Adam Mickiewicz University, Poznań
Faculty of Mathematics and Computer Science

Rafał Bystrzycki

Applications of additive combinatorics methods to some multiplicative problems

Zastosowania metod kombinatoryki addytywnej do wybranych zagadnień multiplikatywnych

PhD dissertation
in the Mathematical Sciences
in the area of Mathematics

Rozprawa doktorska
w dziedzinie Nauk Matematycznych
w zakresie Matematyki

Supervisor:
prof. dr hab. Tomasz Schoen
Discrete Mathematics Department

2019

Abstract

The main aim of this dissertation is the study of different ways in which additive combinatorics may be used to tackle some problems arising in multiplicative number theory. Specific problems studied here concern computational complexity of calculating values of number-theoretic functions, sums of dilates and exponential sums.

The main part of the thesis deals with the following problem: Suppose that for some natural number n and some prime number p we are given the set of residues mod p of all its divisors and we would like to know which of those residues correspond to prime factors of n. An algorithm which approximately solves this problem for p and n satisfying some natural conditions is presented and it is proved that there are plenty of such numbers. One interesting feature of the proof is that it relies on additive combinatorics. The proposed algorithm consists of two algorithms, which performed one after another lead to the solution. Failure of the first part implies the structural properties captured by the notion of additive energy of the set which are then used by the second, more intricate part based on techniques from Fourier analysis.

The main theorem of this part states that for a squarefree integer n satisfying some constraints and a prime number p satisfying some other technical conditions if we are given the set of residues modulo p of all divisors of n (denoted A_p), there exists an efficient deterministic algorithm which finds a set B such that $\Gamma_p \subset B \subset A_p$ (where Γ_p denote the set of residues of prime divisors of n) and $|B| < \epsilon |A_p|$.

All conditions appearing in the assumptions are very weak and in fact occur for almost every squarefree number n and for enough primes p in order to be practical. In this way, we show that for all but $o(x)$ squarefree numbers less than x and a suitable p (dependent only on x, not on n), the set B from theorem can be found. We also give an application of this result to the algorithm which finds factorization of a given number using an oracle for values of functions $\sigma_k(n)$. In fact, the search for deterministic reductions of factorization to some other number-theoretic problems was our original motivation to study this problem.

In the next part of the thesis the problem concerning exponential sums is studied. More specifically the following expression

$$s(a/q) = \sum_{r=1}^{\tau} e\left(\frac{a2^r}{q}\right),$$

where $e(x) := \exp(2\pi i x)$ and τ is multiplicative order of an element corresponding to number 2, is considered. Absolute value of this sum is estimated. The results we obtained in this line of research are the following. We give an upperbound with a better constant than previously known ([15]) and provide some new examples where this bound is close to being tight.

In the last part of the thesis bounds for the size of sums of dilates are considered. Sums of dilates are sets of the form

$$\lambda_1 \cdot A + \cdots + \lambda_h \cdot A,$$

where for any scalar λ and any sets of integers A, B we take the notation $\lambda \cdot A = \{\lambda a : a \in A\}$ and $A + B = \{a + b : a \in A, b \in B\}$. Series of results giving upper-bounds on the size of this set is proved under the small doubling condition, namely A satisfies $|A + A| < K|A|$ for some constant K.

The most general bound obtained here has the form $K^{O\left(\frac{rh}{\log(h)} + h\log(h)\right)}|A|$, where r denotes the maximal number of bits of coefficients and h is the number of summands. It consists an improvement over the result from [6].

Our next theorem applies to the case when K is much smaller than h. It shows that then the dependence on h becomes polynomial under those assumptions. Hence it improves on a previous theorem in such circumstances.

Our last theorem considers the case when Λ - the set of λ_i coefficients - has some additive structure. In such a setting a spectacular improvement is possible. If we denote by L the doubling constant of Λ, then the bound takes the form $K^{O((h+r)L\log L)}|A|$.

Głównym celem pracy jest badanie różnych sposobów, w jakie kombinatoryka addytywna może być wykorzystana do radzenia sobie z pewnymi zagadnieniami pojawiającymi się w multiplikatywnej teorii liczb. Konkretne problemy badane przez nas dotyczą złożoności obliczeniowej obliczania wartości funkcji teorioliczbowych, sum dylatacji i sum eksponencjalnych.

Najważniejsza część pracy dotyczy następującego problemu: Przypuśćmy, że dla pewnej liczby naturalnej n i pewnej liczby pierwszej p jest nam dany zbiór reszt modulo p wszystkich dzielników liczby n i chcielibyśmy stwierdzić, które z nich odpowiadają jej czynnikom pierwszym. Przedstawiony jest algorytm rozwiązujący ten problem dla p i n spełniających pewne naturalne warunki i zostaje pokazane, że jest wiele takich liczb. Interesującą cechą przedstawionego dowodu jest to, że wymaga on użycia kombinatoryki addytywnej. Proponowany algorytm składa się z dwóch algorytmów, które wykonane jedna po drugiej prowadzą do rozwiązania. Niepowodzenie pierwszego z nich wskazuje na istnienie strukturalnych własności zbioru przekładających się na jego energię addytywną, które mogą być następnie wykorzystane w drugiej bardziej skomplikowanej części algorytmu opartej na technikach analizy fourierowskiej.

Główne twierdzenie w tej części mówi, że dla bezkwadratowej liczby całkowitej n spełniającej pewne ograniczenia i liczby pierwszej spełniającej pewne inne techniczne warunki jeśli znamy zbiór reszt modulo p wszystkich dzielników n (oznaczamy ten zbiór A_p), to istnieje efektywny deterministyczny algorytm zwracający zbiór B taki, że $\Gamma_p \subset B \subset A_p$ (gdzie Γ_p oznacza zbiór reszt modulo p czynników pierwszych liczby n) oraz $|B| < \epsilon|A_p|$

Wszystkie warunki pojawiające się w założeniach twierdzenia są bardzo słabe i zachodzą dla prawie każdej liczby bezkwadratowej n oraz wystarczająco wielu liczb pierwszych p, aby możliwe było jego praktyczne zastosowanie. Pokazujemy również zastosowanie tego wyniku do algorytmu, który znajduje rozkład na czynniki danej liczby przy użyciu wyroczni na wartości funkcji $\sigma_k(n)$. Właśnie poszukiwanie deterministycznych redukcji faktoryzacji do innych problemów teorioliczbowych stanowiło oryginalną motywację do badania tego zagadnienia.

W kolejnej części pracy badany jest problem dotyczący sum eksponencjalnych. Dokładniej, następujące wyrażenie

$$s(a/q) = \sum_{r=1}^{\tau} e(\frac{a2^r}{q}),$$

gdzie $e(x) := \exp(2\pi i x)$ i τ jest multiplikatywnym rzędem elementu grupy odpowiadającego liczbie 2, jest rozważane. Oszacowana jest jego wartość bezwzględna. Wynik osiągnięty przez

nas w tej kwestii jest następujący. Podajemy górne oszacowanie z lepszą stałą niż dotychczas znana ([15]) oraz dostarczamy nowych przykładów sytuacji, w których oszacowanie jest bliskie realizacji.

W ostatniej części pracy rozważane są oszacowania na wielkość zbioru sum dylatacji. Zbiory sum dylatacji to zbiory postaci

$$\lambda_1 \cdot A + \cdots + \lambda_h \cdot A,$$

gdzie dla dowolnego skalara λ i dowolnych zbiorów liczb całkowitych A, B przyjmujemy notację $\lambda \cdot A = \{\lambda a : a \in A\}$ oraz $A+B = \{a+b : a \in A, b \in B\}$. Seria wyników dających oszacowania górne wielkości tego zbioru jest udowodniona przy założeniu małego podwojenia, czyli dla A spełniającego $|A + A| < K|A|$ dla pewnej stałej K.

Najogólniejsze oszacowanie osiągnięte przez nas jest postaci $K^{O\left(\frac{rh}{\log(h)} + h\log(h)\right)}|A|$, gdzie r oznacza maksymalną liczbę bitów w zapisie współczynników λ_i, natomiast h jest liczbą sumowanych składników. Ten wynik stanowi wzmocnienie wyniku z [6].

Nasze następne twierdzenie stosuje się do przypadku, gdy K jest znacznie mniejsze niż h. Pokazuje ono, że zależność od h staje się przy takich założeniach wielomianowa. Stanowi wzmocnienie poprzedniego twierdzenia w takich wypadkach.

Ostatnie twierdzenie dotyczy sytuacji gdy Λ - zbiór współczynników λ_i - ma pewną strukturę addytywną. W tym wypadku spektakularne wzmocnienie oszacowania jest możliwe. Jeśli oznaczymy przez L stałą podwojenia zbioru Λ, to oszacowanie to przyjmuje wygodną postać $K^{O((h+r)L\log L)}|A|$.

Contents

Introduction

Additive combinatorics is concerned with subsets of integers or other commutative groups and their behavior under addition. More precisely, it studies sumsets.

Definition 0.0.1. *For two subsets A and B of an abelian group the set*

$$A + B := \{a + b : a \in A, b \in B\}$$

is called the sumset.

In particular, we can take the second set to be $-B$ and then the set

$$A - B := \{a - b : a \in A, b \in B\}$$

is called the difference set.

Both notions are often studied in the special case when $A = B$.In this case, the notion of a doubling constant is introduced.

Definition 0.0.2. *For the subset A of an abelian group the value $K = \frac{|A+A|}{|A|}$ is called the doubling constant of A.*

Doubling constant can be viewed as the simplest measure of an additive structure of a given set. The sets with small doubling constant, i.e. bounded by some constant independent of size of A, are seen as additively structured. Properties of those sets are extensively studied in additive combinatorics.

Operation of taking sumset (or difference set) of sets can be iterated. In such situations, it is often convenient to use the following abbreviation.

Definition 0.0.3. *For the subset A of an abelian group the set*

$$hA := \underbrace{A + \ldots + A}_{h \text{ times}}$$

is called the h-fold sumset of the set A.

It should not be confused with a simpler object that is also studied in this dissertation which is defined below.

Definition 0.0.4. *For the subset A of an abelian group G and a scalar $\lambda \in G$ the set*

$$\lambda \cdot A = \{\lambda \cdot a : a \in A\}$$

is called the dilate of A by λ.

Sometimes, it is useful to restrict ones to attention to the sums of different elements. In the extreme case it leads to the set of all subset sums.

Definition 0.0.5. *Let A be a subset of an abelian group. Then $\mathcal{P}(A)$ denotes the set of all subset sums of A, namely*

$$\mathcal{P}(A) := \{\sum_{a\in T} a : T \subset A\}.$$

A different way to measure additive structure of a set is by its additive energy.

Definition 0.0.6. *Let G be an abelian group and $A \subset G$ a finite subset. The energy of A is defined by*

$$E(A) = |\{(a_1, a_2, a_3, a_4) \in A^4 : a_1 - a_2 = a_3 - a_4\}|.$$

We can think of a set with large additive energy as being in a sense structural. One can also consider more general energy between two sets.

Definition 0.0.7. *Let G be an abelian group and $A, B \subset G$ finite subsets. The energy between A and B is defined by*

$$E(A, B) = |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : a_1 - b_1 = a_2 - b_2\}|.$$

Additive energies can be expressed by cardinalities of intersections of A and translates of B in a way given by the next lemma (Lemma 2.9 from [30]).

Lemma 0.0.8. *Let A, B be subsets of an abelian group G. Then we have the identities*

$$\begin{aligned} E(A,B) &= \sum_{x\in A+B} |A \cup (\{x\} - B)|^2 = \sum_{y\in A-B} |A \cup (B + \{y\})|^2 = \\ &= \sum_{x\in (A-A)\cup(B-B)} |A \cup (\{z\} + A)||B \cup (\{z\} + B)|. \end{aligned} \tag{1}$$

The proof is based on the fact that intersections $|A \cup (\{x\} - B)|$ and $|A \cup (B + \{y\})|$ count the number of solutions of equation $a + b = x$ and $a - b = y$ respectively (where $a \in A, b \in B$ and x, y are given). The following fact can be deduced using Cauchy-Szwarz inequality (Corollary 2.10 from [30]).

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

The relation between additive energy and doubling is described by a very important result first proved by Balog and Szemerédi (with exponential dependence on K). First version with polynomial dependence on K was provided by Gowers. We quote the version with currently the best known dependence on K.

Theorem 0.0.9 (Balog-Szemerédi-Gowers, [27])**.** *Let be a subset of an abelian group such that $E(A) = \frac{1}{K}|A|^3$. Then there exists $A' \subset A$ such that $|A'| = \Omega(\frac{1}{K}|A|)$ and*

$$|A' - A'| = O(K^4|A'|).$$

In finite abelian groups, it is convenient to use the notion of a Fourier transform to examine additive properties of sets. In this setting it is convenient to use the following notion.

Definition 0.0.10. *Characteristic function of a set A is the function that takes the value 1 for elements of A and value 0 otherwise. It is usually denoted by $A(x)$ or $1_A(x)$.*

Definition 0.0.11. *Discrete Fourier transform (with size p) of a function $f : \mathbb{F}_p \to \mathbb{C}$ is a function*

$$\hat{f}(\gamma) = \sum_{x \in \mathbb{F}_p} f(x) e^{\frac{2\pi i}{p} x\gamma}.$$

Discrete Fourier transform enjoys the following nice property.

