3N_5N_6)^{1-\epsilon}N_4$. Also, for both those corollaries, the third terms can be re-arranged using the fact that (5) fails to beat the trivial bound in all the variables and the last term already beats the trivial bound.

In our situation, we can then rewrite Corollary 3.0.15 and 3.0.16 as

$$E_k \ll N_2^{11/12}N_3^{5/6}N_4(\log N_4)^2N_5^{7/6}N_6^{13/12} + (N_2N_3N_5N_6)^{1-\epsilon}N_4$$

and

$$E_k \ll N_2^{7/6} N_3^{5/6} N_4 (\log N_4)^2 N_5^{11/12} N_6^{13/12} + (N_2 N_3 N_5 N_6)^{1-\epsilon} N_4.$$

Averaging these inequalities with weights $1/2$, we obtain

$$E_k \ll N_2^{25/24} N_3^{5/6} N_4 (\log N_4)^2 N_5^{25/24} N_6^{13/12} + (N_2 N_3 N_5 N_6)^{1-\epsilon} N_4.$$

Now combining this and (3.7) with respective weights $3/4$ and $1/4$, we get

$$\begin{aligned} E_k &\ll_\delta \min\{N_2^{25/24} N_3^{5/6} N_4 (\log N_4)^2 N_5^{25/24} N_6^{13/12}, N_2^{2/3+2\delta} N_3^{4/3+4\delta} N_4^1 N_5^{2/3+2\delta} N_6^{1/3+\delta}\} \\ &\quad + (N_2 N_3 N_4 N_5 N_6)^{0.99+4\delta} + (N_2 N_3 N_5 N_6)^{1-\epsilon} N_4 \\ &\ll N_2^{91/96+\delta/2} N_3^{23/24+\delta} N_4 (\log N_4)^2 N_5^{91/96+\delta/2} N_6^{43/48+\delta/4} \\ &\quad + (N_2 N_3 N_4 N_5 N_6)^{0.99+4\delta} + (N_2 N_3 N_5 N_6)^{1-\epsilon} N_4. \end{aligned}$$

Now we use again the fact that $\log N_4 \ll (N_2 N_3 N_5 N_6)^{1/100}$ and fix δ small enough so that the above gives

$$E_k = o(N_2 N_3 N_4 N_5 N_6) \text{ as } N_2 N_3 N_5 N_6 \to \infty.$$

So everything works when (1)-(4) hold, but we still have 4 cases to consider, namely if (1) fails, if (2) fails, if (3) fails and if (4) fails. The idea will be to use some lower derivative tests that give weaker bounds but under weaker conditions. We will see that these weaker bounds will be enough to beat the trivial bound precisely because we assume that the conditions for the 5th derivative test fails, which gives us a specific range of the variables and allow us to re-arrange the bounds from lower derivative tests.

The following is a special case of Theorem 2.2.7 and is stated as such in the introduction of [RS02].

Theorem 3.0.17. (4th derivative test) *If $f^{(4)}(x) \approx \lambda$ and $M \gg \lambda^{-4/7}$ then*

$$\sum_{m \asymp M} e(f(m)) \ll M \lambda^{1/14}.$$

Corollary 3.0.18. *If* $N_2^{19} \ll (N_3^4 N_4^3 N_5^2 N_6)^4$ *then*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{32} N_3^{46} N_4^{45} N_5^{44} N_6^{43})^{1/42}.$$

Proof. This is Theorem 3.0.17 with $m = n_2$, $f(x) = 3kx^{2/3} n_3^{4/3} n_4 n_5^{2/3} n_6^{1/3}$ so we have $\lambda = N_2^{-10/3} N_3^{4/3} N_4 N_5^{2/3} N_6^{1/3}$. □

So if (1) fails but the condition for Corollary 3.0.18 is satisfied i.e. $(N_3^4 N_4^3 N_5^2 N_6)^{8/59} \ll N_2 \ll (N_3^4 N_4^3 N_5^2 N_6)^{4/19}$, we have

$$N_2^9 \gg (N_3^4 N_4^3 N_5^2 N_6)^{1.2}$$

since $9 \cdot 8/59 > 1.2$, so we can use Corollary 3.0.18 and re-arrange it to get

$$\begin{aligned} E_k(N_2, N_3, N_4, N_5, N_6) &\ll (N_2^{32} N_3^{46} N_4^{45} N_5^{44} N_6^{43})^{1/42} \\ &\ll (N_2^{32+9} N_3^{46-4.8} N_4^{45-3.6} N_5^{44-2.4} N_6^{43-1.2})^{1/42} \\ &= (N_2^{41} N_3^{41.2} N_4^{41.4} N_5^{41.6} N_6^{41.8})^{1/42}, \end{aligned} \tag{3.11}$$

which beats the trivial bound in all the variables.

Corollary 3.0.19. *If* $N_3^{11} \ll (N_2^2 N_4^3 N_5^2 N_6)^4$ *then*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{44} N_3^{34} N_4^{45} N_5^{44} N_6^{43})^{1/42}.$$

Proof. This is Theorem 3.0.17 with $m = n_3$, $f(x) = 3kn_2^{2/3} x^{4/3} n_4 n_5^{2/3} n_6^{1/3}$ so we have $\lambda = N_2^{2/3} N_3^{-8/3} N_4 N_5^{2/3} N_6^{1/3}$. □

So if (2) fails but the condition for Corollary 3.0.19 is satisfied i.e. $(N_2^2 N_4^3 N_5^2 N_6)^{8/43} \ll N_3 \ll (N_2^2 N_4^3 N_5^2 N_6)^{4/11}$, we have

$$N_3^7 \gg (N_2^2 N_4^3 N_5^2 N_6)^{1.3}$$

since $7 \cdot 8/43 > 1.3$, so we can use Corollary 3.0.19 and re-arrange it to get

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{44} N_3^{34} N_4^{45} N_5^{44} N_6^{43})^{1/42}$$

$$\ll (N_2^{44-2.6} N_3^{34+7} N_4^{45-3.9} N_5^{44-2.6} N_6^{43-1.3})^{1/42}$$

$$= (N_2^{41.4} N_3^{41} N_4^{41.1} N_5^{41.4} N_6^{41.7})^{1/42},$$

which beats the trivial bound in all the variables.

Corollary 3.0.20. *If* $N_5^{19} \ll (N_2^2 N_3^4 N_4^3 N_6)^4$ *then*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{44} N_3^{46} N_4^{45} N_5^{32} N_6^{43})^{1/42}.$$

Proof. This is Theorem 3.0.17 with $m = n_5$, $f(x) = 3kn_2^{2/3} n_3^{4/3} n_4 x^{2/3} n_6^{1/3}$ so we have $\lambda = N_2^{2/3} N_3^{4/3} N_4 N_5^{-10/3} N_6^{1/3}$. □

So if (3) fails but the condition for Corollary 3.0.20 is satisfied i.e. $(N_2^2 N_3^4 N_4^3 N_6)^{8/58} \ll N_5 \ll (N_2^2 N_3^4 N_4^3 N_6)^{4/19}$, by swapping the exponents of N_2 and N_5 in (3.11), since N_2 and N_5 have the same exponent in the sequence, we get

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{41} N_3^{41.2} N_4^{41.4} N_5^{41.6} N_6^{41.8})^{1/42},$$

which beats the trivial bound in all the variables.

Corollary 3.0.21. *If* $N_6^{23} \ll (N_2^2 N_3^4 N_4^3 N_5^2)^4$ *then*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{44} N_3^{46} N_4^{45} N_5^{44} N_6^{31})^{1/42}.$$

Proof. This is Theorem 3.0.17 with $m = n_6$, $f(x) = 3kn_2^{2/3} n_3^{4/3} n_4 n_5^{2/3} x^{1/3}$ so we have $\lambda = N_2^{2/3} N_3^{4/3} N_4 N_5^{2/3} N_6^{-11/3}$. □

So if (4) fails but the condition for Corollary 3.0.21 is satisfied i.e.

$(N_2^2N_3^4N_4^3N_5^2)^{8/67} \ll N_6 \ll (N_2^2N_3^4N_4^3N_5^2)^{4/23}$, we have

$$N_6^{10} \gg (N_2^2N_3^4N_4^3N_5^2)^{1.1}$$

since $10 \cdot 8/67 > 1.1$, so we can use Corollary 3.0.21 and re-arrange it to get

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{44}N_3^{46}N_4^{45}N_5^{44}N_6^{31})^{1/42}$$

$$\ll (N_2^{44-2.2}N_3^{46-4.4}N_4^{45-3.3}N_5^{44-2.2}N_6^{31+10})^{1/42}$$

$$= (N_2^{41.8}N_3^{41.6}N_4^{41.7}N_5^{41.8}N_6^{41})^{1/42},$$

which beat the trivial bound in all the variables.

We still need to consider individually the cases the conditions for corollaries 3.0.18, 3.0.19, 3.0.20 and 3.0.21 fail.

Let us recall the statement Theorem 2.2.4 from Chapter 2.

Theorem 3.0.22. (3rd derivative test) *If $f^{(3)}(x) \approx \lambda$ then*

$$\sum_{m \asymp M} e(f(m)) \ll M\lambda^{1/6} + M^{1/2}\lambda^{-1/6}.$$

Corollary 3.0.23. *Without any assumption on the variables, we have that*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{11}N_3^{22}N_4^{21}N_5^{20}N_6^{19})^{1/18}$$

$$+(N_2^{16}N_3^{14}N_4^{15}N_5^{16}N_6^{17})^{1/18}.$$

Proof. This is Theorem 3.0.22 with $m = n_2, M = N_2$, $\lambda = N_2^{-7/3}N_3^{4/3}N_4N_5^{2/3}N_6^{1/3}$. □

So if the condition for Corollary 3.0.18 fails, we have that

$$N_2^6 \gg (N_3^4N_4^3N_5^2N_6)^{1.1}$$

since $6 \cdot 4/19 > 1.1$ so we can re-arrange the bound of Corollary 3.0.23 to get that

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{11+6} N_3^{22-4.4} N_4^{21-3.3} N_5^{20-2.2} N_6^{19-1.1})^{1/18}$$

$$+(N_2^{16} N_3^{14} N_4^{15} N_5^{16} N_6^{17})^{1/18}$$

$$\ll (N_2^{17} N_3^{17.6} N_4^{17.7} N_5^{17.8} N_6^{17.9})^{1/18} + (N_2^{16} N_3^{14} N_4^{15} N_5^{16} N_6^{17})^{1/18}, \tag{3.12}$$

which beats the trivial bound in all the variables.

Corollary 3.0.24. *Without any assumption on the variables, we have that*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{20} N_3^{13} N_4^{21} N_5^{20} N_6^{19})^{1/18}$$

$$+(N_2^{16} N_3^{14} N_4^{15} N_5^{16} N_6^{17})^{1/18}.$$

Proof. This is Theorem 3.0.22 with $m = n_3$, $\lambda = N_2^{2/3} N_3^{4/3} N_4 N_5^{-5/3} N_6^{1/3}$. □

So if the condition for Corollary 3.0.19 fails, we have that

$$N_3^4 \gg (N_2^2 N_4^3 N_5^2 N_6)^{1.1}$$

since $4 \cdot 4/11 > 1.1$ so we can re-arrange the bound of Corollary 3.0.24 to get that

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{20-2.2} N_3^{13+4} N_4^{21-3.3} N_5^{20-2.2} N_6^{19-1.1})^{1/18}$$

$$+(N_2^{16} N_3^{14} N_4^{15} N_5^{16} N_6^{17})^{1/18}$$

$$\ll (N_2^{17.8} N_3^{17} N_4^{17.7} N_5^{17.8} N_6^{17.9})^{1/18} + (N_2^{16} N_3^{14} N_4^{15} N_5^{16} N_6^{17})^{1/18},$$

which beats the trivial bound in all the variables.

Corollary 3.0.25. *Without any assumption on the variables, we have that*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{20} N_3^{22} N_4^{21} N_5^{11} N_6^{19})^{1/18}$$

$$+(N_2^{16}N_3^{14}N_4^{15}N_5^{16}N_6^{17})^{1/18}.$$

Proof. This is Theorem 3.0.22 with $m = n_5$, $\lambda = N_2^{2/3}N_3^{4/3}N_4N_5^{-7/3}N_6^{1/3}$. □

So if the condition for Corollary 3.0.20 fails, and using Corollary 3.0.25, we get the same as in swapping N_2 and N_5 in (3.12) since they have the same exponent, that is

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{17.8}N_3^{17.6}N_4^{17.7}N_5^{17}N_6^{17.9})^{1/18}$$

$$+(N_2^{16}N_3^{14}N_4^{15}N_5^{16}N_6^{17})^{1/18},$$

which beats the trivial bound in all the variables.