Lemma 0.0.12 (Parseval identity)**.**

$$\sum_{x \in \mathbb{F}_p} |f(x)|^2 = \frac{1}{p} \sum_{x \in \mathbb{F}_p} |\hat{f}(x)|^2.$$

This fact is particularly useful when applied to the characteristic function of the set $A \subset \mathbb{F}_p$.

Corollary 0.0.13.

$$\sum_{x \in \mathbb{F}_p} |\hat{A}(x)|^2 = p|A|. \tag{3}$$

Mostly the case when f is a characteristic function $A(x)$ of some subset A of $\mathbb{F}_p$ is studied. If the set A has some large nontrivial Fourier coefficients $|\hat{A}(\xi)|$ (for $\xi \neq 0$) it is considered to be additively structured. To see the link between Fourier transform and additive energy, note that the following identity holds (see for example [30]):

$$E(A) = \frac{1}{p} \sum_{\xi} |\hat{A}(\xi)|^4.$$

This approach generalizes so that Fourier transforms can be used to count the number of solutions of any linear equation in $\mathbb{F}_p$.

One classical theorem that we are going to repeatedly use is Plünnecke inequality.

Proposition 0.0.14 (Plünnecke inequality, [21])**.** *If $|A+A| \leq K|A|$ or $|A-A| \leq K|A|$, then*

$$|mA - nA| \leq K^{m+n}|A| \tag{4}$$

for all non-negative integers m, n.

It tells us that control over the size sumset or difference set leads to some control over the size of iterated sumsets.

Another way of describing additive properties of a set is by covering it with a more structured set. Typical examples of sets that are considered structured are arithmetic progressions and its generalization.

Definition 0.0.15. *Let $M = (m_1, \ldots, m_d)$ and $N = (n_1, \ldots, n_d)$ be elements of $\mathbb{Z}^d$ such that $m_j \leq n_j$ for every j. Then the discrete box is a set of the form*

$$[M, N] := \{(x_1, \ldots, x_d) \in \mathbb{Z}^d : m_j \leq x_j \leq n_j \text{ for all } 1 \leq j \leq d\}$$

Let G be an abelian group and d be a positive integer. Generalized arithmetic progression of rank d is a set of the form

$$P = g + v \cdot [M, N],$$

where $a \in G$, $v \in G^d$ and $[M, N]$ is a discrete box.

It should be noted that the same set can be represented as an arithmetic progression in many ways, but we will only consider arithmetic progressions with g, v, M, N explicitly given. Low-rank arithmetic progression are usually considered the most structured. However, in some situations the other extreme case given by the following definition turns out to be useful.

Definition 0.0.16. *For a subset $T = \{t_1, \dots, t_{|T|}\}$ of an abelian group G the set $Span(T) = (t_1, \dots, t_{|T|})\{-1, 1\}^{|T|}$ is called a span of T.*

The set $\mathcal{P}(A)$ can also be seen as an arithmetic progression with $[M, N] = \{0, 1\}^{|A|}$.

Sumsets and iterated sumsets are often more structured than the original set. That is why they are also sometimes treated as structured. One well-known example of a covering result is the following lemma.

Lemma 0.0.17 (Ruzsa covering lemma, [24])**.** *For any non-empty sets A, B in an abelian group G one can cover B by $\frac{|A+B|}{|A|}$ translates of $A - A$.*

Chapter 1

Application to the hardness of computing values of number-theoretic functions

In this chapter we deal with the following problem: Suppose that for some natural number n and some prime number p we are given the set of residues mod p of all its divisors and we would like to know which of those residues correspond to prime factors of n. It is based on the paper [9] For convenience we introduce the following notation:

Notation 1.0.1. *A would stand for the set of all divisors of n. A_p would stand for the set of residues mod p of elements of A. Similarly, Γ would stand for the set of prime factors of n and Γ_p would stand for the set of residues mod p of elements of Γ. Also, $\mathbb{Z}_p$ stands for $\mathbb{Z}/p\mathbb{Z}$.*

Ideally, we would like to find Γ_p, but we were unable to achieve that goal. Moreover, it seems to be impossible to get in general with an algorithm using only the information on residues mod p (see Section 1.6). Therefore, we focus on a simpler but still useful task of finding B, a small subset of A_p containing Γ_p. For our application (see Section 1.5) it turns out to be good enough. We firmly believe that possibly some more applications of this approach could be found in the future. In the sequel, we are going to provide two algorithms ($B_{rand}(A_p)$ and $B_{struct}(A_p)$) to find such a set B. For brevity, we will denote resulting sets obtained from A with those algorithms by B_{rand} and B_{struct} respectively.

Before we formulate our main theorem, let us provide some definitions which are essential to fully explain its meaning and the idea behind its proof. First, let us recall some basic number-theoretic functions. We will need them to express properties of numbers which make our argument to work.

Definition 1.0.2. *$\omega(n)$ denotes the number of prime divisors of a number n.*

Definition 1.0.3. *$P(m)$ denotes the greatest prime divisor of an integer m.*

Another important number-theoretic functions are $\sigma_k(n)$

Definition 1.0.4.

$$\sigma_k(n) = \sum_{d|n} d^k.$$

The problem we look at arise naturally when studying the deterministic reduction of factorization to computing the values of $\sigma_k(n)$. We detail this application in Section 1.5.

We are going to present an algorithm which is deterministic, but works only for some inputs. We next show that for a randomly chosen input the algorithm is almost certain to work properly. To formalize this statement we will need the notion of natural density.

Definition 1.0.5. *Natural density of a set X of integers is the following limit (if it exists)*

$$\lim_{n\to\infty} \frac{\#\{m \in \mathbb{N} : m < n, m \in X\}}{n} \tag{1.1}$$

It turns out that the right way of looking at the problem we consider is actually by looking at numbers as elements of a cyclic group $\mathbb{Z}_p^*$. It leads us to consider the set of subset sums (see Definition 0.0.5).

After taking logarithms of elements of the set of all divisors of a given number we get the structure defined above with C being the set of prime factors.

Now we are ready to state our result. The main theorem of this chapter is

Theorem 1.0.6. *For a given x and $\epsilon, \epsilon' > 0$ let $p = \log x^{3+o(1)}$ be a prime such that $p^{0.5-\epsilon'} < P(p-1) < p^{0.5+\epsilon'}$ and $P(p-1)^2 \nmid (p-1)$ and let $n \leq x$ be a squarefree integer such that $\omega(n) \leq 2\log\log n$, n has at most $\log\log x^{1+o(1)}$ divisors less than p, no pair of distinct divisors of n is congruent modulo p and the number of its divisors $d > p$ for which $d^{\frac{p-1}{P(p-1)}}$ is congruent to $q^{\frac{p-1}{P(p-1)}}$ or $-q^{\frac{p-1}{P(p-1)}}$ for some prime divisor q is less then $\frac{1}{2}\epsilon 2^{\omega(n)}$. Let A (and A_p) denote the set of divisors of n (and their residues modulo p) and let Γ (and Γ_p) denote the set of prime divisors of n (and their residues modulo p). Then there exists a deterministic algorithm with running time $O_\epsilon(p^{0.5+\epsilon'+o(1)}) = O((\log x)^{1.5+\epsilon'+o(1)})$ which finds a set B such that $\Gamma_p \subset B \subset A_p$ and $|B| < \epsilon|A_p|$.*

Close inspection of the proof shows that one can take ϵ to be as small as $\Theta((\log\log x)^{-\frac{1}{12}})$.

Although the statement is a bit technical, we are going to show that all conditions appearing in the assumptions are very weak and in fact occur for almost every squarefree number n and for enough primes p in order to be practical. The most interesting novelty in the proof is the heavy use of additive combinatorics in a problem arising from multiplicative number theory. We also give an application of this result to the algorithm which finds factorization of a given number using an oracle for values of functions $\sigma_k(n)$. In fact, the search for deterministic reductions of factorization to some other number-theoretic problems was our original motivation to study this problem.

1.1. Preliminaries

Let us briefly recall some results from computational number theory, group theory and Fourier analysis. Reader may as well skip this part if he's familiar with those concepts. Concepts from additive combinatorics and analytic number theory are introduced in sections 3 and 4 respectively, where they are used.

Lemma 1.1.1. *Addition (or subtraction) of two numbers on at most n bits can be performed with $O(n)$ bit operations.*

Theorem 1.1.2 (Schönhage - Strassen, [28])**.** *Multiplication of two numbers on at most k bits can be performed with $O(k\log k\log\log k)$ bit operations. In particular it is $O(k^{1+o(1)})$.*

Corollary 1.1.3. *Division (with the remainder) of the number N on at most k bits by the number D on at most k bits can be performed with $O(k(\log k)^2\log\log k)$ bit operations (in particular it is $O(k^{1+o(1)})$).*

Lemma 1.1.4. *Values of a polynomial of degree k at a given point can be found with k multiplications and k additions using Horner scheme.*

Lemma 1.1.5. *Greatest common divisor of polynomials $f, g \in \mathbb{F}_p[X]$ can be found with Euclid algorithm with $O(deg(f)deg(g))$ operations in $\mathbb{F}_p$.*

Lemma 1.1.6. *Exponentiation modulo p to the exponent k can be performed with $O(\log k)$ operations in $\mathbb{F}_p$.*

We recall some basic facts about the structure of $\mathbb{Z}_p^*$. The previous lemma implies that the homomorphism mentioned below can be computed efficiently.

Lemma 1.1.7. *If $p-1 = q_1^{e_1} \cdots q_k^{e_k}$ is a prime powers factorization, then*

$$\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1} \simeq \mathbb{Z}_{q_1^{e_1}} \times \cdots \times \mathbb{Z}_{q_k^{e_k}}.$$

For every $q|(p-1)$

$$a \mapsto a^{\frac{p-1}{q}}$$

is a group homomorphism $\mathbb{Z}_{p-1} \to \mathbb{Z}_q$.

In order to work with the additive notation we will need to take discrete logarithms. It should be stressed that for clarity of discussion in the analysis of the algorithm we consider logarithms starting from early stages of algorithm, before we actually compute them.

Definition 1.1.8. *Let $b, g \in \mathbb{F}_p$. Discrete logarithm of g to the base b is the residue class mod $ord(b)$ of the smallest positive integer k such that $b^k = g$. We denote it with $\log_b(g)$.*

Although the best known algorithms for computing discrete logarithms are usually considered exponential and therefore inefficient, they are sufficient for our purposes.

Theorem 1.1.9 (Pollard, [22])**.** *Discrete logarithm modulo p can be found with $O(\sqrt{p})$ operations in $\mathbb{F}_p$.*

Another advanced computational procedure needed in our algorithm is Fourier transform (see Definition 0.0.11 and discussion following it).

Theorem 1.1.10 (Bluestein, [4])**.** *Discrete Fourier transform with size N can be computed with $O(N \log N)$ arithmetical operations.*

1.2. Algorithms

In this section we present an algorithm which solves the problem stated in the introduction, therefore proving Theorem 1.0.6. The algorithm consists of two algorithms, which performed one after another lead to the solution. They are based on two simple observations. We include them as the next two lemmas.

The idea behind the first one is to look for properties of prime numbers which distinguish them from the composite ones. To be more specific, we are interested in properties which are preserved after taking residues mod p. One such property is the large number of multiples in the set of divisors. Algorithm 1.2.2 is based on this lemma.

Lemma 1.2.1. *If $a \in \Gamma$, then there exist at least $2^{\omega(n)-1}$ elements $b \in A$ such that $ab(mod p) \in A_p$.*

Proof. For every $b \in A$ which is not a multiple of a (for $a \in \Gamma$ there are $2^{\omega(n)-1}$ such b's) $ab \in A$ holds, hence also $ab (\mathrm{mod}\, p) \in A_p$. □

Algorithm 1.2.2 is called B_{rand} to emphasize the intuition given by considering an output with its input being a random set of a given size (then asymptotically almost surely B_{rand} is empty). When we apply Algorithm 1.2.2 to $A_p \subset \mathbb{Z}_p$ all elements of Γ_p are included in B_{rand} and the intuition suggests that typically there should be not much more. But B_{rand} may be too big.

Algorithm 1.2.2. $B_{rand}(A_p)$
For every $a \in A_p$:

1. *set $D_a = 0$*
2. *For every $b \in A_p$:*
   (a) *check whether $ab \in A_p$,*
   (b) *if it's true set $D_a = D_a + 1$.*
3. *if $D_a \geq \frac{1}{2}|A_p|$, add a to the set B_{rand}.*

The idea behind the second lemma is to realize that the problem is really about $\mathcal{P}(C)$ of some set C in the cyclic group $\mathbb{Z}_{p-1}$ and look for other settings where the corresponding problem is easy to solve. It turns out that one such setting is the semigroup of natural numbers under addition.

Lemma 1.2.3. *Let $C \subset \mathbb{N}$. Then there exists a deterministic algorithm which given $\mathcal{P}(C)$ ($|\mathcal{P}(C)| = N$) finds C with running time $O(N \log N)$. Moreover, C can be a multiset and it does not change the conclusion.*

Proof. See Algorithm 1.2.4. □

Algorithm 1.2.4. *C (S)*

1. *Sort the elements of S in nondecreasing order.*
2. *Set $D := \emptyset$ and $C := \emptyset$.*
3. *Move 0 from S to D.*
4. *Until $|C| = \frac{\log(|S|)}{\log 2}$:*
   (a) *Set x - the smallest element still in S.*
   (b) *For all elements d in D move $x + d$ from S to D.*
   (c) *Add x to C.*

This algorithm can be easily adapted to handle also sets containing negative integers. It is going to be important that we can easily generalize this problem (and its solution) to multisets (no changes in the algorithm needed). Notice that in the algorithm given below if an input S is the set of subset sums then the set T from the step 1 is also the set of subset sums (but with some elements replaced with their negations).