Corollary 3.0.26. *Without any assumption on the variables, we have that*

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{20}N_3^{22}N_4^{21}N_5^{20}N_6^{10})^{1/18}$$

$$+(N_2^{16}N_3^{14}N_4^{15}N_5^{16}N_6^{17})^{1/18}.$$

Proof. This is Theorem 3.0.22 with $m = n_6$, $\lambda = N_2^{2/3}N_3^{4/3}N_4N_5^{2/3}N_6^{-8/3}$. □

So if the condition for Corollary 3.0.21 fails, we have that

$$N_6^7 \gg (N_2^2N_3^4N_4^3N_5^2)^{1.1}$$

since $7 \cdot 4/23 > 1.1$ so we can re-arrange the bound of Corollary 3.0.26 to get that

$$E_k(N_2, N_3, N_4, N_5, N_6) \ll (N_2^{20-2.2}N_3^{22-4.4}N_4^{21-3.3}N_5^{20-2.2}N_6^{10+7})^{1/18}$$

$$+(N_2^{16}N_3^{14}N_4^{15}N_5^{16}N_6^{17})^{1/18}$$

$$\ll (N_2^{17.8}N_3^{17.6}N_4^{17.7}N_5^{17.8}N_6^{17})^{1/18} + (N_2^{16}N_3^{14}N_4^{15}N_5^{16}N_6^{17})^{1/18},$$

which beats the trivial bound in all the variables.

Then we covered all the possibles ranges of the variables!

Chapter 4

Abelian varieties over a finite field of dimension 3 with prescribed groups

In this chapter we present the results about Abelian varieties over finite fields of dimension 3 that we can prove using the bound on the exponential sum of five variable found in Chapter 3. These results are actually extensions of the results in [DGS+13] for Abelian surfaces.

In general an Abelian variety of dimension g over $\mathbb{F}_q$ is an algebraic variety, that is the set of solutions of some polynomial equations with coefficients in $\mathbb{F}_q$, with the structure of an Abelian group. For example an elliptic curve is an Abelian variety of dimension 1. Silverman gives more precise definitions in [Sil92].

We then denote by $A(\mathbb{F}_q)$ the group of points of A with coordinates in $\mathbb{F}_q$. Then $A(\mathbb{F}_q)$ is a finite Abelian group of rank at most $2g$. In fact we have that

$$A(\mathbb{F}_q) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_{2g}\mathbb{Z}$$

with unique integers $m_1, \ldots, m_{2g}$ such that $m_i | m_{i+1}$ for all $i = 1, \ldots, 2g-1$, or equivalently

$$A(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \ \times \ \mathbb{Z}/n_1n_2\mathbb{Z} \ \times \cdots \times \ \mathbb{Z}/n_1n_2\cdots n_{2g}\mathbb{Z}$$

with unique integers $n_1, \ldots, n_{2g}$. We will use both notations.

The qth-power-Frobenius is the map that raises each coordinates of the elements of the variety to its qth power. Note that because A is defined over $\mathbb{F}_q$, the image of every point of A under the qth-power-Frobenius will still be in A and then the qth-power-Frobenius is in fact an endomorphism of A. An important property of the qth-power-Frobenius endomorphism is that it fixes $A(\mathbb{F}_q)$.

An isogeny between two Abelian varieties is a morphism that is surjective and has a finite kernel.

Let $f_A(T)$ be the characteristic polynomial of the variety, that is the characteristic polynomial of its Frobenius endomorphism (acting on some ℓ-adic finite dimensional space).

A q-Weil number π is an algebraic number such that its absolute value and the absolute value of all its Galois conjugates on the extension $\overline{Q}/Q$ is $\sqrt{q}$ and a q-Weil polynomial is a monic polynomial with integer coefficients whose roots are q-Weil numbers. We know that if A is an Abelian variety over $\mathbb{F}_q$ then $f_A(T)$ is a q-Weil polynomial.

We say that two Abelian varieties are isogenous if there exists an isogeny between them. We know that A_1 and A_2 are isogenous if and only if they have the same characteristic polynomial, that is $f_{A_1}(T) = f_{A_2}(T)$.

Abelian varieties over a finite field $\mathbb{F}_q$ are classified by the Tate-Honda theory which asserts that there is a one-to-one correspondence between the $\mathbb{F}_q$-isogeny classes of simple Abelian varieties and conjugacy classes of Weil numbers. There is an obvious correspondence between conjugacy classes of Weil numbers and Weil polynomials so we get the following correspondence

$$[A] \longleftrightarrow f_A(T) = P_A(T)^e$$

where $[A]$ is the isogeny class represented by the Abelian variety A and $P_A(T)$ is an

irreducible polynomial whose roots are Weil numbers and e is an integer. Also it is known that $e = 1$ if and only if $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field.

Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then $E(\mathbb{F}_q)$ is a finite Abelian group of rank at most 2 such that

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z}, \tag{4.1}$$

for some positive integers n_1, n_2. Let $S(N_1, N_2)$ be the set of pairs of integers $n_1 \leq N_1, n_2 \leq N_2$ such that (4.1) holds, for some prime p. Banks, Pappalardi and Shparlinski in [BPS12] conjectured that very "split" groups (when n_1 is large compared to n_2) occur with density zero. This was proven by Chandee, David, Koukoulopoulos and Smith in [CDKS12], who showed that if $N_1 \geq \exp(N_2^{1/2+\epsilon})$, for some fixed $\epsilon > 0$, then

$$\#S(N_1, N_2) = o(N_1N_2)$$

as $N_1 \to \infty$.

Let A be an Abelian surface over the finite field $\mathbb{F}_q$. Now the group of rational points on A is a finite Abelian group of rank at most 4 such that

$$A(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}. \tag{4.2}$$

David, Garton, Scherr, Shankar, Smith, Thompson showed in [DGS$^+$13] (Theorem 1.1) that (4.2) do not occur if n_1 is very large compared to n_2, n_3, n_4. More precisely, if n_1, n_2, n_3, n_4 are positive integers such that (4.2) holds, for some prime power q then

$$n_1 < 60n_2^{1/4}n_3^{3/2}n_4^{3/4} + 1.$$

They also showed (Theorem 1.2) that (4.2) occur with density zero in a wider range of the variables. Let $S(N_1, N_2, N_3, N_4)$ be the set of quadruples (n_1, n_2, n_3, n_4), that satisfies

(4.2), for which $N_j \leq n_j \leq 2N_j$ for $j = 1, 2, 3, 4$. They showed that if

$$\frac{N_1 N_2^{1/4}}{N_3^{1/2} N_4^{1/4}} \to \infty$$

as $N_2 N_4 \to \infty$, then

$$\#S(N_1, N_2, N_3, N_4) = o(N_1 N_2 N_3 N_4)$$

as $N_2 N_4 \to \infty$.

We will follow their ideas to get some similar results for the case of Abelian varieties of dimension 3. Starting now and for the rest of this chapter we let q be a prime power, $\mathbb{F}_q$ be a finite field with q elements and A be an Abelian variety of dimension 3 defined over $\mathbb{F}_q$.

Our first tool to study groups of points of Abelian varieties over finite fields is the following elegant criterion of Rybakov's that can be found in [Ryb10].

Theorem 4.0.27. *Let A be an Abelian variety over a finite field $\mathbb{F}_q$ with characteristic polynomial $f_A(T)$. Suppose that $End_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field. Let G be an Abelian group with $\#G = f_A(1)$. Then*

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_{2g}\mathbb{Z}, \quad m_1 | m_2 | \ldots | m_{2g}$$

is the group of points on some variety in the isogeny class of A if and only if

$$\prod_{i=1}^{2g-k} m_i \text{ divides } \frac{f_A^{(k)}(1)}{k!} \text{ for } k = 0, \ldots, 2g-1$$

Remark 4.0.28. *In fact, only looking at one direction of the theorem, Rybakov proves that if G is as above and is the group of points of some Abelian variety $A(\mathbb{F}_q)$ with characteristic polynomial $f_A(T)$ then $\#G = f_A(1)$ and*

$$\prod_{i=1}^{2g-k} m_i \text{ divides } \frac{f_A^{(k)}(1)}{k!} \text{ for } k = 0, \ldots, 2g-1,$$

and we do not need the condition that $End_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ *is a field.*

We apply Remark 4.0.28 to the case $g = 3$ and change the notation of the group to get rid of the divisibility condition that we have on the m_i's.

Corollary 4.0.29. *Suppose that*

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5n_6\mathbb{Z}$$

is the group of points of an Abelian variety of dimension 3 with characteristic polynomial $f_A(T) = T^6 + a_1T^5 + a_2T^4 + a_3T^3 + a_2qT^2 + a_1q^2T + q^3$. *Then following system must be satisfied:*

$$\begin{array}{llllllllll}
(a) & q^2a_1 & +a_1 & +qa_2 & +a_2 & +a_3 & +q^3 & +1 & = & n_1^6n_2^5n_3^4n_4^3n_5^2n_6 =: N \\
(b) & q^2a_1 & +5a_1 & +2qa_2 & +4a_2 & +3a_3 & & +6 & \equiv & 0 \mod n_1^5n_2^4n_3^3n_4^2n_5 \\
(c) & & 10a_1 & +qa_2 & +6a_2 & +3a_3 & & +15 & \equiv & 0 \mod n_1^4n_2^3n_3^2n_4 \\
(d) & & 10a_1 & & +4a_2 & +a_3 & & +20 & \equiv & 0 \mod n_1^3n_2^2n_3 \\
(e) & & 5a_1 & & +a_2 & & & +15 & \equiv & 0 \mod n_1^2n_2 \\
(f) & & a_1 & & & & & +6 & \equiv & 0 \mod n_1
\end{array}$$

Proof. This follows directly by computing the derivatives of $f_A(T)$. □

We call those congruences (a)-(f) because we will use them a lot and refer to them as Rybakov's equations or Rybakov's congruences.

Proposition 4.0.30. (Key Proposition) *Suppose that*

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5n_6\mathbb{Z}$$

is the group of points of an Abelian variety of dimension 3 with characteristic polynomial $f_A(T) = T^6 + a_1T^5 + a_2T^4 + a_3T^3 + a_2qT^2 + a_1q^2T + q^3$ *and that* $15\frac{N^{1/3}}{n_1^2n_2} \notin \mathbb{Z}$. *Let*

$\delta = \left|\left|15\frac{N^{1/3}}{n_1^2 n_2}\right|\right|_{\mathbb{R}/\mathbb{Z}}$ *be the distance between* $15\frac{N^{1/3}}{n_1^2 n_2}$ *and its nearest integer then*

$$n_1 n_2^{1/6} < \frac{16}{\delta} n_3^{2/3} n_4^{1/2} n_5^{1/3} n_6^{1/6}.$$

Proof. The first step is to show that $5a_1 \equiv -15(q+1) \mod n_1^2 n_2$. By adding and subtracting the congruences in Corollary 2.7, we find that

$$\begin{aligned} a_1 &\equiv -q^3 - 5 \mod n_1^2 n_2 \\ a_2 &\equiv 10 + 5q^3 \mod n_1^2 n_2 \\ a_3 &\equiv -10 - 10q^3 \mod n_1^2 n_2 \end{aligned}$$

Lemma 4.0.31. $5(q-1)^2 \equiv 0 \mod n_1^2 n_2$

Proof. Our goal is to imitate the proof of $(q-1)^2 \equiv 0 \mod n_1^2 n_2$ for Abelian surfaces in [DGS+13]. So we need an equation of the form

$$(q-1)(n_1^2 n_2 \alpha + (\pm 5)(q-1)^2) \equiv 0 \mod n_1^3 n_2^2, \tag{4.3}$$

for some integer α. We want to work modulo $n_1^3 n_2^2$ so we can only use Rybakov's equation (a)-(d). By taking $-(a) + 2(b) - 2(c) + (d)$ we get

$$(q-1)(-1 + a_1 + a_2 - q + a_1 q - q^2) \equiv 0 \mod n_1^3 n_2. \tag{4.4}$$

Now respecting their equivalences modulo $n_1^2 n_2$ we let

$$\begin{aligned} a_1 &= -q^3 - 5 + k_1 n_1^2 n_2 \\ a_2 &= 5q^3 + 10 + k_2 n_1^2 n_2 \\ a_3 &= -10q^3 - 10 + k_3 n_1^2 n_2, \end{aligned}$$

for some integers k_1, k_2 and k_3. Plugging those into (4.4) we obtain

$$(q-1)(n_1^2 n_2(k_1(q+1)+k_2) - (q-1)^2(-4-2q+q^2)) \equiv 0 \mod n_1^3 n_2^2.$$

In order to get something like (4.3) we need to reduce the powers of q in the second term. The next step is to get information about q modulo $n_1^2 n_2$ (and not only modulo $n_1^3 n_2^2$). Replacing a_1, a_2 and a_3 by their equivalence modulo $n_1^2 n_2$ and taking $5(a)+(q-3)(c)$ we get that

$$5(q-1)^3 \equiv 0 \mod n_1^2 n_2. \tag{4.5}$$

Now $-(a)+5(q-1)^3$ gives

$$(q-1)^5 \equiv 0 \mod n_1^2 n_2, \tag{4.6}$$

so using (4.5) and (4.6) it is easy to see that

$$(q-1)^4 \equiv 0 \mod n_1^2 n_2.$$

We can then write $(q-1)^4 = k n_1^2 n_2$, for some integer k. Now by adding $0 = (q-1)((q-1)^4 - k n_1^2 n_2)$ to (4.4) we get

$$(q-1)(n_1^2 n_2(-k+k_2+(1+q)k_1) + 5(q-1)^2) \equiv 0 \mod n_1^3 n_2^2, \tag{4.7}$$

which matches (4.3) that is what we were looking for. We can then continue in more or less the same way as in [DGS+13].