Algorithm 1.2.5. *F (S)*

1. *Find* $\min(S)$ *and set* $T = \{s - \min(S) : s \in S\}$.
2. *Apply Algorithm 1.2.4 with* T *as input to find* $\bar{C} = C(T)$.
3. *For every* $c \in \bar{C}$*:*
   (a) *if* $c \in S$ *and* $c > 0$ *- add* c *to* F.
   (b) *if* $-c \in S$ *and* $c < 0$ *- add* $-c$ *to* F.

Corollary 1.2.6. *Let* $C \subset \mathbb{Z}$. *Then there exists a deterministic algorithm which given* $S = \mathcal{P}(C)$ *(*$|\mathcal{P}(C)| = N$*) finds a set* F *such that* $C \subset F$ *and* $|F| < 2|C|$ *with running time* $O(N \log N)$. *Moreover,* C *can be a multiset and it does not change the conclusion (elements of multisets are counted with multiplicity).*

Proof. Algorithm 1.2.5 does the job, since the addition of the constant (which is an element of the input set S) only changes the signs of some elements $g \in C$. Absolute values of elements of C are found in step 2. □

In order to adapt this algorithm to the setting of cyclic group it is desirable to contain the set in some short interval. To perform this task it is convenient to work with a group of prime order. Therefore, we would like to have at least a large subgroup of prime order. To find the sought-after interval efficiently, we need to use Fourier transform. In order to optimize its computational complexity we would not like this prime to be too large. This are the reasons for our assumptions on $P(p-1)$.

Algorithm 1.2.7. $B_{struct}(A_p)$

1. *Set* $q = P(p-1)$.
2. *For every* $a \in A_p$ *compute* $\bar{a} := a^{\frac{p-1}{q}}$.
3. *For every* $a \in A_p$ *compute discrete logarithm* $\tilde{a} := \frac{q}{p-1}\log_g(\bar{a})$ *(for some generator* g *of the group* $\mathbb{Z}_p^*$*). Set* $L_q = \{\frac{q}{p-1}\log_g(\bar{a}) : a \in A\} \subset \mathbb{Z}_q$.
4. *Find using Fourier transform* $d \in \{1, \ldots, q-1\}$ *such that for all* $\tilde{a} \in L_q$ *elements* $d \cdot \tilde{a}$ *are contained in the interval* $[-\frac{q\log(2)}{\log(|A_p|)}, \frac{q\log(2)}{\log(|A_p|)}]$.
5. *Find the set* F *using Algorithm 1.2.5 for* $\mathbb{Z}$ *with* $d \cdot L_q$ *(with elements treated as integers) as an input.*
6. *For every* $c \in F$ *put all corresponding* $a \in A_p$ *into the set* B_{struct} *(if* $a|n$ *as integers include* a *only if it's prime).*

Observe that if $d \in \mathbb{Z}_q$ is such that $dA \subset [-\frac{q\log(2)}{\log(|A_p|)}, \frac{q\log(2)}{\log(|A_p|)}]$, then it corresponds to a large Fourier coefficient, namely $\hat{A}(d)$ is greater than $\frac{|A|}{2}$ (say) if x is large enough. Hence in step 5 of Algorithm 1.2.7 we first find all Fourier coefficients larger than $\frac{|A|}{2}$. There are at most $\frac{p}{|A|}$ of them because of Parseval identity. Then we can check for all of them whether they satisfy the condition.

Now the analysis of computational complexity of those algorithms is straightforward. First algorithm needs only $O(|A|^2)$ operations in $\mathbb{F}_p$. The most costly step of the second algorithm is step 4, which takes $O(p^{\frac{1}{2}+o(1)})$ operations in $\mathbb{F}_p$. Step 3 takes $O(p^{\frac{1}{4}+o(1)}|A|)$ operations.

To find all divisors which can possibly be prime we need to perform those two algorithms. At least one of them should give us desired set. Justification of this statement finishes the proof of Theorem 1.0.6 and it is our main objective in the next section.

1.3. If B_{rand} Fails, then B_{struct} Works

In this section we present the heart of our proof. This is the part where additive combinatorics come into play. For theoretical consideration it is simpler to look at the set of discrete logarithms of elements of the set A_p. We will denote this set by L.

Notation 1.3.1. *Let* $L := \{\log_g(a) : a \in A_p\}$.

Note that to optimize computational complexity of Algorithm 1.2.7, we perform exponentiation first and then take discrete logarithms. Exposition becomes clearer with those operations in reversed order, since then we can phrase structural properties of A_p in additive language. Later we work with corresponding subset of integers under addition what makes additive notation more natural here.

Let us now recall the notion of additive energy (see Definition 0.0.6). The next lemma shows that Algorithm 1.2.2 can only fail for A_p, such that L, the set of discrete logarithms of its elements, is additively structured. We give here slightly strengthened version of the result from [16] with a simple proof.

Lemma 1.3.2 (Katz-Koester)**.** *Let* $0 < \rho < 1$ *and suppose* X *and* Y *are two subsets of* G*, and suppose*

$$X \subset \{z \in G : |(z+Y) \cap Y| \geq \rho|Y|\}.$$

Then

$$\frac{E(X)}{|X|^3}\frac{E(Y)}{|Y|^3} \geq \rho^4 \frac{|X|}{|Y|}.$$

Proof. We have

$$\begin{aligned} \rho|Y||X| &\leq \sum_{z\in X} |(z+Y)\cap Y| = |\{(y_1,y_2,z) \in Y^2 \times X : y_1 - y_2 = z\}| = \\ &= \sum_{y\in Y} |Y \cap (\{y\} - X)| \leq |Y|^{\frac{1}{2}} E(X,Y) \leq |Y|^{\frac{1}{2}} E(X)^{\frac{1}{4}} E(Y)^{\frac{1}{4}}. \end{aligned} \tag{1.2}$$

The first inequality follows from the condition satisfied by X, the second follows from Cauchy-Schwarz inequality and the third is an application of (2). Taking fourth powers we obtain the claimed inequality. □

Applying this lemma with $X = \{\log_g(b) : b \in B_{rand}\}$ (recall that B_{rand} is the output of Algorithm 1.2.2), $Y = L$ and $\rho = \frac{1}{2}$ we obtain the bound for the additive energy of L or its large subset L_1. Namely, at least one of those sets satisfies

$$E(L_1) \geq \kappa\sqrt{\epsilon}|L_1|^3$$

for some explicit constant κ. In each case there is at least some large subset $L_1 \subset L$ (namely $|L_1| > c(\epsilon)|L|$) with $E(L_1) \geq \frac{|L_1|^3}{K(\epsilon)}$. For $\epsilon = \Theta((\log p)^{-\frac{1}{12}})$ we have $c(\epsilon) = \Omega((\log p)^{-\frac{1}{12}})$ and $K(\epsilon) = O((\log p)^{\frac{1}{24}})$.

It is more convenient to use some more restrictive notion of additive structure and work with sets satisfying the condition $|L+L| \leq K|L|$ or $|L-L| \leq K|L|$ (look at the Definition 0.0.1 and the discussion following it) for some constant K (the so called sets with small doubling). Another, even more restrictive notion of additive structure is the one given by the following definition.

Definition 1.3.3. *Let $K \geq 1$. A subset H of an abelian group G is said to be a K-approximate group if it is symmetric ($H = -H$), contains neutral element, and $H + H$ can be covered by at most K traslates of H.*

We will need this notion as well.

The three definitions are not exactly equivalent, but some sort of equivalence between them is captured by the following definition (we follow here Green's exposition [13]).

Definition 1.3.4. *Suppose that A and B are two finite subsets of an abelian group G and that $K \geq 1$ is a parameter. Then we write $A \sim_K B$ to mean that there is some x such that $|A \cap (B + x)| \geq \frac{\max(|A|,|B|)}{K}$. We say that A and B are roughly equivalent with parameter K.*

The relation between the three notions is described by the theorem below.

Theorem 1.3.5. *For every $i, j \in \{1, 2, 3\}$ and every set A_i (and parameter K_i) that satisfies the condition (i) there exists a set A_j roughly equivalent to A_i with parameter K_{ij} which satisfies the condition (j) with parameter K_j, where K_{ij} and K_j depend polynomially on K_i.*

(1) $E(A_1) \geq \frac{|A_1|^3}{K_1}$

(2) $|A_2 - A_2| \leq K_2|A_2|$

(3) A_3 is K_3-approximate group.

Proof. (1) $\Rightarrow$ (2) follows from Balog-Szemerédi-Gowers Theorem (here $K_2 = K_1^4$ and $K_{1,2} = K_1$).

(2) $\Rightarrow$ (1) follows with $A_1 = A_2$ and $K_1 = K_2$ from the fact that

$$E(A) \geq \frac{|A|^4}{|A - A|},$$

which is a simple application of Cauchy-Schwarz inequality.

(3) $\Rightarrow$ (2) and hence (3) $\Rightarrow$ (1) is easily seen to be satisfied with $A_2 = A_3$ and $K_2 = K_3$.

To see that (2) $\Rightarrow$ (3) holds with $K_3 = K_2^3$ and $K_{2,3} = K_2^2$ take $A_3 = A_2 - A_2$ and apply Ruzsa covering lemma (with $A = A_2$ and $B = A_3$). The result follows, since $|A_2| < |A_2 - A_2| < K_2^2|A_2|$ and $|A_2 - A_2 + A_2| < K_2^3|A_2|$ by Plünnecke inequality.

The same argument coupled with (1) $\Rightarrow$ (2) implies (1) $\Rightarrow$ (3) with $K_{1,3} = (K_1^4)^2 = K_1^8$ and $K_3 = (K_1^4)^3 = K_1^{12}$. □

Using this theorem we can find some large more structural subset in our original set, namely the set $L_2 \subset L_1$ such that $|L_2| > c(\epsilon)|L_1|$ and $|L_2 - L_2| < K_2(\epsilon)|L_2|$. We can also find a small superset $L_2 \subset H$ which is a translate of $K_3(\epsilon)$-approximate group and $|H| < K_{2,3}|L_2|$. For $\epsilon = \Theta(\log p)^{-\frac{1}{12}}$ we have $c(\epsilon) = \Omega(\log p)^{-\frac{1}{24}}$ and $K_{2,3} = O(\log p)^{\frac{1}{3}}$, while $K_2 = O((\log p)^{\frac{1}{6}})$ and $K_3 = O((\log p)^{\frac{1}{2}})$.

The main advantage of approximate groups over other notions is that it is well-behaved under homomorphisms.

The following lemma appears as an exercise in [30].

Lemma 1.3.6. *Let G, G' be abelian groups, $H \subset G$ a K-approximate group and $\phi : G \to G'$ - a homomorphism. Then $\phi(H)$ is a K-approximate group.*

Proof. Let $x_1, \ldots, x_K \in G$ be such that $H + H$ is covered by $x_1 + H, \ldots, x_k + H$. Then $\phi(x_1) + \phi(H), \ldots, \phi(x_K) + \phi(H)$ covers $\phi(H) + \phi(H)$. Clearly, $\phi(e_G) = \phi(e_{G'})$ and $\phi(-a) = -\phi(a)$. □

Applying the last lemma to the set H and a homomorphism $\phi : \mathbb{Z}_p^* \to \mathbb{Z}_q$ defined by $a \mapsto \log_g(a^{\frac{p-1}{q}})$, we see that $\phi(H)$ is $K(\epsilon)$-approximate group.

Now, we have got an additively structured set in a large group of prime order. In such a setting we can observe that this set can be compressed to a short interval.

Definition 1.3.7. *The diameter $diamL$ of a set L (in $\mathbb{Z}$ or $\mathbb{Z}_m$) is defined as the smallest integer l for which there exist some a, d such that $L \subset a, a+d, \ldots, a+ld$.*

Theorem 1.3.8 (Green-Ruzsa, [14]). *Let q be a prime and let $H \subset \mathbb{Z}_q$ be a set with $|H| = \alpha q$ and $|2H| = K|H|$. Suppose that $\alpha \leq (16K)^{-12K^2}$. Then the diameter of H is at most*

$$12\alpha^{\frac{1}{4K^2}}\sqrt{\log(\frac{1}{\alpha})}q.$$

We emphasize the fact that small doubling is really needed here (large additive energy is not enough). Obviously, K-approximate group satisfies $|H+H| \leq K|H|$. Using this theorem, we can therefore find an arithmetic progression P such that $|P| \leq p^{1-\delta(\epsilon)}$ for some $\delta(\epsilon) > 0$ and H (and hence also L_2) is contained in P. It is straightforward to verify that the condition $\alpha \leq (16K)^{-12K^2}$ holds for $\alpha = q^{-\frac{1}{3}+o(1)}$ and $K = \Theta((\log p)^{\frac{1}{2}})$.

Next lemma will bring us back to the set L (or more precisely $\phi(L)$, which is equal to the set L_q in step 3 of Algorithm 1.2.7). Roughly speaking, it shows that a structure of $\mathcal{P}(C)$ enables us to control the whole set, when only some part is controlled. The fact that $L = \mathcal{P}(C)$ is crucial here and it is the only part of the proof where we use it.