Take a prime ℓ dividing $n_1 n_2$. Let $r = v_\ell(n_1^2 n_2)$ and suppose for a contradiction that $v_\ell(5(q-1)^2) < r$. It is obvious that $v_\ell(n_1^2 n_2(-k+k_2+(1+q)k_1)) \geq r$ so

$$v_\ell((q-1)(n_1^2 n_2(-k+k_2+(1+q)k_1) + 5(q-1)^2)) = v_\ell(5(q-1)^3) < \frac{3}{2}r,$$

and using (4.7) we get that

$$3v_\ell(n_1) + 2v_\ell(n_2) < \frac{3}{2}(2v_\ell(n_1) + v_\ell(n_2)),$$

which gives that $v_\ell(n_2) < 0$ and contradict the fact that n_2 is an integer. □

This lemma allow us to reduce the power of q in the congruence of a_2 modulo $n_1^2 n_2$ in the following way:

$$a_2 \equiv 10 + 5q^3 \equiv (10 + 5q^3) + (-q - 2)5(q - 1)^2 \equiv 15q \mod n_1^2 n_2.$$

Now plugging this into Rybakov's equation (e) we obtain

$$5a_1 \equiv -a_2 - 15 \equiv -15(q + 1) \mod n_1^2 n_2.$$

The next step is to use this to write $5a_1$ explicitly. We write

$$5a_1 = -15(q + 1) + kn_1^2 n_2, \tag{4.8}$$

for some integer k.

Now we want to use bounds on a_1 and on N to limit what k can be. Haloui provides more precise bounds in [Hal10] but the following two lemmas are enough for this situation.

Lemma 4.0.32. *If* $f_A(T) = T^6 + a_1T^5 + a_2T^4 + a_3T^3 + a_4T^2 + a_5T + a_6$ *is a Weil polynomial then*

$$|a_1| \leq 6\sqrt{q}.$$

Proof. We know $f_A(T)$ is a monic polynomial whose roots are Weil numbers so we can write it as

$$f_A(T) = \prod_{i=1}^{6}(T - \beta_i) \text{ with } |\beta_i| = \sqrt{q} \text{ for all } i.$$

By expanding this we get that a_1 is the sum of 6 numbers with norm $\sqrt{q}$ and then triangle

inequality gives

$$|a_1| \leq 6\sqrt{q}.$$

□

Lemma 4.0.33. *If $f_A(T)$ is the characteristic polynomial of an Abelian variety of dimension 3 over a finite field $\mathbb{F}_q$, let $N = \#A(\mathbb{F}_q)$, then we have*

$$(\sqrt{q}-1)^6 \leq N \leq (\sqrt{q}+1)^6.$$

Proof. We know that f_A is a Weil polynomial, so we can write

$$f_A(T) = \prod_{i=1}^{6}(T-\beta_i) \text{ with } |\beta_i| = \sqrt{q} \text{ for all } i,$$

and then

$$N = f_A(1) = |f_A(1)| = \prod_{i=1}^{6}|T-\beta_i|. \tag{4.9}$$

Now for each i, $|\beta_i| = \sqrt{q}$, which implies that $1-\sqrt{q} \leq |1-\beta_i| \leq 1+\sqrt{q}$. Plugging this into (4.9) gives the result. □

By Lemma 4.0.32, $|5a_1| \leq 30\sqrt{q}$ and using (4.8), we get

$$-30\sqrt{q} \leq -15(q+1) + kn_1^2n_2 \leq 30\sqrt{q}.$$

Rearranging this we get

$$15(\sqrt{q}-1)^2 \leq kn_1^2n_2 \leq 15(\sqrt{q}+1)^2,$$

and combining this with the bound from Lemma 4.0.33,

$$15\frac{N^{1/3}}{n_1^2n_2}\left(\frac{\sqrt{q}-1}{\sqrt{q}+1}\right)^2 \leq k \leq 15\frac{N^{1/3}}{n_1^2n_2}\left(\frac{\sqrt{q}+1}{\sqrt{q}-1}\right)^2. \tag{4.10}$$

Note that as $q \to \infty$ the above inequality forces that $k \to 15\frac{N^{1/3}}{n_1^2 n_2}$, which can only happen if $15\frac{N^{1/3}}{n_1^2 n_2}$ is an integer. Assuming it is not an integer, the next question is how big does q need to be in order to squeeze k between two consecutive integers.

Let $m = 15\frac{N^{1/3}}{n_1^2 n_2}$. If $m - \delta < k < m + \delta$ then k belongs to an interval that contains no integer so we get a contradiction. We then using (4.10) have that one of the two following bound holds

$$m(1 + \delta/m) \leq k \leq m\left(\frac{\sqrt{q}+1}{\sqrt{q}-1}\right)^2$$
$$m\left(\frac{\sqrt{q}-1}{\sqrt{q}+1}\right)^2 \leq k \leq m(1 - \delta/m)$$

or equivalently

$$\sqrt{q} \leq \frac{1 + \sqrt{1-\delta/m}}{1 - \sqrt{1-\delta/m}}$$
$$\sqrt{q} \leq \frac{\sqrt{1+\delta/m}+1}{\sqrt{1-\delta/m}-1}.$$

Now combining those with Lemma 4.0.33, we get

$$N^{1/6} \leq \frac{1 + \sqrt{1-\delta/m}}{1 - \sqrt{1-\delta/m}} + 1 \tag{4.11}$$
$$N^{1/6} \leq \frac{\sqrt{1+\delta/m}+1}{\sqrt{1+\delta/m}-1} + 1. \tag{4.12}$$

So if (4.11) holds then since $1 - \sqrt{1-x} > x/2$ for all $x \in (0,1)$ we have

$$N^{1/6} \leq \frac{m}{2\delta}(1 + \sqrt{1-\delta/m}) + 1$$

and using the value of m this implies that

$$n_1^2 n_2 \leq \frac{15}{2\delta} N^{1/6}(1 + \sqrt{\delta/m}) + \frac{n_1^2 n_2}{N^{1/6}}.$$