Lemma 1.3.9. *Let $L = \mathcal{P}(C)$ be a subset (L is possibly a multiset) of $\mathbb{Z}_q$ and let $L' \subset L$ be such that $|L'| \geq \epsilon|L|$ (elements counted with multiplicity) and $diamL' \leq q^{1-\delta}$. Then there exists a constant $K(\epsilon) > 0$ such that L is contained in $K(\epsilon)$ translates of a set D with $diamD \leq 2q^{1-\delta}$.*

Proof. Let P be a symmetric arithmetic progression such that some translate x of P contains L' (without loss of generality we can assume that P has the common difference 1, otherwise we can multiply every element by d^{-1}). We are going to construct $m = \lceil \frac{2}{\epsilon} \rceil$ translates $x_i + 2P$ such that $C \subset X + 2P$ for $X = \{x_1, \ldots, x_m\}$. For each $g_j \in C$ either g_j belongs to some $x_i + P$ (and then $g_j + L' \subset x_i + x + 2P$ and $L' - g_j \subset x_i + x + 2P$) for some x_i already put in X or there are $|L'| = \epsilon|L|$ elements of L which are of the form $g_j + a'$ or $a' - g_j$ and are not captured by any translate yet. Then we add g_j and $-g_j$ to the set X. We need to add new translates at most $\lceil \frac{1}{\epsilon} \rceil$ times, because it increases by $\epsilon|A|$ the number of elements of A covered. If X is a set of translates covering all $g \in C$, then $\mathcal{P}(X)$ are translates covering $\mathcal{P}(C)$ (and there are $2^{|X|}$ of them). □

Lemma 1.3.10. *Let $L \subset \mathbb{Z}_q$ be a set with $diamA = q^{1-\delta}$. Then there exist $d \in \mathbb{Z}_q^*$ such that $dL \subset [-2q^{1-\frac{\delta}{2}}, 2q^{1-\frac{\delta}{2}}]$. Generally, if L is contained in K translates of a set D with $diamD = q^{1-\delta}$, then there exists $d \in \mathbb{Z}_q^*$ such that $dL \subset [-2q^{1-\frac{\delta}{2K}}, 2q^{1-\frac{\delta}{2K}}]$*

Proof. Let $a \in L$ be any element. By Pigeonhole Principle, there exist $d < q^{\frac{\delta}{2}}$ such that $da \in [q^{1-\frac{\delta}{2}}, q^{1-\frac{\delta}{2}}]$ (there exist two elements $d_1 a, d_2 a$ in one interval of length $q^{1-\frac{\delta}{2}}$, their difference satisfies the condition). For such d the conclusion holds. To prove the second statement, use multidimensional Pigeonhole Principle to find $d < q^{\frac{\delta}{2}}$ such that $da_i \in [q^{1-\frac{\delta}{2K}}, q^{1-\frac{\delta}{2K}}]$ for $i = 0, \ldots, K-1$, where $a_i + D$ are given translates. □

Using the last two lemmas we see that we can find d such that $dL \subset [-2q^{1-\frac{\delta(\epsilon)}{2K(\epsilon)}}, 2q^{1-\frac{\delta(\epsilon)}{2K(\epsilon)}}]$ what proves that a suitable d in step 4 of Algorithm 1.2.7 can be found, since $p^{\frac{\delta(\epsilon)}{2K(\epsilon)}} > \frac{\log(|A_p|)}{\log(2)}$ if n is large enough. It finishes the proof of Theorem 1.0.6, since the number of elements $a \in A_p$ corresponding to the same $c \in F$ is small by our assumptions (specifically the last, more technical one).

1.4. There are Plenty of Numbers Satisfying the Conditions

First of all, observe that the fact that for all but $o(x)$ numbers $n \leq x$ the number of prime divisors is right follows from the classical result quoted below.

Theorem 1.4.1 (Erdős-Kac, [12]). *Denote by $N(x; a, b)$ the number of integers m belonging to the interval $[3, x]$ for which the following inequality holds:*

$$a \leq \frac{\Omega(m) - \log\log m}{\sqrt{\log\log m}} \leq b, \tag{1.3}$$

where $a < b$ are real numbers with additional possibilities $a = -\infty$ and $b = \infty$. Then, with x tending to infinity, we have

$$\lim_{x\to\infty} \frac{N(x; a, b)}{x} = \frac{1}{\sqrt{2\pi}} \int_a^b \exp(-\frac{t^2}{2})dt. \tag{1.4}$$

It is easy to observe that a typical number cannot have to many small divisors. We will need this fact later.

Lemma 1.4.2. *There are $o(x)$ numbers $n \leq x$ such that the number of divisors of n smaller than $(\log x)^4$ is greater than $C(\log\log x)$.*

Proof. It follows from the fact that

$$\sum_{n<(\log x)^4} \frac{x}{n} = O(x \log\log x).$$

□

It is possible to find for x large enough the prime with the desired properties of $p - 1$. To prove that we need two classical results from analytic number theory. We are going to need the following definitions.

Definition 1.4.3. *The von Mangoldt function is defined as*

$$\Lambda(n) = \begin{cases} \log p & \text{when } n = p^k \text{for some prime } p \text{ and } k \geq 1 \\ 0 & \text{otherwise.} \end{cases}$$

The function $\pi(x; q, a)$ counts the primes not exceeding x in the residue class a modulo q.

$$\pi(x; q, a) = \sum_{p\leq x, p\equiv a (mod\ q)} 1.$$

The function $\psi(x; q, a)$ is defined similarly.

$$\pi(x; q, a) = \sum_{n\leq x, n\equiv a (mod\ q)} \Lambda(n).$$

Lemma 1.4.4 (Mertens, [17]). *We have*

$$|\sum_{p\leq n}\frac{\log p}{p}-\log n|\leq 2.$$

Theorem 1.4.5 (Bombieri - Vinogradov, [31]). *Let x and Q be any two positive real numbers with $x^{1/2}\log^{-A}x\leq Q\leq x^{1/2}$. Then*

$$\sum_{q\leq Q}\max_{y<x}\max_{\substack{1\leq a\leq q\\(a,q)=1}}\left|\psi(y;q,a)-\frac{y}{\varphi(q)}\right|=O\left(x^{1/2}Q(\log x)^5\right).$$

This leads to the following statement.

Corollary 1.4.6. *Let $\epsilon>0$. Then there exist efficiently computable constants $X_1(\epsilon)$, $\delta(\epsilon)>0$, such that, if $x>X_1$, we have*

$$\sum_{p\leq x, x^{\frac{1}{2}-\epsilon}<P(p-1)<x^{\frac{1}{2}+\epsilon}}1>\delta(\epsilon)\frac{x}{\log x}.$$

Proof. It suffices to lowerbound the sum $\sum_{x^{\frac{1}{2}-\epsilon}<q<x^{\frac{1}{2}}(\log x)^{-B}}\pi(x;q,1)$. By Bombieri-Vingradov theorem (and trivial observations that $\pi(x;q,a)\log x\geq\psi(x;q,a)$ and $\frac{\log p}{\log x}\leq 1$)

$$\sum_{x^{\frac{1}{2}-\epsilon}<q<x^{\frac{1}{2}}(\log x)^{-B}}\pi(x;q,1)\log x\geq\frac{x}{\log x}\sum_{x^{\frac{1}{2}-\epsilon}<q<x^{\frac{1}{2}}(\log x)^{-B}}\frac{\log q}{q-1}+O(\frac{x}{\log x}).$$

The last sum is equal $\epsilon\log x+O(1)$ by Mertens' theorem. □

To ensure that $P(p-1)^2\nmid(p-1)$ we need the following lemma.

Lemma 1.4.7. *There are $O\left(\frac{x^{\frac{1}{2}+2\epsilon}}{\log x}\right)$ numbers $n\leq x$ such that $q^2|(n-1)$ for some prime number $q>x^{\frac{1}{2}-\epsilon}$. In particular, for $\epsilon<\frac{1}{4}$ there are $o(\frac{x}{\log x})$ such prime numbers.*

Proof. We simply count

$$\sum_{x^{\frac{1}{2}-\epsilon}<q<x^{\frac{1}{2}}}\frac{x}{q^2}=O\left(\frac{x^{\frac{1}{2}}}{\log x}x^{2\epsilon}\right),\tag{1.5}$$

since there are $O\left(\frac{x^{\frac{1}{2}}}{\log x}\right)$ primes in this range and for any fixed q there are at most $\frac{x}{x^{2(\frac{1}{2}-\epsilon)}}=x^{2\epsilon}$ numbers divisible q^2. □

Now, we will prove that given such a prime p we can expect different divisors of n to give different residues. In the proof we are going to use the following lemma which is a discrete analogue of integration by parts (lemma 2.5.1 in [2]).

Lemma 1.4.8. *Let $(a_n)_{n\in\mathbb{N}}$ be the sequence of complex numbers, $A(t):=\sum_{n\leq t}a_n$ and let $f:[1,x]\to\mathbb{C}$ be a C^1-class function. Then:*

$$\sum_{n\leq x}a_nf(n)=A(x)f(n)-\int_1^xA(t)f'(t)dt.\tag{1.6}$$

Lemma 1.4.9. *Let $\epsilon > 0$. For a given prime number such that $p > (\log x)^{2+\epsilon}$ the set of numbers $n \leq x$ such that there exists a pair of distinct divisors of n congruent modulo p respectively has size $o(x)$.*

Proof. Clearly, there are $o(x)$ number $n < x$ divisible by p. We need to bound the size of the set of numbers n such that there exist a pair d_1, d_2 such that $d_1|n$, $d_2|n$ and $d_1 - d_2$ is divisible by p. For n not divisible by p at least one such pair d_1, d_2 (if it exists) must consist of relatively prime numbers. Therefore, the size of the set can be crudely bounded by the following expression

$$\sum_{r<\frac{x}{p}} \sum_{d<\frac{x}{rp}} \frac{x}{d(d+rp)} \tag{1.7}$$

To bound those sums we can use the following bound for the series $\sum_{n\geq 1} \frac{1}{n(n+r)}$ with parameter r.

$$\sum_{n\geq 1} \frac{1}{n(n+r)} = \sum_{n\geq 1} \frac{1}{r}(\frac{1}{n} - \frac{1}{n+r}) = \frac{1}{r}\sum_{n=1}^{r} \frac{1}{n} = O(\frac{\log r}{r}) \tag{1.8}$$

Using (1.8) with parameter rp we can bound (1.7) by

$$\sum_{r<\frac{x}{p}} \frac{x(\log rp)}{rp} = O(\frac{x(\log x)^2}{p}),$$

using Lemma 1.4.8 to get the last inequality. □

What has left to show is that a condition set on $d^{\frac{p-1}{P(p-1)}}$'s is satisfied by typical n. First we deal with possible obstruction caused by a divisor which satisfies $d^{\frac{p-1}{P(p-1)}} \equiv \pm 1$.

Lemma 1.4.10. *Let p be a prime number and let $I \subset \mathbb{Z}_p^*$ be such that $|I| \leq p^\delta$. If $\log x = o(p^{1-\delta})$, then the set of numbers $n < x$ such that there exists a number $d > p$ which satisfies $d \equiv a$ for some $a \in I$ and $d|n$ has size $o(x)$.*

Proof. It follows from

$$\sum_{1\leq r\frac{x}{p}} \frac{x}{a+pr} = O(\frac{x}{p}\log(\frac{x}{p})).$$

□

Using this fact we can prove what we need. Notice that for our purposes the assumption in the next theorem could be strengthened to $P(p-1) > (\log x)^{\frac{3}{2}-\epsilon}$.

Lemma 1.4.11. *Let $\epsilon > 0$. Let p be a prime number with $p \geq (\log x)^3$ such that $P(p-1) > (\log x)^{2-\log 2+\epsilon}$ For all but $o(x)$ numbers $n \leq x$ the set of divisors d of n such that $d^{\frac{p-1}{P(p-1)}} \equiv q^{\frac{p-1}{P(p-1)}} \pmod p$ for some $q > p$ prime divisor of n has size $o((\log x)^{\log 2})$.*

Proof. We can estimate the number of triples consisting of a number $n \leq x$ and a pair (d_1, d_2) of relatively prime divisors of n such that $d_1 > p, d_2 > p$ which satisfies $d_1^{\frac{p-1}{P(p-1)}} \equiv d_2^{\frac{p-1}{P(p-1)}}$. Let $I \subset \mathbb{Z}_p^*$ be a subgroup of $P(p-1)$-th powers and let $I_d \subset \mathbb{Z}_p^*$ be a coset of this subgroup containing d. We know that $|I| \leq \frac{p-1}{P(p-1)}$.

$$\sum_{d\leq x} \frac{1}{d} \sum_{a\in I_d} \sum_{1\leq r\leq \frac{x}{p}} \frac{x}{a+rp} = O(\frac{x\frac{p}{P(p-1)}(\log x)^2}{p}) = O(\frac{x(\log x)^2}{P(p-1)}). \tag{1.9}$$

All divisors d for which $d^{\frac{p-1}{P(p-1)}} \equiv \pm q^{\frac{p-1}{P(p-1)}} \pmod{p}$ holds for some $q > p$ which is a prime divisor of n are either relatively prime to q (first kind) or they are of the form ds, where $s < p$ and d is either q or a divisor of the first kind (then we call them divisors of the second kind). The number of the divisors of the first type can be bounded by $O((\log x)^{\log 2-\epsilon})$ for all but at most $o(x)$ numbers $n \leq x$ using (1.9) and the assumption on $P(p-1)$. Taking into account the divisors of the second kind raises this number only $(\log\log x)^{1+o(1)}$ times for all but $o(x)$ numbers $n \leq x$ by Lemma 1.4.2. □

1.5. Application

Here we present an application of our result to deterministic polynomial-time reduction of factorization to computing $\sigma_1(n), \ldots, \sigma_M(n)$. This reduction is only proved to work for numbers forming a dense set (not necessarily for all numbers). The reduction is already polynomial-time in its simplest form. If a sufficiently efficient polynomial factoring algorithm is used (namely Shoup's Algorithm for polynomial with linear factors) it can be made to run in time $O((\tau(n))^2 \log n \log\log n \log\log\log n)$. Then our main result only reduces implied constant in $O()$ notation.

It is worth noting here that probabilistic polynomial-time reductions to computing $\sigma_k(n)$ (for a single k) are known [3]. Much more is known about the similar problem concerning Euler totient function $\phi(n)$. There exists a probabilistic polynomial-time reduction which can be easily derandomized under Extended Riemann Hypotheses [19]. Moreover, it can be shown unconditionally to work in deterministic polynomial time for the dense set of integers [7]. There is also unconditional subexponential-time reduction proved to work for any integer [32]. Paper [1] provides extensive survey of problems studied and results obtained in this area.

Algorithm 1.5.1. *N* $(n, P_1, P_2, \ldots, P_M)$

1. *For every* $k = 1, \ldots, M$ *compute* $S_k = \frac{(-1)^{k+1}}{k}(P_k + \sum_{i=1}^{k-1}(-1)^i P_{k-i} S_i)$.
2. *Set as* m *the greatest* k *such that* $S_k \neq 0$.
3. *Set as* $W \in \mathbb{Z}[X]$ *the polynomial* $W(X) = X^m + \sum_{i=1}^{m}(-1)^i S_i X^{m-i}$.
4. *Factor the polynomial* $W(X)$ *in* $\mathbb{Z}[X]$.
5. *If the result consists of linear terms* $(X - d_i)$ *(for* $i = 1, \ldots, m$*), sort* d_i *in nonincreasing order.*
6. *For each* i *check whether* $d_j | d_i$ *for some* $j < i$*; if not, check with what multiplicity* d_i *divides* n *and write out* d_i *with that multiplicity.*

Theorem 1.4.1 implies that in Algorithm 1.5.1 parameter $M = \lfloor (\log n)^{\log 2+o(1)} \rfloor$ can be used and the algorithm would still work for the numbers from the set of natural density equal 1.

We prove

Theorem 1.5.2. *There exists a deterministic algorithm which using an oracle for monic polynomial* W *with all divisors of a given number* m *as roots computes the factorization of* n *for numbers* n *belonging to the set of natural density 1 (it uses the oracle at most twice) with running time* $O((\tau(n))^2 \log n \log\log n \log\log\log n)$. *In particular, for* n *belonging to this set this time is* $(\log n)^{1+2\log 2+o(1)}$.

We can assume that n is squarefree because of the following observation.

Lemma 1.5.3. *The set of natural numbers $n \leq x$ divisible by a square of an integer larger than $\log\log x$ is of cardinality $o(x)$.*

Proof. The cardinality of the considered set can be upperbounded by

$$x \sum_{\log\log x \leq d < \sqrt{x}} \frac{1}{d^2} + O(\sqrt{x}) \tag{1.10}$$

(as $\lfloor \frac{x}{d^2} \rfloor = \frac{x}{d^2} + O(1)$) which is $o(x)$ because of the convergence of the series $\sum \frac{1}{d^2}$. □

Divisibility by squares of the numbers smaller than $\log\log n$ can be checked by trial division with $(\log n)^{1+o(1)}$ bit operations. If $p^\alpha || n$ the values of functions $\sigma_k(\frac{n}{p^\alpha})$ can be determined using formula $\sigma_k(\frac{n}{p^\alpha}) = \frac{\sigma_k(n)}{\sigma_k(p^\alpha)}$ at the cost of $O(k \log n)$ bit operations.

All divisors which can possibly be prime numbers can be found with Algorithm 1.5.4. To find the factorization of n perform the last step of Algorithm 1.5.1 on elements of B.

Algorithm 1.5.4. *S(W)*

1. *Find a prime number p of the order $(\log n)^{3+o(1)}$ with $P(p-1) = p^{0.5+o(1)}$.*
2. *Factor W_p with Shoup algorithm and find set of residues A.*
3. *Find the set B with Algorithm 1.2.2.*
4. *If $|B| > \epsilon|A|$, find the set B with Algorithm 1.2.7.*
5. *For every element in B perform Hensel lift to the residue modulo p^e (with $e = \lceil \frac{\log n}{\log p} \rceil$).*

We need to define some special types of symmetric polynomials.

Definition 1.5.5. *Elementary k-th symmetric polynomial of variables $x_1, \ldots, x_m$ is given by*

$$s_k(x_1, \ldots, x_m) = \sum_{1 \leq i_1 < \ldots < i_k \leq m} x_{i_1} \cdots x_{i_k}. \tag{1.11}$$

k-th Newton function of variables $x_1, \ldots, x_m$ is given by

$$p_k(x_1, \ldots, x_m) = \sum_{i=1}^{m} x_i^k. \tag{1.12}$$

Function $\sigma_k(n)$ is equal to $p_k(d_1, \ldots, d_{\tau(n)})$, where $d_1, \ldots, d_{\tau(n)}$ are all divisors of n.

The correctness of the algorithm follows from the two sets of identities given below. For a nice proof see [18].

Lemma 1.5.6 (Newton identities)**.** *For $1 \leq k \leq m$ the following identity holds:*

$$p_k + \sum_{i=1}^{k-1} (-1)^i p_{k-i} s_i + (-1)^k k s_k = 0, \tag{1.13}$$

and for $m < k$:

$$p_k + \sum_{i=1}^{m} (-1)^i p_{k-i} s_i = 0. \tag{1.14}$$

Lemma 1.5.7 (Vieta's formulas). *Let R be an unique factorization domain and let $a_m x^m + \ldots + a_0 \in R[X]$ be a polynomial with m roots $x_1, \ldots, x_m$ (in the field of fractions of R). Then the following holds*

$$s_k(x_1, \ldots, x_m) = (-1)^k \frac{a_{m-k}}{a_m}. \tag{1.15}$$

To bound its running time we need the following two results from algorithmic number theory.

Theorem 1.5.8 (Shoup, [29]). *Let f be a polynomial over $\mathbb{Z}_p$ of degree m which is a product of m distinct monic polynomials of degree 1. Then f can be factored deterministically with $O(p^{\frac{1}{2}}(\log p)^2 m^{1+o(1)})$ operations in $\mathbb{Z}_p$.*

Lemma 1.5.9 ([2]). *Hensel lift of a root of polynomial f modulo p to a root modulo p^k can be found with $O(deg(f)(k \log p)^{1+o(1)})$ operations.*

Factorization can be found with Algorithm 1.5.4. Computing the coefficients of the polynomial modulo p can be performed in time $O((\tau(n))^2 \log n \log\log n \log\log\log n)$. Factorization of a polynomial with distinct roots over $\mathbb{F}_p$ can be done with Shoup algorithm in time $(\log n)^{\frac{3}{2}+\log 2+o(1)}$. Algorithms 1.2.2 and 1.2.7 work in time $(\log n)^{2\log 2+o(1)}$ and $O((\log n)^{1.08+\log 2+o(1)})$ respectively. Hensel lift can be performed in time

$$o((\tau(n))^2 \log n \log\log n \log\log\log n).$$

In this last bound we used our main result to reduce the number of Hensel lifts needed so that their cost does not dominate computational complexity of the algorithm.

From this result we can deduce the following.

Corollary 1.5.10. *There exists a deterministic algorithm which for almost every n if the values of functions $\sigma_1(n), \ldots, \sigma_{\lfloor(\log n)^{\log 2+o(1)}\rfloor}(n)$ are given, computes the full factorization of n in time $O((\log n)^{1+2\log 2+o(1)})$.*

Proof. Values of $\sigma_k(\frac{n}{p^\alpha})$ can be computed effectively. After computing the residues of $\sigma_k(n)$ modulo $p^{\lceil\frac{\log n}{\log p}\rceil}$ coefficients of the polynomial can be found in time $O((\log n)^{1+2\log 2+o(1)})$. The rest proceeds exactly as in the previous proof. □

The approach presented here does not seem to extend to the cases of a single $\sigma_k(n)$ or $\phi(n)$ mentioned in the beginning of this section, neither is it possible to work for any integer as it critically relies on n having the right number of prime factors. On the other hand, it does appear to be possible to significantly reduce the amount of information used by algorithm. It is not needed to know residues of all divisors, knowing a large fraction of them should suffice.

1.6. Open Problems

The problem considered here leads to the following questions: For a dissociated set C (a dissociated set is a set with all subset sums distinct) in an abelian group G, is C determined uniquely by $S = \mathcal{P}(C)$? Can we find it efficiently?

In general, already the answer to the first question is negative, as the following examples show.

$$\mathcal{P}(\{2,5\}) = \mathcal{P}(\{5,7\}) \qquad \text{in } \mathbb{Z}_{10}$$

$$\mathcal{P}(\{3,5,6,7\}) = \mathcal{P}(\{1,9,13,15\}) = \mathbb{Z}_{17} \setminus \{2\} \qquad \text{in } \mathbb{Z}_{17}$$

The first example illustrates the obstruction caused by even order of the group and in the second one the set $\mathcal{P}(C)$ almost covers the whole group.

So, probably the right question to ask would be rather: Under what conditions is C determined uniquely by $S = \mathcal{P}(C)$? (Under what conditions can we find it efficiently?)

Chapter 2

Exponential sums

In this chapter we present results published in [10]. Bounding exponential sums is a very active area of research. Here we consider the special case of sums over subgroups generated by 2. If the order of a subgroup is large, then there is a general result proved by Bourgain, Glibichuk and Konyagin, which gives a good upper bound.

Theorem 2.0.1 ([5]). *Let $F = \mathbb{F}_p$ be a finite field of prime order, and let H be a multiplicative subgroup of F such that $|H| \geq p^\delta$ for some $0 < \delta < 1$. Then if p is sufficiently large depending on δ, for some $\epsilon(\delta) > 0$ we have*

$$\sup_{\xi \in \mathbb{Z}_p \setminus \{0\}} \left| \sum_{x \in H} e(x\xi) \right| \leq p^{-\epsilon} |H|.$$

Throughout the rest of this paper we concentrate on small subgroups. This line of investigation was essentially started by the work of Molteni [20]. We are going to use the following notation. For some fixed odd integer q:

- $\tau := ord_q(2)$
- $\mathcal{L} := \lfloor \log_2(q) \rfloor$
- $e(x) := \exp(2\pi i x)$
- $s(a/q) := \sum_{r=1}^{\tau} e(a2^r/q)$

When subgroups are small much less cancellation is expected. In fact, Kaczorowski and Molteni provided infinitely many examples showing that in general the cancellation may be as small as some explicit constant.

Theorem 2.0.2 ([15]). *There exists a positive constant c and a sequence of integers $q \to \infty$ such that*

$$\max_{(a,q)=1} |s(a/q)| \geq \tau - c + O\left(\frac{1}{q}\right).$$

Moreover $c \leq 2\sum_{r=1}^{\infty} \sin^2\left(\frac{\pi}{2^r}\right) = 3.394\ldots$.

They also proved the following upper bound.

Theorem 2.0.3 ([15]). *If $\tau \geq \kappa(\mathcal{L}+1)+2$ for a nonnegative integer κ and $q > 3$, then*

$$\max_{(a,q)=1} |s(a/q)| < \tau - \kappa - 1.$$

We improve the above bound. Here is the main result of this part of the dissertation.

Theorem 2.0.4. *If $\tau \geq \kappa(\mathcal{L}+4)+5$ for some positive integer κ, then*

$$\max_{(a,q)=1} |s(a/q)| < \tau - 2(\kappa+1). \tag{2.1}$$

2.1. Proof of Theorem 2.0.4

The following fact plays a key role in the proof of Theorem 2.0.3.

Lemma 2.1.1 ([15]). *Suppose $\zeta = e(\theta)$ for some real number θ with $\Re(\zeta) \leq 0$ and $\zeta \neq -1$. Then:*

$$|\zeta^2 - 1| < |\zeta - 1| \qquad \text{or} \qquad |\zeta^4 - 1| < |\zeta^2 - 1|.$$

Similarly, our proof relies on the following lemma.