Now $(1+\sqrt{\delta/m}) < 2$ and $\frac{n_1^2 n_2}{N^{1/6}} \leq n_1^2 n_2 \leq N^{1/6} < \frac{N^{1/6}}{\delta}$ so

$$n_1^2 n_2 < \frac{16}{\delta} N^{1/6},$$

and similarly if (4.12) holds then since $\sqrt{1+x} - 1 > x/3$ for all $x \in (0,1)$ we have

$$\begin{aligned} N^{1/6} &\leq \frac{m}{3\delta}(\sqrt{1+\delta/m}+1)+1 \\ &\leq \frac{15}{\delta}\frac{N^{1/3}}{n_1^2 n_2} + 1 \end{aligned}$$

and then

$$\begin{aligned} n_1^2 n_2 &\leq \frac{15}{\delta} N^{1/6} + \frac{n_1^2 n_2}{N^{1/6}} \\ &< \frac{4}{\delta} N^{1/6}. \end{aligned}$$

In both cases we have

$$n_1^2 n_2 < \frac{16}{\delta}(n_1^6 n_2^5 n_3^4 n_4^3 n_5^2 n_6)^{1/6},$$

which implies the result. □

This already gives an intuition that the group is not too "split" since n_1 and n_2 are small compared to the other n_i's. But we would like a formula that does not involve δ since we do not know how small it can be at first sight.

The following lemma will allow us to get a strict bound on δ so we can replace it in Proposition 4.0.30. It has been done more generally by Alex in his generalization to Abelian varieties of any dimension.

Lemma 4.0.34. *If x be a positive integer with $x^{1/3} \notin \mathbb{Z}$, then*

$$\|x^{1/3}\|_{\mathbb{R}/\mathbb{Z}} > \frac{1}{8x^{2/3}}.$$

Proof. First, we write

$$x = (\lfloor x^{1/3} \rfloor + \{x^{1/3}\})^3,$$

that we then expand and re-arrange to get

$$\{x^{1/3}\} = \frac{x - \lfloor x^{1/3} \rfloor^3}{3\lfloor x^{1/3} \rfloor^2 + 3\lfloor x^{1/3} \rfloor \{x^{1/3}\} + \{x^{1/3}\}^2}. \tag{4.13}$$

Now because, $x^{1/3} \notin \mathbb{Z}$, we have that $\lfloor x^{1/3} \rfloor^3 < x$ and since both sides are integers, we actually have that $\lfloor x^{1/3} \rfloor^3 + 1 \leq x$ so the numerator in the right hand side of (4.13) is at least 1. Now since $\{x^{1/3}\} < 1$, the denominator is less than $3\lfloor x^{1/3} \rfloor^2 + 3\lfloor x^{1/3} \rfloor + 1$, which gives

$$\{x^{1/3}\} > \frac{1}{(\lfloor x^{1/3} \rfloor + 1)^3 - \lfloor x^{1/3} \rfloor^3}. \tag{4.14}$$

Similarly, we can write

$$x = \Big(\big(\lfloor x^{1/3} \rfloor + 1 \big) - \big(1 + \{x^{1/3}\} \big) \Big)^3,$$

and the same process gives

$$1 - \{x^{1/3}\} > \frac{1}{(\lfloor x^{1/3} \rfloor + 1)^3 - \lfloor x^{1/3} \rfloor^3}. \tag{4.15}$$

Now combining (4.14) and (4.15) we obtain

$$\|x^{1/3}\| > \frac{1}{(\lfloor x^{1/3} \rfloor + 1)^3 - \lfloor x^{1/3} \rfloor^3}$$

and since $\lfloor x^{1/3} \rfloor + 1 < x^{1/3} + 1$ and $\lfloor x^{1/3} \rfloor > x^{1/3} - 1$, we have that

$$\begin{aligned} \|x^{1/3}\| &> \frac{1}{(x^{1/3} + 1)^3 - (x^{1/3} - 1)^3} \\ &= \frac{1}{2(3x^{2/3} + 1)} \\ &\geq \frac{1}{8x^{2/3}}, \end{aligned}$$

since $x \geq 1$. □

So this applied to $x = m^3$ and $\delta = \|x\|$ where m and δ are as before gives

$$\delta > \frac{1}{8m^2},$$

which together with Proposition 4.0.30 (Key Proposition) gives the following theorem that is an analogue of Theorem 1.1 in [DGS+13].

Theorem 4.0.35. *Suppose that*

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4n_5n_6\mathbb{Z}$$

is the group of points of an Abelian variety of dimension 3. If $15\frac{N^{1/3}}{n_1^2n_2} \notin \mathbb{Z}$, *then*

$$n_1 \leq 2800n_2^{7/6}n_3^{10/3}n_4^{5/2}n_5^{5/3}n_6^{5/6}.$$

We will see later that $15\frac{N^{1/3}}{n_1^2n_2}$ is equidistributed modulo one as a sequence on 5 variables. We then know that this number will usually not be an integer.

Now we would like to get a stronger bound but in a probabilistic sense. That is getting an analogue of Theorem 1.2 in [DGS+13].

The idea is to look at $m = f(n_2, n_3, n_4, n_5, n_6) = 15n_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}$ as a sequence of 5 variables and to show that this sequence is equidistributed modulo 1 to say that "most of the time" δ will not be too small.

Let

$$\mathcal{T}(N_2, N_3, N_4, N_5, N_6) = \{(n_2, n_3, n_4, n_5, n_6) : n_i \asymp N_i \text{ for all } i\}$$

and for $0 \leq \alpha < \beta \leq 1$, let

$$\begin{aligned} Z_f(N_2, N_3, N_4, N_5, N_6; \alpha, \beta) &= \{(n_2, n_3, n_4, n_5, n_6) \in \mathcal{T}(N_2, N_3, N_4, N_5, N_6) : \\ &\quad \alpha \leq \{f(n_2, n_3, n_4, n_5, n_6)\} \leq \beta\} \end{aligned}$$

where $\{f(n_2, n_3, n_4, n_5, n_6)\}$ denote the fractional part of $f(n_2, n_3, n_4, n_5, n_6)$. We say that the sequence $f(n_2, n_3, n_4, n_5, n_6)$ is equidistributed modulo one if

$$\lim_{N_2,N_3,N_4,N_5,N_6\to\infty} \frac{Z_f(N_2, N_3, N_4, N_5, N_6; \alpha, \beta)}{N_2N_3N_4N_5N_6} = \beta - \alpha.$$

Note that this limit is letting all the variable one by one go to infinity. The method that we will use actually gives this limit by only letting the product $N_2N_3N_5N_6$ of all the variables but N_4 go to infinity, which is indeed a stronger statement. But will see that we need to assume a small condition on the relative size of the variable. Our goal is then to show that for a region of the 5 dimensional plane as large as possible, we have that

$$\lim_{N_2N_3N_5N_6\to\infty} \frac{Z_f(N_2, N_3, N_4, N_5, N_6; \alpha, \beta)}{N_2N_3N_4N_5N_6} = \beta - \alpha. \tag{4.16}$$

For a single variable sequence $f(n)$, it is well known (Weyl's criterion) that equiditribution modulo one in equivalent to

$$\sum_{n\asymp N} e(kf(n)) = o(N) \tag{4.17}$$

for each integer $k \neq 0$. The same can be done to prove the equidistribution of a multivariable sequence. The next theorem is explained in Chapter 1 of [Mon94] for a sequence of one variable and an analogue of this for three variables has been done in [DGS+13] (Theorem 5.1) and in fact their proof can easily be extended to any number of variables. We will state it for our case which is five variables.