Lemma 2.1.2. *Suppose $\zeta = e(\theta)$ for some real number θ with $\Re(\zeta) \leq 0$ and $\zeta \neq -1$. Then*

$$|\zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^{16}| < 3.$$

Proof. Let $f(\theta) = |\zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^{16}|$. Based on the well known Euler identity $e^z = \cos z + i \sin z$, we have

$$\begin{aligned} f(\theta) \;:=\; & ((\sin 2\pi\theta + \sin 4\pi\theta + \sin 8\pi\theta + \sin 16\pi\theta + \sin 32\pi\theta)^2 \\ & + (\cos 2\pi\theta + \cos 4\pi\theta + \cos 8\pi\theta + \cos 16\pi\theta + \cos 32\pi\theta)^2)^{\frac{1}{2}}. \end{aligned} \tag{2.2}$$

In order to prove the lemma, it suffices to show that values of the function f on the interval $[\frac{1}{4}, \frac{3}{4}]$ are less than 3 (except of the point $\theta = \frac{1}{2}$). Repeatedly using the formulae $\sin(2x) = 2\sin(x)\cos(x)$ and $\cos(2x) = 2\cos(x)^2 - 1$, and then using substitution $x = \cos 2\pi\theta$ we get the following polynomial

$$\begin{aligned} w(x) &= 32768x^{15} + 16384x^{14} - 122880x^{13} - 53248x^{12} \\ &+ 184320x^{11} + 66560x^{10} - 140800x^9 - 39680x^8 + 57728x^7 \\ &+ 11200x^6 - 12320x^5 - 1216x^4 + 1240x^3 + 12x^2 - 48x + 5. \end{aligned} \tag{2.3}$$

We need to show that it is bounded by 9 on the interval $(-1, 0]$. By standard tools (we used wxMaxima 16) one can verify that the 14 roots of $w'(x)$ are: $-1.057176\ldots$, $-0.948631\ldots$, $-0.855344\ldots$, $-0.720103\ldots$, $-0.531527\ldots$, $-0.344771\ldots$, $-0.123226\ldots$, $0.148074\ldots$, $0.266689\ldots$, $0.405528\ldots$, $0.631112\ldots$, $0.794703\ldots$, $0.907195\ldots$, $0.960809\ldots$.

Only the points $-0.948631\ldots$, $-0.855344\ldots$, $-0.720103\ldots$, $-0.531527\ldots$, $-0.344771\ldots$, $-0.123226\ldots$ belong to the considered interval. The polynomial $w(x)$ takes the values $0.8492539\ldots$, $5.0979332\ldots$, $0.0739295\ldots$, $7.3947072\ldots$, $2.1874524\ldots$ and $8.8596675\ldots$ at those points; furthermore $w(-1) = 9$ and $w(0) = 5$. Hence $w(x) < 9$ for any $x \in (-1, 0]$. Since $f(\theta) = \sqrt{w(\cos 2\pi\theta)}$ the assertion follows. □

The graphs of $f(\theta)$ and $w(x)$ in the relevant ranges are shown at Figures 1 and 2, respectively.

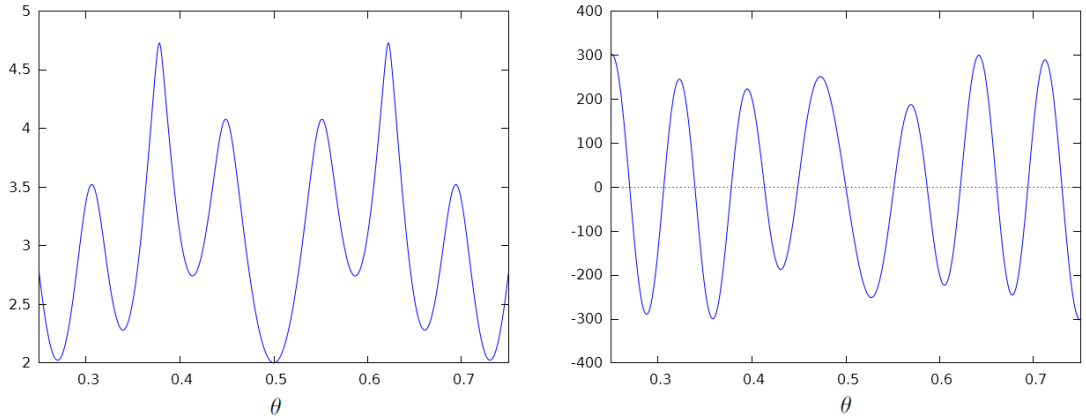

Figure 2.1: Values of trigonometric polynomial and its derivative.

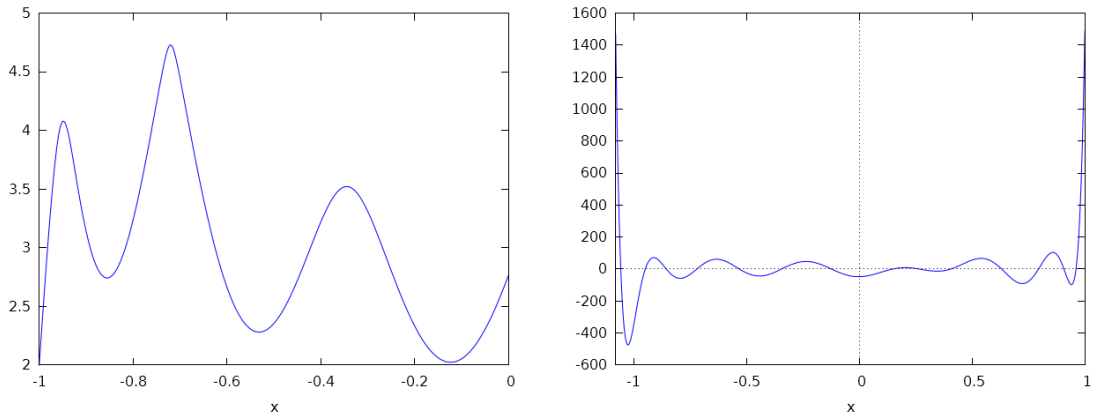

Figure 2.2: Values of corresponding algebraic polynomial and its derivative.

Lemma 2.1.3. *Let $(a,q)=1$ and $q>5$. Then for any integer $m\geq 0$ there exists an integer l such that $m\leq l<\mathcal{L}+m$ and*

$$s_5(a2^l/q):=\left|e\left(\frac{2^l a}{q}\right)+e\left(\frac{2^{l+1}a}{q}\right)+e\left(\frac{2^{l+2}a}{q}\right)+e\left(\frac{2^{l+3}a}{q}\right)+e\left(\frac{2^{l+4}a}{q}\right)\right|<3.$$

Proof. Without loss of generality we may assume that $m=0$ (otherwise $2^m a$ should be considered instead of a). If $\Re e(2^L a/q)\leq 0$ for some $0\leq L<\mathcal{L}$, then the claim follows from Lemma 2.1.2. Further we assume that $\Re e(2^L a/q)>0$ for any $0\leq L<\mathcal{L}$. Denote by θ the real number satisfying $|\theta|<\frac{1}{4}$ and $e(2^{\mathcal{L}-1}a/q)=e(\theta)$. Then the numbers $e(\frac{2^l a}{q})$ for $0\leq l\leq \mathcal{L}-1$ are equal to $e(\frac{\theta}{2^k})$ for $\mathcal{L}-1\geq k\geq 0$, correspondingly. In particular $e(a/q)=e(\theta/2^{\mathcal{L}-1})$ and so

$$\frac{1}{q}\leq\left|\frac{\theta}{2^{\mathcal{L}-1}}\right|<\frac{1}{2^{\mathcal{L}+1}}<\frac{1}{q},$$

which leads to a contradiction. □

Now we are ready to prove Theorem 2.0.4.

Proof. By Lemma 2.1.3 and the assumption of the theorem there exists a number l_0 such that $s_5(a2_0^l/q) < 3$. By the periodicity of $e(2^l a)$ it follows that $s(a/q) = \sum_{l=l_0}^{l_0+\tau-1} e\left(\frac{2^l a}{q}\right)$. We divide the set of summand indices into intervals: $\{l_0, l_0+1, l_0+2, l_0+3, l_0+4\}$ and at least κ intervals of length $\mathcal{L}+4$. By the previous lemma each interval contains some number l such that $s_5(2^l a/q) < 3$; furthermore it can be chosen from the first $\mathcal{L}$ elements of the interval. Hence using the triangular inequality we get

$$|s(a/q)| < \tau - 5(\kappa+1) + 3(\kappa+1) = \tau - 2(\kappa+1).$$

□

The above proof differs from the proof of Theorem 2 by considering the sum of five consecutive summands instead of only two. Apart from that, the argument is analogous.

2.2. Further Improvement

If we consider taking more than 5 summands, we can improve the result, however, the argument becomes more technical. The next theorem is an example of such an improvement.

Theorem 2.2.1. *If $\tau \geq \kappa(\mathcal{L}+5)+6$ for a nonnegative integer κ, then*

$$\max_{(a,q)=1} |s(a/q)| < \tau - 2.37(\kappa+1). \tag{2.4}$$

Proof. Let $\zeta = e(\theta)$ for some real number θ such that $-0.999118 \leq \Re(\zeta) \leq 0.021$. First we show that

$$|\zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^{16} + \zeta^{32}| < 3.63. \tag{2.5}$$

By almost the same arguments as in the proof of Lemma 2.1.2, we come to the conclusion that it is enough to bound the polynomial

$$\begin{aligned} w(x) = {} & 2147483648\,x^{31} + 1073741824\,x^{30} - 16642998272\,x^{29} \\ & - 7784628224\,x^{28} + 58250493952\,x^{27} + 25300041728\,x^{26} \\ & - 121701924864\,x^{25} - 48637149184\,x^{24} + 169030451200\,x^{23} \\ & + 61446553600\,x^{22} - 164479631360\,x^{21} - 53589573632\,x^{20} \\ & + 115135741952\,x^{19} + 32967491584\,x^{18} - 58595868672\,x^{17} \\ & - 14351925248\,x^{16} + 21655027712\,x^{15} + 4363173888\,x^{14} \\ & - 5741977600\,x^{13} - 895791104\,x^{12} + 1066528768\,x^{11} + 115973120\,x^{10} \\ & - 133433856\,x^9 - 8054272\,x^8 + 10580864\,x^7 + 131264\,x^6 \\ & - 484512\,x^5 + 15376\,x^4 + 11160\,x^3 - 704\,x^2 - 110\,x + 10 \end{aligned} \tag{2.6}$$

on $[-0.999118, 0.021]$.

Its extrema are approximately at points: -1.074387, -0.989143, -0.971382, -0.939692, -0.890416, -0.829615, -0.776161, -0.717199, -0.637236, -0.564463, -0.466427, -0.359011, -0.252928, -0.159027, -0.043114, 0.173648, 0.309891, 0.406477, 0.508774, 0.579395, 0.672828, 0.766044, 0.812919, 0.849519, 0.910000, 0.950689, 0.978700, 0.990701.

For a clearer view, let us first calculate the values of the function $h(x) = 6 - \sqrt{w(x)}$. At the first 16 points we obtain: $-94.6222693\ldots$, $4.5876861\ldots$, $3.6328312\ldots$, $5.9968304\ldots$, $3.0354921\ldots$, $4.8466566\ldots$, $3.9512462\ldots$, $4.7487580\ldots$, $3.4408042\ldots$, $4.3572044\ldots$, $2.6267897\ldots$,

$5.4964278\ldots$, $2.9328713\ldots$, $4.0850766\ldots$, $2.4415242\ldots$, 6.0. At the point -0.999118 it takes the value $2.3703688\ldots$. We see that all the values are greater than 2.37 so $w(x) < 3.63$ for $x \in [-0.999118, 0.021]$ unless there exists some another minimum of h in this interval.

To exclude this possibility, we consider the second and the third derivative of $w(x)$. The second derivative has a root $0.0211231\ldots$, while the third derivative has roots $0.0683720\ldots$ and $0.1498680\ldots$. If f has an additional minimum in the interval $[-0.999118, 0.021]$, then w' has two additional roots in this interval. As a derivative always has some zero between two zeros of a function, that would imply that w'' has 16 roots smaller than 0.02, a root $0.0211231\ldots$ and 12 roots greater than $0.1736481\ldots$. That in turn would imply that w''' has 29 roots: 16 roots smaller than $0.0211231\ldots$, points $0.0683720\ldots$ and $0.1498680\ldots$, and 11 roots greater than $0.1736481\ldots$. But this is a polynomial of degree 28, so we come to the contradiction. We conclude that $h(x) > 2.37$ and thereby $w(x) < 3.63$ for $x \in [-0.999118, 0.021]$.

Now we show that there exists an integer l such that $m \leq l < \mathcal{L} + m$ and

$$s_6(a2^l/q) := \left| \sum_{j=0}^{5} e\left(\frac{2^{l+j}a}{q}\right) \right| < 3.63.$$

For this purpose we repeat the argument from the proof of Lemma 2.1.3. If $\Re e(2^L a/q) > 0$ for any $0 \leq L < \mathcal{L}$, then the argument is the same. If $\Re e(2^L a/q) \leq 0$ for some $0 \leq L < \mathcal{L}$, then the claim follows from (2.5) by taking $l = L$ or $l = L-1$, as $\cos(2\arccos(0.021)) = -0.999118$.

The proof of Theorem 2.2.1 proceeds in the same way as the proof of Theorem 2.0.4. □

The graphs for $h(x)$ and the derivative of $w(x)$ in the ranges critical to the twist in the argument are shown in Figure 3.

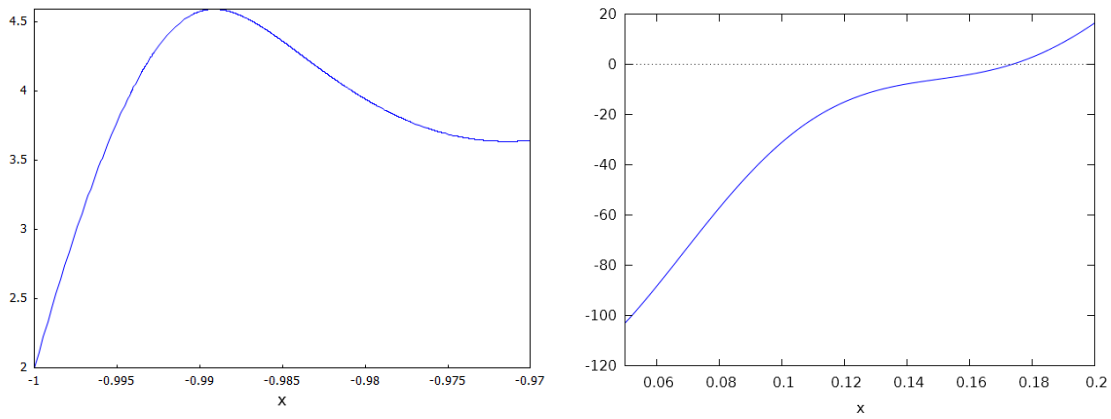

Figure 2.3: $h(x)$ for points close -1. Derivative of $w(x)$ for points near 0.

It seems reasonable to conjecture that with this method the constant 2.37 in the bound (2.4) may be replaced with any number less than the constant $c = 3.394\ldots$ from Theorem 2.0.2.

2.3. Concluding Remarks

We conclude the paper by providing another infinite family of small subgroups generated by 2 for which the cancellation may be bounded by some constant. The constant is worse than that in [15], but subgroups are a bit larger.

Proposition 2.3.1. *For $q = \frac{2^{3n}+1}{2^n+1}$ we have*

$$\max_{(a,q)=1} |s(a/q)| \geq \tau - c' + O\left(\frac{1}{\sqrt{q}}\right)$$

with $c' = 4c = 4 \cdot 2\sum_{r=1}^{\infty} \sin^2\left(\frac{\pi}{2^r}\right) = 13.57\ldots$.

Observe that Theorem 2.0.4 (with $\kappa = 2$) gives in this case $\max_{(a,q)=1} |s(a/q)| < \tau - 7.11$. Thus the true value of the maximum for such q is in the range $[\tau - 13.57 - \epsilon, \tau - 7.11]$ if only n is large enough.

Proof. Obviously, we have $\mathcal{L} = 2n$ and $\tau = 6n = 3\mathcal{L}$. Next, observe that $q = 2^{2n} - 2^n + 1$ and so

$$2^{2n} \equiv 2^n - 1 \,(\mathrm{mod}\, q), \quad 2^{3n} \equiv -1 \,(\mathrm{mod}\, q), \quad 2^{5n} \equiv -2^n + 1 \,(\mathrm{mod}\, q), \quad 2^{6n} \equiv 1 \,(\mathrm{mod}\, q).$$

We are going to bound the difference between τ and the real part of the sum. We split the range of the summation into four intervals: $[0, 2n-1], [2n, 3n-1], [3n, 5n-1], [5n, 6n-1]$. We only consider the first two sums as the calculations for the other two are analogous. Using Taylor expansion of a cosine and changing the order of summation (just as in [15]), we arrive at

$$\sum_{r=0}^{2n-1} \left(1 - \cos\left(\frac{2\pi 2^r}{q}\right)\right) = -\sum_{m=1}^{\infty} \frac{(-1)^m}{2m!} \frac{(2\pi)^{2m}}{4^m - 1} \left(\frac{q + 2^n - 1}{q}\right)^{2m} + O\left(\frac{1}{q^2}\right) \tag{2.7}$$

and

$$\sum_{r=2n}^{3n-1} \left(1 - \cos\left(\frac{2\pi 2^r}{q}\right)\right) = \sum_{r=0}^{n-1} \left(1 - \cos\left(\frac{2\pi 2^r (2^n - 1)}{q}\right)\right) =$$
$$= -\sum_{m=1}^{\infty} \frac{(-1)^m}{2m!} \frac{(2\pi)^{2m}}{4^m - 1} \left(\frac{q+1}{q}\right)^{2m} + O\left(\left(\frac{2^n}{q}\right)^2\right). \tag{2.8}$$

Now we write the series as a sum of three parts as in [15]. The first part is the same for (2.7) and (2.8) and equals

$$\Sigma_1 := -\sum_{m=1}^{\infty} \frac{(-1)^m}{(2m)!} \frac{(2\pi)^{2m}}{4^m - 1} = 2\sum_{r=1}^{\infty} \sin^2\left(\frac{\pi}{2^r}\right)$$

The second part for (2.7) is equal to

$$\Sigma_2 := -\sum_{m < \sqrt{q}} \frac{(-1)^m}{(2m)!} \frac{(2\pi)^{2m}}{4^m - 1} \left(\left(1 + \frac{2^n - 1}{q}\right)^{2m} - 1\right).$$

Using $e^x - 1 \ll x$ we see that $|\Sigma_2| \ll \frac{1}{\sqrt{q}}$.

The second part for (2.8) is the same as in [15] and also smaller than $\frac{1}{\sqrt{q}}$. The third part for (2.7) and (2.8) is negligible (see [15] for details). We infer that

$$\sum_{r=2n}^{3n-1} \left(1 - \cos\left(\frac{2\pi 2^r}{q}\right)\right) = c + O\left(\frac{1}{q}\right)$$

and

$$\sum_{r=0}^{2n-1} \left(1 - \cos\left(\frac{2\pi 2^r}{q}\right)\right) = c + O\left(\frac{1}{\sqrt{q}}\right).$$

We conclude that $\tau - |\max_{(a,q)=1} |s(a/q)|| \geq 4c + O(\frac{1}{\sqrt{q}})$. □

Chapter 3

Sums of dilates

In this chapter we explore the sums of dilates. Results presented here were published in [11]. One of the classical results in additive combinatorics is Plünnecke inequality, bounding the maximal size of the set of sums of k elements of A by $K^k|A|$. One natural generalization of the problem of bounding the size of the set of sums of k elements is a problem of finding a good bound for the size of set of sums of the form $\lambda_1 a_1 + \ldots + \lambda_k a_k$ for some given integers $\lambda_1, \ldots, \lambda_k$ (in Plünnecke inequality they are all equal ± 1), where $a_1, \ldots, a_k$ are elements of A. Recalling Definition 0.0.4 we can write it down as $\lambda_1 \cdot A + \ldots + \lambda_k \cdot A$. In this case until recently there were no known bounds out of those easily following from Plünnecke inequality, namely that

$$|\lambda_1 \cdot A + \ldots + \lambda_k \cdot A| \leq K^{\sum_{i=1}^{k} |\lambda_i|}.$$

Breakthrough result was obtained in 2008 by Boris Bukh, who used binary expansion to get a bound in terms of logarithms of number $|\lambda_i|$ rather than those numbers themselves. He proved

Theorem 3.0.1 ([6]). *Let $\lambda_1, \ldots, \lambda_h$ be given integers and let $A \subset \mathbb{Z}$. If either $|A+A| \leq K|A|$ or $|A - A| \leq K|A|$, then $|\lambda_1 \cdot A + \cdots + \lambda_h \cdot A| \leq K^p|A|$ where*

$$p = 7 + 12 \sum_{i=1}^{h} \log_2(1 + |\lambda_i|)$$

In particular, this result can be presented in the following simpler form:

Corollary 3.0.2. *If $|A + A| \leq K|A|$ and $|\lambda_i| \leq 2^r$ then*

$$|\lambda_1 \cdot A + \cdots + \lambda_h \cdot A| \leq K^{O(rh)}|A|.$$

Bukh himself supposed that this result can be further improved in case where there are many summands involved. Slight improvement was recently obtained by Bush and Zhao, who proved the theorem below.

Theorem 3.0.3 ([8]). *If $|A + A| \leq K|A|$ and $|\lambda_i| \leq 2^r$ then*

$$|\lambda_1 \cdot A + \cdots + \lambda_h \cdot A| \leq K^{O\left(\frac{(r+h)^2}{\log(r+h)}\right)}|A|.$$

The main innovation in their proof is the use of graph theoretic methods. The main aim of this paper is to improve this bound using different (more direct) method.

It seems clear that if the set of λ_i coefficients have some good additive properties it should be possible to get some better bounds. Formalizing this intuition is the main focus in the second part of this chapter. This line of investigation was started by the Schoen and Shkredov, who proved the following

Theorem 3.0.4 ([26]). *Let $A \subset G$ be a finite set and $\lambda_i \in \mathbb{Z} \setminus \{0\}$. Suppose that $|A+A| \leq K|A|$, then*

$$|\lambda_1 \cdot A + \cdots + \lambda_h \cdot A| \leq e^{O(\log^8 K)(h+\log(\sum_i |\lambda_i|))}|A|.$$

The novelty here is that the result shows that the problem turns out to be much easier for some specific choice of parameters K and h, i.e. when h is sufficiently large compared to K.

3.1. Tools

Basic tools we are going to use include primarily the so called Ruzsa calculus. It consists of inequalities bounding cardinalities of certain sumsets by expressions involving other sumsets. In our arguments we are going to use the following inequality.

Lemma 3.1.1 (Sum triangle inequality, [24]). *For any finite $X, Y, Z \subset \mathbb{Z}$ we have*

$$|X+Z| \leq \frac{|X+Y||Y+Z|}{|Y|}.$$

It is analogous to classical Ruzsa triangle inequality.

Lemma 3.1.2 ([23]). *For any finite $X, Y, Z \subset \mathbb{Z}$ we have*

$$|X-Z| \leq \frac{|X-Y||Y-Z|}{|Y|}.$$

It should be remarked that in our approach we could use this inequality in place of sum triangle inequality. Using sums only makes the exposition a little bit clearer.

We are going to repeatedly use Plünnecke (Proposition 4) inequality as well as Bukh's theorem (Theorem 3.0.1).

In [26] the theorem of Sanders stated below is used to improve the bound when K is small compared to k.

Lemma 3.1.3 ([25]). *Suppose that G is an abelian group and $A, S \subset G$ are finite non-empty sets such that $|A+S| \leq K \min\{|A|, |S|\}$. Then $(A-A)+(S-S)$ contains a proper symmetric $d(K)$-dimensional coset progression P of size $\exp(-h(K))|A+S|$. Moreover, we may take $d(K) = O(\log^6 K)$ and $h(K) = O(\log^6 K \log\log K)$.*

In the same paper the following corollary is proved, which we will use to continue investigation in this line of reasoning by proving theorem 3.2.2.

Corollary 3.1.4 ([26]). *Let A be a subset of abelian group G such that $|A+A| \leq K|A|$. Then*

$$|kA| \leq \left(\frac{3ek}{K}\right)^{O(K\log^8 K)} |A|.$$

for every $k \geq K$.

Covering lemmas turn out to be very useful in bounding sums of dilates. Bukh in his proof used Ruzsa covering lemma (Lemma 0.0.17).

We use another lemma proved by Chang to improve the bounds when then set of λ coefficients has some additive structure. Recall Definition 0.0.16.

Lemma 3.1.5 (Chang covering lemma, [30]). *Suppose that G is an abelian group and $A, S \subset G$ are finite sets with $|nA| \leq K^n|A|$ for all $n \geq 1$ and $|A+S| \leq L|S|$. Then there is a set T with $|T| = O(K\log 2KL)$ such that*

$$A \subset \mathrm{Span}(T) + S - S.$$

3.2. Results

Now we state our first theorem.

Theorem 3.2.1. *Let $|A+A| \leq K|A|$ and let $|\lambda_i| < 2^r$ for $i = 1, \dots, h$. Then*

$$|\lambda_1 \cdot A + \dots + \lambda_h \cdot A| \leq K^{O\left(\frac{rh}{\log(h)} + h\log(h)\right)}|A|.$$

Proof. Without loss of generality we can assume that $h \geq 16$, since otherwise it follows from theorem 3.0.1. If $r \leq \log h$, then again the claim follows from theorem 3.0.1. We are going to show that it holds for every h and r using induction on r with additional assumption that $\lambda_1 = 1$.

Let $S_\lambda = \lambda_1 \cdot A + \dots + \lambda_h \cdot A$. Take $d = \lfloor \frac{h}{\log h} \rfloor$. Write λ_i as a sum $d\lambda_i' + \alpha_i$ with $0 \leq \alpha_i < d$. Then with $\lambda' = (1, \lambda_2', \dots, \lambda_h')$ and $\alpha = (\alpha_1, \dots, \alpha_h, d)$

$$\frac{|S_\lambda(A)|}{|A|} \leq \frac{|S_\alpha(A)|}{|A|}\frac{|S_{\lambda'}(A)|}{|A|}$$

by Ruzsa triangle inequality with $X = \alpha_1 \cdot A + \dots + \alpha_h \cdot A$, $Y = d \cdot A$ and $Z = \lambda_1' \cdot A + \dots + \lambda_h' \cdot A$.

We can bound the first term by collecting summands with the α_i and then repeatedly using Ruzsa triangle inequality. Writing k_i for the number of summands with $\alpha_j = i$ we get

$$\frac{|S_\alpha(A)|}{|A|} = \frac{|k_1 1 \cdot A + \dots + k_{d-1}(d-1) \cdot A|}{|A|} \leq$$
$$\leq \frac{|(k_1+1)A|}{|A|}\frac{|A+2\cdot A|}{|A|}\prod_{i=2}^{d-1}\left(\frac{|(k_i+2)i\cdot A|}{|A|}\frac{|i\cdot A + (i+1)\cdot A|}{|A|}\right)\frac{|d\cdot A + d\cdot A|}{|A|}$$

At each step we used Ruzsa triangle inequality twice: first time with $X_i^{(1)} = k_i i \cdot A$, $Y_i^{(1)}) = i \cdot A$ and $Z_i = k_{i+1}(i+1)\cdot A + \dots + k_{d-1}(d-1)\cdot A$ and then the second time with $X_i^{(2)} = i \cdot A$, $Y_i^{(2)} = (i+1)\cdot A$.