Theorem 4.0.36. *Let $f(n_2, n_3, n_4, n_5, n_6)$ be a sequence of real numbers, and let $0 \leq \alpha \leq \beta \leq 1$ then*

$$\left|\#Z_f(N_2, N_3, N_4, N_5, N_6; \alpha, \beta) - (\beta - \alpha)\#\mathcal{T}(N_2, N_3, N_4, N_5, N_6)\right|$$

$$\leq \frac{\#\mathcal{T}(N_2, N_3, N_4, N_5, N_6)}{K+1} + 2\sum_{k=1}^{K} \left(\frac{1}{K+1} + \min\left(\beta - \alpha, \frac{1}{\pi k}\right)\right) |E_k(N_2, N_3, N_4, N_5, N_6)|$$

for any positive integers N_2, N_3, N_4, N_5, N_6 and K.

Proof. For each positive integer K, let

$$S_K^+(n) = \sum_{-K \le k \le K} \hat{S}_K^+(k) e(kn)$$

be the Selberg polynomial upper bounding $\chi_{[\alpha,\beta]}$ the characteristic function of $[\alpha, \beta]$ as defined in [Mon94] and its Fourier transform $\hat{S}_K^+$. Then

$$\begin{aligned} Z_f(N_2, N_3, N_4, N_5, N_6; \alpha, \beta) &= \sum_{n_i \asymp N_i} \chi_{[\alpha,\beta]}(f(n_2, n_3, n_4, n_5, n_6)) \\ &\le \sum_{n_i \asymp N_i} S_K^+(f(n_2, n_3, n_4, n_5, n_6)) \\ &= \sum_{-K \le k \le K} \hat{S}_K^+(k) \sum_{n_i \asymp N_i} e(kf(n_2, n_3, n_4, n_5, n_6)) \\ &= \sum_{-K \le k \le K} \hat{S}_K^+(k) E_k(N_2, N_3, N_4, N_5, N_6). \end{aligned}$$

Now we know that

$$\hat{S}_K^+(0) = \beta - \alpha + \frac{1}{K+1}$$

and

$$E_0(N_2, N_3, N_4, N_5, N_6) = \#\mathcal{T}(N_2, N_3, N_4, N_5, N_6),$$

so we have

$$\begin{aligned} Z_f(N_2, N_3, N_4, N_5, N_6; \alpha, \beta) - (\beta - \alpha)\#\mathcal{T}(N_2, N_3, N_4, N_5, N_6) \le \\ \frac{\#\mathcal{T}(N_2, N_3, N_4, N_5, N_6)}{K+1} + \sum_{1 \le |k| \le K} \hat{S}_K^+(k) E_k(N_2, N_3, N_4, N_5, N_6). \end{aligned}$$

It follows by properties of Selberg polynomials (upper or lower) that for $1 \le |k| \le K$ we have

$$\left| \hat{S}_K(k) \right| \le \frac{1}{K+1} + \min\left(\beta - \alpha, \frac{1}{\pi |k|}\right),$$

which implies that

$$Z_f(N_2,N_3,N_4,N_5,N_6;\alpha,\beta)-(\beta-\alpha)\#\mathcal{T}(N_2,N_3,N_4,N_5,N_6)\leq \\ \frac{\#\mathcal{T}(N_2,N_3,N_4,N_5,N_6)}{K+1}+ \\ 2\sum_{1\leq k\leq K}\left(\frac{1}{K+1}+\min\left(\beta-\alpha,\frac{1}{\pi\left|k\right|}\right)\right)\left|E_k(N_2,N_3,N_4,N_5,N_6)\right|.$$

Now using S_K^- the Selberg polynomial lower bounding the characteristic function of $[\alpha,\beta]$, we get that

$$Z_f(N_2,N_3,N_4,N_5,N_6;\alpha,\beta)\geq\sum_{-K\leq k\leq K}\hat{S}_K^-(k)E_k(N_2,N_3,N_4,N_5,N_6),$$

and this time we have

$$\hat{S_K^-}(0)=\beta-\alpha-\frac{1}{K+1},$$

which gives

$$Z_f(N_2,N_3,N_4,N_5,N_6;\alpha,\beta)-(\beta-\alpha)\#\mathcal{T}(N_2,N_3,N_4,N_5,N_6)\geq \\ -\frac{\#\mathcal{T}(N_2,N_3,N_4,N_5,N_6)}{K+1}+\sum_{1\leq|k|\leq K}\hat{S}_K^-(k)E_k(N_2,N_3,N_4,N_5,N_6).$$

The other inequality follows similarly. □

Corollary 4.0.37. (Weyl's criterion for five variables) *Let $f(n_2,n_3,n_4,n_5,n_6)$ be a sequence of real numbers, and let $0\leq\alpha\leq\beta\leq 1$.If for each integer $k\neq 0$ we have that*

$$E_k(N_2,N_3,N_4,N_5,N_6)=o(N_2N_3N_4N_5N_6)\ \text{as}\ P\to\infty,$$

where $P=P(N_2,N_3,N_4,N_5,N_6)$, then

$$\lim_{P\to\infty}\frac{Z_f(N_2,N_3,N_4,N_5,N_6;\alpha,\beta)}{N_2N_3N_4N_5N_6}=\beta-\alpha.$$

Proof. Dividing the inequality of Theorem 4.0.36 by $N_2N_3N_4N_5N_6$, we get that for any

positive integer K,

$$\left|\frac{Z_f(N_2,N_3,N_4,N_5,N_6;\alpha,\beta)}{N_2N_3N_4N_5N_6}-(\beta-\alpha)\right|$$

$$\leq \frac{1}{K+1}+2\sum_{k=1}^{K}\left(\frac{1}{K+1}+\min\left(\beta-\alpha,\frac{1}{\pi k}\right)\right)\frac{|E_k(N_2,N_3,N_4,N_5,N_6)|}{N_2N_3N_4N_5N_6}. \tag{4.18}$$

Note that

$$\left(\frac{1}{K+1}+\min\left(\beta-\alpha,\frac{1}{\pi k}\right)\right)\leq 1,$$

so the sum in (4.18) is bounded by

$$K\frac{|E_k(N_2,N_3,N_4,N_5,N_6)|}{N_2N_3N_4N_5N_6}.$$

Thus if $E_k(N_2,N_3,N_4,N_5,N_6)=o(N_2N_3N_4N_5N_6)$ as $P\to\infty$, then there exist a function $g=g(N_2,N_3,N_4,N_5,N_6)$ such that

$$g\to\infty \text{ as } P\to\infty,$$

but

$$g\frac{|E_k(N_2,N_3,N_4,N_5,N_6)|}{N_2N_3N_4N_5N_6}\to \text{ as } P\to\infty.$$

Take $K=\lceil g\rceil$ then all the terms in (4.18) vanish as $P\to\infty$, which implies the result. □

In Chapter 3, we considered the sequence $f(n_2,n_3,n_4,n_5,n_6)=15n_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}$ and showed the following.