Using Plünnecke inequality to bound each term with repeated summand and theorem 3.0.1 to bound expressions with different summands we obtain

$$\frac{|S_\alpha(A)|}{|A|} \leq K^{\sum_{i=1}^{d-1}(k_i+2)+1} K^{O(d\log d)} \leq K^{O(2d+1+h+d\log d)}$$

By the definition of d we have

$$\frac{|S_\alpha(A)|}{|A|} \leq K^{O(h)}.$$

To bound the second term we can use induction assumption. By our additional assumption ($\lambda_1 = 1$) there will be only at most h summands. By assumption on h and the definition of d the number of bits in λ's will drop by at least $\frac{1}{2}\log h$. Hence

$$\frac{|S_\lambda(A)|}{|A|} \leq K^{O(h)} K^{O\left((r-\frac{1}{2}\log h)\frac{h}{\log h}+h\log h\right)} \leq K^{O\left(\frac{rh}{\log(h)}+h\log(h)\right)}|A|$$

Without assumption on λ_1 we can use the theorem for the set $A + \lambda_1 \cdot A + \cdots + \lambda_h \cdot A$ with $(h+1)$ summands, which contains a translate of the original set. It follows that in this case the claim holds with slightly larger constant implicit in $O()$ notation. □

Our next theorem applies to the case when K is much smaller than h. It shows that then the dependence on h becomes polynomial under those assumptions. Hence it improves on Theorem 3.0.4 in such circumstances.

Theorem 3.2.2. *Let $|A+A| \leq K|A|$ and let $|\lambda_i| < 2^r$ for $i = 1, \ldots, h$. If $h \geq K$, then*

$$|\lambda_1 \cdot A + \cdots + \lambda_h \cdot A| \leq (C(K)h^{f(K)})^r |A|,$$

where $C(K) = \frac{15e}{2K}$ and $f(K) = O(K\log^8 K)$

Proof. Again we are going to use induction on r with additional assumption that $\lambda_1 = 1$. For $r = 1$ it follows from corollary 3.1.4. To show it for greater r we use binary expansion, namely we write λ_i as a sum $2\lambda_i' + \alpha_i$ with $\alpha_i \in \{0, 1\}$. Then with $\lambda' = (1, \lambda_2', \ldots, \lambda_h')$ and $\alpha = (\alpha_1, \ldots, \alpha_h, 2)$ we have (just as in the proof of the previous theorem)

$$\frac{|S_\lambda(A)|}{|A|} \leq \frac{|S_\alpha(A)|}{|A|}\frac{|S_{\lambda'}(A)|}{|A|}.$$

We can bound the first term using corollary 3.1.4 and the fact that $2 \cdot A \subset A + A$ by

$$\frac{|S_\alpha(A)|}{|A|} \leq \frac{|(h+2)A|}{|A|} \leq \left(\frac{3e(h+2)}{K}\right)^{O(K\log^8 K)}.$$

Using induction assumption to bound the second term we get

$$\frac{|S_{\lambda'}(A)|}{|A|} \leq (C(K)h^{f(K)})^{r-1}.$$

Multiplying the last two equations we get

$$\frac{|S_\lambda(A)|}{|A|} \leq \left(\frac{3e(h+2)}{K}\right)^{O(K\log^8 K)} (C(K)h^{f(K)})^{r-1} = (C(K)h^{f(K)})^r.$$

It finishes the proof of the claim with additional assumption. We get rid of this assumption in the same way as in the previous proof. □

Our last theorem considers the case when Λ - the set of λ_i coefficients - has some additive structure. In such setting spectacular improvement is possible.

Theorem 3.2.3. *Let $|A+A| \leq K|A|$ and let $\Lambda \subset [2^r]$. Furthermore, assume that $|\Lambda+\Lambda| < L|\Lambda|$. Then*

$$|\lambda_1 \cdot A + \cdots + \lambda_h \cdot A| \leq K^{O((h+r)L\log L)}|A|.$$

Proof. By Chang covering lemmma (with $A=\Lambda$, $K=L$, $S=\{0\}$), we know that there is a set Γ such that $\Lambda \subset Span(\Gamma)$ and $|\Gamma| = O(L\log 2L)$. Write each λ_i as a sum $\lambda_i = \sum_{j=1}^{|\Gamma|} \epsilon_{i,j}\gamma_j$, where $\epsilon_{i,j} \in \{-1,1\}$ for every i,j. Then

$$|\lambda_1 \cdot A + \cdots + \lambda_h \cdot A| = |\sum_{i=1}^{h}(\sum_{j=1}^{|\Gamma|}\epsilon_{i,j}\gamma_j)\cdot A| \leq |\sum_{i=1}^{h}\sum_{j=1}^{|\Gamma|}\epsilon_{i,j}\gamma_j \cdot A| = |\sum_{j=1}^{|\Gamma|}\sum_{i=1}^{h}\epsilon_{i,j}\gamma_j \cdot A|$$

We can use Ruzsa triangle inequality twice (the first time with $X_1 = \sum_{i=1}^{h}\epsilon_{i,1}\gamma_1 \cdot A$, $Y_1 = \gamma_1 \cdot A$, $Z = \gamma_1 \cdot A \sum_{i=2}^{h}\epsilon_{i,j}\gamma_j \cdot A$, the second time with $X_2 = \gamma_1 \cdot A$ and $Y_2 = \gamma_2 \cdot A$) to bound the last expression by

$$|\sum_{j=1}^{|\Gamma|}\sum_{i=1}^{h}\epsilon_{i,j}\gamma_j \cdot A| \leq \frac{|\sum_{i=1}^{h}\epsilon_{i,1}\gamma_1 \cdot A + \gamma_1 \cdot A|}{|A|}\frac{|\gamma_1 \cdot A + \gamma_2 \cdot A|}{|A|}|\gamma_2 \cdot A + \sum_{j=2}^{|\Gamma|}\sum_{i=1}^{h}\epsilon_{i,j}\gamma_j \cdot A|$$

Using Plünnecke inequality to bound the term with repeated (up to sign) summand and Theorem 3.0.1 to bound the expression with different summands we obtain

$$|\sum_{j=1}^{|\Gamma|}\sum_{i=1}^{h}\epsilon_{i,j}\gamma_j \cdot A| \leq K^{O((h+1)+r)}|\gamma_2 \cdot A + \sum_{j=2}^{|\Gamma|}\sum_{i=1}^{h}\epsilon_{i,j}\gamma_j \cdot A|$$

Continuing in this way, we can prove by induction that

$$|\sum_{j=1}^{|\Gamma|}\sum_{i=1}^{h}\epsilon_{i,j}\gamma_j \cdot A| \leq K^{O((h+2)+r)}|\gamma_k \cdot A + \sum_{j=k}^{|\Gamma|}\sum_{i=1}^{h}\epsilon_{i,j}\gamma_j \cdot A|,$$

which for $k = |\Gamma|$ gives the claim (after another application of Plünnecke inequality). □

We conclude with a simple lemma showing once again how additive structure of Λ may influence the bounds.

Lemma 3.2.4. *For any i,j, if we take $\lambda_i' = \lambda_i \pm \lambda_j$ and $\lambda_k' = \lambda_k$ for $k \neq i$, we have*

$$\frac{|S_\lambda(A)|}{|A|} \leq K^3\frac{|S_{\lambda'}(A)|}{|A|} \tag{3.1}$$

Proof. To see this we use the fact that $S_\lambda(A) \subset S_{\lambda'} \mp \lambda_j \cdot A$. Let $\lambda_j'' = 0$ and $\lambda_k'' = \lambda_k'$ for $k \neq j$. Now we use Ruzsa triangle inequality with $X = S_{\lambda''}$, $Y = \lambda_j \cdot A$ and $Z = \lambda_j \cdot A \mp \lambda_j \cdot A$.

$$\frac{|S_\lambda(A)|}{|A|} \leq \frac{|S_{\lambda'}(A) \mp \lambda_j \cdot A|}{|A|} \leq \frac{|S_{\lambda'}(A)|}{|A|}\frac{|\lambda_j \cdot A + \lambda_j \cdot A \mp \lambda_j \cdot A|}{|\lambda_j \cdot A|}.$$

Now (3.1) follows from Plünnecke inequality. □

Bibliography

[1] L. M. Adleman, K. S. McCurley, Open problems in number theoretic complexity II. In: Algorithmic Number Theory, First nternational Symposium, ANTS I, Ithaka, NY USA, 291-322 (1994), Springer Verlag.

[2] E. Bach, J. Shallit, *Algorithmic Number Theory*, MIT Press, 1996.

[3] E. Bach, G. Miller, J. Shallit, Sums of divisors, perfect numbers and factoring, *SIAM Journal on Computing*, Vol. **15**, No. 4 (1986).

[4] L.I. Bluestein, A linear filtering approach to the computation of the discrete Fourier transform, *Northeast Electronics Research and Engineering Meeting Record* **10** (1968), 218-219.

[5] J. Bourgain, A.A. Glibichuk and S.V. Konyagin, Estimate for the number of sums and products and for exponential sums in fields of prime order, *J. London Math. Soc.* **73**(2006), 380-398.

[6] B. Bukh, Sums of dilates, *Combin. Probab. Comput.* Vol. 17, 2008, 627–639.

[7] R. J. Burthe, Jr., The average least witness is 2, *Acta Arithmetica*, **80** (1997), 327-341.

[8] A.Bush and Y. Zhao, New Upper Bound for Sums of Dilates, *The Electronic Journal of Combinatorics* **24**(3), 2017, # P3.37.

[9] R. Bystrzycki, Detection of primes in the set of residues of divisors of a given number, J. Kaczorowski et al. (Eds.): NuTMiC 2017, LNCS 10737, pp. 178–194, 2018 `https://doi.org/10.1007/978-3-319-76620-1_11`.

[10] R. Bystrzycki, Exponential sums over subgroups generated by 2, *Integers: Electronic Journal of Combinatorial Number Theory* 18, 2018, # A24.

[11] R. Bystrzycki, T. Schoen, Alternative approach to sums of dilates, *Notes on Number Theory and Discrete Mathematics* Vol. 24, 2018, Issue 2.

[12] P. Erdős, M. Kac, The Gaussian Law of Errors in the Theory of Additive Number Theoretic Functions, *American Journal of Mathematics* **62** (1940), 738-742.

[13] B.J. Green, Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak, *Current Events Bulletin of the AMS*, *arXiv*:0911.3354 (2010).

[14] B.J. Green and I.Z. Ruzsa, Sets with small sumsets and rectification, *Bull. London Math. Soc.* **38**(1) (2006), 43-52.

[15] J.Kaczorowski and G. Molteni, Extremal values for the sum $\sum_{r=1}^{\tau} e(a2^r/q)$, *J. Number Theory* **132** (2012), 2595-2603.

[16] N.H. Katz and P. Koester, On additive doubling and energy, *SIAM J. Discrete Math.* **24**(4) (2010), 1684-1693.

[17] F. Mertens, Ein Beitrag zur analytischen Zahlentheorie, *J. reine angew. Math.* **78** (1874), 46-62.

[18] D. G. Mead, Newton's Identities, *The American Mathematical Monthly* **99** (8) (1992), 749-751.

[19] G. Miller, Riemann's hypothesis and tests for primality, *Journal on Computing System Science* **13** (1976), 300-317.

[20] G. Molteni, Cancellation in a short exponential sum, *J. Number Theory* **130** (2010), 2011-2027.

[21] H. Plünnecke, Eine zahlentheorische anwendung der graphtheorie, *J. Reine Angew. Math.* **243**, 171-183, 1970.

[22] J.M. Pollard, Monte Carlo methods for index computation (mod p),*Mathematics of Computation* **32**(143) (1978), 918–924.

[23] I. Ruzsa, Sums of finite sets. In *Number Theory: New York Seminar* (1996), 281-293.

[24] I. Ruzsa, Sumsets and structure. In *Combinatorial Number Theory and Additive Group Theory*, 87-210, 2009.

[25] T.Sanders, On the Bogolyubov-Ruzsa Lemma, *Anal. PDE* Vol. 5 , 2012, 627–655.

[26] T. Schoen and I. D. Shkredov, Additive dimension and a theorem of Sanders, *J. Aust. Math. Soc.* Vol. 100, 2016, 124-144.

[27] T. Schoen, New bounds in Balog-Szemer'edi-Gowers theorem, *Combinatorica* **34**(5) (2014), 1-7.

[28] A. Schönhage, V. Strassen, Schnelle Multiplikation großer Zahlen, *Computing* **7** (1971), 281–292.

[29] V. Shoup, On the deterministic complexity of factoring polynomials over finite fields, *Information Processing Letters* **33** (1990), 261-267.

[30] T.C. Tao and H.V. Vu *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 2006.

[31] A.I. Vinogradov, The density hypothesis for Dirichlet L-series, *Izv. Akad. Nauk SSSR Ser. Mat.* (in Russian). **29** (4) (1965), 903–934.

[32] B. Źrałek, A deterministic version of Pollard's p-1 algorithm, *Mathematics of Computation*,**79** (2010), 513-533.