Proposition 4.0.38. *Suppose that*

$$\log N_4\ll(N_2N_3N_5N_6)^{1/100}, \tag{4.19}$$

then for all non zero integer k,

$$E_k=o(N_2N_3N_4N_5N_6) \text{ as } N_2N_3N_5N_6\to\infty.$$

From now we will assume that (4.19) holds. By Corollary 4.0.37 and the Proposition 4.0.38, we have

$$\lim_{N_2N_3N_5N_6\to\infty} \frac{Z_f(N_2,N_3,N_4,N_5,N_6;\alpha,\beta)}{N_2N_3N_4N_5N_6} = \beta - \alpha \tag{4.20}$$

This allows us to prove the following theorem, which is an analogue of Theorem 1.2 in [DGS+13].

Theorem 4.0.39. *Suppose that*

$$\log N_4 \ll (N_2N_3N_5N_6)^{1/100}.$$

If

$$\frac{N_1N_2^{1/6}}{N_3^{2/3}N_4^{1/2}N_5^{1/3}N_6^{1/6}} \to \infty$$

as $N_2N_3N_5N_6 \to \infty$*, then*

$$\#S(N_1,N_2,N_3,N_4,N_5,N_6) = o(N_1N_2N_3N_4N_5N_6)$$

as $N_2N_3N_5N_6 \to \infty$*.*

Proof. Let $F = F(N_2,N_3,N_4,N_5,N_6)$ be a function that tends to infinity with $N_2N_3N_5N_6$ and satisfying the bound

$$F \le \frac{N_1N_2^{1/6}}{52N_3^{2/3}N_4^{1/2}N_5^{1/3}N_6^{1/6}}.$$

Without loss of generality, we may assume that $N_2N_3N_5N_6$ is large enough so that $F \ge 1$. Hence we may write

$$\#S = \#S_1 + \#S_2$$

where

$$S_1 := \{(n_1,n_2,n_3,n_4,n_5,n_6) \in S : \|3n_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}\| \le 1/F\}$$

$$S_2 := \{(n_1,n_2,n_3,n_4,n_5,n_6) \in S : \|3n_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}\| > 1/F\}.$$

It follows from (4.20) that $\#S_1 = o(N_1N_2N_3N_4N_5N_6)$ as $N_2N_3N_5N_6 \to \infty$ and if

$(n_1, n_2, n_3, n_4, n_5, n_6) \in S_2$ then $15n_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}$ cannot be an integer so by the Key Proposition

$$\begin{aligned} N_1 \leq n_1 &< \frac{16n_3^{2/3}n_4^{1/2}n_5^{1/3}n_6^{1/6}}{\|3n_2^{2/3}n_3^{4/3}n_4n_5^{2/3}n_6^{1/3}\|n_2^{1/6}} \\ &\leq \frac{16(2N_3)^{2/3}(2N_4)^{1/2}(2N_5)^{1/3}(2N_6)^{1/6}}{(1/F)N_2^{1/6}} \\ &< 52F\frac{N_3^{2/3}N_4^{1/2}N_5^{1/3}N_6^{1/6}}{N_2^{1/6}} \end{aligned}$$

which contradicts the choice of F. We then conclude that S_2 is empty and therefore $S = o(N_1N_2N_3N_4N_5N_6)$ as $N_2N_3N_5N_6 \to \infty$. □

Bibliography

[Apo76] Tom M Apostol. *Introduction to analytic number theory*, volume 1. Springer, 1976.

[BPS12] William D Banks, Francesco Pappalardi, and Igor E Shparlinski. On group structures realized by elliptic curves over arbitrary finite fields. *Experimental Mathematics*, 21(1):11–25, 2012.

[CDKS12] Vorrapan Chandee, Chantal David, Dimitris Koukoulopoulos, and Ethan Smith. Group structures of elliptic curves over finite fields. *arXiv preprint arXiv:1210.3880*, 2012.

[DGS+13] Chantal David, Derek Garton, Zachary Scherr, Arul Shankar, Ethan Smith, and Lola Thompson. Abelian surfaces over finite fields with prescribed groups. *arXiv preprint arXiv:1307.0863*, 2013.

[FI89] Étienne Fouvry and Henryk Iwaniec. Exponential sums with monomials. *Journal of Number Theory*, 33(3):311–333, 1989.

[GKK91] Sidney W Graham, Grigori Kolesnik, and G Kolesnik. *Van der Corput's method of exponential sums*, volume 126. Cambridge University Press, 1991.

[Hal10] Safia Haloui. The characteristic polynomials of abelian varieties of dimensions 3 over finite fields. *Journal of Number Theory*, 130(12):2745–2752, 2010.

[Hel95] H. Helson. *Harmonic Analysis*. Texts and readings in mathematics. Hindustan Book Agency, 1995.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic Number Theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Krä89] Ekkehard Krätzel. *Lattice points*, volume 33. Springer, 1989.

[Mon94] Hugh L Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84. American Mathematical Soc., 1994.

[RS02] O Robert and P Sargos. A fourth derivative test for exponential sums. *Compositio Mathematica*, 130(3):275–292, 2002.

[Ryb10] Sergey Rybakov. The groups of points on abelian varieties over finite fields. *Central European Journal of Mathematics*, 8(2):282–288, 2010.

[Sar00] Patrick Sargos. Un critère de la dérivée cinquième pour les sommes d'exponentielles. *Bulletin of the London Mathematical Society*, 32(4):398–402, 2000.

[Sil92] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[SS11] Elias M Stein and Rami Shakarchi. *Functional analysis: Introduction to further topics in analysis*, volume 4. Princeton University Press, 2011.

[Ten95] Gérald Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory*, volume 46 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas.