UNIVERSITÀ DEGLI STUDI DI TRENTO

Facoltà di Scienze Matematiche, Fisiche e Naturali

DOTTORATO DI RICERCA IN MATEMATICA

XXIII CICLO

A thesis submitted for obtaining the degree of Doctor of Philosophy

Luca Goldoni

PhD Thesis

PRIME NUMBERS
AND
POLYNOMIALS

Advisor:
Prof. Alberto Perelli

Academic Year 2009 - 2010

Abstract

This thesis deals with the classical problem of prime numbers represented by polynomials. It consists of three parts. In the first part I collected many results about the problem. Some of them are quite recent and this part can be considered as a survey of the state of art of the subject. In the second part I present two results due to P. Pleasants about the cubic polynomials with integer coefficients in several variables. The aim of this part is to simplify the works of Pleasants and modernize the notation employed. In such a way these important theorems are now in m a more readable form. In the third part I present some original results related with some algebraic invariants which are the key-tools in the works of Pleasants. The hidden diophantine nature of these invariants let them very difficult to study. Anyway some results are proved. These results let the results of Pleasants somewhat more effective.

Acknowledgments

First off, thank you to my advisor, Professor Alberto Perelli. His very broad knowledge of Analytic Number Theory and his hands-on approach to theory have provided me with many wonderful opportunities to learn. I am especially grateful for his patience with all manner of questions. His commitment to communicating mathematics clearly and energetically to a variety of audiences is a true model for me. Equally, thank you to Professor Edoardo Ballico for his role as a mentor, mathematical resource and teacher have been invaluable to me. Thank you to Professor Italo Tamanini, Professor Domenico Luminati and Professor Stefano Baratella, for encouraging me to pursue Mathematics as a graduate student and giving me not only many and many mathematical support but their friendship also. A special thank you to Professor Lucia Beretta: Her continuing belief in me and her thoughtful advice throughout this journey have been touchstones for me. Thank you to the Università di Trento Mathematics Department, faculty, staff and fellow graduate students for making this a wonderful place to study and work. Thank you to the Head of Liceo Scientifico "A.F. Formiggini", Professor Salvatore Manco, for encouraging me to pursue graduate studies after many years since my Laurea's Diploma. Last but not least, I am also indebted with my wife and my daughter for their patience during these years. Without their sympathy I can not finish this enterprise. Although she is not still alive, I would like to express also a special thank you to my High School Mathematics teacher, Professor Giuseppina Rovatti: from her I received my first Mathematical Education and more than this, the Love for Mathematics.

"*All men dream: but not equally.*
Those who dream by night in the dusty recesses of their minds
wake in the day to find that it was vanity:
but the dreamers of the day are dangerous men,
for they may act their dream with open eyes to make it possible. This I did."

T.E. Lawrence (Lawrence of Arabia) Seven Pillars of Wisdom

To my wife
Gloria Isabella Mandagie
and my daughter
Lucia Goldoni
as well as
to the Memory of my Parents.

Contents

Part I

Some background

Chapter 1

Polynomials in one variable

1.1 Introduction

Since form the time of Euclid it is known that there exists an infinite set of prime numbers. The proof by Euclid [11] is the following: assume there are only finitely many primes, say $p_1...p_m$ and consider the number

$$Q = \prod_{k=1}^{m} p_k + 1.$$

Either Q is prime or there exists a prime q such that $q|Q$. If Q is prime we have a contradiction because $Q > p_k$ for every $k = 1...m$. If Q is not a prime it follows that $q \neq p_k$ for $k = 1...m$ because none of the primes among p_k divides Q. So even in this case we have a contradiction. If we read the result in a different way, we can say that among the polynomials in one variable, there exists one which assumes infinitely many prime values, namely $P(x) = x$. It is natural ask if this result can be generalized in some way. Actually in some special cases, if one try to imitate Euclid's method, it is possible to prove that polynomials of the form P(x)=$mx+q$ with $a, b \in \mathbb{N}$ and $(a, b) = 1$ contains infinitely many primes among their values. For instance Euclid's method is working with the polynomial $P(x) = 4x + 3$. Many other special cases are tractable with elementary arithmetic methods,[1] but so far no purely arithmetic proof is known in the general case.

[1] See [27] for a characterization of arithmetic progressions which are tractable with some extent of the Euclidean proof.

1.2 Primes in arithmetic progressions

The first correct proof for the general case of an arithmetical progression, goes back to Dirichlet [10] after a faulty proof by Legendre [20]. Dirichlet proved that

$$P(x) = qx + a.$$

the condition $(a, q) = 1$ is necessary and sufficient in order to takes infinitely many prime values. Dirichlet's original proof of this theorem is analytic and non-elementary: this means that tools from Complex Analysis has been used. An "elementary" proof was found, much later, by Selberg [37]. The word "elementary", in this case, is a short-cut for the statement"without the use of Complex Analysis" and it does not mean, in any way, "simple". Actually it is rather complicated. The Dirichlet's proof is a very deep and broad generalization of an Euler's idea. I shall try to get a very basically sketch of it.

1.2.1 Sketch Proof of Dirichlet's Theorem

- Euler [12] defined the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad s \in \mathbb{R}, \;\; s > 1. \tag{1.1}$$

  and he showed that it has a deep and profound connection with prime numbers. Namely, due to **unique factorization** in the ring of integers the following formula hold:

$$\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \qquad s \in \mathbb{R}, \;\; s > 1.$$

- Euler considered

$$\lim_{s \to 1^+} \zeta(s).$$

  and due to the divergence of harmonic series, he was able to show that

$$\lim_{s \to 1^+} \log \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} = \infty.$$

  Upon taking logarithms of both sides in (1.1) and discarding negligible terms, this implies that

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty.$$

This of course implies that the set of primes in infinite and, for the first time provides an analytic method to deal with similar problems. That's why it mark's the beginning of **Analytic Number Theory**.

- Dirichlet generalized Euler's method but he had to set some non trivial modifications to it. The main reason for this is that, while the characteristic function of the progression $P(x) = 2x + 1$ is totally multiplicative and leads to the "Euler product" as in the ζ function, the the characteristic functions of any other arithmetic progression has no longer this property.

- In order to overcome this problem, Dirichlet introduced a special kind of functions now called "**Dirichlet characters**"which may regarded as a sort of "**arithmetical harmonics**" in the sense that they play the role of what we now call "**an orthogonal basis in a finite Fourier Analysis context**. I shall quote definition and the most important properties of the characters.

  - **A completely multiplicative arithmetic periodic function**

    $$\chi : \mathbb{Z} \to \mathbb{C}.$$

    with period m that is not identically zero is called a **Dirichlet character with conductor** q.
  - For every m there are exactly $\varphi(q)$ Dirichlet characters where $\varphi(q)$ stands for the Euler's totient function.
  - The character

    $$\chi_0(n) = \begin{cases} 1 & if \quad (n, m) = 1 \\ 0 & otherwise. \end{cases}$$

    is called "**principal character**"
  - The Dirichlet characters with conductor q form a **multiplicative group** with $\phi(q)$ elements and identity element χ_0
  - For every character χ and every character χ' we have

    $$\frac{1}{\phi(q)} \sum_{n \,(\bmod\, q)} \chi(n)\overline{\chi'}(n) = \begin{cases} 1 \;\; if\, \chi = \chi' \\ 0 \;\; otherwise. \end{cases} \tag{1.2}$$

- For every character χ and for every integers n, a,we have

  $$\frac{1}{\phi(q)} \sum_{\chi \,(\bmod\, q)} \chi(n)\overline{\chi}(a) = \begin{cases} 1 \;\; if\, n \equiv a \;(\bmod q) \\ 0 \;\; otherwise. \end{cases} \tag{1.3}$$

- The relations (1.2) and (1.3) are called **"Orthogonality Relations"** and in some sense they let us remember the well known orthogonality relations in **Classical Fourier Analysis**.

- For each character Dirichlet defined the function

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \qquad s \in \mathbb{R} \quad s > 1.$$

  The series on the right hand side is a special cases of more general series called Dirichlet series.

- For each L-series we have

$$L(s,\chi) = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \quad s > 1.$$

  because χ is totally multiplicative.

- Moreover we have

$$\log L(s,\chi) = \sum_{p\in\mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{sk}} \ .$$

- Using the orthogonality relations we have

$$\frac{1}{\phi(q)} \sum_{\chi} \overline{\chi}(a) \log L(s,\chi) = \sum_{p\in\mathbb{P}} \sum_{k=1}^{\infty} \sum_{p^k \equiv a \ (\mathrm{mod}\ q)} \frac{1}{kp^{sk}} \ .$$

  and from this, after some calculations

$$\frac{1}{\phi(q)} \sum_{\chi} \overline{\chi}(a) \log L(s,\chi) = \sum_{p \equiv a \ (\mathrm{mod}\ q)} \frac{1}{p^s} + O(1). \tag{1.4}$$

  as $s \to 1^+$.

- It is quite easy to show that

$$L(s,\chi_0) = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right) \ .$$

  and so that

$$\lim_{s\to 1^+} L(s,\chi_0) = \infty.$$

- If one is able to show that $\chi \neq \chi_0$ imply $L(1,\chi) \neq 0$ for all χ of conductor m, then immediately it follows that there are infinitely many primes p of the form $p \equiv a(\mod q)$. So this is the crux of Dirichlet's proof. The difficult part of Dirichlet's proof is showing $L(1,\chi) \neq 0$ for **real characters** i.e for characters which take only real values. Anyway Dirichlet was able to do this and produced a valid proof. At the present, for polynomials in **one variable**, this is **the only case** where it is possible to reach a result of this kind. Not only it is not known any example of a polynomial in one variable with degree $d > 1$ producing infinitely many primes but even worse, it is not known if a such polynomial does exists. In other words, even no result of "**pure existence** " (possibly non-constructive) is known. Roughly speaking, in handling such a kind of polynomials, the difficulties arise from the fact that the values of them are "widely scattered" among the integers. For this kind of polynomials there are, at the present, only conjectures as illustrated in the following section.

1.3 Conjectures

1.3.1 The conjecture of Bouniakowsky

Let $P(x) \in \mathbb{Z}[x]$: in order to represent infinitely many primes, trivially, it must be irreducible. However this conditions is by no means enough to ensure that the range of the polynomial contains an infinite subset of primes. In order to show why it is so, one can consider the following simple example:

Example 1.1. *Let $P(x) = x^2 + x + 2$. This is an irreducible polynomial in $\mathbb{Z}[x]$ but his values are all even because if we write*

$$P(x) = x\,(x+1) + 2.$$

we notice that the right hand side is the sum of two even numbers.

In 1857 **Bouniakowsky** [2] made a conjecture concerning prime values of polynomials that would, for instance, imply that $P(x) = x^2 + 1$ is prime for infinitely many integers x.

Conjecture 1.1. *Let $P(x)$ be a polynomial in $\mathbb{Z}[x]$ and define the fixed divisor of $P(x)$, written $d(P)$, as the largest integer d such that d divides $P(x)$ for all integers x. If $P(x)$ and $d(P) = 1$ is nonconstant and irreducible over the integers, then there exist infinitely many integers x such that $P(x)$ is a prime.*

1.3.2 The conjecture of Dickson

In [9] Dickson stated the following conjecture

Conjecture 1.2. *Let*

$$\mathfrak{L} = \{P_j(x) = q_j x + a_j \in \mathbb{Z}[x] \ , \ \ \forall \ j = 1 \cdots k\} .$$

any finite set of linear polynomials with $q_j \geq 1$ and $(q_j, a_j) = 1$ for every $j = 1...k$. Suppose that no integer $m > 1$ divides $P_(x)P_2(x)...P_k(x)$ for every $x \in \mathbb{N}$. Then there are infinitely many natural numbers n for which all the numbers $P_1(n)...P_k(n)$ are simultaneously primes.

1.3.3 The conjecture of Schinzel and Sierpinski

In [35] Schinzel stated the following conjecture better known as " **Schinzel's hypothesis H**" which is a wide generalisation of a Dickson's conjecture.

Conjecture 1.3. *Let*

$$\mathfrak{P} = \{P_j(x) \in \mathbb{Z}[x] \ , \ j = 1 \cdots k\} .$$

any finite set of irreducible polynomials in one variable with positive leading coefficients . Suppose that no integer $m > 1$ divides $P_(x)P_2(x)...P_k(x)$ for every $x \in \mathbb{N}$. Then there are infinitely many natural numbers n for which all the numbers $P_1(n)...P_k(n)$ are simultaneously primes.

1.3.4 The conjecture of Bateman and Horn

In [1] Bateman and Horn made the following

Conjecture 1.4. *Let*

$$\mathfrak{P} = \{P_j(x) \in \mathbb{Z}[x] \ , \ j = 1 \cdots k\} .$$

any finite set of polynomials in one variable with positive leading coefficients, and of degree $h_1...h_k$ respectively. Let each of these polynomials is irreducible over the field of rational numbers and no two of them differ by a constant factor. Let

$$\mathcal{A} = \{n \in \mathbb{N} : \ 1 \leq n \leq N, \ P_j(n) \in \mathbb{P} \ \forall j = 1 \cdots k \} .$$

Finally, let

$$Q = Q(P_1, \cdots P_k; N) = |\mathcal{A}| .$$

then

$$Q \sim (h_1 \cdots h_k)^{-1} C(P_1, \cdots P_k) \int_2^N \frac{1}{\log^k(t)} dt. \tag{1.5}$$

where

$$C(P_1, \cdots P_k) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{w(p)}{p}\right).$$

being $w(p)$ the number of solutions x of the congruence

$$P_1(x)P_2(x)\cdots P_k(x) \equiv 0 \mod p.$$

with $1 \leq x \leq p$.

The heuristic argument in support of (1.5)essentially amounts to the following. From the PNT, in some sense, the chance that a large positive integer m is prime is around $\frac{1}{\log m}$. Since

$$P_j(n) = a_{0j}n^{h_j} + a_{1j}n^{h_j-1} + \ldots a_{h_jj} = a_{0j}n^{h_j}\left(1 + \frac{a_{1j}}{a_{0j}n} + \cdots \frac{a_{h_jj}}{a_{0j}n^{h_j}}\right).$$

we have that and so $\log P_j(n) \approx h_j \log n$. If we could treat the values of these polynomials at n as independent random variables, then the chance that they would be simultaneously prime at n would be

$$\prod_{j=1}^{k} \frac{1}{\log P_j(n)} = \prod_{j=1}^{k} \frac{1}{h_j \log n} = (h_1 \cdots h_k)^{-1} \log^{-k}(n).$$

and hence we would expect

$$Q \approx (h_1 \cdots h_k)^{-1} \sum_{n=2}^{N} \log^{-k}(n). \tag{1.6}$$

However, the polynomials $P_1 ... P_k$ are unlikely to behave both randomly and independently. For example, if $P_1(x) = x$ and $P_2(x) = x + 2$ we have that either $P_1(n), P_2(n)$ are both even or they are both odd. Thus for each prime p we must apply a correction factor $k_p = r_p/s_p$ where

- r_p is the chance that for random n none of the integers $P_1(n), ...P_k(n)$ is divisible by p.
- s_p is the chance that none of the integers in a random k-tuple is divisible by p.

If we remember the meaning of $w(p)$,we have that

$$r_p = \frac{p - w(p)}{p} = 1 - \frac{w(p)}{p}.$$

Moreover

$$s_p = \left(1 - \frac{1}{p}\right)^k.$$

because the chance of x_j being divisible by p is $1/p$ and we have that the element of the k-tuple are independent. So the correction factor for (1.6) is

$$C\left(P_1, \cdots P_k\right) = \prod_p k_p = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{w\left(p\right)}{p}\right).$$

which leads to

$$Q \sim \left(h_1 \cdots h_k\right)^{-1} C\left(P_1, \cdots P_k\right) \sum_{n=2}^{N} \frac{1}{\log^k(t)}.$$

which is essentially the same as the approximation given in (1.5). The conjecture of Bateman-Horn is stronger than the conjecture of Bouniakowsky and is a quantitative version of the conjectures of Schinzel and Sierpinski. The truth of this conjecture is known only in the case $n = 1$. In this case the conjecture is equivalent to the Dirichlet's theorem.

1.3.5 The Hardy-Littlewood Circle Method

I shall get an informal introduction to the Hardy-Littlewood Circle Method. At this stage the main purpose of this introduction is to explain the tool by means of which Hardy and Littlewood were able to formulate some conjectures about polynomials. The Circle Method is a clever idea for investigating many problems in additive number theory. It originated in investigations by Hardy and Ramanujan [14] on the partition function $p(n)$. Now it is a foundamental tool in Analytic Number Theory and in particular in Additive Number Theory. Consider the problem of writing n as a sum of s perfect k-powers. If $k = 1$ there is a quite simple combinatorial solution: the number of ways of writing n as a sum of s non-negative integers is

$$r_{1,s}(n) = \left(\begin{array}{c} n + s - 1 \\ s - 1 \end{array} \right).$$

Unfortunately, the combinatorial argument does not generalize to higher k. There is another method, of analytical type which solves the $k = 1$ case and can be generalized. Let $z \in \mathbb{C}$ with $|z| < 1$, then the series

$$f(z) = \sum_{m=0}^{\infty} z^m.$$

is convergent and we have

$$f(z) = \frac{1}{1-z}.$$

From now on, we shall call this function as "**generating function**". Let $r_{1,s}(n)$ denote the number of solutions to the equation

$$m_1 + \cdots m_s = n.$$

where each m_i is a non-negative integer. We claim that

$$(f(z))^s = \left(\sum_{m_1=0}^{\infty} z^{m_1}\right) \cdots \left(\sum_{m_s=0}^{\infty} z^{m_s}\right) = \sum_{n=0}^{\infty} r_{1,s}(n) z^n. \tag{1.7}$$

This follows by expanding the product in (1.7) and collecting the products

$$z^{m_1} \cdots z^{m_s} = z^{m_1 + \cdots m_s}.$$

of the same degree $n = m_1 + ...m_s$. On the other hand, we have

$$(f(z))^s = \left(\frac{1}{1-z}\right)^s = \frac{1}{(s-1)!} \frac{d^{s-1}}{dz^{s-1}} \left(\frac{1}{1-z}\right).$$

and so

$$(f(z))^s = \frac{1}{(s-1)!} \frac{d^{s-1}}{dz^{s-1}} \left(\sum_{n=0}^{\infty} z^n\right) = \sum_{n=0}^{\infty} \left(\begin{array}{c} n+s-1 \\ s-1 \end{array} \right) z^n.$$

which yields

$$r_{1,s}(n) = \left(\begin{array}{c} n+s-1 \\ s-1 \end{array} \right).$$

Actually, it is easy to see that all series does converge so this kind of approach is not only formal but analytical and, more important, this method of proof can be generalized. I shall try to get a very basically sketch of it. Let A some given subset of $\mathbb{N}$ and s a positive integer. We define the formal series

$$F_A(z) = \sum_{a \in A} z^a.$$

and we call it, as before, "generating function". Next, we write

$$(F_A(z))^s = \left(\sum_{a \in A} z^a \right)^s = \sum_{n=1}^{\infty} r\,(n, s, A) z^n.$$

It is not hard to prove that $r(n; s, A)$ is the number of ways of writing n as a sum of s elements of A. In order to extract individual coefficients from a power series we have the following standard fact from Complex Analysis. As it is well known if γ stand for the unit circle of center O in the complex plane, oriented counter-clockwise then

$$\frac{1}{2\pi i} \int_{\gamma} z^n dz = \begin{cases} 1 & if\ n = -1 \\ 0 & otherwise. \end{cases}$$

so, if we have a power series with radius of convergence **larger than one**,

$$G(z) = \sum_{k=0}^{\infty} a_k z^k.$$

then

$$\frac{1}{2\pi i} \int_{\gamma} G(z) z^{-(n+1)} dz = a_n.$$

Consequently, if for a while we ignore convergence problems this result yields

$$r\,(n, s, A) = \frac{1}{2\pi i} \int_{\gamma} (F_A(z))^s\, z^{-(n+1)} dz.$$

An alternative, but equivalent, formulation is to consider a different generating function for A. If we set

$$e\,(\alpha) = e^{2\pi i \alpha}.$$

the immediately we see that

$$\int_0^1 e\,(n\alpha)\, e\,(-m\alpha) d\alpha = \begin{cases} 1 & if\ n = m \\ 0 & otherwise. \end{cases}$$

Now we have that the generating function is

$$f_A(\alpha) = \sum_{a \in A} e\,(a\alpha).$$

and

$$\int_0^1 (f_A(\alpha))^s e(-n\alpha)\, d\alpha = r(n,s,A).$$

again, ignoring for now any convergence problems. If we can evaluate the above integral, not only will we know which n can be written as the sum of s elements of A, but we will know in how many ways. This is the basic formal context for the circle method. Now we turn to convergence issues. If A is an infinite subset [2] the defining series for the generating function $f_A(x)$ need not converge, or may not have a large enough radius of convergence. We get around this trouble in the following way: for each N, we define

$$A_N = \{a \in A : a \leq N\}.$$

For each N, we consider the truncated generating function attached to A_N:

$$f_N(\alpha) = \sum_{a \in A_N} e(a\alpha).$$

As $f_N(\alpha)$ is a finite sum, all the convergence issues vanish. A similar argument as before yields

$$(f_A(\alpha))^s = \sum_{n \leq sN} r_N(n,s,A) e(n\alpha).$$

where, in this case, $r_N(n,s,A)$ is the number of ways of writing n as the sum of s elements of A with each element **at most** N. But if $n \leq N$ then

$$r_N(n,s,A) = r(n,s,A).$$

because no element of A greater than n is used in representing n. So we have proved

Proposition 1.1. *If $n \leq N$ then*

$$r(n,s,A) = r_N(n,s,A) = \int_0^1 (f_N(\alpha))^s e(-n\alpha)\, d\alpha. \tag{1.8}$$

However, having an integral expression for $r_N(n,s,A)$ is not enough: we must be able to evaluate the integral either exactly, or at least bound it away from zero. We notice that $f_N(\alpha)$ is defined as a sum of A_N terms, each of

[2] If A is finitewe can just enumerate $a_1 + ...a_s$ in a finite number of steps.

absolute value 1 but if this terms does have a "random" distribution on the unit circle, the size of $|f_N(\alpha)|$ should be much smaller than the trivial upper bound N. This is the so called "**Philosophy of Square-root Cancellation**": in general, if one adds a "random" set of N numbers of absolute value 1, the sum could be as large as N, but often is roughly at most of size $\sqrt{N}$. [3] In many problems, for most $\alpha \in [0,1]$ the size of $f_N(\alpha)$ is about $\sqrt{N}$ while for special $\alpha \in [0,1]$, the size of $f_N(\alpha)$ is about $|N|$. We expect the main contribution to come from $\alpha \in [0,1]$ where $f_N(\alpha)$ is large so

1. **If the contribution of the set of these α can be evalutated**.
2. **If we can show that the contribution of the remaining α is smaller**.

then we will have that $r_N(n,s,A)$ is bounded **away from zero**. In order to do this we split $[0,1]$ into two disjoint subsets: the so called the **Major arcs** $\mathcal{M}$ and **Minor arcs** m. So

$$r(n,s,A) = \int_{\mathcal{M}} (f_N(\alpha))^s e(-n\alpha)\, d\alpha + \int_m (f_N(\alpha))^s e(-n\alpha)\, d\alpha.$$

The construction of $\mathcal{M}$ and m depend on N and the problem under investigation. On the Major arcs $\mathcal{M}$ we must be able to find a function which, up to lower order terms, agrees with $(f_N(\alpha))^s$ and is easily integrated. This will be the contribution over the Major arcs and must be of a "good shape" away from zero and possibly tends to infinity with N. After, we must be able to show that the "Minor arcs" contribution is of lower order than the "Major arcs" as $N \to \infty$. The last is the most difficult step because often it is highly non-trivial to obtain the required cancellation over the Minor arcs. Just to mention one among the most famous example of application of the Circle Method we quote the Vinogradov's Three primes Theorem, where $A = \mathbb{P}$ and $s = 3$. So every large odd number is the sum of three primes. So far no one was able to apply the method to the case $A = \mathbb{P}$ and $s = 2$ and solve the Goldbach binary conjecture. In all Circle Method investigations, the contribution from the Major arcs is of the form

$$\mathfrak{S}(N) f(N).$$

where $f(N)$ is a"simple function like N^δ or $N^\delta log(N)$ or something like that and $\mathfrak{S}(N)$ is a series which is called the **Singular Series** of the problem. The Singular Series encodes the arithmetical properties (and difficulties) of the problem and, as general rule, we must be able to show that $\mathfrak{S}(N) > 0$ in order to obtain non trivial results.

[3] This is what happens, for instance, in the Theory of Random walks on integers.

Note 1.1. *We briefly comment on the terminology: we have been talking about the Circle Method and arcs, but where is the circle? As we mentioned before Hardy and Ramanujan devised the circle method in order to study the partition problem which generating function is*

$$F(z) = \frac{1}{(1-z)(1-z^2)(1-z^3)\cdots} = 1 + \sum_{n=1}^{\infty} P(n) z^n.$$

If, for a while, we ignore convergence issues, we need to consider

$$P(n) = \frac{1}{2\pi i} \int_{\gamma} F(z) z^{-n-1} dz.$$

The integrand is not defined at any point of the form

$$z_{a,q} = e\left(\frac{a}{q}\right).$$

The idea is to consider a small arc around each of such point where $|F(z)|$ is large. At least intuitively one expects that the integral of $F(z)$ along these arcs should be the major part of the integral.Thus, we break the unit circle into two disjoint sets, the Major arcs (where we expect the generating function to be large), and the Minor arcs (where we expect the function to be small). While many problems proceed through generating functions that are sums of exponentials, as well as integrating over $[0,1]$ instead of a circle, we keep the original terminology.

1.3.6 The conjectures of Hardy and Littlewood

In a famous paper [13], with the use of Circle Method, Hardy and Littlewood developed a number of conjectures concerning, among others, some conjectures related with polynomials and prime numbers.

Conjecture 1.5. *If a b c are integers and*

1. *$a > 0$.*
2. *$(a, b, c) = 1$.*
3. *$a + b$ and c are not both even.*
4. *$\Delta = b^2 - 4ac$ is not a square in $\mathbb{Z}$.*

if $\pi_{a,b,c}(x)$ *denotes the number of primes of the form* an^2+bn+c*, then*

$$\pi_{a,b,c}(x) \sim \frac{\varepsilon C\sqrt{x}}{\sqrt{a}\log x}\prod_{p\geq 3}\left(\frac{p}{p-1}\right).$$

where

$$\varepsilon = \begin{cases} 1 \ \ if\, 2 \not| a+b \\ 2 \ if\, 2|a+b. \end{cases}$$

and

$$C = \prod_{\substack{p\geq 3 \\ p\not| a}}\left(1-\frac{1}{p-1}\left(\frac{\Delta}{p}\right)\right).$$

being $\left(\frac{\Delta}{p}\right)$ *the Legendre's symbol.*

In particular, for primes of the form n^2+1 they obtained

Conjecture 1.6.

$$\pi_1(x) \sim \mathfrak{S}\frac{\sqrt{x}}{\log x}.$$

where

$$\mathfrak{S} = \prod_{p\geq 3}\left(1-\frac{1}{p-1}\left(\frac{-1}{p}\right)\right).$$

Finally

Conjecture 1.7. *There are infinitely many prime pairs* n^2+1*,* n^2+3 *and if* $\pi_2'(x)$ *denotes the number of such pairs less than* x *then*

$$\pi_2'(x) \sim 6\frac{\sqrt{x}}{\log^2 x}\mathfrak{S}.$$

where

$$\mathfrak{S} = \prod_{p\geq 5}\left(\frac{p-\upsilon(p)}{(p-1)^2}\right).$$

and where $\upsilon(p)$ *denotes the number of quadratic residues* $\bmod p$ *in the set* $\{-1,-3\}$.

In all these cases, so far, it is not possible to obtain good extimates for the contribution of Minor Arcs.

Chapter 2

Polynomials in several variables

2.1 Quadratic polynomials

The prime numbers that can be written in the form m^2+n^2 were characterized around 300 years ago by Fermat. No prime $q \equiv 3 \mod 4$ can be a sum of two squares, and Fermat proved that every prime $q \equiv 1 \mod 4$ can be written as $p = m^2 + n^2$. In the eighteenth and nineteenth centuries,thanks to the efforts of Lagrange and Gauss, this result was found to be a special case of a more general result: given any irreducible binary quadratic form

$$\phi(m, n) = am^2 + bmn + cn^2.$$

with integral coefficients the primes represented by ϕ are characterized by congruence and class group conditions. With this situation, following the on prime counting by Dirichlet, Hadamard, and Valleé-Poussin, it is possible to give asymptotic formulae for the number of primes up to x, which are represented by such a form. If we exclude a minority of ϕ that fail to satisfy some local condition and hence cannot represent more than one prime, we find that a **positive density** of all primes are represented by such a form. For more general polynomials we cannot expect such a simple characterization. In the case of two variables the result is known for general quadratic polynomials as given by a paper of Iwaniec [16]. Let

$$P(m, n) = am^2 + bmn + cn^2 + em + fn + g.$$

be a primitive polynomial with integer coefficients. If $P(m, n)$ is reducible in $\mathbb{Q}[, m, n]$ the question whether it represents infinitely many primes can be settled using Dirichlet's theorem on arithmetic progression. If $P(m, n)$ is irreducible the following theorem complete the frame:

Theorem 2.1. *(Iwaniec)Let*

$$P(m,n) = am^2 + bmn + cn^2 + em + fn + g \in \mathbb{Z}\left[m,n\right].$$

with

- $\deg P = 2$.
- $(a,b,c,e,f,g) = 1$.
- $P[m,n]$ *irreducible in* $\mathbb{Q}[m,n]$.
- $\frac{\partial P}{\partial m}, \frac{\partial P}{\partial n}$ *linearly independent.*
- P *represent arbitrarily large odd numbers.*

If

$$D = af^2 - bef + ce^2 + \left(b^2 - 4ac\right)g = 0.$$

or $\Delta = b^2 - 4ac$ *is a perfect square then*

$$\frac{N}{\log N} \ll \sum_{\substack{p \leq N \\ p = P(m,n) \\ p \in \mathbb{P}}} 1.$$

If

$$D = af^2 - bef + ce^2 + \left(b^2 - 4ac\right)g \neq 0.$$

and $\Delta = b^2 - 4ac$ *is not a perfect square then*

$$\frac{N}{\log^{3/2} N} \ll \sum_{\substack{p \leq N \\ p = P(m,n) \\ p \in \mathbb{P}}} 1 \ll \frac{N}{\log^{3/2} N}.$$

2.2 Higher degree polynomials

In trying to understand what happens with polynomials in more than one variable and degree higher than two, one needs to be rather careful even in formulating conjectures concerning the representation of primes by such a kind of polynomials, as the next example shows

Example 2.1. *(Heath-Brown) Let*

$$P(m,n) = \left(n^2 + 15\right)\left\{1 - \left(m^2 - 23n^2 - 1\right)^2\right\} - 5.$$

then

- *$P(m,n)$ takes arbitrarily large positive values for $m,n \in \mathbb{Z}$.*
- *$P(m,n)$ is irreducible.*
- *$P(m,n)$ takes values co-prime to any prescribed integer or in other words it does not have fixed divisors.*

However $P(m,n)$ ***does not take any positive prime value*** *(see Appendix A for more details)*

If the degree of the polynomials in several variables is greater than two, only very special cases are known. The most relevant results in this directions are:

Theorem 2.2. *(Friedlander-Iwaniec)[17] If Λ denotes the von Mangoldt function then*

$$\sum_{\substack{a>0 \\ a^2+b^4 \leq x}} \sum_{b>0} \Lambda\left(a^2+b^4\right) = 4\pi^{-1}\kappa x^{3/4}\left\{1+O\left(\frac{\log\log x}{\log x}\right)\right\}.$$

as $x \to \infty$, where

$$\kappa = \int_0^1 \left(1-t^4\right)^{\frac{1}{2}} dt.$$

Theorem 2.3. *(Heath-Brown)[15] There is a positive constant c such that, if*

$$\eta = \eta(x) = (\log x)^{-c}.$$

then

$$\sum_{\substack{x<a\leq x(1+\eta) \\ x<b\leq x(1+\eta) \\ a^3+2b^3 \in P}} 1 = \sigma_0 \frac{\eta^2 x^2}{3\log x}\left\{1+O\left((\log\log x)^{-1/6}\right)\right\} \quad .$$

as $x \to \infty$, where

$$\sigma_0 = \prod_p \left(1-\frac{w(p)-1}{p}\right).$$

and $w(p)$ denotes the number of solutions of the congruence $X^3 \equiv 2 \mod p$

In the proof of both these theorems parity sensitive sieve methods have been used. For a very basic introduction of Sieve Methods see Appendix B.

Note 2.1. *In measuring the quality of any theorem on the representation of primes by a polynomial $P \in \mathbb{Z}[x_1...x_n]$ it is useful to consider the exponent $\alpha(P)$,defined as follows. Let Q denote the polynomial obtained by replacing each coefficient of P by its absolute value and let*

$$A(X) = \{(x_1, \dots x_n) \in N^n : Q(x_1, \dots x_n) \leq X\}.$$

Define

$$\alpha = \alpha(P) = \inf\{\alpha \in R : |A(X)| \ll X^{\alpha}, X \to \infty\}.$$

In some sense $\alpha(P)$ measures the "frequency" of values taken by P. If $\alpha(P) \geq 1$ we expect P to represent, for every $\varepsilon > 0$, at least $X^{1-\varepsilon}$ of the integers up to X, while if $\alpha(P) < 1$ we expect around X^{α} such integers to be representable. Thus the smaller the value of $\alpha(P)$, the harder it will be to prove that P represents primes. For the theorem of Dirichlet we have $\alpha = 1$ as well as for binary quadratic forms. For the theorem of Friedlander and Iwaniec we have $\alpha = 3/4$ while for the theorem of Heath-Brown we have $\alpha = 2/3$. The conjecture about $P(x) = x^2 + 1$ has $\alpha = 1/2$.

Note 2.2. *If we have a polynomial in more than one variable, the degree of polynomial is not a good "measure" of the quality of results about the representation of primes. For example the following Proposition is true but it is nearly to be trivial*

Proposition 2.1. *For every $k \in \mathbb{N}$, $k \geq 1$ there exist a polynomial $F(x_1, x_2, x_3) \in \mathbb{Z}[x_1, x_2, x_3]$ of degree $k+1$ such that it represent infinitely many positive primes.*

Proof. It is enough to choose

$$F(x_1, x_2, x_3) = 3x_1 x_3^k + x_2(x_2 + 1).$$

and then fix $x_2 = 1$. We obtain

$$F(x_1, x_2, 1) = 3x_1 + x_2(x_2 + 1).$$

Let $f(x_2) = x_2(x_2 + 1)$. We have that $2|f(x_2)$ for every $x_2 \in \mathbb{Z}$ and hence, if we choose $\overline{x_2} \equiv 1 \pmod 3$ we have that $(3, f(\overline{x_2})) = 1$ and so, by the Theorem of Dirichlet on arithmetic progression, it follows that

$$g(x_1) = F(x_1, \overline{x_2}, 1).$$

is prime for infinitely many $x_1 \in \mathbb{Z}$ and so F represent infinitely many primes. □

2.3 Primes in non-polynomial sequences with low density

In a paper published in 1953 Piatetski-Shapiro [30] proved the following theorem, now known as "Piatetski-Shapiro Prime Number Theorem"

Theorem 2.4. *(Piatetski-Shapiro) Let c a real number such that $1 < c < 12/11$ and let $n \in \mathbb{N}$. If*

$$q_n = [n^c]\,.$$

where, as usual $[n^c]$ denotes the integral part of n^c, then for infinitely many values of n q_n is a prime number, and, moreover, if

$$\pi_c\,(x) = \sum_{\substack{p \leq x \\ p \in P \\ p = [n^c]}} 1.$$

then

$$\pi_c\,(x) \sim \frac{x}{c \log x}.$$

This theorem is very interesting because it is the **first example** of a sequence with density lower than one which produce infinitely many primes although it is not a polynomial. By the way, the admissible value for c has been improved a bit over the years. In particular: in [23] H.Q. Liu and J.Rivat proved that it is possible to take $1 < c < 15/13$. A very interesting result is due to Hongze Li [21] where he proved the following

Theorem 2.5. *(Hongze Li) Let $1 \leq c < \frac{23}{21}$ and let*

$$\mathbb{P}_c = \{p \in \mathbb{P} : \exists n \in N, p = [n^c]\}\,.$$

If

$$T(n) = \sum_{\substack{p_1 + p_2 = n \\ p_1, p_2 \in \mathbb{P}_c}} 1.$$

then for almost all sufficiently large even integers

$$T(n) \geq \rho_0 C(n) \frac{n^{2\gamma - 1}}{\log^2 n}.$$

where ρ_0 is a definite positive constant and

$$C(n) = \frac{n}{\phi\,(n)} \prod_{p \not| n} \left(1 - \frac{1}{(p-1)^2}\right).$$

Part II

The results of Pleasants

Chapter 3

The first theorem of Pleasants

3.1 Introduction

In the paper [31] Pleasants proves a Theorem about the representability of infinitely many primes by means of a quite general class of cubic polynomials several variables. An nearly obvious necessary condition becomes a sufficient conditions too in certain circumstances of reasonable generality. Asymptotic estimates are obtained as well by means of the **Circle Method** as modified by H. Davenport in his treatment of homogeneous cubic equations as in [6] and [5]. **We will get now a very brief sketch of the path toward the proof:**

- In 3.2 we introduce the terminology and we formulate the statement of the Theorem as well as some geometrical notions related to the cubic part of the polynomial (which will turn to be the most important.) The most important geometrical notions are the invariant h and the invariant $h*$.
- In 3.3 we will set up some further notation.
- In 3.5 we will develop some heuristic in order to understand better the result.
- In section 3.6 a machinery based on a set of suitable bilinear forms, which are obtained from the cubic part of the polynomial, is devised, in order to dealing with estimates of the exponential cubic sum later.
- In section 3.7 the machinery of the previous section is applied in order to get expression of the exponential sum in term of bilinear forms.
- In section 3.8 the case $h = n$ is studied.

- In section 3.9 the case $h < n$ is studied.
- In section 3.10 we dealing with the estimates of the exponential cubic sum $S(\alpha)$ and its approximant $S_(a,q)$ using the results obtained last two sections.
- In section 3.11we dealing with the **minor arcs**.
- In section 3.12 we dealing with the **Major arcs**.
- In section 3.13 we dealing with the **singular series** of the problem.
- In section 3.14 the **First Theorem of Pleasant** is proved.

A graphical "road map" towards the proof of FTP is given in Appendix H.

3.2 Preliminaries

Let be $\mathbf{x} \in \mathbb{Z}^n$ and

$$\phi = \phi(\mathbf{x}) = C(\mathbf{x}) + Q(\mathbf{x}) + L(\mathbf{x}) + N. \tag{3.1}$$

a cubic polynomial in $\mathbb{Z}[\mathbf{x}]$ where

- $C(\mathbf{x})$ denotes the cubic part of ϕ.
- $Q(\mathbf{x})$ denotes the quadratic part of ϕ.
- $L(\mathbf{x})$ denotes the linear part of ϕ.

and where $N \in \mathbb{Z}$.

Definition 3.1. *Let*

$$\mathcal{L} = \{L : \mathbb{R}^n \to \mathbb{R},\ L \in \mathbb{Z}[\mathbf{x}]\}.$$

be the set of real linear forms defined on $\mathbb{R}^n$ with integers coefficients.

$$\mathcal{Q} = \{Q : \mathbb{R}^n \to \mathbb{R},\ Q \in \mathbb{Z}[\mathbf{x}]\}.$$

the set of real quadratic forms on on $\mathbb{R}^n$ with integers coefficients. Let

$$A = \left\{ k \in \mathbb{N} : \exists\, L_1 \dots L_k \in L, Q_1 \dots Q_k \in Q :\ C(\mathbf{x}) = \sum_{j=1}^{k} L_j(\mathbf{x})\, Q_j(\mathbf{x}) \quad \forall \mathbf{x} \in \mathbb{Z}^n \right\}.$$

The number $h = h(C) = \min A$ is called the ***number of Davenport-Lewis****.*

In [7] Davenport and Lewis proved the following

Proposition 3.1. ***If*** C *is a cubic form in* $\mathbb{Z}[\mathbf{x}]$ *then*

1. $1 \leq h \leq n$.
2. *If* $T : \mathbb{R}^n \to \mathbb{R}^n$ *is a non-singular linear transformation defined by an integral matrix and* $C' = C \circ T$ *then* $h(C') = h(C)$.

Given a cubic form $C(\mathbf{x}) \in \mathbb{Z}(\mathbf{x})$ it is always possible to find a set of positive integers $I = \{r_1 ... r_s\}$ and a non-singular linear transformation T as in 3.1 such that:

1. $\sum_{j=1}^{s} r_j = n$.
2. $\mathbb{R}^n = \mathbb{R}^{r_1} \oplus, \ldots, \oplus \mathbb{R}^{r_s}$ where $\oplus$ denotes the direct sum of subspaces.
3. $T : \mathbb{R}^{r_1} \oplus \ldots \oplus \mathbb{R}^{r_s} \to \mathbb{R}^n$.
4. $C(\mathbf{x}) = C\left(T\left(\mathbf{y_1}, \ldots \mathbf{y}_s\right)\right) = \sum_{j=1}^{s} C_j\left(\mathbf{y}_j\right) \quad \forall \mathbf{x} \in \mathbb{Z}^n$ where $(\mathbf{y_1}, \ldots \mathbf{y}_s)$ is the uniquely defined ordered $s-tuple$ of vectors in $\mathbb{Z}^{r_1} \oplus, \ldots, \oplus \mathbb{Z}^{r_s}$ such that $T\left(\mathbf{y_1}, \ldots \mathbf{y}_s\right) = \mathbf{x}$.

For each of such set I we define

$$k = \sum_{j=1}^{s} h(C_j).$$

Clearly k depends from the set I. We denote the set of all such I as $\mathcal{I}$.

Definition 3.2. *Following [7] we define*

$$h^* = h^*(C) = \max_{I \in \mathcal{I}} \{k\}.$$

It is not difficult to prove that

Proposition 3.2. *For every cubic form* $C \in \mathbb{Z}(\mathbf{x})$ *it is* $h \leq h^* \leq n$.

3.3 Notation

Let $\mathcal{P}$ a closed parallelepiped of $\mathbb{R}^n$. Assume that if $\mathbf{x} \in \mathcal{P}$ is a point with integer coordinates then $\phi(\mathbf{x}) > 0$. We denotes with $V_{\mathcal{P}}$ its volume. Let P a large real parameter and let $P\mathcal{P}$ the parallelepiped obtained from $\mathcal{P}$ by a dilatation of each edge of a factor P. If

$$\mathcal{A} = \{\mathbf{x} \in P\mathcal{P} : \phi(\mathbf{x}) \in \mathbb{P}\}.$$

we denote with $\mathcal{M}(P) = |\mathcal{A}|$. In [31] it is proved the following

3.4 The First Theorem of Pleasants

Theorem 3.1. *Given a cubic polynomial $\phi \in \mathbb{Z}(\mathbf{x})$* ***if*** *$C$ denotes its cubic part and if*

1. *$h^*(C) \geq 8$.*
2. *For every $m \in \mathbb{Z}$ there exists $\mathbf{x} \in \mathbb{Z}^n$ such that $\varphi(\mathbf{x}) \equiv 0 \pmod m$.*

then

$$\mathcal{M}(P) \sim \mathfrak{S}\frac{V_{\mathcal{P}}P^n}{\log P^3}. \tag{3.2}$$

as $P \to +\infty$.

Before to see the proof of this theorem we get some heuristic for this result.

3.5 The heuristic

Let $\mathcal{P}$ a closed parallelepiped of $\mathbb{R}^n$. Assume that if $\mathbf{x} \in \mathcal{P}$ is a point with integer coordinates then $\phi(\mathbf{x}) > 0$. If $\mathcal{V}_{\mathcal{P}}$ denotes the volume of $\mathcal{P}$ and if we dilate each edge of a factor P we have that the new parallelepiped $P\mathcal{P}$ has a volume

$$V_{P\mathcal{P}}(P) = V_{\mathcal{P}}P^n.$$

and it will contains a number of points with integer coordinates of the same order of magnitude. For every $\mathbf{x} \in \mathcal{P}$ $\phi(\mathbf{x})$ is an integer belongs to an interval $I = (aP^3, bP^3)$ where $a, b \in \mathbb{R}$ depends only from the cubic part C. The number of integers in I is of magnitude order P^3. If we think the integer points of $\mathcal{P}$ as objects and the integer values in I as boxes the situation is the following:

- We have $\mathcal{N} = V_{\mathcal{P}}P^n$ objects.
- We must distribute them among P^3 boxes.

Heuristically, we can imagine an uniform distribution and so in every box we will contains $\mathcal{N}_1 = V_{\mathcal{P}}P^{n-3}$ objects. This means that we will expects that each of the integer values in I is taken P^{n-3} times. Again,from the PNT, heuristically, we can say that the "probability" that an integer in $[2, x]$ be prime is around $x/\log x$. In our case this "probability" will be

$$\mathfrak{p} = \frac{P^3}{\log P^3}.$$

Hence, among the values of our polynomial, we will have a number of prime values $\mathcal{M}(P)$ proportional to $\mathcal{N}_1\mathfrak{p}$. In other words

$$\mathcal{M}(P) = \mathfrak{S}\frac{V_{\mathcal{P}}P^n}{\log P^3}.$$

The constant $\mathfrak{S}$ is strictly related with the "**arithmetical nature**" of the polynomial. For instance, if the polynomial admits a fixed divisor, then $\mathfrak{S} = 0$. Even in case of $\mathfrak{S} > 0$ it depends form the coefficients of ϕ and in particular form those of C.

3.6 The setup for the proof: the bilinear forms

We set up a basic terminology frame:

- It is convenient to write a cubic form $C(\mathbf{x})$ as

$$C(\mathbf{x}) = \sum_{1\le i\le j\le k} c_{ijk}x_ix_jx_k. \tag{3.3}$$

- For a given cubic form $C(\mathbf{x})$ it is defined a set of bilinear forms

$$\mathbf{B}_C = \left\{ B_j(\mathbf{x}|\mathbf{y}) = \sum_{i=1}^{n}\sum_{k=1}^{n} c'_{ijk}x_iy_k \;\; j = 1\dots n \right\}. \tag{3.4}$$

  where the function

$$(i,j,k) \to c'_{ijk}.$$

  is invariant by any permutation of i,j,k and for $i \le j \le k$ is defined by

$$c'_{ijk} = \begin{cases} 6c_{ijk} \; if \;\; i = j = k \\ 2c_{ijk} \, if \;\; i = j < k \;\; or \;\; i < j = k \\ c_{ijk} \;\; if \;\; i < j < k. \end{cases} \tag{3.5}$$

- Let $\mathbf{D} = \{\psi_j : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R} \;\; j = 1...m\}$ a set of bilinear forms. For any $\mathbf{x_0} \in \mathbb{R}^n$ we define

$$K = K(\mathbf{D}, \mathbf{x_0}) = \{\mathbf{y} \in \mathbb{R}^n : \psi_j(\mathbf{x_0}|\mathbf{y}) = 0 \;\; j = 1...m\}.$$

  By definition K is a vector subspace and we denote with

$$l = l(\mathbf{D}, \mathbf{x_0}) = \dim K.$$

With this setup we are going to prove the following

Lemma 3.1. *Let $C : \mathbb{R}^n \to \mathbb{R}^n$ a cubic form with integer coefficients such that $h = h(C)$. Let $r \in \mathbb{N}$ such that $n - h < r \leq n$ and let $R \in \mathbb{R}^+$. Let*

$$\widetilde{A}_R = \{\mathbf{x} \in \mathbb{Z}^n : |\mathbf{x}| < R\}.$$

and

$$B_r = \{\mathbf{x} \in A_R : l(\mathbf{B}_C, \mathbf{x}) = r\}.$$

then

$$|B_r| \ll R^{2n-h-r} \quad R \to +\infty. \tag{3.6}$$

Proof. **First case:** $h = n$.

We notice that for each fixed $\mathbf{x} \in \mathbb{Z}^n$

$$\begin{cases} B_1(\mathbf{x}|\mathbf{y}) = 0 \\ \vdots \\ B_n(\mathbf{x}|\mathbf{y}) = 0. \end{cases}$$

is a system of linear equations. The matrix of this linear system is

$$\mathcal{H}(\mathbf{x}) = \begin{pmatrix} \frac{\partial^2 C(\mathbf{x})}{\partial x_1^2} & \cdots & \frac{\partial^2 C(\mathbf{x})}{\partial x_1 x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 C(\mathbf{x})}{\partial x_n x_1} & \cdots & \frac{\partial^2 C(\mathbf{x})}{\partial x_n^2} \end{pmatrix}.$$

and we call as

$$H(\mathbf{x}) = \det \mathcal{H}(\mathbf{x}).$$

its determinant. In other words the determinant of the system's matrix is the hessian determinant of $C(\mathbf{x})$. For any $\mathbf{x} \in B_r$ we can construct a set $S = \left\{\mathbf{y}^{(1)} \dots \mathbf{y}^{(r)}\right\}$ of linearly independent solution of the above system by taking, as the components of these vectors, certain particular minors of order $n - r$. Each of such minor is a homogeneous polynomial of degree $n - r$ belongs to $\mathbb{Z}^n[\mathbf{x}]$. For every $\mathbf{x} \in \mathbb{Z}^n$ (not necessarily in B_r) and for every $\mathbf{y}^{(p)} \in S$ we have that, identically in $\mathbf{x}$, we have that

$$\sum_{i=1}^{n} c_{i,jk} x_i y_k^{(p)} = \Delta_{j,p}(\mathbf{x}) \quad p = 1 \dots r. \tag{3.7}$$

where $\Delta_{j,p}\mathbf{x}$ are certain minors of order $n - r + 1$ of the hessian matrix. Since $x_1 ... x_n$ are independent variables, we can differentiate partially (3.7) with respect to x_ν, obtaining

$$\sum_{k=1}^{n} c_{\nu jk} y_k^{(p)}(\mathbf{x}) + \sum_{i=1}^{n}\sum_{k=1}^{n} c_{ijk} x_i \frac{\partial y_k^{(p)}(\mathbf{x})}{\partial x_\nu} = \frac{\partial \Delta_{j,p}(\mathbf{x})}{\partial x_\nu}. \tag{3.8}$$

with $j = 1...n$ and $\nu = 1...n$ and $p = 1...r$. Let $K_1, ...K_r$ be constants, to be determined later, and put

$$Y = K_1 \mathbf{y}^{(1)} + \dots K_r \mathbf{y}^{(r)}. \tag{3.9}$$

From (3.8) we have that

$$\sum_{k=1}^{n} c_{\nu,j,k} Y_k (\mathbf{x}) + \sum_{i=1}^{n} \sum_{k=1}^{n} c_{i,j,k} x_i \frac{\partial Y_k (\mathbf{x})}{\partial x_\nu} = \sum_{p=1}^{r} K_p \frac{\partial \Delta_{j,p} (\mathbf{x})}{\partial x_\nu}.$$

for every $j = 1...n$ and every $\nu = 1...n$. Multiply by Y_j and sum over j. Since

$$\sum_{j=1}^{n} \sum_{i=1}^{n} c_{i,j,k} x_i Y_j (\mathbf{x}) = \sum_{p=1}^{r} K_p \Delta_{k,p}.$$

from (3.7) and (3.9), we obtain [1]

$$\sum_{j=1}^{n} \sum_{k=1}^{n} c_{\nu,j,k} Y_j Y_k + \sum_{k=1}^{n} \sum_{p=1}^{r} K_p \Delta_{k,p} \frac{\partial Y_k}{\partial x_\nu} = \sum_{j=1}^{n} \sum_{p=1}^{r} Y_j K_p \frac{\partial \Delta_{j,p}}{\partial x_\nu}. \tag{3.10}$$

for $\nu = 1...n$. We now appeal to E.2 taking the polynomials $f_1...f_N$ to be al the minors $\Delta_{j,p} (\mathbf{x})$ for $j = 1..n$ and $p = 1...r$. By that Proposition, if A is sufficiently large, there is a point $\mathbf{x_0}$ in $\mathcal{A}_R$ for which

$$\begin{cases} \Delta_{j,p} (\mathbf{x}_0) = 0 \\ \nu (J (\mathbf{x}_0)) \leq r - 1 \end{cases}$$

This implies that for $j = 1...n$ and $p = 1...r$ we have

$$\frac{\partial \Delta_{j,p}}{\partial x_\nu} (\mathbf{x}_0) = \sum_{\rho=1}^{r-1} t_{j,p,\rho} u_{\rho,\nu}.$$

where

- $\mathbf{T} = (t_{j,p,\rho})$ is a tensor $n \times r \times (r-1)$.
- $\mathbf{U} = (u_{\rho,\nu})$ is a $(r-1) \times n$.

Since the values of the derivatives are integers, we can take the components of the tensor $\mathbf{T}$ and the matrix $\mathbf{U}$ in $\mathbb{Q}$. For $\mathbf{x} = \mathbf{x}_0$ we have that (E.5) becomes

$$\sum_{j=1}^{n} \sum_{k=1}^{n} c_{\nu,j,k} Y_j Y_k = \sum_{j=1}^{n} \sum_{p=1}^{r} Y_j K_p \sum_{\rho=1}^{r-1} t_{j,p,\rho} u_{\rho,\nu}.$$

[1] We are omitting, in this equation, the dependence from $\mathbf{x}$ for space's reason.

We can rewrite this as

$$\sum_{j=1}^{n}\sum_{k=1}^{n} c_{\nu,j,k} Y_j Y_k = \sum_{\rho=1}^{r-1} V_\rho u_{\rho,\nu}. \tag{3.11}$$

where, for every $\rho = 1...r-1$, it is

$$V_\rho = \sum_{j=1}^{n}\sum_{k=1}^{n} Y_j K_p t_{j,p,\rho}.$$

The (3.11) holds for $\nu = 1...n$ hence multiplying by Y_ν, summing over ν and using (3.9) we obtain

$$\sum_{\nu=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} c_{\nu,j,k} Y_\nu Y_j Y_k = \sum_{\rho=1}^{r-1} V_\rho \sum_{\nu=1}^{n}\sum_{\sigma=1}^{r} K_\sigma y_\nu^{(\sigma)} u_{\rho,\nu}.$$

We choose $K_1...K_r$ to satisfy

$$\sum_{\sigma=1}^{r} K_\sigma \left(y_\nu^{(\sigma)} u_{\rho,\nu}\right) = 0.$$

for $\rho = 1,..,r-1$. These are $r-1$ homogeneous linear equations in r unknowns, with rational coefficients, an so can be solved in **integers** $K_1,...K_r$, not all 0. the vector Y, given by (3.9), now satisfies

$$\sum_{\nu=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} c_{\nu,j,k} Y_\nu Y_j Y_k = 0.$$

Also Y is a vector with integer components and it is not the null vector because $\mathbf{y}^{(1)} \dots \mathbf{y}^{(r)}$ are linearly independent and this is a contradiction.

Second case:

The proof is quite similar except that the rank of the Jacobian matrix is now at most $h-n+r-1$ instead $r-1$. In the same way as before we obtain a system of $h-n+r-1$ homogeneous linear equations in r unknowns $K_1,...K_r$. The solution of this system provide a vector space of dimension at least $n-h+1$. On the other side, the cubic form C vanish identically on this space. This contradicts the definition of h, since $n-h$ is the greatest dimension of any vector space contained in the cubic cone $C(\mathbf{x}) = 0$. □

Definition 3.3. *A cubic form is said to split if there exists r_1, r_2 positive integers with $r_1 + r_2 = n$ and a non-singular linear transformation defined by an integra matrix*

$$T : \mathbb{R}^{r_1} \oplus \mathbb{R}^{r_2} \to \mathbb{R}^n.$$

and two cubic forms

$$C_1(\mathbf{y}_1) : \mathbb{R}^{r_1} \to \mathbb{R}.$$

$$C_2(\mathbf{y}_2) : \mathbb{R}^{r_2} \to \mathbb{R}.$$

neither vanishing identically such that

$$C(\mathbf{x}) = C_1(\mathbf{y}_1) + C_2(\mathbf{y}_2) \quad \forall \mathbf{x} \in \mathbb{Z}^n.$$

Lemma 3.2. *Let $C : \mathbb{R}^n \to \mathbb{R}^n$ a cubic form with integer coefficients such that $h = h(C)$ which does not split and let $R \in \mathbb{R}^+$. Let*

$$\mathcal{Z}_C(R) = \left\{(\mathbf{x}, \mathbf{y}) \in A_R^2 : \ B_j(\mathbf{x}|\mathbf{y}) = 0, \ j = 1 \dots n\right\}.$$

then *there exists a constant $c > 0$ such that*

$$|\mathcal{Z}_C(R)| \leq R^{2n-h-n^{-1}} (\log R)^c. \tag{3.12}$$

Proof. We suppose that

$$|\mathcal{Z}_C(R)| > R^{2n-h-n^{-1}} (\log R)^c.$$

and reach a contradiction if c is large enough. For $1 \leq r \leq n$ let B_r as in Lemma 3.1. Then there exists some $\overline{r}$ for which

$$|\mathcal{N}_{\mathcal{R}}| > \frac{R^{2n-h-n^{-1}} (\log R)^c}{n}.$$

where

$$\mathcal{N}_R = \left\{(\mathbf{x}, \mathbf{y}) \in A_R^2 : \ \mathbf{x} \in B_{\overline{r}} \ , \ B_j(\mathbf{x}, \mathbf{y}) = 0 \ \forall j = 1...n\right\}.$$

For each $\mathbf{x} \in B_r$ we define

$$\mathcal{N}_R(\mathbf{x}) = \{\mathbf{x} \in B_{\overline{r}} : \ \exists \mathbf{y} \in \mathbb{Z}^n : \ (\mathbf{x}, \mathbf{y}) \in \mathcal{N}_R\}.$$

Then, we have

$$\sum_{\mathbf{x} \in B_{\overline{r}}} |\mathcal{N}_R(\mathbf{x})| > \frac{R^{2n-h-n^{-1}} (\log R)^c}{n}. \tag{3.13}$$

Further, by Lemma 3.1, if $\overline{r} > n - h$, we have

$$\sum_{\mathbf{x} \in B_{\overline{r}}} 1 \ll R^{2n-h-\overline{r}}. \tag{3.14}$$

and this estimate remains trivially valid if $\overline{r} \leq n - h$. We divide the vectors $\mathbf{x} \in B_{\overline{r}}$ into disjoint subsets $\mathcal{E}_s$ such that

$$\mathcal{E}_s = \left\{ \mathbf{x} \in B_{\overline{r}} : c_1 R^{\overline{r}} 2^{-(s+1)} \leq |\mathcal{N}_R(\mathbf{x})| < c_1 R^{\overline{r}} 2^{-s} \right\}.$$

with $s = 0, 1...$ and where c_1 so chosen [2] that $|N_R(\mathbf{x})| < c_1 R^{\overline{r}} \ \ \forall \mathbf{x} \in B_{\overline{r}}$. If we define

$$C(\mathcal{E}_s) = \{ (\mathbf{x}, \mathbf{y}) \in \mathcal{N}_R : \mathbf{x} \in \mathcal{E}_s \}.$$

then, we can write

$$\sum_{\mathbf{x} \in B_{\overline{r}}} |\mathcal{N}_R(\mathbf{x})| = \sum_{s \geq 0} |C(\mathcal{E}_s)| > \frac{R^{2n-h-n^{-1}} (\log R)^c}{n}.$$

Since the parameter s a number of values which is $\ll \log R$, there must exist some subset $\mathcal{E}_{\overline{s}}$ such that

$$|C(\mathcal{E}_{\overline{s}})| \gg R^{2n-h-n^{-1}} (\log R)^{c-1}.$$

If ρ is defined by the equation $2^{\overline{s}} = R^{\rho}$, we must have

$$|\mathcal{E}_{\overline{s}}| \gg R^{2n-h-n^{-1}-(\overline{r}-\rho)} (\log R)^{c-1}. \tag{3.15}$$

and to each vector $\mathbf{x} \in \mathcal{E}_{\overline{s}}$ the number of correspondent vectors $\mathbf{y}$ must be $\gg R^{(\overline{r}-\rho)}$. By (3.14) we must have $0 \leq \rho < n^{-1}$. For each $\overline{\mathbf{x}} \in \mathcal{E}_{\overline{s}}$ we choose a basis $\left\{ \mathbf{y^1}(\overline{\mathbf{x}}) \dots \mathbf{y^{\overline{r}}}(\overline{\mathbf{x}}) \right\}$ for the linear system

$$\begin{cases} B_1(\overline{\mathbf{x}}|\mathbf{y}) = 0 \\ \vdots \\ B_n(\overline{\mathbf{x}}|\mathbf{y}) = 0. \end{cases}$$

in accordance with Proposition E.3. It can be shown [3] that

$$\begin{cases} |\mathbf{y^1}(\overline{\mathbf{x}})| \ll R^{\rho} \\ \vdots \\ |\mathbf{y^r}(\overline{\mathbf{x}})| \ll R^{\rho}. \end{cases}$$

[2] As it can be done, for cardinality reasons.

[3] See the proof of Proposition E.4 as developed in Lemma 6 of [6]

For every $j = 1...n$ we have that $\left|\mathbf{y^{(j)}}\right| = U_j \in \mathbb{Z}^+$. Hence for a given value of U_j, the number λ_j of possible vectors $\mathbf{y^{(j)}}$ is such that

$$\lambda_j \ll U_j^{n-1}.$$

It follows that the number of possible basis, as above, is

$$L \ll \sum_{U_1 \dots U_{\overline{r}} \ll R^\rho} (U_1 \dots U_{\overline{r}})^{n-1}.$$

If we denote with $d_{\overline{r}}(U)$ the number of ways of expressing a positive integer U as a product of $\overline{r}$ positive integers we can also write

$$L \ll R^{\rho(n-1)} \sum_{U \ll R^\rho} d_{\overline{r}}(U).$$

and the right hand side is independent of $\overline{\mathbf{x}}$. By a well known estimate, we have that

$$\sum_{U \leq M} d_{\overline{r}}(U) \ll M (\log M)^{\overline{r}-1}.$$

Hence

$$L \ll R^\rho (\log R)^{\overline{r}-1}.$$

It follows now from (3.15) that there must be some basis which occurs for a set of points $\mathbf{x}$ numbering

$$\gg R^{2n-h-n^{-1}-\overline{r}-(n-1)\rho} (\log R)^{c-\overline{r}}.$$

All points $\mathbf{x}$ which give rise to this basis constitute a lattice, a provided $c > \overline{r}$ the last inequality shows that the dimension of this lattice must be at least $2n - h - r$ since $\rho < 1/n$. Hence there exist a set of $2n - h - \overline{r}$ points $\mathbf{x^{(p)}}$ and a set of $\overline{r}$ points $\mathbf{y^{(q)}}$ such that

$$B_j\left(\mathbf{x^{(p)}}|\mathbf{y^{(q)}}\right) = 0.$$

for every $j = 1...n$, for every $p = 1...2n - h - \overline{r}$ and for every $q = 1...\overline{r}$. Each set of such points is linearly independent. If we consider the Grassman's relation for general linear subspaces

$$\dim V_1 + \dim V_2 - \dim(V_1 + V_2) = \dim(V_1 \cap V_2).$$

we see that the two linear space, of dimension $2n - h - \overline{r}$ and $\overline{r}$ intersect in a linear space of dimension at least [4] $n - h$. If they intersected in a space of

[4] We can think to V_1 as a subspace of dimension $2n - h - \overline{r}$ and to V_2 as a subspace of dimension $\overline{r}$. Moreover it is clear that $dim(V_1 + V_2) \leq n$. Hence $\dim(V_1 \cap V_2) \geq (2n - h - \overline{r}) + (\overline{r}) - (n) = n - h$

higher dimension than this we should have a contradiction to the definition of h, since all the vectors $\mathbf{z}$ of the intersection subspace are representable as linear combinations both of vectors $\mathbf{x^{(p)}}$ and $\mathbf{y^{(q)}}$, and therefore $C(\mathbf{z}) = 0$. Hence there exists $n - \overline{r}$ of the vectors $\mathbf{x^{(p)}}$ with together with $\overline{r}$ vectors $\mathbf{y^{(q)}}$ form a linearly independent set of n vectors. The substitution

$$\mathbf{x} = u_1\mathbf{x^{(1)}} + \ldots u_{n-\overline{r}}\mathbf{x^{(n-\overline{r})}} + v_1\mathbf{y^{(1)}} + \ldots v_r\mathbf{y^{(\overline{r})}}.$$

from $(x_1 \ldots x_n)$ to $(u_1, \ldots, u_{n-\overline{r}}, v_1 \ldots v_{\overline{r}})$. gives

$$C\left(x_1 \ldots x_n\right) = C_1\left(u_1, \ldots, u_{n-\overline{r}}\right) + C_2\left(v_1 \ldots v_{\overline{r}}\right).$$

identically. This contradicts the hypotesis that $C(\mathbf{x})$ does not split and the proof is complete. □

3.7 The cubic exponential sum: the use of $S^*(\alpha, \mathbf{B})$

Lemma 3.3. *There exists a non-singular linear transformation*

$$U : \mathbb{R}^n \to \mathbb{R}^n.$$

such that:

1. $U(\mathbb{Q}^n) \subseteq \mathbb{Q}^n$.
2. $\forall \mathbf{z} \in \mathbb{Z}^n \Rightarrow U\left(\mathbf{z}\right) = \mathbf{x} \in \mathbb{Z}^n$.
3. *The components of* $\mathbf{z}$ *satisfies certain homogeneous linear congruences to a fixed modulus* d.
4. *There exists* $\psi_1 \ldots \psi_s \in \mathbb{Q}\left[\mathbf{z}\right]$ *cubic polynomials such that*

$$\phi\left(\mathbf{x}\right) = \phi\left(U\left(\mathbf{z}\right)\right) = \psi_1\left(\mathbf{z}\right) + \ldots + \psi_s\left(\mathbf{z}\right) \quad \forall \mathbf{x} \in \mathbb{Z}^n. \tag{3.16}$$

5. $d^3\psi_i\left(\mathbf{z}\right) = \psi_i'\left(\mathbf{z}\right) \in \mathbb{Z}\left[\mathbf{z}\right] \quad \forall i = 1 \ldots s$.
6. *There exists* $n_1 ... n_s$ *positive integers such that*
   - $n_1 + ... n_s \leq n$.

- *If $\overline{C}_i$ denotes the cubic part of ψ_i then we have*

$$\begin{array}{l}\overline{C}_1\left(z_1 \ \ldots \quad z_{n_1}\right)\\ \overline{C}_2\left(z_{n_1+1}\ldots z_{n_2}\right)\\ \vdots\\ \overline{C}_s\left(z_{n_{s-1}+1}\ldots z_{n_s}\right).\end{array}$$

  i.e these cubic parts are defined over disjoint sets of variables.
- *Each form $\overline{C}_i$ as form [5] of n_i variables does not split.*
- $$\sum_{i=1}^{s} h(\overline{C}_i) = h^*\left(C\right) = h^*. \tag{3.17}$$

Proof. Assume

$$C\left(\mathbf{x}\right) = C_1\left(\mathbf{y}_1\right) + \ldots C_s\left(\mathbf{y}_s\right).$$

as in Proposition 3.1. We can suppose that none of the cubic forms C_i does not split. For if, say, C_1 splits, i.e

$$C_1\left(\mathbf{y_1}\right) = C_1'\left(\mathbf{y_1'}\right) + C_1''\left(\mathbf{y_1''}\right).$$

where

$$\begin{cases}\mathbf{y_1} = \left(y_1 \ldots y_{n_1}\right)\\ \mathbf{y_1'} = \left(y_1 \ldots y_m\right)\\ \mathbf{y_1''} = \left(y_{m+1} \ldots y_{n_1}\right)\\ 1 \leq m \leq n_1 - 1.\end{cases}$$

a further non singular integral linear transformation gives

$$C\left(\mathbf{x}\right) = C_1'\left(\mathbf{y_1'}\right) + C_1''\left(\mathbf{y_1''}\right) + C_2\left(\mathbf{y_2}\right) + \ldots C_s\left(\mathbf{y_s}\right).$$

where

$$\begin{cases}\mathbf{y_2} = \left(y_{n_1+1} \ldots y_{n_2}\right)\\ \vdots\\ \mathbf{y_s} = \left(y_{n_{s-1}+1} \ldots y_{n_s}\right).\end{cases}$$

We have that, by definition of h,

$$\begin{cases} C_1' = \sum\limits_{j=1}^{h(C_1')} L_j' Q_j'\\ C_1'' = \sum\limits_{j=1}^{h(C_1'')} L_j'' Q_j''. \end{cases}$$

[5] Of course, properly speaking, each of such forms is defined on $\mathbb{R}^n$. We suppose that each of them depends effectively only from a subset of variables and so we can think to them as forms of n_i variables.

hence

$$C_1 = \sum_{j=1}^{t} L_j Q_j.$$

where

- $t = h(C_1') + h(C_1'')$.
- $L_j = \begin{cases} L_j' & if \quad 1 \leq j \leq h(C_1') \\ L_j'' & if \quad h(C_1') < j \leq t. \end{cases}$
- $Q_j = \begin{cases} Q_j' & if \quad 1 \leq j \leq h(C_1') \\ Q_j'' & if \quad h(C_1') < j \leq t. \end{cases}$

and from this follows that [6]

$$h(C_1) \leq h(C_1') + h(C_1'').$$

by definition of h. By definition of h^* we have that

$$h^* = h\left(C_1\right) + \ldots h\left(C_s\right).$$

On the other side, if we consider

$$C = C_1' + C_1'' + C_2 + \ldots C_s.$$

we see that

$$h\left(C_1'\right) + h\left(C_1''\right) + h\left(C_2\right) + \ldots h\left(C_s\right) \leq h^*.$$

because h^* the definition of h^* as the maximum integer with the property that a decomposition of this kind exists. This means that

$$h\left(C_1'\right) + h\left(C_1''\right) \leq h\left(C_1\right).$$

Hence

$$h(C_1') + h(C_1'') \leq h(C_1).$$

Thus

$$h(C_1') + h(C_1'') + h(C_2) + \ldots h(C_s) = h^*\left(C\right).$$

[6] If we know only that the cubic form C_1 splits into $C_1 = C_1' + C_1''$, in general, it is not true that $h(C_1) = h(C_1') + h(C_1'')$. For instance, if $C_1\left(y_1, y_2\right) = y_1^3 + y_2^3$ then $h(C_1) = 1$. On the other side, if we call $C_1'\left(y_1\right) = y_1^3$ and $C_2'\left(y_2\right) = y_2^3$ then $h(C_1') = h(C_1'') = 1$ and so $h(C1) < h(C_1') + h(C_1'')$

Repeating this process at most n times we obtain an integral non-singular linear transformation

$$T : \mathbb{R}^n \to \mathbb{R}^n.$$
$$\mathbf{y} \to T(\mathbf{y}) = \mathbf{x}.$$

which gives

$$C(\mathbf{x}) = C_1(\mathbf{y}_1) + \ldots C_s(\mathbf{y}_s).$$

and

- $\sum_{i=1}^{s} h(C_i) = h^*$.
- None of $\overline{C}_i$ splits $(i = 1...s)$.

While $\mathbf{y} \in \mathbb{Z}^n$ always gives rise to $\mathbf{x} \in \mathbb{Z}^n$, the converse in not necessary true. If $d = |\det T|$ then the vectors $\mathbf{y} \in \mathbb{Z}^n$ which correspond to $\mathbf{x} \in \mathbb{Z}^n$ are of the kind $\mathbf{y} = d^{-1}\mathbf{z}$ with $\mathbf{z} \in \mathbb{Z}^n$ with the components of $\mathbf{z}$ satisfy certain homogeneous linear congruences to the modulus d. Taking

$$U : \mathbb{R}^n \to \mathbb{R}^n$$
$$U = d^{-1}T.$$

we have

- U is linear and non-non singular.
- $U(\mathbb{Q}) \subseteq \mathbb{Q}$.
- $U(\mathbf{z}) = \mathbf{x}$.

If we call

$$C_i\left(d^{-1}\mathbf{z}\right) = \overline{C}_i(\mathbf{z}) \qquad i = 1...s.$$

we obtain the desired result. □

Definition 3.4. *Given any bounded subset $\mathcal{R}$ of $\mathbb{R}^n$ we define the subset*

$$P\mathcal{R} = H(\mathcal{R}).$$

where

$$H : \mathbb{R}^n \to \mathbb{R}^n$$
$$\mathbf{x} \to P\mathbf{x}.$$

Definition 3.5. *Let $\phi : \mathbb{R}^n \to \mathbb{R}$ a cubic polynomial and $\mathcal{R}$ any bounded subset of $\mathbb{R}^n$ we define*

$$S(\alpha, \phi, \mathcal{R}, P) = \sum_{\substack{\mathbf{x} \in P\mathcal{R} \\ \mathbf{x} \in \mathbb{Z}^n}} e(\alpha\phi(\mathbf{x})). \tag{3.18}$$

In order to obtain estimates for such exponential sums, the general principle is that $\mathcal{R}$ has to be of the kind

$$\mathcal{R} = \prod_{i=1}^{n} [a_i, b_i].$$

from now on we will call this kind of subset as "**n-box**".

Note 3.1. *From now on, we shall suppose, without loose generality, that the n-box $\mathcal{B}$ is defined by the cartesian product of intervals (a_j, b_j) such that $0 < b_j - a_j < 1$ for all $j = 1...n$.*

Lemma 3.4. *Let $\mathcal{B}$ be a n-box and let ϕ be a given cubic polynomial. Then*

$$|S(\alpha, \phi, \mathcal{B}, P)|^4 \ll P^n \sum_{\substack{\mathbf{x} \in P\mathcal{B} \\ |\mathbf{x}| < P}} \sum_{\substack{\mathbf{y} \in P\mathcal{B} \\ |\mathbf{y}| < P}} \prod_{j=1}^{n} \min\left\{P, \|\alpha B_j(\mathbf{x}|\mathbf{y})\|^{-1}\right\}. \tag{3.19}$$

Proof. The proofs follows, with minor modifications, the proof of Lemma 3.1 in [5]. First off all we write

$$S(\alpha) = S(\alpha, \phi, \mathcal{B}, P).$$

as a shortcut. Since

$$S(\alpha) = \sum_{\substack{\mathbf{z}' \in P\mathcal{B} \\ \mathbf{z}' \in \mathbb{Z}^n}} e(\alpha\varphi(\mathbf{z}')).$$

and

$$\overline{S(\alpha)} = \sum_{\substack{\mathbf{z} \in P\mathcal{B} \\ \mathbf{z} \in Z^n}} e(-\alpha\varphi(\mathbf{z})).$$

We can write

$$|S(\alpha)|^2 = \sum_{\substack{\mathbf{z} \in P\mathcal{B} \\ \mathbf{z} \in \mathbb{Z}^n}} \sum_{\substack{\mathbf{z}' \in P\mathcal{B} \\ \mathbf{z}' \in \mathbb{Z}^n}} e(\alpha(\phi(\mathbf{z}') - \phi(\mathbf{z}))).$$

Hence

$$|S(\alpha)|^2 = \sum_{\substack{\mathbf{z} \in P\mathcal{B} \\ \mathbf{z} \in \mathbb{Z}^n}} \sum_{\substack{\mathbf{y} \in Q_{\mathbf{z}}\mathcal{B} \\ \mathbf{y} \in \mathbb{Z}^n}} e(\alpha(\phi(\mathbf{z} + \mathbf{y}) - \phi(\mathbf{z}))).$$

where

$$Q_{\mathbf{z}}\mathcal{B} = \{\mathbf{y} \in \mathbb{R}^n : \mathbf{z}' = \mathbf{z} + \mathbf{y} \in P\mathcal{B}\}.$$

If

$$\mathcal{C}_P = \{\mathbf{y} \in \mathbb{R}^n : |\mathbf{y}| < P\}.$$

then, from Note 3.1, it follows that $Q_{\mathbf{z}}\mathcal{B} \subseteq \mathcal{C}_P$. If

$$\mathcal{R}(\mathbf{y}) = P\mathcal{B} \cap Q_{\mathbf{y}}\mathcal{B}.$$

then, it is itself an n- box, with edges less than P in length and

$$|S(\alpha)|^2 \leq \sum_{\substack{|\mathbf{y}| < P \\ \mathbf{y} \in \mathbb{Z}^n}} \left| \sum_{\mathbf{z} \in \mathcal{R}(\mathbf{y}) \cap \mathbb{Z}^n} e(\alpha(\varphi(\mathbf{z}+\mathbf{y}) - \varphi(\mathbf{z}))) \right|.$$

We call now

$$S'(\alpha) = \sum_{\mathbf{z} \in \mathcal{R}(\mathbf{y}) \cap Z^n} e(\alpha(\varphi(\mathbf{z}+\mathbf{y}) - \varphi(\mathbf{z}))).$$

and we consider $|S'(\alpha)|^2$.
Using the same argument as before, we have

$$|S'(\alpha)|^2 \leq \sum_{|\mathbf{x}|<P} \left| \sum_{\mathbf{z} \in \mathcal{S}(\mathbf{x},\mathbf{y}) \cap \mathbb{Z}^n} e(\alpha(\phi(\mathbf{z}+\mathbf{x}+\mathbf{y}) - \phi(\mathbf{z}+\mathbf{x}) - \phi(\mathbf{z}+\mathbf{y}) + \phi(\mathbf{z}))) \right|.$$

where

$$\mathcal{S}(\mathbf{x},\mathbf{y}) = \mathcal{R}(\mathbf{y}) \cap Q_{\mathbf{x}}\mathcal{R}(\mathbf{y}).$$

and

$$Q_{\mathbf{x}}R(y) = \{\mathbf{z} \in \mathbb{R}^n : \mathbf{z}+\mathbf{x} \in R(\mathbf{y})\}.$$

If

$$F(\mathbf{x},\mathbf{y},\mathbf{z}) = (\phi(\mathbf{z}+\mathbf{x}+\mathbf{y}) - \phi(\mathbf{z}+\mathbf{x}) - \phi(\mathbf{z}+\mathbf{y}) + \phi(\mathbf{z}).$$

we have

$$F(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} c'_{i,j,k}x_i y_j z_k + \eta(\mathbf{x},\mathbf{y}).$$

where $\eta(\mathbf{x},\mathbf{y})$ does not depends [7] from $\mathbf{z}$. Hence

$$F(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{j=1}^{n} B_j(\mathbf{x}|\mathbf{y})\, z_j + \eta(\mathbf{x},\mathbf{y}).$$

It is well known that if k is any **fixed** integer and

$$\mathcal{A} = \{m \in \mathbb{Z} : m = k+h, \quad h = 1 \ldots P\}.$$

[7] All the details are in Appendix F

then

$$\sum_{m\in\mathcal{A}} e\left(m\lambda\right) \ll \min\left\{P, \|\lambda\|^{-1}\right\}.$$

From this inequality we have

$$\left|\sum_{\mathbf{z}\in\mathcal{S}(\mathbf{x},\mathbf{y})\cap\mathbb{Z}^n} e\left(\alpha\left(\sum_{j=1}^{n} B_j\left(\mathbf{x}|\mathbf{y}\right) z_j\right)\right)\right| \ll \prod_{j=1}^{n} \min\left\{P, \|\alpha B_j\left(\mathbf{x}|\mathbf{y}\right)\|^{-1}\right\}.$$

Now using the last estimate in the estimate for $|S^2(\alpha)|$ combined with Cauchy's inequality, we have the result stated. □

From now on, we write

$$S\left(\alpha\right) = S\left(\alpha, \phi, \mathcal{P}, P\right). \tag{3.20}$$

where $\mathcal{P}$ is the parallelepiped in the $\mathbb{R}^n_{\mathbf{x}}$ space obtained from the box $\mathcal{B}$ in the $\mathbb{R}^n_{\mathbf{z}}$ space by means of the linear transformation $\mathbf{z} \to U(\mathbf{z}) = \mathbf{x}$ of Lemma 3.3

Definition 3.6. *For a given set of bilinear forms*

$$\mathbf{B} = \left\{B_j : \mathbb{R}^m \times \mathbb{R}^m \to \mathbb{R}, j = 1 \ldots n\right\}.$$

we define

$$S^*(\alpha, \mathbf{B}, P) = P^m \sum_{\substack{|\mathbf{x}|<P\\ \mathbf{x}\in\mathbb{Z}^n}} \sum_{\substack{|\mathbf{y}|<P\\ \mathbf{y}\in\mathbb{Z}^n}} \prod_{j=1}^{m} \min\left\{P, \|\alpha B_j\left(\mathbf{x}|\mathbf{y}\right)\|^{-1}\right\}. \tag{3.21}$$

Lemma 3.5. ***If***

- $\psi_i' : \mathbb{R}^n \to \mathbb{R}\,, \quad i = 1 \ldots s$ *are the cubic polynomials of Lemma 3.3.*
- $\overline{C}_i : \mathbb{R}^{n_i} \to \mathbb{R}\,, \quad i = 1 \ldots s$ *their cubic parts (which depends only form* n_i *variables).*
- $\mathbf{B}_i$ *the set of bilinear forms associated to each* $\overline{C}_i$.

then

$$|S\left(\alpha\right)|^4 \ll P^{4n-4\sum_{i=1}^{s} n_i} \prod_{i=1}^{s} S^*(\alpha, \mathbf{B}_i, P). \tag{3.22}$$

Proof. Let $\mathcal{M}$ the finite set of the representative solutions of the homogeneous linear congruences $(\mathrm{mod}\, d)$ as in Lemma 3.3 and let $\mathbf{z_0} \in \mathcal{M}$. We put $\mathbf{z} = d\mathbf{u} + \mathbf{z_0}$ where $\mathbf{u} \in \mathbb{Z}^n$ is an arbitrary vector with integer components. Substituting in (3.16) and (3.18) with $\mathcal{P}$ in place of $\mathcal{R}$, we have

$$S(\alpha) = \sum_{\mathbf{z_0} \in \mathcal{M}} \left(\sum_{\mathbf{u} \in B'(\mathbf{z_0})} e\left(\alpha \sum_{i=1}^{s} \psi_i'(d\mathbf{u} + \mathbf{z_0}) \right) \right).$$

where

$$\mathcal{B}'(\mathbf{z_0}) = \left\{ \mathbf{u} \in \mathbb{Z}^n : \mathbf{u} \in d^{-1} Q_{\mathbf{z_0}} \mathcal{B} \right\}.$$

and $Q_{\mathbf{z_0}}\mathcal{B}$ is defined as in Lemma 3.4. We notice that For every $\mathbf{z_0} \in M$ there is an exponential sum of the form

$$\sum_{\mathbf{u} \in \mathcal{B}'(\mathbf{z_0})} e\left(\alpha \sum_{i=1}^{s} \psi_i'(d\mathbf{u} + \mathbf{z_0}) \right). \tag{3.23}$$

Hence $S(\alpha)$ is expressed as a **finite sum** of exponential sums of such a form. We apply to this sum the estimate given by Lemma 3.4. Since this estimate depends only on the cubic part of the polynomial, it is independent of $\mathbf{z_0}$. There is a minor discrepancy in that the box of summation depends on $\mathbf{z_0}$. Anyway the dependence is only by a bounded translation of vector $\mathbf{z_0}$ and this trouble can be remedied by modifying the constants involved in the conditions

$$\begin{cases} |\mathbf{x}| \ll P \\ |\mathbf{y}| \ll P. \end{cases}$$

We obtain (3.19) with bilinear forms which are associated with the cubic part of

$$\psi'(\mathbf{u}) = \sum_{i=1}^{s} \psi_i'(d\mathbf{u} + \mathbf{z_0}).$$

which is

$$\overline{C}(\mathbf{u}) = \sum_{i=1}^{s} \overline{C_i}(d\mathbf{u}).$$

Since the cubic forms $\overline{C}_i$ are defined on disjoint sets, the bilinear forms fall into sets of cardinality $n_1 ... n_s$ and m_s, where [8] $m_s = n - \sum_{i=1}^{s} n_i$ The m_s bilinear forms of the last set are identically zero. Accordingly, the right hand

[8] Of course not all the variables of the polynomial have to be present in its cubic part $\overline{C}(\mathbf{u})$

side of (3.19) can be factored. The factors are $S^*(\alpha, \mathbf{B_i}, P)$ where $\mathbf{B_i}$ is the set of n_i bilinear forms associated with the cubic form $\overline{C}_i$. We must observe that there is also a factor of the kind AP^{4m_s} corresponding to the bilinear forms which are identically zero (being A a constant not depending on P) This proves the lemma. □

3.8 The estimation of $S^*(\alpha, \mathbf{B}, P)$ if $h(C) = n$

We introduce a parameter U to be specified later as well as the shortcut

$$L = \log P. \tag{3.24}$$

Now we shall reason indirectly and we develop some consequences if, for a given α it is

$$S^*(\alpha, \mathbf{B}, P) > P^{4n}U^{-n}. \tag{3.25}$$

We have the following

Lemma 3.6. *If* (3.25) *holds and if*

$$\mathcal{N}_P = \left\{(\mathbf{x}, \mathbf{y}) \in \widetilde{A}_P^2 : \|\alpha B_j(\mathbf{x}|\mathbf{y})\| < P^{-1} \ j = 1...n\right\}. \tag{3.26}$$

then

$$|\mathcal{N}_P)| \gg P^{2n}U^{-n}L^{-n}. \tag{3.27}$$

Proof. For every $\mathbf{x} \in \mathbb{Z}^n$ let

$$\mathcal{N}_P(\mathbf{x}) = \{\mathbf{y} \in \mathbb{Z}^n : (\mathbf{x}, \mathbf{y}) \in \mathcal{N}_P\}.$$

so that

$$|\mathcal{N}_P| = \sum_{|\mathbf{x}|<P} |\mathcal{N}_P(\mathbf{x})|.$$

Let $f(t) = t - [t]$ denote the fractional part of any $t \in \mathbb{R}$. Then, for any integer $\mathbf{x}$ and any integers $r_1...r_n$ such that $0 \leq r_j < P \quad j = 1...n$ the inequalities

$$\begin{cases} P^{-1}r_1 \leq f(\alpha B_1(\mathbf{x}|\mathbf{y})) < P^{-1}(r_1 + 1) \\ \vdots \\ P^{-1}r_n \leq f(\alpha B_n(\mathbf{x}|\mathbf{y})) < P^{-1}(r_n + 1). \end{cases}$$

cannot have more than $|\mathcal{N}_P(\mathbf{x})|$ integer solutions $\mathbf{y} = (y_1, \dots y_n)$ such that

$$\begin{cases} y_1 \in (a, b) \\ \vdots \\ y_n \in (a, b). \end{cases}$$

and $b-a=P$. For if $\mathbf{y}'$ is one solution of the system of inequalities and $\mathbf{y}$ denotes the general solution, then

$$\|\alpha B_j(\mathbf{x}|\mathbf{y}-\mathbf{y}')\| < P^{-1} \qquad (j=1\dots n).$$

and $|\mathbf{y}-\mathbf{y}'|<P$. Thus the number of possibilities for $\mathbf{y}$ is at most $|\mathcal{N}_P(\mathbf{x})|$. We consider now

$$\mathcal{T}=\sum_{|\mathbf{y}|<P}\prod_{j=1}^{n}\min\left\{P,\|\alpha B_j(\mathbf{x}|\mathbf{y})\|^{-1}\right\}.$$

and we think to the hypercube

$$Q_P=\{\mathbf{y}\in\mathbb{R}^n:|\mathbf{y}|<P\}.$$

as the union of 2^n smaller hypercubes which edges have a length P. With more details: if we consider the n hyperplanes $y_1=0$, $y_2=0$ ... $y_n=0$ we divide Q_P into 2^n hypercubes which edges have length P. Of course it is not to hard define them so that they become disjoint hypercubes. (see Fig 3.1 for cases in low dimension). Dividing the summation over these 2^n hypercubes, since the length of their edges is P,we have

$$\mathcal{T}\ll|\mathcal{N}_P(\mathbf{x})|\sum_{r_1=0}^{P-1}\cdots\sum_{r_n=0}^{P-1}\prod_{j=1}^{n}\min\left\{P,\frac{P}{P-r_j-1}\right\}.$$

But

$$|\mathcal{N}_P(\mathbf{x})|\sum_{r_1=0}^{P-1}\cdots\sum_{r_n=0}^{P-1}\prod_{j=1}^{n}\min\left\{P,\frac{P}{P-r_j-1}\right\}\ll|\mathcal{N}_P(\mathbf{x})|(P\log P)^n.$$

By summing over $\mathbf{x}$ and multiplying by P^n we have

$$P^n\sum_{|\mathbf{x}|<P}\sum_{|\mathbf{y}|<P}\prod_{j=1}^{n}\min\left\{P,\|\alpha B_j(\mathbf{x}|\mathbf{y})\|^{-1}\right\}\ll P^n(P\log P)^n\sum_{|\mathbf{x}|<P}|\mathcal{N}_P(\mathbf{x})|.$$

Hence

$$P^{4n}U^{-n}<S^*(\alpha,\mathbf{B},P)\ll P^n(P\log P)^n|\mathcal{N}_P|.$$

and so

$$P^{2n}U^{-n}L^{-n}\ll|\mathcal{N}_P|.$$

□

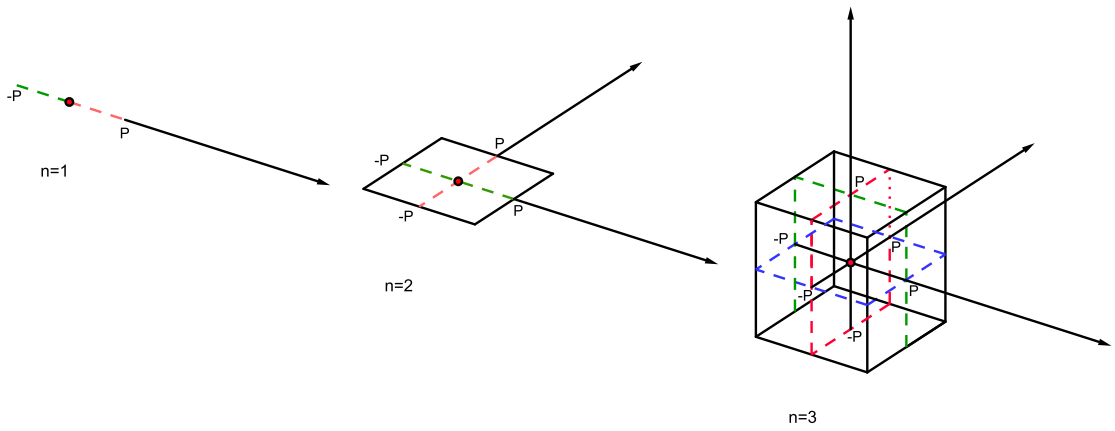

Figure 3.1: An hypercube $|\mathbf{y}| < P$ is divided into 2^n hypercubes which edges have length P

Lemma 3.7. *Let*

$$1 < T < U < PL^{-2}. \tag{3.28}$$

and suppose that (3.25) *holds. Then we have one of the following three alternatives:*

I *If*

$$\mathcal{A}_1 = \left\{(\mathbf{x}, \mathbf{y}) \in \mathfrak{A}^2_{UL^2} : \mathbf{B}\left(\mathbf{x}|\mathbf{y}\right) = 0\right\}.$$

then

$$|\mathcal{A}_1| \gg U^n T^{-n} L^{2n-1}. \tag{3.29}$$

II *If*

$$\mathcal{A}_2 = \left\{\mathbf{x} \in \mathfrak{A}_{UL^2} : \exists \mathbf{y} \in \mathfrak{A}_{UL^2},\, \|\alpha B\left(\mathbf{x}|\mathbf{y}\right)\| \ll P^{-3}U^2L^4\right\}.$$

then

$$|\mathcal{A}_2| \gg U^n T^{-n} L^{2n-1}. \tag{3.30}$$

III *The number α has a rational approximation a/q satisfying*

$$\begin{cases} (a,q) = 1 \\ 1 \le q < U^2L^4T^{-1} \\ |q\alpha - a| < P^{-3}U^2L^5. \end{cases} \tag{3.31}$$

Proof. By hypotesis $U < PL^{-2}$, thus from (3.27) we have

$$|\mathcal{N}_P| \gg P^n L^n.$$

This means that $|N_P|$ is "substantially" greater than P^n. Hence the result of Lemma 3.6 is still correct if we add to (3.26) the supplementary condition

$$\begin{cases} \mathbf{x} \neq \mathbf{0} \\ \mathbf{y} \neq \mathbf{0}. \end{cases}$$

We call

$$\mathcal{N}'_P = \left\{ (\mathbf{x}, \mathbf{y}) \in \mathfrak{A}_P^2 : \|\alpha B_j (\mathbf{x}|\mathbf{y})\| < P^{-1} \ j = 1...n, \ \mathbf{x} \neq \mathbf{0}, \ \mathbf{y} \neq \mathbf{0} \right\}.$$

and

$$\mathcal{N}'_P (\mathbf{y}) = \{ \mathbf{x} \in \mathbb{Z}^n : (\mathbf{x}, \mathbf{y}) \in \mathcal{N}_P, \mathbf{x} \neq \mathbf{0} \}.$$

Hence, by the initial remark, we have

$$\sum_{0<|\mathbf{y}|\ll P} |\mathcal{N}'_P (\mathbf{y})| \gg P^{2n} U^{-n} L^{-n}. \tag{3.32}$$

If we restrict to the subset Γ of $\mathbf{y}$ such that [9]

$$|\mathcal{N}'_P (\mathbf{y})| > c_2 P^n U^{-n} L^{-n}.$$

we have that (3.32) is still true, because the number of possible $\mathbf{y}$ is $\ll P^n$. For each such $\mathbf{y}$ we apply E.5 with

$$\begin{cases} \mathbf{u} = \mathbf{x} \\ L_j (\mathbf{u}) = \alpha B_j (\mathbf{x}|\mathbf{y}) \quad j = 1 \dots n. \end{cases}$$

We take $A = P$ and $Z = c_3$. Proceeding like in the proof of Lemma 9 of [6],and we have

$$|V(Z)| = |N'_P| > c_2 P^n U^{-n} L^{-n}.$$

We can choose Z_1 subject to (E.6) and this condition takes the form

$$c_4 P^{-1} UL < Z_1 < 1.$$

We take

$$Z_1 = c_4 P^{-1} UL^2.$$

Then form (E.7) gives

$$|V(Z_1)| \gg \left(P^{-1} UL^2\right)^n |V(Z)| = \left(P^{-1} UL^2\right)^n |N'_P (\mathbf{y})|.$$

If

$$\Omega = \left\{ \mathbf{x} \in \mathfrak{A}_{UL^2} : \|\alpha \mathbf{B} (\mathbf{x}|\mathbf{y})\| \ll P^{-2} LU^2 \right\}. \tag{3.33}$$

[9] From now on, when necessary we shall indicate suitable constants as c_2, c_3...

we have that

$$|\Omega| \gg \left(P^{-1}UL^2\right)^n |N'_P(\mathbf{y})|.$$

Thus, if

$$\Lambda = \left\{(\mathbf{x},\mathbf{y}) : \mathbf{x} \in \mathfrak{A}_{UL^2} : \|\alpha \mathbf{B}(\mathbf{x}|\mathbf{y})\| \ll P^{-2}LU^2, |\mathbf{y}| \in \mathfrak{A}_P\right\}.$$

we have

$$|\Lambda| \gg \left(P^{-1}UL^2\right)^n \sum_{0<|\mathbf{y}|\ll P} |N'_P(\mathbf{y})| \gg P^n L^n. \tag{3.34}$$

If we indicate as $N_1(\mathbf{x})$ the number of points $\mathbf{y}$ for every $\mathbf{x}$, we have

$$\sum_{0<|\mathbf{x}|\ll UL^2} N_1(\mathbf{x}) = |\Lambda| \gg P^n L^n. \tag{3.35}$$

This remains true if we limit ourselves to points $\mathbf{x}$ for which

$$N_1(\mathbf{x}) \gg c_5 P^n L^n \left(UL^2\right)^{-n}.$$

We divide these points into s subsets

$$\mathcal{D}_s = \left\{\mathbf{x} : \mathbf{x} \in \mathfrak{A}_{UL^2}, 2^s c_5 P^n U^{-n} L^{-n} < N_1(\mathbf{x}) < 2^{s+1} c_5 P^n U^{-n} L^{-n}\right\}. \tag{3.36}$$

with $(s = 0, 1, ..)$. Since $N_1(\mathbf{x}) \ll P^n$, we have $2^s \ll U^n L^n$, so the number of values of s is $\ll L$. Hence there is some $\overline{s}$ such that

$$|\mathcal{D}_{\overline{s}}| \gg P^n L^n \left(2^{\overline{s}} P^n U^{-n} L^{-n}\right)^{-1} L^{-1} = 2^{-\overline{s}} U^n L^{2n-1}.$$

For each $\mathbf{x} \in \mathcal{D}_{\overline{s}}$ we apply Proposition E.5 with $\mathbf{u} = \mathbf{y}$ and with

$$L_j(\mathbf{u}) = \alpha B_j(\mathbf{x}|\mathbf{y}) \quad (j = 1...n).$$

We take

$$\begin{cases} Z = c_6 P^{-1/2} U^{1/2} L \\ A = P^{3/2} U^{-1/2} L^{-1}. \end{cases}$$

In this way, we have that the conditions

$$\begin{cases} 0 < |\mathbf{y}| \ll P \\ \\ \|\alpha \mathbf{B}\| \ll P^{-2} LU^2. \end{cases}$$

become the (E.5). Hence, for the present application, we have

$$|V(Z)| = N_1(\mathbf{x}) \gg 2^{\overline{s}} P^n U^{-n} L^{-n}. \tag{3.37}$$

because $\mathbf{x} \in \mathcal{D}_{\overline{s}}$ and so we have the correspondent inequalities for $N_1(\mathbf{x})$. We distinguish now two cases:

First case: $2^{\overline{s}} \geq T^n$.

The condition (E.6) becomes

$$c_7 P^{-1/2} U^{1/2} L 2^{-s/n} P^{-1} UL \leq Z_1 \leq P^{-1/2} U^{1/2} L.$$

and it is satisfied if we take

$$Z_1 = c_7 P^{-3/2} U^{3/2} L^2 T^{-1}.$$

Then

$$|V(Z_1)| \gg \left(P^{-3/2} U^{3/2} L^2 T^{-1} P^{1/2} U^{-1/2} L^{-1}\right)^n |V(Z)| \gg 2^{\overline{s}} T^{-n}.$$

The inequalities (E.5) with Z_1 in place of Z become

$$\begin{cases} 0 < |\mathbf{y}| \ll ULT^{-1} \\ \\ \|\alpha \mathbf{B}(\mathbf{x}|\mathbf{y})\| \ll P^{-3} U^2 L^3 T^{-1}. \end{cases} \tag{3.38}$$

Since the number of points $\mathbf{x}$ is $\gg 2^{-s} U^n L^{2n-1}$, if Φ is the set

$$\Phi = \left\{(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in \mathfrak{A}_{UL^2}, \mathbf{y} \in \mathfrak{A}_{ULT^{-1}}, \|\alpha \mathbf{B}\| \ll P^{-3} U^2 L^3 T^{-1}\right\}.$$

we have that

$$|\Phi| \gg U^n L^{2n-1} T^{-n}.$$

Now,

- **If** $\mathbf{B}(\mathbf{x}|\mathbf{y}) = 0 \ \ \forall (\mathbf{x}, \mathbf{y}) \in \Phi$ **then** alternative (I) of the enunciation holds
- **If** $\exists (\overline{\mathbf{x}}, \overline{\mathbf{y}}) \in \Phi : \mathbf{B}(\overline{\mathbf{x}}|\overline{\mathbf{y}}) \neq 0$ **then** we obtain, as in the proof of Lemma 9 of [6], a rational approximation a/q to α such that

$$\begin{cases} 1 \leq q \ll U^2 L^3 T^{-1} \\ |q\alpha - a| < P^{-3} U^2 L^3 T^{-1}. \end{cases}$$

  This implies alternative (III) of the enunciation.

Second case: $2^{\overline{s}} > T^n$.

In this hypotesis, if

$$\Theta = \left\{\mathbf{x} \in \mathfrak{A}_{UL^2} : \ \ 2^{\overline{s}} c_5 P^n U^{-n} L^{-n} < N_1(\mathbf{x}) < 2^{\overline{s}+1} c_5 P^n U^{-n} L^{-n}\right\}.$$

then

$$|\Theta| \gg T^{-n} U^n L^{2n-1}.$$

The first thesis of E.5 tells us that there exist an integer point $\mathbf{y}_0$ such that

$$\begin{cases} 0 < |\mathbf{y}| \ll P^n \left\{ N_1 (\mathbf{x}) \right\}^{-\frac{1}{n}} \ll UL \\ \| \alpha \mathbf{B} (\mathbf{x}|\mathbf{y}) \| \ll P^{-3} U^2 L^3. \end{cases}$$

This implies alternative (II) of the enunciation. The proof is now complete. □

Lemma 3.8. *Suppose that*

- *alternative* (II) *of Lemma 3.7 holds.*
- *alternatives* (I) *and* (III) *of the same Lemma do not hold.*
- $$U^4 L^8 < P^3 T. \tag{3.39}$$

There exists

$$\begin{cases} m_1 = m_1 (P) \\ \vdots \qquad\qquad\quad \in \mathbb{Z}. \\ m_n = m_n (P) \end{cases} \tag{3.40}$$

such that, ***if***

$$\Psi = \left\{ \mathbf{x} \in \mathfrak{A}_{UL^2} : \exists \mathbf{y} \in \mathfrak{A}_{UL^2}, B_j (\mathbf{x}|\mathbf{y}) = m_j, \;\; j = 1 \dots n \right\}. \tag{3.41}$$

then

$$|\Psi| \gg U^n T^{-3n} L^{2n-1}. \tag{3.42}$$

Proof. We consider the set of points $\mathbf{x}$ as in Alternative (II) of previous Lemma. Let $\mathbf{x} \in \mathcal{A}_2$, we denote as $(\mathbf{x}, \mathbf{y})$ the correspondent pair. It is not possible that for all these pairs and for every $j = 1...n$ it is

$$B_j (\mathbf{x}|\mathbf{y}) = 0.$$

For if we would have that alternative (I) holds. Let $\overline{j}$, $(\overline{\mathbf{x}}, \overline{\mathbf{y}})$ such that

$$B_{\overline{j}} (\overline{\mathbf{x}}|\overline{\mathbf{y}}) \neq 0.$$

we obtain integers a, q such that

$$\begin{cases} (a, q) = 1 \\ 1 \leq q \ll U^2 L^4 \\ |\alpha q - a| < P^{-3} U^2 L^4. \end{cases} \tag{3.43}$$

$$q \gg U^2 L^4 T^{-1}. \tag{3.44}$$

We must have

$$q \gg U^2 L^4 T^{-1}. \tag{3.45}$$

since otherwise alternative (III) would hold. Now [10] , for each $\mathbf{x}$, $\mathbf{y}$ occurring in alternative (II), we put

$$\alpha B_j(\mathbf{x}|\mathbf{y}) = qt_j + u_j.$$

where t_j u_j are integers and $|u_j| \leq \frac{1}{2}q$. We obtain

$$|u_j| \leq q \|\alpha B_j(\mathbf{x}|\mathbf{y})\| + |\alpha q - a| \, |B_j(\mathbf{x}|\mathbf{y})| \ll .$$

$$\ll qP^{-3}U^2L^4 + P^{-3}U^2L^4U^2L^4 \ll P^{-3}U^4L^8.$$

Thus

$$|u_j| < T.$$

by (3.39). The integers u_j and t_j depend on $\mathbf{x}$ but the number of possibilities for $u_1 ... u_n$ is $\ll T^n$ and these are independent of $\mathbf{x}$. so the number of $\mathbf{x}$ for which $u_1 ... u_n$ have the same values (for suitable values) is $\gg U^n T^{-2n} L^{2n-1}$. For these $\mathbf{x}$ the values of $B_j(\mathbf{x}|\mathbf{y})$ is determined to the modulus q, and since

$$\begin{cases} |B_j(\mathbf{x}|\mathbf{y})| \ll U^2L^4 \\ q \gg U^2L^4T^{-1}. \end{cases}$$

for every $j = 1...n$ the number of possibilities for the values of the $B_j(\mathbf{x}|\mathbf{y})$ is $\ll T^n$. It follows that the number of points $\mathbf{x}$ for which

$$B_j(\mathbf{x}|\mathbf{y}) = m_j, \;\; j = 1 \dots n.$$

is $\gg U^n T^{-3n} L^{2n-1}$ for suitable $m_1 ... m_n$. This proves the result. □

Lemma 3.9. *The alternative (II) of Lemma 3.7 is superfluous if there exists $\varepsilon_0 > 0$ such that*

$$\begin{cases} T^{3n} < (UL)^{1-\varepsilon_0} \\ U^4L^8 < P^3T. \end{cases} \tag{3.46}$$

Proof. For any given $\mathbf{x}$ we consider the non-homogeneous linear system

$$\begin{cases} B_1(\mathbf{x}|\mathbf{y}) = m_1 \\ \vdots \\ B_n(\mathbf{x}|\mathbf{y}) = m_n. \end{cases}$$

[10] We follow closely the proof of Lemma 10 of [6]

The determinant of this system $H(\mathbf{x})$ is not identically zero by Proposition E.1. If

$$\mathcal{G}(\mathbf{x}) = \{\mathbf{x} : \mathbf{x} \in A_{UL^2}, H(\mathbf{x}) = 0\}.$$

then

$$|\mathcal{G}(\mathbf{x})| \ll \left(UL^2\right)^{n-1}. \tag{3.47}$$

Thus, by the first inequality of (3.46) we have that (3.42) becomes

$$|\Psi| \gg U^{n-1+\varepsilon_0} L^{2n-2+\varepsilon_0}. \tag{3.48}$$

Hence $|\mathcal{G}|$ small compared with $|\Psi|$. This means that the assertion of Lemma 3.8 remains true if we add to its hypotesis the supplementary condition $H(\mathbf{x}) \neq 0$. More formally if

$$\Psi' = \{\mathbf{x} \in \mathfrak{A}_{UL^2} : \exists \mathbf{y} \in \mathfrak{A}_{UL^2}, B_j(\mathbf{x}|\mathbf{y}) = m_j,\ H(\mathbf{x}) \neq 0,\ \ j = 1 \dots n.\}$$

it is still true that

$$|\Psi'| \gg U^n T^{-3n} L^{2n-1}. \tag{3.49}$$

We now argue as in Lemma 12 of [6] and appeal to Proposition E.7 with $R = UL^2$: this is still permissible because, the set of

$$\mathcal{M} = \{m_1 ... m_n\}.$$

of integers as in Lemma 3.8 is such that

$$|\mathcal{M}| \ll \left(UL^2\right)^2.$$

Following the proof of the cited Lemma 12 of [6] we infer that

$$|\Psi'| \ll R^{n-1+\frac{1}{2}\varepsilon_0} \ll \left(UL^2\right)^{n-1+\frac{1}{2}\varepsilon_0} = U^{n-1+\frac{1}{2}\varepsilon_0} L^{2n-2+\frac{1}{2}\varepsilon_0}.$$

But, by the first inequality of (3.46), we have that

$$|\Psi'| \gg U^{n-1+\varepsilon_0} L^{2n-2+\varepsilon_0}.$$

and this is a contradiction. □

Lemma 3.10. *There exists positive real numbers c_8 c_9 c_{10} depending only on n such that* ***if***

$$\begin{cases} U > L^{c_8} \\ U^{4-n^{-2}} < P^3 L^{-c_9}. \end{cases} \tag{3.50}$$

then *for any real α* ***either***

$$S^*(\alpha, \mathbf{B}, P) \leq P^{4n} U^{-n}. \tag{3.51}$$

***or**, there exist a rational approximation a/q to α satisfying*

$$\begin{cases} (a,q)=1 \\ 1 \le q < U^{2-n^{-2}} L^{c_{10}} \\ |q\alpha - a| < P^{-3} U^2 L^5. \end{cases} \tag{3.52}$$

Proof. We define T by

$$T^n L^{1+c} = U^{n^{-1}}.$$

where c is the constant of Lemma 3.2. The condition (3.28) of Lemma 3.7 is satisfied by (3.50) provided c_8 is suitably chosen. Similarly the condition (3.39) of Lemma 3.8 and the first condition (3.46) of Lemma 3.9 are satisfied. If (3.51) does not hold, then one of the three alternatives of Lemma 3.7 must hold. Alternative (II) is superfluous by Lemma 3.9. We are going to show now that alternative (I) is impossible. We appeal to Lemma 3.2 with $h = n$ and with $R = UL^2$. If alternative (I) were to hold we should have

$$R^{n-n^{-1}} (L)^c \gg U^n T^{-n} L^{2n-1}.$$

that is

$$U^{n-n^{-1}} L^{2n-2n^{-1}+c} \gg U^n U^{-n^{-1}} L^{2n+c}.$$

which is false.There remains only alternative (III), which gives the result stated since

$$T^{-1} = U^{-n^{-2}} L^{\frac{1+c}{n}}.$$

and so

$$1 \le q \le U^2 L^4 T^{-1} = U^{2-n^{-2}} L^{c_{10}}.$$

with $c_{10} = \frac{1+c}{n}$. □

3.9 The estimation of $S^*(\alpha, \mathbf{B}, P)$ if $h(C) < n$

Lemma 3.11. *There exists positive real numbers c_8, c_9, c_{10} depending only on n such that **if***

$$\begin{cases} U > L^{c_8} \\ U^{4-n^{-2}} < P^3 L^{-c_9}. \end{cases} \tag{3.53}$$

then** for any real α **either

$$S^*(\alpha, \mathbf{B}, P) \le P^{4n} U^{-n} \tag{3.54}$$

***or** there exist a rational approximation a/q to α satisfying*

$$\begin{cases} (a,q)=1 \\ 1 \le q < U^{2-n^{-2}} L^{c_{10}} \\ |q\alpha - a| < P^{-3} U^2 L^5. \end{cases} \tag{3.55}$$

Proof. If

$$S^*(\alpha, \mathbf{B}, P) > P^{4n}U^{-h}. \tag{3.56}$$

we have, as the analogue of Lemma 3.6 that if

$$\mathcal{N}_P = \left\{(\mathbf{x}, \mathbf{y}) \in \mathfrak{A}_P^2 : \|\alpha B_j(\mathbf{x}|\mathbf{y})\| < P^{-1}\ j = 1...n\right\}.$$

then

$$|\mathcal{N}_P| \gg P^{2n}U^{-h}L^{-n}.$$

We follow now the lines of proof of Lemma 3.7.

- With the same choice of Z_1 we obtain that **if**

  $$\mathcal{K} = \left\{(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in \mathfrak{A}_{UL^2}, \mathbf{y} \in \mathfrak{A}_P \ \ \|\alpha \mathbf{B}(\mathbf{x}|\mathbf{y})\| < P^{-2}UL^2\right\}.$$

  then

  $$|\mathcal{K}| \gg P^n U^{n-h}L^{-n}.$$

- The equation (3.37) is replaced by

  $$|V(Z)| = N_1(\mathbf{x}) \gg 2^{\overline{s}}P^nU^{-h}L^{-n}.$$

- The set defined by (3.36) is replaced by

  $$D_s = \left\{\mathbf{x} : \mathbf{x} \in \mathfrak{A}_{UL^2}, 2^s c_5 P^n U^{-h}L^{-n} < N_1(\mathbf{x}) < 2^{s+1}c_5 P^n U^{-h}L^{-n}\right\}.$$

  although the lover bound for the number of points $\mathbf{x}$ is the same as before.

- We apply Proposition E.5 with

  $$Z_1 = c_7 P^{-3/2}U^{3/2}L^2T_1^{-1}.$$

  where $T_1 > 1$ is to be chosen later. This satisfies the condition (E.6) provided

  $$T_1 < U^{1-\frac{h}{n}}. \tag{3.57}$$

- Further, we have that if

  $$\mathcal{J} = \left\{(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in A_{UL^2}, \mathbf{y} \in A_{c_7 ULT_1^{-1}}, \|\alpha \mathbf{B}(\mathbf{x}|\mathbf{y})\| < c_7 P^{-3}U^2L^3T_1^{-1}\right\}.$$

  then

  $$|\mathcal{J}| \gg U^{2n-h}L^{2n-1}T_1^{-n}. \tag{3.58}$$

Now, if we would have that for every $(\mathbf{x},\mathbf{y}) \in \mathcal{J}$ and for every $j = 1...n$ we have that $B_j(\mathbf{x}|\mathbf{y}) = 0$ we could appeal to Lemma 3.2. Taking $R = UL^2$ we would have that

$$|J| \ll \left(UL^2\right)^{2n-h-n^{-1}} L^c.$$

But, if we would choose [11]

$$T_1 = U^{n^{-2}} L^{-c_{11}}.$$

with c_{11} a suitable constant, we would obtain a contradiction with (3.58). Hence, there exist $(\overline{\mathbf{x}},\overline{\mathbf{y}})$ and $\overline{j}$ such that

$$B_{\overline{j}}(\overline{\mathbf{x}}|\overline{\mathbf{y}}) \neq 0.$$

This leads, in the usual way, from the condition $\|\alpha \mathbf{B}(\mathbf{x}|\mathbf{y})\| < c_7 P^{-3} U^2 L^3 T_1^{-1}$ to a rational approximation a/q to α satisfying

$$\begin{cases} (a,q) = 1 \\ 1 \leq q \ll U^2 L^3 T_1^{-1} \\ |q\alpha - a| \ll P^{-3} U^2 L^3 T_1^{-1}. \end{cases}$$

These conditions are somewhat stronger than those asserted in the enunciate. □

3.10 The estimates of $S(\alpha)$ and $S_{a,q}$

Lemma 3.12. *Let $\phi(\mathbf{x})$ a cubic polynomial as before. let $\mathcal{P}$ a fixed parallelepiped of suitable shape in $\mathbb{R}^n$. Let P a "large" positive real parameter and let $S(\alpha)$ defined as before. Let U satisfying the conditions* (3.50). ***Then*** *either*

$$|S(\alpha)| \leq P^n U^{-\frac{h^*}{4}}. \tag{3.59}$$

or there exist a rational approximation a/q to α such that

$$\begin{cases} (a,q) = 1 \\ 1 \leq q < U^{2-n^{-2}} L^{c_{10}} \\ |q\alpha - a| < P^{-3} U^2 L^5. \end{cases} \tag{3.60}$$

Proof. By Lemma 3.5 we have that

$$|S(\alpha)|^4 \ll P^{4n-4-\sum_{i=1}^{s} n_i} \prod_{i=1}^{s} S^*(\alpha, \mathbf{B}_i, P). \tag{3.61}$$

[11] The present choice is fully compatible with (3.57)

Let α such that it does not have a rational approximation satisfying (3.60). Then, *a fortiori*, it is impossible to have

$$\begin{cases} (a,q)=1 \\ 1 \le q < U^{2-n_i^{-2}} L^{c_{10}} \\ |q\alpha - a| < P^{-3} U^2 L^5. \end{cases}$$

for every $i = 1...s$ because $n_i < n$. Now,

- **If** $h_i = n_i$ **then**, by Lemma 3.10, we have that

$$|S^*(\alpha, \mathbf{B_i}, P)| \le P^{4n_i} U^{-n_i} = P^{4n_i} U^{-h_i}.$$

- **If** $h_i < n_i$ then, by Lemma 3.11, we have that

$$|S^*(\alpha, \mathbf{B_i}, P)| \le P^{4n_i} U^{-h_i}.$$

Hence, by (3.61), we have that

$$|S(\alpha)|^4 \ll P^{4n-4-\sum_{i=1}^{s} n_i} \prod_{i=1}^{s} P^{4n_i} U^{-h_i}.$$

Thus

$$|S(\alpha)|^4 \ll P^{4n-4\sum_{i=1}^{s} n_i} P^{4\sum_{i=1}^{s} n_i} U^{-\sum_{i=1}^{s} h_i} \ll P^{4n} U^{-h^*}.$$

and from this the result follows. □

Lemma 3.13. *Let a, q integers with*

$$\begin{cases} q > 0 \\ (a,q) = 1. \end{cases}$$

If

$$S_{a,q} = \sum_{\mathbf{z}(\bmod q)} e\left(\frac{a}{q}\phi(\mathbf{z})\right). \tag{3.62}$$

then

$$|S_{a,q}| \ll q^{n-h^*/\left(8-4n^{-2}\right)} (\log q)^{c_{12}}. \tag{3.63}$$

Proof. We appeal to Lemma 3.12 with $\alpha = a/q$ and with P to be chosen later. the second alternative of Lemma 3.12 is the existence of integers a' and q' such that

$$\begin{cases} (a',q') = 1 \\ 1 \le q' < U^{2-n^{-2}} L^{c_{10}} \\ \left| q' \frac{a}{q} - a' \right| < P^{-3} U^2 L^5. \end{cases}$$

Suppose that

$$P^3U^{-2}L^{-5} > q. \tag{3.64}$$

We have

$$\left|\frac{aq' - a'q}{qq'}\right| < \frac{P^{-3}U^2L^5}{q'}.$$

and so

$$|aq' - a'q| < P^{-3}U^2L^5q < 1.$$

which means

$$\frac{a}{q} = \frac{a'}{q'}.$$

Since $(a, q) = 1$ and $(a', q') = 1$ this means that $a = a'$ and $q = q'$. But if we choose

$$U^{2-n^{-2}}L^{c_{10}} \leq q. \tag{3.65}$$

this is impossible. Hence, in order to avoid this alternative, it is enough to let (3.64) and (3.65) hold. In this case we have that the estimate (3.59) is applicable. The parallelepiped $P\mathcal{P}$ in the definition of $S(\alpha)$ is given by conditions of the type

$$\begin{cases} \lambda_1 P < a_{11}x_1 + \ldots a_{1n}x_n < \mu_1 P \\ \vdots \\ \lambda_n P < a_{n1}x_1 + \ldots a_{nn}x_n < \mu_n P. \end{cases} \tag{3.66}$$

where

- $a_{i,j} \in \mathbb{Q}$ for every $i, j = 1...n$.
- $\lambda_i \in \mathbb{R}$ for every $i = 1...n$.
- $\mu_i \in \mathbb{R}$ for every every $i = 1...n$.

The number of integer points $\mathbf{x}$ satisfying (3.66) and lying in a given residue class (mod q) is

$$n(P) = A\left(\frac{P}{q}\right)^n + O\left(\left(\frac{P}{q}\right)^{n-1}\right).$$

where A is a positive constant. We have that

$$S\left(\frac{a}{q}\right) = n(P)\, S_{a,q}.$$

hence

$$S\left(\frac{a}{q}\right) = AP^n q^{-n} S_{a,q} + S_{a,q} O\left(\left(\frac{P}{q}\right)^{n-1}\right).$$

But trivially $|S_{a,q}| \ll q^n$ and so

$$S\left(\frac{a}{q}\right) = AP^n q^{-n} S_{a,q} + O\left(P^{n-1} q\right).$$

We can write

$$AP^n q^{-n} |S_{a,q}| \leq \left|S\left(\frac{a}{q}\right)\right| + O\left(P^{n-1} q\right).$$

From (3.59) we have

$$\left|S\left(\frac{a}{q}\right)\right| \leq P^n U^{-\frac{h^*}{4}}.$$

an so we can deduce that

$$|S_{a,q}| \ll q^n U^{-\frac{h^*}{4}} + P^{-1} q^{n+1}.$$

If we choose $P = q^{n+1}$, we have that the term $P^{-1} q^{n+1}$ becomes negligible. We can also choose

$$U^{2-n^{-2}} (\log P)^{c_{10}} = q.$$

With this choice, we have that (3.64) and (3.65) hold as well as (3.50) and this let Lemma 3.12 applicable. Now, we have

$$U = q^{\frac{1}{2-n^{-2}}} (\log P)^{\frac{c_{10}}{2-n^{-2}}}.$$

and this get immediately

$$|S_{a,q}| \ll q^{n-\frac{h^*}{8-4n^{-2}}} (\log q)^{\frac{c_{10}}{2-n^{-2}}}.$$

The result is achieved, with $c_{12} = \frac{c_{10}}{2-n^{-2}}$. □

3.11 Minor arcs

Definition 3.7. *Let $I = (0,1) \subset \mathbb{R}$. We shall denote as*

$$\mathcal{E}(U) = \left\{\alpha \in I : \exists a, q \in \mathbb{Z}, (a,q) = 1, 1 \leq q \leq U^{2-n^{-2}} L^{c_{10}}, |q\alpha - a| < P^{-3} U^2 L^5\right\}.$$

We shall write also

$$\mathcal{CE}(U) = I - \mathcal{E}(U).$$

Definition 3.8. *If*

$$U_1 = L^{c_{13}}. \tag{3.67}$$

with c_{13} is a suitable "large" positive constant, we shall define the ***minor arcs*** *as*

$$\mathfrak{m} = \mathcal{CE}\left(U_1\right).$$

Definition 3.9. *We shall denote as*

$$f_1 = \inf_{\mathbf{x}\in\mathcal{P}} C\left(\mathbf{x}\right).$$

and

$$f_2 = \sup_{\mathbf{x}\in\mathcal{P}} C\left(\mathbf{x}\right).$$

We need to use also two real numbers g_1 and g_2 such that

$$0 < g_1 < f_1 < f_2 < g_2. \tag{3.68}$$

Their choice is arbitrary and from now onward we shall suppose them as fixed.

Definition 3.10. *We define*

$$T\left(\alpha\right) = \sum_{\substack{g_1 P^3 < p < g_2 P^3 \\ p\in\mathbb{P}}} e\left(\alpha p\right). \tag{3.69}$$

Lemma 3.14. *If $h^* \geq 8$ we have*

$$\int_{\mathfrak{m}} \left|S\left(\alpha\right) T\left(-\alpha\right)\right| d\alpha \ll P^n L^{-c_{14}}. \tag{3.70}$$

where c_{14} is "large" when c_{13} is "large"

Proof. If we consider the set-function

$$U \to \mathcal{E}\left(U\right).$$

we have that it is an increasing function i.e

$$U_1 < U_2 \Rightarrow \mathcal{E}\left(U_1\right) \subseteq \mathcal{E}\left(U_2\right).$$

and, if

$$U^{4-n^{-2}} L^{c_{10}-5} > P^3. \tag{3.71}$$

we have that

$$\mathcal{E}(U) = (0,1).$$

For, by the classical Theorem of Dirichlet on Diophantine approximation, there is always a rational approximation to α satisfying

$$\begin{cases} (a,q) = 1 \\ 1 \leq q \leq U^{2-n^{-2}} L^{c_{10}} \\ |q\alpha - a| \leq U^{-2+n^{-2}} L^{-c_{10}}. \end{cases}$$

and condition (3.71) ensures that this implies (3.60).
Now, if

$$\mathcal{F}(U) = \mathcal{E}(2U) - \mathcal{E}(U).$$

then, we can write

$$I = \mathcal{E}(U_1) \cup \left\{ \bigcup_{j=0}^{s} \mathcal{F}\left(2^j U_1\right) \right\}.$$

where s is the least integer such that $U = 2^{s+1}U_1$ satisfies (3.71). The subsets $\mathcal{F}(2^j U_1)$ are pairwise disjoints and

$$\mathfrak{m} = \bigcup_{j=0}^{s} \mathcal{F}\left(2^j U_1\right).$$

It is not hard to see that $s \ll L$. We take now

$$\begin{cases} U = 2^t U_1 \\ 0 \leq t \leq s. \end{cases}$$

By Lemma 3.12, if $\alpha \in \mathcal{F}(U)$ we have

$$|S(\alpha)| \ll P^n U^{-\frac{h^*}{\cdot}4}$$

since the values of U under consideration satisfy (3.50) We have also that

$$\mu_{\mathcal{L}}(\mathcal{F}(U)) \leqslant \mu_{\mathcal{L}}(\mathcal{E}(2U)) \leqslant \sum_{1 \leqslant q \leqslant M(U)} \sum_{1 \leqslant a \leqslant q} 2q^{-1} P^{-3} (2U)^2 L^5.$$

where $\mu_{\mathcal{L}}$ denotes the Lebesgue's measure on $\mathbb{R}$ and $M(U) = (2U)^{2-n^{-2}} L^{c_{10}}$.
Hence

$$\mu_{\mathcal{L}}(\mathcal{F}(U)) \ll \left(P^{-3} U^2 L^5\right) \left(U^{2-n^{-2}} L^{c_{10}}\right).$$

It follows that

$$\int\limits_{\mathcal{F}(U)} |S(\alpha)|\,|T(-\alpha)|\,d\alpha \leqslant P^n U^{-\frac{h^*}{4}} \int\limits_{\mathcal{F}(U)} |T(-\alpha)|\,d\alpha.$$

But

$$\int\limits_{\mathcal{F}(U)} |T(-\alpha)|\,d\alpha \leqslant \{\mu_{\mathcal{L}}(\mathcal{F}(U))\}^{\frac{1}{2}} \left\{\int\limits_0^1 |T(-\alpha)|\,d\alpha\right\}^{\frac{1}{2}}.$$

Hence

$$\int\limits_{\mathcal{F}(U)} |S(\alpha)|\,|T(-\alpha)|\,d\alpha \ll \left\{P^n U^{-\frac{h^*}{4}}\right\} \left\{P^{-3} U^{4-n^{-2}} L^{c_{10}+5}\right\}^{\frac{1}{2}} \left\{P^3 L^{-1}\right\}^{\frac{1}{2}}.$$

and so

$$\int\limits_{\mathcal{F}(U)} |S(\alpha)|\,|T(-\alpha)|\,d\alpha \ll P^n U^{2-\frac{h^*}{4}-\frac{n^{-2}}{2}} L^{c_{15}}.$$

where $c_{15} = \frac{c_{10}}{2} + 2$ and it depends on n only. Since $h^* \geq 8$ we can write

$$\int\limits_{\mathcal{F}(U)} |S(\alpha)|\,|T(-\alpha)|\,d\alpha \ll P^n U^{-\frac{n^{-2}}{2}} L^{c_{15}}. \tag{3.72}$$

Now,

$$\int\limits_m |S(\alpha)|\,|T(-\alpha)|\,d\alpha = \sum_{j=0}^{s} \int\limits_{\mathcal{F}(2^{j+1}U_1)} |S(\alpha)|\,|T(-\alpha)|\,d\alpha.$$

and

- The number of sets $\mathcal{F}$ is $\ll L$
- To each of such sets we can apply (3.72)
- The least value of U is $U_1 = L^{c_1 3}$

Since

$$\int\limits_{\mathfrak{m}} |S(\alpha)|\,|T(-\alpha)|\,d\alpha = \sum_{j=0}^{s} \mathcal{I}_j.$$

where

$$\mathcal{I}_j = \int\limits_{\mathcal{F}(2^{j+1}U_1)} |S(\alpha)|\,|T(-\alpha)|\,d\alpha \ll P^n \left\{2^{j+1}\right\}^{-\frac{n^{-2}}{2}} L^{-\frac{n^{-2}}{2}c_{13}+c_{15}}.$$

we have

$$\sum_{j=0}^{s} \mathcal{I}_j \ll P^n L^{-\frac{n^{-2}}{2} c_{13}+c_{15}} 2^{-\frac{L}{2n^2}} \ll P^n L^{-\frac{n^{-2}}{2} c_{13}+c_{15}}.$$

Hence

$$\int_m |S(\alpha)| \, |T(-\alpha)| \, d\alpha \ll P^n L^{-c_{14}}.$$

as stated. □

3.12 Major arcs

Definition 3.11. *We denotes with*

$$\mathfrak{M}_{a,q} = \left\{ \alpha \in I : \left| \alpha - \frac{a}{q} \right| < P^{-3} L^k \right\}. \tag{3.73}$$

where k is a positive constant while a and q are the same as in the previous section.

Definition 3.12. *We denote by*

$$\mathfrak{M} = \bigcup_{1 \le q \le L^k} \bigcup_{\substack{1 \le a < q \\ (a,q)=1}} M_{a,q}. \tag{3.74}$$

*and we call it "**major arcs**"*

It easy to show that the intervals $\mathfrak{M}_{a,q}$ are disjoint. Moreover, if we choose k so that

$$\begin{cases} k > (2 - n^{-2}) \, c_{13} + c_{10} \\ k > 2c_{13} + 5. \end{cases} \tag{3.75}$$

then, we have

$$\mathcal{E}(U_1) \subseteq \mathfrak{M}.$$

Lemma 3.15. ***If** $\alpha \in \mathfrak{M}_{a,q}$ **then***

$$S(\alpha) = q^{-n} S_{a,q} I(\beta) + O\left(P^{n-1} L^{2k}\right). \tag{3.76}$$

where

$$I(\beta) = \int_{P\mathcal{P}} e(\beta \phi(\xi)) d\xi. \tag{3.77}$$

and

$$\beta = \alpha - \frac{a}{q}.$$

Proof. We consider

$$S(\alpha) = \sum_{\mathbf{x} \in P\mathcal{P}} e(\alpha\phi(\mathbf{x})).$$

and we write it as

$$S(\alpha) = \sum_{\mathbf{x} \in P\mathcal{P}} e\left(\left(\beta + \frac{a}{q}\right)\phi(\mathbf{x})\right).$$

and so

$$S(\alpha) = \sum_{\substack{\mathbf{x} \in P\mathcal{P} \\ \mathbf{x} = q\mathbf{y}+\mathbf{z} \\ \mathbf{y},\mathbf{z} \in \mathbb{Z}^n}} e\left(\frac{a}{q}\phi(q\mathbf{y}+\mathbf{z})\right) \sum_{\substack{\mathbf{x} \in P\mathcal{P} \\ \mathbf{x} = q\mathbf{y}+\mathbf{z} \\ \mathbf{y},\mathbf{z} \in \mathbb{Z}^n}} e(\beta\phi(q\mathbf{y}+\mathbf{z})).$$

Hence

$$S(\alpha) = \sum_{\mathbf{z} \ (\mathrm{mod}\ q)} e\left(\frac{a}{q}\phi(\mathbf{z})\right) \sum_{\substack{\mathbf{x} \in P\mathcal{P} \\ \mathbf{x} = q\mathbf{y}+\mathbf{z} \\ \mathbf{y},\mathbf{z} \in \mathbb{Z}^n}} e(\beta\phi(q\mathbf{y}+\mathbf{z})).$$

We can also write

$$S(\alpha) = \sum_{\mathbf{z} \ (\mathrm{mod}\ q)} e\left(\frac{a}{q}\phi(\mathbf{z})\right) \sum_{\mathbf{y} \in \mathcal{P}'} e(\beta\phi(q\mathbf{y}+\mathbf{z})).$$

where

$$\mathcal{P}' = \left(Pq^{-1}\right)\mathcal{P} - q^{-1}\mathbf{z}.$$

is the parallelepiped obtained from $\mathcal{P}$ by means of an homothetic transformation of constant $Pq^{-}1$ and a translazion of vector $-q^{-1}\mathbf{z}$. We can regard $\mathcal{P}'$ as a union of cubes of side 1 together with a boundary zone. We have that

- The number of cubes is [12]

$$n_{cubes} = V_{\mathcal{P}}\left(Pq^{-1}\right)^n + O\left(\left(Pq^{-1}\right)^{n-1}\right).$$

- The boundary zone contains $O\left(\left(Pq^{-1}\right)^{n-1}\right)$ integer point and also has a volume $O\left(\left(Pq^{-1}\right)^{n-1}\right)$.

[12] We remember here that $V_{\mathcal{P}}$ stands for the volume of $\mathcal{P}$

Each cube correspond to a single term of the exponential sum and we can replace this term by

$$\int_c e\left(\beta\phi\left(q\eta+\mathbf{z}\right)\right)d\eta+O\left(\left|\beta\right|q^3\left(Pq^{-1}\right)^2\right).$$

where c stands for a cube. If $\mathfrak{C}$ stands for the set of all the cubes which split the parallelepiped $\mathcal{P}'$ and if we consider the contribute of the boundary zone, we have

$$S\left(\alpha\right)=\sum_{c\in\mathfrak{C}}\left\{\int_c e\left(\beta\phi\left(q\eta+\mathbf{z}\right)\right)d\eta+O\left(\left|\beta\right|q^3\left(Pq^{-1}\right)^2\right)\right\}+O\left(q^n\left(Pq^{-1}\right)^{n-1}\right).$$

This gives

$$S\left(\alpha\right)=q^{-n}S_{a,q}I\left(\beta\right)+O\left(q^n\left|\beta\right|q^3\left(Pq^{-1}\right)^{n+2}\right)+O\left(q^n\left(Pq^{-1}\right)^{n-1}\right).$$

Since

$$\begin{cases}\left|\beta\right|<P^{-3}L^k\\ q\leq L^k.\end{cases}$$

we obtain the result. □

Lemma 3.16. *If $\alpha\in\mathcal{M}_{a,q}$ we have*

$$T\left(\alpha\right)=\frac{\mu\left(q\right)}{\phi\left(q\right)}I_1\left(\beta\right)+O\left(P^3\exp\left(-c_{16}L^{1/2}\right)\right).$$

where

$$I_1\left(\beta\right)=\int_{g_1P^3}^{g_2P^3}\frac{e\left(\beta x\right)}{\log x}dx.$$

Proof. It is possible to find the proof in [34] VI Satz 3.3. The only difference is that while here we have an integral, in that book is considered a series of the kind

$$\sum_{n=m_1}^{m_2}\frac{e\left(\beta n\right)}{\log n}.$$

where

$$\begin{cases}m_1=[g_1P^3]\\ m_2=[g_2P^3]+1.\end{cases}$$

Anyway, with the standard comparison's technique of a series

$$\sum_{n=m_1}^{m_2} f(n).$$

with

$$\int_{m_1}^{m_2} f(x)\,dx.$$

where f is monotone, it is easily seen that the difference between them is $O(L^{k-1})$ hence negligible. □

Lemma 3.17. ***If*** $h^* \geq 8$ ***then***

$$\int_{\mathfrak{M}} S(\alpha)T(-\alpha)\,d\alpha = \{\mathfrak{S} + E_1\} \int_{|\beta|<P^{-3}L^k} I(\beta)\,I_1(-\beta)\,d\beta + E_2. \tag{3.78}$$

where

- $E_1 = O(L^{-c_{17}})$.
- $E_2 = O\left(P^n e^{-c_{18}L^{1/2}}\right)$.
- c_{18} *is any real number such that* $0 < c_{18} < c_{16}$.

and

$$\mathfrak{S} = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)} q^{-n} S_{a,q}. \tag{3.79}$$

is the singular series of the problem.

Proof. If $\alpha \in \mathfrak{M}_{a,q}$, from 3.15 and 3.16 we have

- $S(\alpha) = \underbrace{q^{-n}S_{a,q}I(\beta)}_{F_1} + e_1$.
- $T(-\alpha) = \underbrace{\frac{\mu(q)}{\phi(q)}I_1(-\beta)}_{F_2} + e_2$.

where

- $e_1 = O\left(P^{n-1}L^{2k}\right)$.

- $e_2 = O\left(P^3 \exp\left(-c_{16} L^{1/2}\right)\right)$.

Hence

$$S(\alpha) T(-\alpha) = \frac{\mu(q)}{\phi(q)} q^{-n} S_{a,q} I(\beta) I_1(-\beta) + E.$$

where

$$E = e_1 F_2 + e_2 F_1 + e_1 e_2.$$

Thus

$$\int\limits_{|\beta|<P^{-3}L^k} S(\alpha) T(-\alpha)\, d\alpha = \frac{\mu(q)}{\varphi(q)} q^{-n} S_{a,q} \int\limits_{|\beta|<P^{-3}L^k} I(\beta) I_1(-\beta)\, d\beta + \int\limits_{|\beta|<P^{-3}L^k} E d\beta.$$

On summing over a and then q, we obtain

- $$\int\limits_M S(\alpha) T(-\alpha)\, d\alpha.$$

  for the right-hand side.

- $$\sum_{q \le L^k} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)} q^{-n} S_{a,q} \int\limits_{|\beta|<P^{-3}L^k} I(\beta) I_1(-\beta)\, d\beta.$$

  for the main term in the left-hand side

- $$\int\limits_{|\beta|<P^{-3}L^k} \mathcal{E} d\beta.$$

  for the error's term, where $\mathcal{E} = \sum\limits_{q \le L^k} \sum\limits_{\substack{a=1 \\ (a,q)=1}}^{q} E$.

Since

- $\frac{|\mu(q)|}{|\varphi(q)|} \le 1$ for every $q \ge 1$.
- By Lemma 3.13 with the fact that $h^* \ge 8$, there exists a $\delta > 0$ such that, for every $q \ge 1$ and for every $1 \le a \le (a,q) = 1$, it is $|q^{-n} S_{a,q}| \ll q^{-1-\delta}$.

we have that the series

$$\mathfrak{S}=\sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q}\frac{\mu\left(q\right)}{\varphi\left(q\right)}q^{-n}S_{a,q}. \tag{3.80}$$

is convergent and we can write

$$\mathfrak{S}-\sum_{q\leq L^{k}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\frac{\mu\left(q\right)}{\varphi\left(q\right)}q^{-n}S_{a,q}=O\left(L^{-c_{17}}\right).$$

where c_{17} is a suitable positive constant. Thus,so far we have

$$\int_{\mathfrak{M}}S\left(\alpha\right)T\left(-\alpha\right)d\alpha=\left(\mathfrak{S}+O\left(L^{-c_{17}}\right)\right)\int_{|\beta|<P^{-3}L^{k}}I\left(\beta\right)I_{1}\left(-\beta\right)d\beta+\int_{|\beta|<P^{-3}L^{k}}Ed\beta.$$

Now, we are dealing with

$$\int_{|\beta|<P^{-3}L^{k}}\mathcal{E}d\beta.$$

With the definition of E, F_1, F_2, e_1, e_2 given above, and using the trivia estimates

- $|I\left(\beta\right)|\ll P^{n}$.
- $|I_{1}\left(\beta\right)|\ll P^{3}L^{-1}$.

it is easy to show that

$$E\ll q^{-1-\delta}P^{n+3}e^{-c_{16}L^{1/2}}+\frac{1}{\varphi\left(q\right)}P^{n+2}L^{2k-1}+P^{n+2}L^{2k}e^{-c_{16}L^{1/2}}.$$

and from this we have

$$\int_{|\beta|<P^{-3}L^{k}}Ed\beta\ll P^{-3}L^{k}\max_{|\beta|<P^{-3}L^{k}}\left(E\right)\ll q^{-1-\delta}P^{n}e^{-c_{16}L^{1/2}}.$$

and so

$$\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{|\beta|<P^{-3}L^{k}}Ed\beta\ll q^{-\delta}P^{n}e^{-c_{16}L^{1/2}}.$$

and from this

$$\sum_{q\leq L^k}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{|\beta|<P^{-3}L^k} Ed\beta \ll L^k P^n e^{-c_{16}L^{1/2}}.$$

If we choose $0 < c_{18} < c_16$ we can write

$$L^k P^n e^{-c_{16}L^{1/2}} \ll P^n e^{-c_{18}L^{1/2}}.$$

Hence

$$\int_{|\beta|<P^{-3}L^k} \mathcal{E}d\beta = O\left(P^n e^{-c_{18}L^{1/2}}\right).$$

and the result follows. □

3.13 The singular series

Lemma 3.18. ***If*** *for every integer $m > 1$ there is a $\mathbf{x} \in \mathbb{Z}^n$ such that $\phi(\mathbf{x}) \not\equiv 0 \pmod m$* ***then***

$$\mathfrak{S} > 0.$$

Proof. We consider

$$A(q) = \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-n} S_{a,q}.$$

It is a standard task to show that this $A(q)$ is a multiplicative function. [13] Hence, by (3.79)

$$\mathfrak{S} = \prod_{p\in\mathbb{P}}\left(1 - \frac{1}{p-1}p^{-n}\sum_{a=1}^{p-1} S_{a,p}\right).$$

If we consider

$$F_p = \left(1 - \frac{1}{p-1}p^{-n}\sum_{a=1}^{p-1} S_{a,p}\right).$$

we have that

$$F_p \ll 1 + \frac{1}{p-1}(p-1)\left|p^{-n}S_{a,p}\right| \ll 1 + p^{-1-\delta}.$$

[13] See, for example,[28]

because we know, from Lemma 3.13 that there exist $\delta > 0$ such that $|p^{-n}S_{a,p}| < p^{-1-\delta}$ for every p. It follows that the infinite product is absolutely convergent and, in order to show that it is different from zero, it is enough to show that

$$p^{-n}\sum_{a=1}^{p-1} S_{a,p} < p-1.$$

for every $p \in \mathbb{P}$. If $\mathfrak{S} = 0$ it would means that there exists a $p_0 \in \mathbb{P}$ such that

$$\sum_{a=1}^{p_0-1} p_0^{-n} S_{a,p_0} = p_0 - 1.$$

But

$$\left|\sum_{a=1}^{p_0-1} p_0^{-n} S_{a,p_0}\right| \leq \sum_{a=1}^{p-1} \left|p^{-n} S_{a,p_0}\right| \leq p_0 - 1.$$

Since, for every $1 \leq a \leq p_0$ we have $\left|p_0^{-n} S_{a,p_0}\right| \leq 1$, we must have

$$p_0^{-n} S_{a,p_0} = 1.$$

This means

$$p_0^{-n} \sum_{\mathbf{z} \,(\bmod\, p_0)} e\left(\frac{a}{p_0}\phi(\mathbf{z})\right) = 1.$$

and so

$$e\left(\frac{a}{p_0}\phi(\mathbf{z})\right) = 1.$$

for every $1 \leq a \leq p_0 - 1$. This means

$$\phi(\mathbf{z}) = 0 \quad \forall\, \mathbf{z} \,(\bmod\, p_0).$$

and this contradicts the hypothesis. □

3.14 The proof of the first theorem of Pleasants

Proof. By (3.68) we have

$$g_1 P^3 < \phi(\mathbf{x}) < g_2 P^3.$$

for every $\mathbf{x} \in \ P\mathcal{P}$. Hence

$$\mathcal{M}(P) = \int_0^1 S(\alpha) T(-\alpha) d\alpha. \tag{3.81}$$

We write

$$\int_0^1 S(\alpha) T(-\alpha) d\alpha = \int_{\mathfrak{M}} S(\alpha) T(-\alpha) d\alpha + \int_{\mathcal{C}\mathfrak{M}} S(\alpha) T(-\alpha) d\alpha.$$

where $\mathcal{C}\mathfrak{M} = I - \mathfrak{M}$. We have already observed that if (3.75) holds then $\mathcal{E}(U_1) \subseteq \mathfrak{M}$ hence

$$\mathcal{C}\mathfrak{M} \subseteq \mathcal{C}\mathcal{E}(U_1) = \mathfrak{m}.$$

Hence, by Lemma 3.14

$$\int_{\mathcal{C}\mathfrak{M}} |S(\alpha) T(-\alpha)| d\alpha \ll P^n L^{-c_{14}}.$$

where c_{14} can be taken large by taking k large. From Lemma 3.17 it follows that

$$\mathcal{M}(P) = \left\{\mathfrak{S} + O\left(L^{-c_{17}}\right)\right\} J(P) + O\left(P^n L^{-c_{14}}\right). \tag{3.82}$$

where

$$J(P) = \int_{|\beta| < P^{-3} L^k} I(\beta) I_1(-\beta) d\beta. \tag{3.83}$$

- By definition of $I(\beta)$, we have

$$I(\beta) = \int_{P\mathcal{P}} e(\beta\varphi(\xi')) d\xi'.$$

Thus, by means of the substitution $\xi' = P\xi$, we have

$$I(\beta) = P^n \int_{\mathcal{P}} e(\beta\varphi(P\xi)) d\xi.$$

By writing

$$\phi(P\xi) = P^3 C(\xi) + P^2 Q(\xi) + PL(\xi) + N.$$

we easily obtain

$$I(\beta) = P^n \int_{\mathcal{P}} e\left(\beta P^3 C(\xi)\right) d\xi + O\left(P^n |\beta| P^2\right).$$

and finally

$$I(\beta) = \underbrace{P^n \int_{\mathcal{P}} e\left(\beta P^3 C(\xi)\right) d\xi}_{A(\beta)} + \underbrace{O\left(P^{n-1} L^k\right)}_{E_1}. \tag{3.84}$$

- By definition of $I_1(\beta)$, we have

$$I_1(\beta) = \int_{g_1 P^3}^{g_2 P^3} \frac{e(\beta x')}{\log x'} dx'.$$

Thus by means of the substitution $x' = P^3 x$, we have

$$I_1(\beta) = P^3 \int_{g_1}^{g_2} \frac{e(\beta P^3 x)}{\log P^3 x} dx.$$

Thus

$$I_1(\beta) = \frac{P^3}{3L} \int_{g_1}^{g_2} e\left(\beta P^3 x\right) dx - \frac{P^3}{3L} \int_{g_1}^{g_2} \frac{e(\beta P^3 x) \log x}{3L + \log x} dx.$$

Integrating by part and using the mean value theorem it is possible to show that

$$\frac{P^3}{3L} \int_{g_1}^{g_2} \frac{e(\beta P^3 x) \log x}{3L + \log x} dx = O\left(P^3 L^{-2} \min\left\{1, \left|\beta P^3\right|^{-1}\right\}\right).$$

Hence

$$I_1(\beta) = \underbrace{\frac{P^3}{3L} \int_{g_1}^{g_2} e\left(\beta P^3 x\right) dx}_{B(\beta)} + \underbrace{O\left(P^3 L^{-2} \min\left\{1, \left|\beta P^3\right|^{-1}\right\}\right)}_{E_2(\beta)}. \tag{3.85}$$

Now, from (3.84) and (3.85) we have

$$I(\beta) I_1(-\beta) = A(\beta) B(-\beta) + A(\beta) E_2(-\beta) + B(-\beta) E_1 + E_1 E_2(-\beta).$$

thus

$$J(P) = \int\limits_{|\beta|<P^{-3}L^k} I(\beta) I_1(-\beta) d\beta = \sum_{m=1}^{4} \mathcal{J}_m(P).$$

where

1.
$$\mathcal{J}_1(P) = \int\limits_{|\beta|<P^{-3}L^k} A(\beta) B(-\beta) d\beta.$$

2.
$$\mathcal{J}_2(P) = \int\limits_{|\beta|<P^{-3}L^k} A(\beta) E_2(-\beta) d\beta.$$

3.
$$\mathcal{J}_3(P) = \int\limits_{|\beta|<P^{-3}L^k} B(-\beta) E_1 d\beta.$$

4.
$$\mathcal{J}_4(P) = \int\limits_{|\beta|<P^{-3}L^k} E_1 E_2(-\beta) d\beta.$$

We shall see that $\mathcal{J}_1(P)$ is the **main term** while $E = \mathcal{J}_2(P) + \mathcal{J}_3(P) + \mathcal{J}_4(P)$ is the **error term**. We have that

$$\mathcal{J}_1(P) = \frac{P^{n+3}}{3L} \int\limits_{|\beta|<P^{-3}L^k} \left\{ \int\limits_{\mathcal{P}} e\left(\beta P^3 C(\xi)\right) d\xi \right\} \left\{ \int\limits_{g_1}^{g_2} e\left(-\beta P^3 x\right) dx \right\} d\beta.$$

If we call $\gamma = \beta P^3$ and $\lambda = \frac{L^k}{P_3}$ and we define

$$J_1(\lambda) = \int\limits_{-\lambda}^{\lambda} \left\{ \int\limits_{\mathcal{P}} e(\gamma C(\xi)) d\xi \right\} \left\{ \int\limits_{g_1}^{g_2} e(-\gamma x) dx \right\} d\gamma.$$

we can write

$$\mathcal{J}_1(P) = \frac{P^n}{3L} J_1\left(L^k\right). \tag{3.86}$$

If we write $AE_2 = A(\beta) E_2(-\beta)$, $BE_1 = B(-\beta) E_1$, $E_1E_2(-\beta)$, we have

$$AE_2 \ll \frac{P^{n+3}}{L^2} \min\left\{1, \left|\beta P^3\right|^{-1}\right\}. \tag{3.87}$$

$$BE_1 \ll P^{n+2} L^{k-1}. \tag{3.88}$$

$$E_1E_2 \ll P^{n+2} L^{k-2} \min\left\{1, \left|\beta P^3\right|^{-1}\right\}. \tag{3.89}$$

From (3.87),(3.88),(3.89), it follows that

$$J_2(P) \ll \frac{P^{n+3}}{L^2} \int\limits_{|\beta|<P^{-3}L^k} \min\left\{1, \left|\beta P^3\right|^{-1}\right\} d\beta. \tag{3.90}$$

$$J_3(P) \ll P^{n+2} L^{k-1} \int\limits_{|\beta|<P^{-3}L^k} d\beta. \tag{3.91}$$

$$J_4(P) \ll P^{n+2} L^{k-2} \int\limits_{|\beta|<P^{-3}L^k} \min\left\{1, \left|\beta P^3\right|^{-1}\right\} d\beta. \tag{3.92}$$

Hence

$$E \ll P^{n+2} L^{k-1} \int\limits_{|\beta|<P^{-3}L^k} d\beta + \frac{P^{n+3}}{L^2} \int\limits_{|\beta|<P^{-3}L^k} \min\left\{1, \left|\beta P^3\right|^{-1}\right\} d\beta.$$

Now it is easy to see that

$$\int\limits_{|\beta|<P^{-3}L^k} \min\left\{1, \left|\beta P^3\right|^{-1}\right\} d\beta \ll P^{-3} \log L.$$

thus

$$E \ll P^{n-1} L^{2k-1} + P^n L^{-2} \log L \ll P^n L^{-2} \log L.$$

It follows that

$$J(P) = \frac{P^n}{3L} J_1\left(L^k\right) + O\left(P^n L^{-2} \log L\right). \tag{3.93}$$

From its definition, we have that

$$J_1(\lambda) = \int_{-\lambda}^{\lambda} d\gamma \int_{\mathcal{P}} d\xi \left\{ \int_{g_1}^{g_2} e\left(\gamma\left(C\left(\xi\right) - x\right)\right) dx \right\}.$$

that we can write as

$$J_1(\lambda) = \int_{\mathcal{P}} d\xi \int_{g_1}^{g_2} dx \int_{-\lambda}^{\lambda} \left\{ e\left(\gamma\left(C\left(\xi\right) - x\right)\right) \right\} d\gamma.$$

Hence

$$J_1(\lambda) = \int_{\mathcal{P}} d\xi \int_{g_1}^{g_2} \left\{ \frac{\sin 2\pi\lambda\left(C\left(\xi\right) - x\right)}{\pi\left(C\left(\xi\right) - x\right)} \right\} dx = \int_{\mathcal{P}} d\xi \int_{g_1 - C(\xi)}^{g_2 - C(\xi)} \frac{\sin 2\pi\lambda t}{\pi t} dt.$$

We consider now

$$\lim_{\lambda \to +\infty} J_1(\lambda) = \lim_{\lambda \to +\infty} \int_{\mathcal{P}} d\xi \int_{g_1 - C(\xi)}^{g_2 - C(\xi)} \frac{\sin 2\pi\lambda t}{\pi t} dt.$$

Since, by the choice of g_1 and g_2, we have that

$$\begin{cases} g_1 - C\left(\xi\right) \leqslant g_1 - f_1 < 0 \\ g_2 - C\left(\xi\right) \geqslant g_2 - f_2 > 0. \end{cases}$$

we can write

$$\lim_{\lambda \to +\infty} J_1(\lambda) = \int_{\mathcal{P}} d\xi \lim_{\lambda \to +\infty} \int_{g_1 - C(\xi)}^{g_2 - C(\xi)} \frac{\sin 2\pi\lambda t}{\pi t} dt.$$

because the inner limit is uniform in ξ. From Classical Analysis it is well known that

$$\lim_{\lambda \to +\infty} \int_{g_1 - C(\xi)}^{g_2 - C(\xi)} \frac{\sin 2\pi\lambda t}{\pi t} dt = 1.$$

Hence

$$\lim_{\lambda \to +\infty} J_1(\lambda) = \int_{\mathcal{P}} d\xi = V_{\mathcal{P}}.$$

It follows that

$$J(P) \sim \frac{P^n}{3L} V_{\mathcal{P}} \quad (P \to \infty).$$

and, finally

$$\mathcal{M}(P) \sim \mathfrak{S} \frac{P^n}{3L} V_{\mathcal{P}} \quad (P \to \infty).$$

□

Chapter 4

The second theorem of Pleasants

4.1 Introduction

The second theorem of Pleasants, proved from the author in [32], the condition $1 \leq h \leq 7$ has ben considered and under further conditions on ϕ it has been proved that it still represent infinitely many primes. However, in this second theorem, due to the nature of the method used, no asymptotic formulas has been obtained. The proof depends on some results on the representation of primes by quadratic polynomials. The cubic polynomials considered in this theorem have n the number of variables n substantially greater than the invariant h The method is to fix some of the variables in such a way that ϕ reduce to a suitable quadratic or linear polynomial in the remaining variables and the apply to this resulting polynomial either a result from the theory of Quadratic Polynomials or else the theorem of Dirichlet on primes in an arithmetical progression. Both these theorem are also used in the initial reduction of ϕ. to a polynomial of smaller degree. For these reasons the lower bounds for the number of primes represented by a such polynomials are related with polynomials of second or first degree. **We will get now a very brief sketch of the path towards the proof**:

- In 4.2 and 4.3 it is stated some terminology and notation about Quadratic polynomials.
- In 4.4 we get the statement of an Auxiliary Theorem on the primes represented by a quadratic polynomials.
- In 4.5 we get the statement of the Second Theorem of Pleasants.

- In 4.6 the tools for the proof of the Auxiliary Theorem are developed.
- In 4.7 the **Auxiliary Theorem** is proved.
- In 4.8 a useful Corollary of the Auxiliary theorem is explicitly stated.
- In 4.9 some other further lemmas about polynomials of second and first degree are proved.
- In 4.10 some specific Lemmas about cubi polynomials are proved.
- In 4.11 the **Second Theorem of Pleasants** is proved in all its several cases.

A graphical "road map" towards the proof of FTP is given in Appendix H.

4.2 Preliminaries

Definition 4.1. *Let be* $\mathbf{x} \in \mathbb{R}^n$. *Let* $P \in \mathbb{R}^+$. *A quadratic polynomial*

$$\phi_P \in \mathbb{Z}[\mathbf{x}].$$

is said ***weakly dependent*** *on* P *if and only if*

$$\phi_P(\mathbf{x}) = Q(\mathbf{x}) + L_P(\mathbf{x}) + N_P. \tag{4.1}$$

where the coefficients of the quadratic part Q *are fixed while the coefficients of the linear part as well as the constant term* N_P *may depend of* P.

Definition 4.2. *Given a weakly dependent polynomial* $\phi_P \in \mathbb{Z}[\mathbf{x}]$ *we will say that it is* ***suitable****, if and only if*

1. *For every* $P \in \mathbb{R}^+$ *all the coefficients of* ϕ_Q *are rational.*
2. *For every* $\mathbf{x} \in \mathbb{Z}^n$ *we have that* [1] $\phi_P(\mathbf{x}) \in \mathbb{Z}$.

We shall suppose that there exists two positive real numbers f_1 f_2 and a box

$$B = \prod_{j=1}^{n} [a_j, b_j] \subseteq \mathbb{R}^n.$$

[1] Of course, the polynomial does not to have integral coefficients: for example, the polynomial $\phi_P(\mathbf{x}) = \sum_{j=1}^{n} \frac{x_j(x_j-1)}{2!}$ is an integer valued quadratic polynomial

$$f_1 P^2 \leqslant \phi_P(\xi) \leqslant f_2 P^2. \tag{4.2}$$

for every $\xi \in P\mathcal{B}$ where $P\mathcal{B}$ denotes, as usual, the homothetic expanded box obtained from $\mathcal{B}$ by means of a dilatation of each side of a factor P. A sufficient condition for the existence of such a kind of box is given by the following easy

Proposition 4.1. *Let*

$$\phi_P(\mathbf{x}) = Q(\mathbf{x}) + L_P(\mathbf{x}) + N_P.$$

a suitable polynomial with

- $Q(\mathbf{x}) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j \quad a_{ij} = a_{ji} \in \mathbb{R}^+ \ \ \forall i,j = 1\ldots n.$
- $L_P(\mathbf{x}) = \sum_{i=1}^{n} l_i(P)x_i.$
- $N_P = aP^2 + bP + c \quad a,b,c \in \mathbb{R}.$

if

1. *There exists $m \in \mathbb{R}^+$ such that $|l_i(P)| \leqslant mP \quad \forall P \in \mathbb{R}^+, \forall i = 1\ldots n.$*
2. $\min\{a_{ij}, i,j = 1\ldots n\} > m + |a|.$

then *there exist a box $\mathcal{B}$ for which* (4.2) *holds.*

4.3 Notation

It will be used

$$\mathcal{N}(P) = \{\mathbf{x} \in P\mathcal{B} : \phi_P(\mathbf{x}) \in \mathbb{P}\}.$$

With r it will be denoted the rank of the quadratic form Q. We shall use many suitable constants as in the proof of the First Theorem. We shall restart from c_1 c_2 and so on.

4.4 The Auxiliary Theorem

With these preliminaries and this notation it will be proved the following

Theorem 4.1. *Let*

$$\phi_P(\mathbf{x}) = \sum_{i=1}^{n}\sum_{j=1}^{n}\frac{r_{ij}}{s_{ij}}x_i x_j + \sum_{i=1}^{n}\frac{k_i(P)}{m_i(P)}x_i + \frac{u(P)}{v(P)}.$$

a suitable polynomial. ***If***

1. $r \geq 3$.
2. $(r_{ij}, s_{ij}) = 1 \ \forall i, j = 1 \dots n$.
3. $(k_i(P), m_i(P)) = 1 \ \forall i = 1...n \ \forall P$.
4. $(u(P), v(P)) = 1 \quad \forall P$.
5. *There exists* $P_0 \in \mathbb{R}^+$ *such that for every* $P > P_0$ *it is*

$$(r_{11} \dots r_{1n}, r_{22} \dots r_{2n}, \dots r_{nn}, k_1(P) \dots k_n(P), u(P)) = 1.$$

6. *There exists* $\mathbf{x}_0 \in \mathbb{Z}^n : \phi_P(\mathbf{x}_0) \not\equiv 0 \pmod 2$.

Then *there exists a function*

$$\mathfrak{S}(P) : \mathbb{R}^+ \to \mathbb{R}^+.$$

two positive real numbers γ_1, γ_2 *and a positive value* P_1, *such that*

1. $\gamma_1 < \mathfrak{S}(P) < \gamma_2 \quad \forall P > P_1$.
2. $$|\mathcal{N}(P)| \sim \mathfrak{S}(P)\frac{V_{\mathcal{B}}P^n}{\log P^2} \quad P \to \infty.$$

Note 4.1. *Let* $c \in \mathbb{Z}$, *if we denote as*

$$D_c = \{\mathbf{x} \in P\mathcal{B} : \ \phi_P(\mathbf{x}) = c\}.$$

it can be proved that

$$|D_c| \ll_{n,\mathcal{B}} P^{n-1}.$$

where $\ll_{n,\mathcal{B}}$ *means that the implied constant depends only by* n *and* $\mathcal{B}$. *Thus, if*

$$M_P = \{p \in \mathbb{P} : \exists \mathbf{x} \in P\mathcal{B}, \ \phi_P(\mathbf{x}) = p\}.$$

using Theorem 4.1 we have that

$$|\mathcal{M}_P| \gg \frac{P}{\log P}.$$

and in particular infinitely many ***distinct*** *primes occur as values of* ϕ_P.

4.5 The Second Theorem of Pleasants

Definition 4.3. *Let $\mathbf{x} \in \mathbb{Z}^n$. A cubic polynomial $\phi \in \mathbb{Z}[\mathbf{x}]$ is said to be* ***non-degenerate*** *it does not exist an affine transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ such that*

1. *$T(\mathbf{y}) = \mathbf{A}\mathbf{y} + \mathbf{b}$ where $\mathbf{A}$ is a nonsingular $n \times n$ matrix and $\mathbf{b} \in \mathbb{R}^n$.*
2. *$|\det \mathbf{A}| = 1$.*
3. *$\mathbf{y} \in \mathbb{Z}^n \Rightarrow \mathbf{x} = T(\mathbf{y}) \in \mathbb{Z}^n$.*
4. *If $\phi' = \phi \circ T$ then ϕ' is a cubic polynomial in n' variables with $n' < n$.*

Theorem 4.2. *Given cubic polynomial ϕ as in (3.1)* ***if*** *and let h the same invariant as before.*

- *ϕ is non degenerate.*
- *ϕ is irreducible.*
- *For every $m \in \mathbb{Z}$ there exists $\mathbf{x} \in \mathbb{Z}^n$ such that $\phi(\mathbf{x}) \equiv 0 \pmod m$.*

if one of the following three condition holds:

- *$h = 1$ and $n \geq 5$.*
- *$h \geq 2$ and $n \geq 9$.*
- *$h \geq 3$ and $n \geq h + 3$.*

and if

$$\mathcal{M} = \{p \in \mathbb{P} : \exists \mathbf{x} \in \mathbb{Z}^n, \phi(\mathbf{x}) = p\}.$$

then

$$|\mathcal{M}| = \infty . \tag{4.3}$$

Note 4.2. *While the polynomial ϕ has to be irreducible, its cubic part C does not. Namely, the first condition in Theorem 4.2 is given with $h = 1$ that means C is reducible.*

As already said before, we need to develop some theory about the quadratic polynomials, in order to explain the proof of the last Theorem.

4.6 Theorems about Quadratic polynomials

4.6.1 Elementary Lemmas

Lemma 4.1. ***If***

$$\phi(\mathbf{x}) = \phi(x_1 \dots x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j + \sum_{i=1}^{n} l_i x_i + N.$$

is a quadratic polynomial such that $\mathbf{x} \in \mathbb{Z}^n \Rightarrow \phi(\mathbf{x}) \in \mathbb{Z}^n$. *Write*

$$\varphi(\mathbf{x}) = \sum_{i=1}^{n}\sum_{j=1}^{n} \frac{r_{ij}}{s_{ij}} x_i x_j + \sum_{k=1}^{n} \frac{k_i}{m_i} x_i + \frac{u}{v}.$$

with

$$\begin{cases} (r_{ij}, s_{ij}) = 1 & \forall i, j = 1 \dots n \\ (k_i, m_i) = 1 & \forall i = 1 ... n \\ (u, v) = 1. \end{cases}$$

then

1. $v = 1$.
2. $1 \leqslant s_{ij} \leqslant 2 \quad \forall i, j = 1 \dots n$.
3. $1 \leqslant m_i \leqslant 2 \quad \forall i = 1 \dots n$.

Proof. Trivially

$$\frac{u}{v} = \phi(\mathbf{0}) \in \mathbb{Z}.$$

thus $u = 1$. Since

$$\begin{aligned} &\phi(1, 1, 0, \dots, 0) = a_{11} + 2a_{12} + a_{22} + l_1 + l_2 + u. \\ &\phi(1, 0, \dots, 0) = a_{11} + l_1 + u. \\ &\phi(0, 1, 0, \dots, 0) = a_{22} + l_2 + u. \\ &\phi(0, \dots, 0) = u. \end{aligned}$$

we have

$$\phi(1, 1, 0, \dots, 0) - \phi(1, 0, \dots, 0) - \phi(0, 1, 0, \dots, 0) - \phi(0, \dots, 0) = 2a_{12}.$$

By hypotesis, the left-hand side is an integer, thus $2a_{12} \in \mathbb{Z}$ and so $1 \leq s_{12} \leq 2$. In the same way we can prove that $2a_{ij} \in \mathbb{Z}$ and so $1 \leq s_{ij} \leq 2$, whenever $i \neq j$. Now, let $x \in \mathbb{Z}$; we have

$$\begin{aligned} &\phi(x + 1, 0, \dots, 0) = a_{11}(x + 1)^2 + l_1(x + 1) + u. \\ &\phi(x, 0, \dots, 0) = a_{11}x^2 + l_1 x + u. \end{aligned}$$

thus

$$\phi(x+1,0,\ldots,0)-\phi(x,0,\ldots,0)=2a_{11}x+a_{11}+l_1.$$

Hence, we must have $2a_{11}x+a_{11}+l_1\in\mathbb{Z}$ whenever $x\in\mathbb{Z}$. From this, we deduce that

- $a_{11}+l_1\in\mathbb{Z}$ by setting $x=0$.
- $2a_{11}\in\mathbb{Z}$ by setting $x=1$ and by the previous deduction.

It follows that $1\leq s_{11}\leq 2$, $1\leq m_1\leq 2$. Similarly, we have that $1\leq s_{ii}\leq 2$, $1\leq m_i\leq 2$ for every $2\leq i\leq n$. This proves the Lemma. □

Lemma 4.2. ***If***

$$\phi(\mathbf{x})=\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{r_{ij}}{s_{ij}}x_ix_j\ +\sum_{i=1}^{n}\frac{k_i}{m_i}x_i+\frac{u}{v}.$$

is a quadratic polynomial with rational coefficients such that:

1. $\mathbf{x}\in\mathbb{Z}^n\Rightarrow\phi(\mathbf{x})\in\mathbb{Z}^n$.
2. $$\begin{cases}(r_{ij},s_{ij})=1 & \forall i,j=1\ldots n\\ (k_i,m_i)=1 & \forall i=1...n\\ (u,v)=1.\end{cases}$$
3. $(r_{11}\ldots r_{1n},r_{22}\ldots r_{2n},\ldots r_{nn},k_1\ldots k_n,u)=1$.
4. $\mathbf{x}_0\in Z^n:\phi(\mathbf{x}_0)\not\equiv 0 \pmod 2$.

then *for every $m\in\mathbb{Z}$ there exists $\mathbf{y}\in\mathbb{Z}^n$*

$$(\phi(\mathbf{y}),m)=1.$$

Proof. First we prove the result for $m=p\in\mathbb{P}$.

- If $p=2$ there is anything to prove, because the fourth point in the hypotesis.
- Suppose $p>2$. If the result were not true, we should have

  $$\phi(\mathbf{x})\equiv 0 \pmod p.$$

  for every $\mathbf{x}\in\mathbb{Z}^n$, and so the polynomial

  $$\phi'(\mathbf{x})=p^{-1}\phi(\mathbf{x}).$$

  would be integer valued at all integer points. Hence, by Lemma 4.1 the coefficients of ϕ' have denominators at most 2 and so all the numerators of the coefficients of ϕ are divisible by p, contradicting the hypothesis.

Now, let m be any integer.

- If $m = \pm 1$ the conclusion of the Lemma holds for all $\mathbf{y} \in \mathbb{Z}$
- If $m \neq \pm 1$ let

$$P_m = \{p_1, \dots p_s \in \mathbb{P} : p_j | m \ \ \forall j = 1 \dots s\}.$$

be the set of the distinct prime factors of m. For each $p_i \in P_m$ there exist $\mathbf{y}_i \in \mathbb{Z}^n$ such that

$$\phi(\mathbf{y}_i) \not\equiv 0 \pmod{p_i}.$$

Let

$$m' = \prod_{i=1}^{s} p_i.$$

and write

$$\mathbf{y} = \sum_{i=1}^{s} \frac{m'}{p_i} \mathbf{y}_i.$$

Then $\mathbf{y} \in \mathbb{Z}^n$ and

$$\phi(\mathbf{y}) \not\equiv 0 \pmod{p_i} \ \ \forall i = 1 \dots s.$$

which is the conclusion of the Lemma.

□

4.6.2 Exponential sums

Definition 4.4. *Let g_1, g_2 be real numbers satisfying*

$$0 < g_1 < f_1 < f_2 < g_2. \tag{4.4}$$

where f_1 and f_2 are the numbers occurring in (4.2)*. We define the exponential sums $T(\alpha)$ and $S(\alpha)$ by*

$$T(\alpha) = \sum_{\substack{g_1 P^3 < p < g_2 P^3 \\ p \in \mathbb{P}}} e(\alpha p). \tag{4.5}$$

$$S(\alpha) = \sum_{\mathbf{x} \in P\mathcal{B}} e(\alpha \phi_P(\mathbf{x})). \tag{4.6}$$

where ϕ_P is a suitable polynomial as before.

With these definitions, we have

$$|N(P)| = \int_0^1 S(\alpha)\, T(-\alpha) d\alpha. \tag{4.7}$$

Note 4.3. *We can write the quadratic part of ϕ_P in matrix form*

$$Q(\mathbf{x}) = \mathbf{x}^t \mathbf{A} \mathbf{x}.$$

where a_{ij} those of Proposition 4.1. From Lemma 4.1 and hypotheses of Theorem 4.1 it follows that $2a_{ij} \in \mathbb{Z}$ for every $1 \leq i, j \leq n$.

Definition 4.5. *Given a quadratic form*

$$Q(\mathbf{x}) = \mathbf{x}^t \mathbf{A} \mathbf{x}.$$

we define the set of associated linear forms as

$$\mathbf{L_Q} = \left\{ A_i(\mathbf{x}) = \sum_{j=1}^{n} a_{ij} x_j, \;\; i = 1 \ldots n \right\}.$$

Definition 4.6. *For every fixed $\mathbf{x} \in \mathbb{R}^n$, we shall call*

$$\mathbf{A}(\mathbf{x}) = (A_1(\mathbf{x}), \ldots A_n(\mathbf{x})) \in \mathbb{R}^n.$$

associated linear forms vector *to the quadratic form Q.*

Note 4.4. *By Note 4.3 we have that for every $1 \leq i \leq n$ the linear form*

$$A_i'(\mathbf{x}) = 2A_i(\mathbf{x}).$$

has integer coefficients.

Lemma 4.3. ***If*** *$\mathcal{B}$ is a fixed box in $\mathbb{R}^n$* ***then***

$$|S(\alpha)|^2 \ll \sum_{\substack{|\mathbf{x}| \ll P \\ \mathbf{x} \in \mathbb{Z}^n}} \prod_{i=1}^{n} \min\left\{P, \|2\alpha A_i(\mathbf{x})\|^{-1}\right\}. \tag{4.8}$$

Proof. We have

$$|S(\alpha)|^2 = S(\alpha)\,\overline{S(\alpha)} = \sum_{\substack{\mathbf{y} \in P\mathcal{B} \\ \mathbf{y} \in \mathbb{Z}^n}} \sum_{\substack{\mathbf{z} \in P\mathcal{B} \\ \mathbf{z} \in \mathbb{Z}^n}} e(\alpha\phi_P(\mathbf{y}) - \alpha\phi_P(\mathbf{z})).$$

so

$$|S(\alpha)|^2 = \sum_{\substack{\mathbf{z}\in P\mathcal{B}\\ \mathbf{z}\in\mathbb{Z}^n\\ \mathbf{x}+\mathbf{z}\in Z^n}} \sum_{\mathbf{x}\in\mathcal{P}_\mathbf{z}} e\left(\alpha\phi_P(\mathbf{x}+\mathbf{z}) - \alpha\phi_P(\mathbf{z})\right).$$

where

$$\mathcal{P}_\mathbf{z} = P\mathcal{B} - \mathbf{z}.$$

is the transformed box $P\mathcal{B}$ after a translation of vector $-\mathbf{z}$. It is not hard to prove that

$$\forall \mathbf{x}\in\mathcal{P}_\mathbf{z} \Rightarrow |\mathbf{x}| \ll_{\mathcal{B}} P.$$

Hence

$$|S(\alpha)|^2 \leq \sum_{|\mathbf{x}|\ll P} \left| \sum_{\mathbf{z}\in\mathcal{R}(\mathbf{x})} e\left(\alpha\phi_P(\mathbf{x}+\mathbf{z}) - \alpha\phi_P(\mathbf{z})\right)\right|. \tag{4.9}$$

where

$$\mathcal{R}(\mathbf{x}) = P\mathcal{B}\cap(P\mathcal{B}-\mathbf{x}).$$

Now

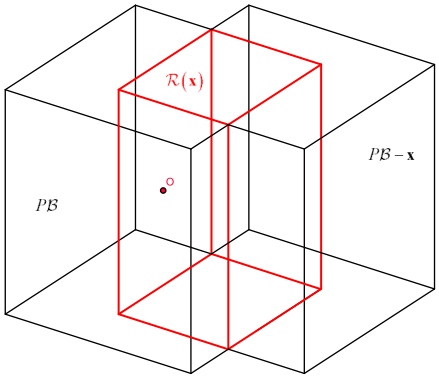

Figure 4.1: The box $\mathcal{R}(\mathbf{x})$

$$\phi_P(\mathbf{x}+\mathbf{z}) - \phi_P(\mathbf{z}) = 2\sum_{i=1}^{n} A_i(\mathbf{x})\, z_i + Q(\mathbf{x}) + L_P(\mathbf{x}).$$

We notice that the last two terms of the right-hand side are independent of $\mathbf{z}$ and so

$$\left|\sum_{\mathbf{z}\in\mathcal{R}(\mathbf{x})} e\left(\alpha\phi_P(\mathbf{x}+\mathbf{z}) - \alpha\phi_P(\mathbf{z})\right)\right| = \left|\sum_{\mathbf{z}\in\mathcal{R}(\mathbf{x})} e\left(2\alpha\sum_{i=1}^{n} A_i(\mathbf{x})\, z_i\right)\right|.$$

We can obtain a special partition of $\mathcal{R}(\mathbf{x})$ in the following way (see figure 4.2):

1. Let $\mathbf{z}_0 = (z_{01}, z_{02} \dots z_{0n})$ the integer point of $\mathcal{R}(\mathbf{x})$ such that whenever $\mathbf{z} = (z_1 \dots z_n)$ is any other integer point of $\mathcal{R}(\mathbf{x})$ it is

$$\begin{cases} z_1 \geq z_{01} \\ \vdots \\ z_n \geq z_{0n}. \end{cases}$$

2. Let

$$\begin{aligned} &\Omega_1 = \{\mathbf{z} \in \mathcal{R}(\mathbf{x}) : (z_{01} + \tau, z_{02} \dots z_{0n}), \tau = 1 \dots H_1\}. \\ &\Omega_2 = \{\mathbf{z} \in \mathcal{R}(\mathbf{x}) : (z_{01} + \tau, z_{02} + 1, \dots z_{0n}), \tau = 1 \dots H_1\}. \\ &\vdots \\ &\Omega_{N_{\mathcal{R}}} = \{\mathbf{z} \in \mathcal{R}(\mathbf{x}) : (z_{01} + \tau, z_{02} + H_2, \dots z_{0n} + H_n), \tau = 1 \dots H_1\}. \end{aligned}$$

3. $H_1 \ll P, \dots H_n \ll P$.

Of course we have

- $\mathcal{R}(\mathbf{x}) = \bigcup_{j=1}^{N_R} \Omega_j$.
- $\Omega_j \cap \Omega_{j'} = \emptyset \quad \forall j \neq j'$.
- $|\Omega_j| = H_1 \ll P$.

and

$$\sum_{\mathbf{z} \in \mathcal{R}(\mathbf{x})} e\left(2\alpha \sum_{i=1}^{n} A_i(\mathbf{x}) z_i\right) = \sum_{j=1}^{N_{\mathcal{R}}} \sum_{\mathbf{z} \in \Omega_j} e\left(2\alpha \sum_{i=1}^{n} A_i(\mathbf{x}) z_i\right).$$

Now, we remember that, if

$$N(P) = \{m_0, m_0 + 1, , \dots m_0 + H : \ \ m_0 \in \mathbb{Z},\ H \in \mathbb{N},\ H \ll P\}.$$

it is well known that

$$\left| \sum_{z \in N(P)} e(\alpha z) \right| \leq \min\left\{P, \|\lambda\|^{-1}\right\}. \tag{4.10}$$

If we apply this inequality to each of

$$\sum_{\mathbf{z}\in\Omega_j} e\left(2\alpha\sum_{i=1}^{2} A_i\left(\mathbf{x}\right) z_i\right).$$

and we sum over j we obtain

$$\sum_{j=1}^{N_{\mathcal{R}}}\sum_{\mathbf{z}\in\Omega_j} e\left(2\alpha\sum_{i=1}^{2} A_i\left(\mathbf{x}\right) z_i\right) \ll \prod_{i=1}^{n} \min\left\{P, \|2\alpha A_i\left(\mathbf{x}\right)\|^{-1}\right\} \prod_{i=1}^{n} e\left(2\alpha A_i\left(\mathbf{x}\right) z_{0i}\right).$$

This means

$$\left|\sum_{\mathbf{z}\in\mathcal{R}(\mathbf{x})} e\left(2\alpha\sum_{i=1}^{n} A_i\left(\mathbf{x}\right) z_i\right)\right| \ll \prod_{i=1}^{n} \min\left\{P, \|2\alpha A_i\left(\mathbf{x}\right)\|^{-1}\right\}. \tag{4.11}$$

A substitution in (4.9) gives the result.

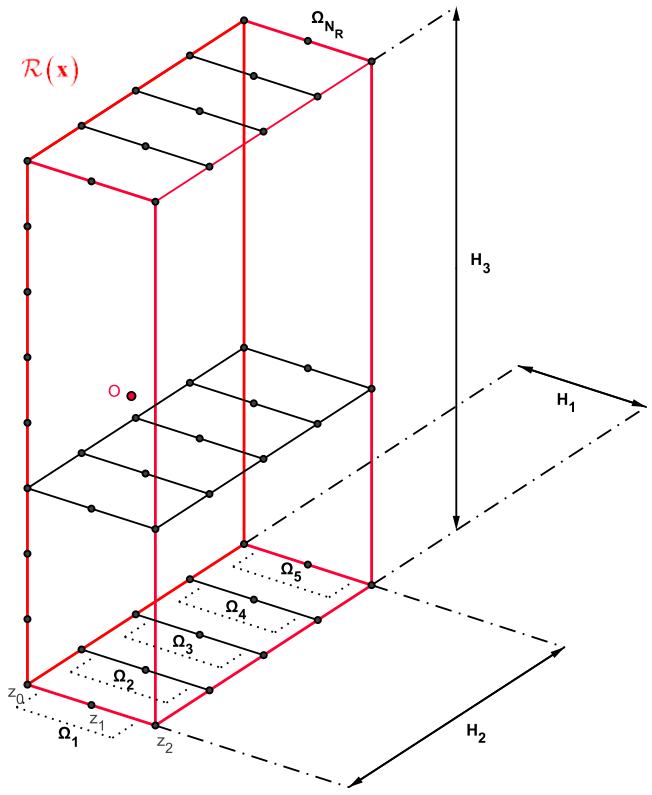

Figure 4.2: The partition of $\mathcal{R}(\mathbf{x})$

□

Lemma 4.4. *Let $L = \log P$ and U a parameter satisfying*

$$L \ll U \ll PL^{1/4}. \tag{4.12}$$

and let be

$$\mathcal{A}(P) = \left\{\mathbf{x} \in \mathfrak{A}'_P : \|2\alpha \mathbf{A}(\mathbf{x})\| < P^{-1}\right\}. \tag{4.13}$$

If *α is such that*

$$|S(\alpha)| > P^n L^n U^{-r/2}. \tag{4.14}$$

then

$$|\mathcal{A}(P)| \gg P^n L^n U^{-r}. \tag{4.15}$$

Proof. The proof follows from Lemma 4.3 in just the same way as Lemma 3.2 of [5] follows from Lemma 3.1 in that paper. □

Lemma 4.5. ***If*** (4.12) *and* (4.14) *hold and* ***if***

$$\mathcal{B}(P) = \left\{\mathbf{x} \in \mathfrak{A}'_{UL^{-1/2}} : \|2\alpha \mathbf{A}(\mathbf{x})\| < UP^{-2}L^{-1/2}\right\}.$$

then

$$|\mathcal{B}(P)| \gg P^{n-r} L^{n/2}. \tag{4.16}$$

Proof. We apply Proposition E.5 to the symmetric linear forms of the set

$$\mathbf{L}'_{\mathbf{Q}} = \{A'_i(\mathbf{x}) = 2\alpha A_i(\mathbf{x}) : A_i(\mathbf{x}) \in \mathbf{L}_{\mathbf{Q}}, i = 1 \dots n\}.$$

with

- A of Proposition E.5 equal to P.
- Z of Proposition E.5 equal to a suitable constant c_1.
- $Z_1 = UP^{-1}L^{-1/2}$.

The Condition (E.6) now takes the form

$$cU^{r/n}P^{-1}L^{-1} \leq Z_1 \leq c_1.$$

which is satisfied by our choice of Z_1 provided P is large enough. Now, equation (E.7) gives

$$|V(Z_1)| \gg P^{n-r}L^{n/2}.$$

which is equivalent to (4.16). □

Lemma 4.6. ***If*** (4.12) *and* (4.14) *hold there exist a* P_0 *such that for every* $P > P_0$ *the number* α *admits a rational approximation such that*

$$\begin{cases} (a,q) = 1 \\ |q| \leq U \\ |\alpha q - a| < UP^{-2}. \end{cases} \tag{4.17}$$

Proof. We consider the linear system

$$\begin{cases} A_1(\mathbf{x}) = 0. \\ \vdots \\ A_n(\mathbf{x}) = 0. \end{cases}$$

that we can write as $\mathbf{A}(\mathbf{x}) = 0$ and we observe that its solutions form a lattice of dimension $d = n - r$. Hence, if we consider the set

$$\mathcal{D}(P) = \left\{ \mathbf{x} \in \mathfrak{A}'_{UL^{-1/2}} : \mathbf{A}(\mathbf{x}) = 0 \right\}.$$

we have

$$|\mathcal{D}(P)| \ll U^{n-r} L^{-(n-r)/2}.$$

Hence, from Lemma 4.5 we have that there exists a $P_1 > 0$ such that if $P > P_1$ then

$$\mathcal{B}'(P) = \left\{ \mathbf{x} \in A'_{UL^{-1/2}} : \|2\alpha \mathbf{A}(\mathbf{x})\| < UP^{-2}L^{-1/2}, \mathbf{A}(\mathbf{x}) \neq 0 \right\} \neq \emptyset.$$

Let $\overline{\mathbf{x}} \in \mathcal{B}'(P)$ and suppose that $A_{i_0}(\overline{\mathbf{x}}) \neq 0$ where i_0 is a fixed index such that $1 \leq i_0 \leq n$. Then $2A_{i_0}(\overline{\mathbf{x}}) \in \mathbb{Z} - \{0\}$ and there exist $b \in \mathbb{Z}$ such that

$$|2\alpha A_{i_0}(\overline{\mathbf{x}}) - b| \ll UP^{-2}L^{-1/2}.$$

We consider the rational number

$$\beta = \frac{b}{2A_{i_0}(\overline{\mathbf{x}})}.$$

and we chose the fraction a/q such that $(a,q) = 1$. We have

$$|q| \ll |A_{i_0}(\overline{\mathbf{x}})| \ll |\overline{\mathbf{x}}| \ll UL^{-1/2}.$$

Hence there exist a $P_2 > 0$ such that if $P > P_2$ then $|q| \leq U$. Also there is a $P_3 > 0$ such that

$$|\alpha q - a| \leq |2\alpha A_{i_0}(\overline{\mathbf{x}}) - b| \ll UP^{-2}L^{-1/2}.$$

so

$$|\alpha q - a| \ll UP^{-2}.$$

If we chose $P_0 > \max\{P_1, P_2, P_3\}$ the result follows. □

4.6.3 Minor arcs

Let $\overline{I} = [0,1]$. We shall denote as

Definition 4.7.

$$\mathcal{E}(U) = \left\{\alpha \in \overline{I} : \exists a, q \in \mathbb{Z}, (a,q) = 1, |q| \leq U, |\alpha q - a| < UP^{-2}\right\}.$$

We shall write also

$$\mathcal{CE}(U) = \overline{I} - \mathcal{E}(U).$$

Definition 4.8. *If*

$$U_1 = L^{4n}. \tag{4.18}$$

we shall define the ***minor arcs***

$$\mathfrak{m} = \mathcal{CE}(U_1). \tag{4.19}$$

Lemma 4.7. ***If*** $r \geq 3$ ***then***

$$\int_{\mathfrak{m}} |S(\alpha) T(-\alpha)| \, d\alpha \ll P^n L^{-2}. \tag{4.20}$$

Proof. The proof follows the same lines as the proof of Lemma 3.14. If we consider the set-function

$$U \to \mathcal{E}(U).$$

we have that it is an increasing function i.e

$$U_1 < U_2 \Rightarrow \mathcal{E}(U_1) \subseteq \mathcal{E}(U_2).$$

and, by Dirichlet's theorem on Diophantine approximation, if $U \geq P$, we have that

$$\mathcal{E}(U) = \overline{I}.$$

Now, if

$$\mathcal{F}(U) = \mathcal{E}(2U) - \mathcal{E}(U).$$

then, we can write

$$\overline{I} = \mathcal{E}(U_1) \cup \left\{\bigcup_{j=0}^{t} \mathcal{F}\left(2^j U_1\right)\right\}.$$

where t is the least integer such that $2^{t+1} U_1 \geq P$. The subsets $\mathcal{F}(2^j U_1)$ are pairwise disjoints and

$$\mathfrak{m} = \bigcup_{j=0}^{t} \mathcal{F}\left(2^j U_1\right).$$

Moreover $t \ll L$. We take now

$$\begin{cases} U = 2^u U_1 \\ 0 \le u \le t. \end{cases}$$

Then U satisfies (4.12). If $\alpha \in \mathcal{F}(U)$, then α does not have a rational approximation satisfying (4.17) and it follows from Lemma 4.6 that the hypothesis (4.14) fails to hold for such an α. Thus for every $\alpha \in \mathcal{F}(U)$ we have

$$|S(\alpha)| \le P^n L^n U^{-r/2}.$$

Also

$$|\mathcal{F}(U)| \leqslant |\mathcal{E}(2U)| \leqslant \sum_{1 \leqslant q \leqslant 2U} \sum_{a=1}^{q} \left(2q^{-1}\right)\left(2UP^{-2}\right) \leqslant 8U^2P^{-2}.$$

It follows that

$$\int_{\mathcal{F}(U)} |S(\alpha)\,T(-\alpha)|d\alpha \leqslant P^n L^n U^{-r/2} \int_{\mathcal{F}(U)} |T(-\alpha)|d\alpha \leqslant$$

$$\leqslant P^n L^n U^{-r/2}\{|\mathcal{F}(U)|\}^{1/2}\left\{\int_0^1 |T(-\alpha)|^2\right\}^{1/2} \ll$$

$$\ll P^n L^n U^{-r/2}\left\{U^2P^{-2}\right\}^{1/2}\left\{P^2L^{-1}\right\}^{1/2} \ll$$

$$\ll P^n U^{1-r/2} L^{n-1/2} \ll P^n U^{-1/2} L^{n-1/2}.$$

since $r \ge 3$. Hence

$$\int_{\mathcal{F}(U)} |S(\alpha)\,T(-\alpha)|d\alpha \ll P^n U^{-1/2} L^{n-1/2}. \tag{4.21}$$

Now

$$\int_{\mathfrak{m}} |S(\alpha)\,T(-\alpha)|d\alpha = \sum_{j=0}^{t} \int_{\mathcal{F}(2^{j+1}U_1)} |S(\alpha)\,T(-\alpha)|d\alpha.$$

and

- The number of sets $\mathcal{F}$ is $\ll L$.

- To each of such sets we can apply (4.21)
- The least value of U is $U_1 = L^{4n}$.

we deduce that

$$\int_m |S(\alpha) T(-\alpha)| d\alpha \ll P^n L^{-n+1/2} \ll P^n L^{-2}.$$

and this concludes the proof. □

4.6.4 The Major arcs

Definition 4.9. *We denote with*

$$\mathfrak{M}_{a,q} = \left\{ \alpha \in I : \left| \alpha - \frac{a}{q} \right| < P^{-2} L^k \right\}.$$

and with

$$\mathfrak{M}_{0,1} = \mathfrak{I}_{0,1} \cup \mathfrak{I}_{1,1}.$$

where

$$\mathfrak{I}_{0,1} = \left\{ \alpha \in \overline{I} : \left| \frac{a}{q} \right| < P^{-2} L^k \right\}.$$

$$\mathfrak{I}_{1,1} = \left\{ \alpha \in \overline{I} : \left| 1 - \frac{a}{q} \right| < P^{-2} L^k \right\}.$$

and where k is a positive constant.

Definition 4.10. *We denote with*

$$\mathfrak{M} = \bigcup_{1 \le q \le L^k} \bigcup_{\substack{1 \le a \le q \\ (a,q)=1}} \mathfrak{M}_{a,q} \cup \mathfrak{M}_{0,1}.$$

and we call it " ***major arcs****"*

The sets $\mathfrak{M}_{a,q}$ are disjoint if P is large enough. Moreover, if we choose $k \ge P^{4n}$ then

$$\mathcal{E}(U_1) \subseteq \mathfrak{M}.$$

Lemma 4.8. ***If*** $\alpha \in \mathfrak{M}_{a,q}$ ***then***

$$S(\alpha) = q^{-n} S_{a,q}(P) I(\beta) + O\left(P^{n-1} L^{2k}\right). \tag{4.22}$$

where

$$S_{a,q}(P) = \sum_{\mathbf{x}\,(\bmod\ q)} e\left(\frac{a}{q}\phi_P(\mathbf{x})\right).$$

$$I(\beta) = \int_{P\mathcal{B}} e(\beta\phi_P(\xi))\, d\xi. \tag{4.23}$$

and

$$\beta = \alpha - \frac{a}{q}.$$

Proof. The proof is very similar to the proof of Lemma 3.15 with only trivial differences. □

Lemma 4.9. ***If*** $\alpha \in \mathfrak{M}_{a,q}$ ***then***

$$T(\alpha) = \frac{\mu(q)}{\varphi(q)} I_1(\beta) + O\left(P^2 e^{-c_2 L^{1/2}}\right). \tag{4.24}$$

where

$$I_1(\beta) = \int_{g_1 P^2}^{g_2 P^2} \frac{e(\beta x)}{\log x} dx.$$

and c_2 *is a suitable constant.*

Proof. This is just Lemma 3.16. □

Lemma 4.10. ***If*** $(a,q) = 1$ ***then***

$$|S_{a,q}| \ll q^{n-r/2} (\log q)^n. \tag{4.25}$$

where the implied constant does not depends on a, q, P.

Proof. We note that the implied constants occuring in Lemmas 4.3, 4.4, 4.5, 4.6 depend only on n and $\mathcal{B}$ and the coefficients a_{ij} of Q and that they in no way depend on the other coefficients of ϕ_P. Hence we can apply Lemma 4.6 to $S_{a,q}$. Using this Lemma, we take

$$\begin{cases} P = q \\ U = q - 1 \\ \alpha = \frac{a}{q}. \end{cases}$$

and we use a unit cube $\mathcal{U}_{cube}$ in place of $\mathcal{B}$. The inequalities (4.12) are then satisfied, but $\alpha = \frac{a}{q}$ does not have a rational approximation satisfying the

third condition of (4.17). For if $\frac{a'}{q'}$ is any rational number such that $q' \leq q-1$ then

$$\frac{a'}{q'} \neq \frac{a}{q}.$$

because $(a,q)=1$. It follows that

$$\left| q' \frac{a}{q} - a' \right| \geq \frac{1}{q} > \frac{q-1}{q^2}.$$

We deduce that the inequality (4.14) does not hold with this choice of α P U and $\mathcal{U}_{cube}$ provided $q > c_3$ where c_3 is a constant large enough. Thus,

- If $q > c_3$ then

$$|S_{a,q}(P)| \leq q^n (\log q)^n (q-1)^{-r/2} \ll q^{n-r/2} (\log q)^n.$$

- If $q \leq c_3$ the, trivially

$$|S_{a,q}(P)| \leq q^n \leq c_3^n.$$

Hence, in either case (4.25) holds. □

Lemma 4.11. ***If*** $r \geq 3$ ***then***

$$\int_{\mathfrak{M}} S(\alpha) T(-\alpha) = \{\mathfrak{S}(P) + E_1\} \int_{|\beta| < P^{-2} L^k} I(\beta) I_1(-\beta) \, d\beta + E_2. \tag{4.26}$$

where

- $E_1 = O(L^{-c_4})$.
- $E_2 = O(P^n L^{-2})$.
- $c_4 > 0$ *is a suitable constant*

and

$$\mathfrak{S}(P) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)} q^{-n} S_{a,q}(P). \tag{4.27}$$

Proof. The proof follows the same lines as the proof of Lemma 3.17 with only trivial differences. Here we must use Lemmas 4.8, 4.9, 4.10 in place of Lemmas 3.15, 3.16, 3.13. □

4.6.5 The singular series

Lemma 4.12. *With the hypothesis of Theorem 4.1 there exist* $\gamma_1 > 0$ *and* $\gamma_2 > 0$ *such that*

$$\gamma_1 < \mathfrak{S}(P) < \gamma_2.$$

for every P *large enough.*

Proof. From (4.27) and (4.25) we have that the series $\mathfrak{S}(P)$ is uniformly absolutely convergent. Moreover, by well-known arguments, we have that

$$A(q,P) = \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-n} S_{a,q}(P).$$

is a multiplicative function of q. Hence,

$$\mathfrak{S}(P) = \prod_{p\in\mathbb{P}} F_p(P). \tag{4.28}$$

where

$$F_p(P) = 1 - \frac{1}{p-1} p^{-n} \sum_{a=1}^{p-1} S_{a,q}(P). \tag{4.29}$$

The infinite product (4.28) converges uniformly and so there exists a constant $c_5 > 0$ such that

$$\frac{1}{2} < \prod_{\substack{p>c_5\\p\in\mathbb{P}}} F_p(P) < 2. \tag{4.30}$$

Also for any $\mathbf{x} \in \mathbb{Z}^n$ and any prime $p \in \mathbb{P}$ we have

$$\sum_{a=1}^{p-1} e\left(\frac{a}{p}\phi_P(\mathbf{x})\right) = \begin{cases} p-1 \ if \ \phi_P(\mathbf{x}) \equiv 0 \pmod p \\ -1 \quad if \ \phi_P(\mathbf{x}) \not\equiv 0 \pmod p. \end{cases} \tag{4.31}$$

We consider the quotient set $\mathfrak{Q} = {}^{\mathbb{Z}^n}/_{\mathrm{mod}p}$ and its subset

$$\mathfrak{P} = \{[\mathbf{x}] \in \mathfrak{Q} : \phi_P(\mathbf{x}) \not\equiv 0 \pmod p\}.$$

If $M = |\mathfrak{P}|$ from (4.31) we have

$$\sum_{a=1}^{p-1} S_{a,p}(P) = \sum_{a=1}^{p-1} \sum_{\mathbf{x}\,(\bmod\ p)} e\left(\frac{a}{p}\varphi_P(\mathbf{x})\right) = (p^n - M)(p-1) - M. \tag{4.32}$$

Substituting (4.32) in (4.29) we obtain

$$F_p(P) = \frac{M}{p^{n-1}(p-1)}.$$

Now trivially $M \leq p^n$ and it follows from Lemma 4.2, with p in place of m, that $M \geq 1$ for every P large enough. Hence,

$$\frac{1}{p^{n-1}(p-1)} \leq F_p(P) \leq \frac{p}{(p-1)}.$$

and so there exist $0 < \gamma_1' < \gamma_2'$ such that

$$\gamma_1' < \prod_{\substack{p \leq c_5 \\ p \in \mathbb{P}}} F_p(P) < \gamma_2'. \tag{4.33}$$

From (4.30) and (4.33) it follows that

$$\frac{1}{2}\gamma_1' \leq \prod_{p \in \mathbb{P}} F_p(P) \leq 2\gamma_2'.$$

and from (4.28) the result with $\gamma_1 = \frac{1}{2}\gamma_1'$ and $\gamma_2 = 2\gamma_2'$. □

4.7 The proof of the Auxiliary Theorem

Proof. We have already observed that if $k \geq 4n$ then $\mathcal{E}(U_1) \subseteq \mathfrak{M}$ and so

$$\mathcal{C}\mathfrak{M} \subseteq \mathcal{C}\mathcal{E}(U_1) = \mathfrak{m}.$$

Hence, we can write

$$\mathcal{N}(P) = \int_0^1 S(\alpha) T(-\alpha)\, d\alpha = \int_{\mathfrak{M}} S(\alpha) T(-\alpha)\, d\alpha + \int_{\mathcal{C}\mathfrak{M}} S(\alpha) T(-\alpha)\, d\alpha.$$

and from (4.7), (4.20), (4.26) we have

$$\mathcal{N}(P) = \left\{S(P) + O\left(L^{-c_4}\right)\right\} J(P) + O\left(P^n L^{-2}\right). \tag{4.34}$$

where

$$J(P) = \int_{|\beta| < P^{-2}L^k} I(\beta) I_1(-\beta)\, d\beta. \tag{4.35}$$

Proceeding as in the proof of the First Theorem of Pleasants 3.14, we have

$$I_1(-\beta) = \frac{P^2}{2L}\int_{g_1}^{g_2} e\left(-\beta P^2 x\right) dx + O\left(P^2 L^{-2} \min\left\{1, \left|\beta P^2\right|^{-1}\right\}\right). \tag{4.36}$$

From (4.23) and (4.36) by multiplication we have

$$J(P) = M_{\mathcal{T}} + E_{\mathcal{T}}.$$

where

- $M_{\mathcal{T}} = \frac{P^2}{2L} \int\limits_{|\beta|<P^{-2}L^k} \left\{ \int\limits_{P\mathcal{B}} e\left(\beta\varphi_P(\xi)\right) d\xi \right\} \left\{ \int\limits_{g_1}^{g_2} e\left(-\beta P^2 x\right) dx \right\} d\beta.$
- $E_T \ll P^{n+2}L^{-2} \int\limits_{|\beta|<P^{-2}L^k} \min\left\{1, |\beta P^2|^{-1}\right\}.$

being $M_{\mathcal{T}}$ the **main term** and $E_{\mathcal{T}}$ the **error term**. □

If we call

$$J_1(P) = \int_{-L^k}^{L^k} \left\{ \int_{\mathcal{B}} e\left(\gamma P^{-2}\varphi_P(P\xi)\right) d\xi \right\} \left\{ \int_{g_1}^{g_2} e\left(-\gamma x\right) dx \right\} d\gamma. \tag{4.37}$$

we have

$$M_{\mathcal{T}} = \frac{P^n}{2L} J_1(P). \tag{4.38}$$

while

$$E_T \ll P^{n+2}L^{-2}P^{-2}\log L \ll P^n L^{-2}\log L. \tag{4.39}$$

From (4.38),(4.39) we have

$$J(P) = \frac{P^n}{2L} J_1(P) + O\left(P^n L^{-2}\log L\right). \tag{4.40}$$

Interchanging the order of integration in (4.37) and integrating with respect to γ we have

$$J_1(P) = \int_{\mathcal{B}} d\eta \int_{g_1}^{g_2} dx \int_{-L^k}^{L^k} e\left(\gamma\left(P^{-2}\varphi_P(P\eta) - x\right)\right) d\gamma.$$

and so

$$J_1(P) = \int_{\mathcal{B}} d\eta \int_{g_1}^{g_2} \frac{\sin 2\pi L^k \left(P^{-2}\varphi_P\left(P\eta\right) - x\right)}{\pi\left(P^{-2}\varphi_P\left(P\eta\right) - x\right)} dx.$$

and finally

$$J_1(P) = \int_{\mathcal{B}} d\eta \int_{a(\eta,P)}^{b(\eta,P)} \frac{\sin 2\pi L^k t}{\pi t} dt.$$

where

- $a\left(\eta, P\right) = g_1 - P^{-2}\varphi_P\left(P\eta\right).$
- $b\left(\eta, P\right) = g_2 - P^{-2}\varphi_P\left(P\eta\right).$

From (4.2) and (4.4), for P large enough and for all η and $\mathcal{B}$

- $a\left(\eta, P\right) \leq g_1 - f_1 < 0.$
- $b\left(\eta, P\right) \geq g_2 - f_2 > 0.$

Since

$$\lim_{P\to+\infty} \int_{a(\eta,P)}^{b(\eta,P)} \frac{\sin 2\pi L^k t}{\pi t} dt = 1.$$

uniformly in η we have that

$$\lim_{P\to+\infty} J_1(P) = \int_{\mathcal{B}} d\eta = V_{\mathcal{B}}. \tag{4.41}$$

Now, from (4.35), (4.40), (4.41) we have

$$\mathcal{N}\left(P\right) = \mathfrak{S}\left(P\right)\frac{V_{\mathcal{B}}P^n}{\log P^2} + o\left(P^n L^{-1}\right).$$

With the result of Lemma 4.12 this completes the proof of the Auxiliary Theorem.

4.8 A Corollary of the Auxiliary Theorem

It will be convenient for latter applications to have the following straightforward Corollary to the Auxiliary Theorem stated explicitly.

Corollary 4.1. *Let*

$$\phi(\mathbf{x}) = Q(\mathbf{x}) + L(\mathbf{x}) + N.$$

a quadratic polynomial in $\mathbb{Q}(\mathbf{x})$ *with constant coefficients that we write as*

$$\phi(\mathbf{x}) = \sum_{i=1}^{n}\sum_{j=1}^{n}\frac{r_{ij}}{s_{ij}}x_i x_j + \sum_{i=1}^{n}\frac{k_i}{m_i}x_i + \frac{u}{v}.$$

Suppose

$$\begin{cases} (r_{ij}, s_{ij}) = 1 & \forall i, j = 1 \dots n \\ (k_i, m_i) = 1 & \forall i = 1 \dots n \\ (u, v) = 1. \end{cases}$$

If

- $\mathbf{x} \in \mathbb{Z}^n \Rightarrow \phi(\mathbf{x}) \in \mathbb{Z}^n$.
- *There exists a* $\mathbf{x_0} \in \mathbb{Z}^n$ *such that* $\phi(\mathbf{x}_0) \equiv 1 \pmod 2$.
- *If* r *denotes the rank of* Q, $r \geq 3$.
- Q *is neither* ***negative definite*** *nor* ***negative semi-definite***.
- $\mathcal{B} \subset \mathbb{R}^n$ *is any closed box with volume* $V_{\mathcal{B}}$ *such that* $\mathbf{x} \in \mathcal{B} \Rightarrow Q(\mathbf{x}) > 0$
- $\mathcal{N}(P) = \{\mathbf{x} \in P\mathcal{B} : \phi(\mathbf{x}) \in \mathbb{P}\}$.

then

$$|\mathcal{N}(P)| \sim \mathfrak{S}\frac{P^n V_{\mathcal{B}}}{\log P^2} \qquad P \to +\infty.$$

where $\mathfrak{S}$ *is a positive constant.*

Proof. Let

- $e_1 = \min_{\mathbf{x}\in\mathcal{B}} Q(\mathbf{x})$.
- $e_2 = \max_{\mathbf{x}\in\mathcal{B}} Q(\mathbf{x})$.

and let f_1, f_2 real numbers such that

$$0 < f_1 < e_1 < e_2 < f_2.$$

For every $\mathbf{x} \in \mathcal{B}$ we have

$$\phi(P\mathbf{x}) = P^2 Q(\mathbf{x}) + O(P).$$

Hence, for any $\mathbf{y} \in \mathbb{B}$ and for P large enough we have

$$f_1 P^2 < \phi(\mathbf{y}) < f_2 P^2.$$

Thus ϕ satisfies all the requirements of the Auxiliary Theorem. To obtain the result of the corollary we observe that since the coefficients of ϕ are constant, the exponential sums $S_{a,q}(P)$ defined in Lemma 4.8 are independent of P. Thus from (4.27) we have that the function $P \to \mathfrak{S}(P)$ is a constant function a by Lemma 4.12 the value of this constant is positive. □

4.9 Further Lemmas

In order to prove the Second Theorem of Pleasants we still need a number of results about polynomials.

Lemma 4.13. *Let* $\mathbf{x} \in \mathbb{R}^n$ *and*

$$\phi(\mathbf{x}) = \phi(x_1 \dots x_n) \in \mathbb{Q}[\mathbf{x}].$$

that we write as

$$\phi(\mathbf{x}) = \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{r_{ij}}{s_{ij}} x_i x_j + \sum_{i=1}^{n} \frac{k_i}{m_i} x_i + \frac{u}{v}.$$

Suppose that

1. $\mathbf{x} \in \mathbb{Z}^n \Rightarrow \phi(\mathbf{x}) \in \mathbb{Z}$.
2. $$\begin{cases} (r_{ij}, s_{ij}) = 1 & \forall i, j = 1 \dots n \\ (k_i, m_i) = 1 & \forall i = 1 \dots n \\ (u, v) = 1. \end{cases}$$
3. *There exists a* $\mathbf{x_0} \in \mathbb{Z}^n$ *such that* $.\phi(\mathbf{x}_0) \equiv 1 \pmod 2$
4. $\frac{\partial Q(\mathbf{x})}{\partial x_1} = 0 \ \forall \mathbf{x} \in \mathbb{R}^n$.
5. $\exists \overline{\mathbf{x}} \in \mathbb{R}^n : \ \frac{\partial L(\overline{\mathbf{x}})}{\partial x_1} \neq 0$.

If

$$\mathcal{H} = \left\{ \mathbf{x} \in \mathbb{Z}^n : |x_1| < P^2, |x_i| < P, \ i = 2 \dots n, \ \phi(\mathbf{x}) \in \mathbb{P} \right\}.$$

then

$$|\mathcal{H}| \gg \frac{P^{n+1}}{\log P} \qquad (P \to \infty).$$

Proof. By condition (4) we have that ϕ is of the form

$$\phi(x_1, x_2, \dots x_n) = \phi_1(x_2, \dots x_n) + ax_1. \tag{4.42}$$

where ϕ_1 is a polynomial that depends only on $x_2 ... x_n$ and a is a constant. Since form condition (1) it is

$$\phi(0, 0, \dots 0) = \phi_1(0, \dots 0) = m_0 \in \mathbb{Z}.$$

and

$$\phi(1, 0, \dots, 0) = m_1 \in \mathbb{Z}.$$

we have that $a \in \mathbb{Z}$ and $\phi_1(x_2, ...x_n) \in \mathbb{Z}$ for every $(x_2, ...x_n) \in \mathbb{Z}^{n-1}$. By (1), (2), (3), it follows that ϕ satisfies the conditions of Lemma 4.2 and so there exists $\mathbf{y} = (y_1, \dots y_n) \in \mathbb{Z}^n$ such that $(\phi(\mathbf{y}), a) = 1$.
If now $\mathbf{x}' = (x_2, \dots, x_n) \in \mathbb{Z}^{n-1}$ is any integer point such that

$$(x_2', \dots, x_n') \equiv (y_2, \dots, y_n) \pmod{a}. \tag{4.43}$$

we have

$$(\phi_1(x_2' \dots x_n'), a) = 1. \tag{4.44}$$

We observe now that if $Q_1(\mathbf{x}') = Q(\mathbf{x})$ and we choose

$$\mathcal{B}' = \left\{ \xi' \in \mathbb{R}^{n-1} : |\xi'| < 1, |Q_1(\xi')| < \frac{1}{4}|a| \right\}. \tag{4.45}$$

This can be done, for instance, by taking $\mathcal{B}'$ to be a sufficiently small box containing the origin $O \in \mathbb{R}^{n-1}$. Now we consider the expanded box $P\mathcal{B}'$ and any integer point $\mathbf{x}' \in P\mathcal{B}'$ satisfying (4.43). It follows that $\mathbf{x}'$ also satisfies (4.44) and if we take

$$\xi' = \frac{\mathbf{x}'}{|\mathbf{x}'|}.$$

by the second condition in the the definition of $\mathcal{B}'$, we deduce

$$|\phi_1(\mathbf{x}')| < P^2 \frac{1}{4}|a| + O(P) < \frac{1}{2}|a| P^2.$$

for P large enough. It follows that if we consider the intervals

$$I_{a,P} = \left[-|a| P^2 + \varphi_1(\mathbf{x}'), |a| P^2 + \varphi_1(\mathbf{x}') \right].$$

$$J_{a,P} = \left[0, \frac{1}{2}|a| P^2 \right].$$

we have

$$J_{a,P} \subseteq I_{a,P}.$$

Now we apply the Proposition E.9 and deduce that if

$$\mathfrak{P}(P) = \{p \in \mathbb{P} : p \in I_{a,P}, p \equiv \phi_1(\mathbf{x}') \pmod a\}.$$

then

$$|\mathfrak{P}(P)| \gg \frac{P^2}{\log P}. \tag{4.46}$$

and this estimate is uniform in $\mathbf{x}'$. Also, if

$$\mathcal{D}(P) = \{\mathbf{x}' \in P\mathcal{B}' \cap \mathbb{Z}^n : (x_2, \ldots, x_n) \equiv (y_2, \ldots, y_n) \pmod a\}.$$

then

$$|\mathcal{D}(P)| \gg P^{n-1}. \tag{4.47}$$

and, by the first condition in the definition of $\mathcal{B}'$, all these points satisfy $|\mathbf{x}'| < P$. Now from (4.42), (4.46), (4.47) we obtain the result. □

Lemma 4.14. *Let be* $\mathbf{x} = (x_1, \ldots x_n) \in \mathbb{R}^n$ *and let*

$$L(\mathbf{x}) = l_0 + \sum_{j=1}^{n} l_j x_j.$$

be a non-constant polynomial of first degree such that

- $l_j \in \mathbb{Z}$ *for* $j = 0...n$.
- $(l_0, \ldots l_n) = 1$.
- *There exists an open box* $\mathcal{A} \subset \mathbb{R}^n$ *and* $.\mathbf{a} = (a_1, \ldots a_n) \in \mathcal{A}$ *for which*

$$\sum_{j=1}^{n} a_j l_j \geq 0.$$

If

$$\mathcal{G}(P) = \{\mathbf{x} \in P\mathcal{A} \cap \mathbb{Z}^n : L(\mathbf{x}) \in \mathbb{P}\}.$$

then

$$|\mathcal{G}(P)| \gg \frac{P^n}{\log P}.$$

Proof. Since $L(\mathbf{x})$ is non-constant, we can find a point $\mathbf{b} \in \mathcal{A}$ such that

$$\sum_{j=1}^{n} b_j l_j > 0. \tag{4.48}$$

Since $\mathcal{A}$ is open, we can find a box $\mathcal{B}$ such that

- $\mathcal{B} \subseteq \mathcal{A}$.
- $\xi \in \mathcal{B} \Rightarrow \sum_{j=1}^{n} \xi_j l_j \geq 0$.

We write

$$\mathcal{B} = \prod_{j=1}^{n} (a_j, b_j).$$

and

- $\mathcal{B}^1 = (\alpha_1, \beta_1)$.
- $\mathcal{B}^{n-1} = \prod_{j=2}^{n} (\alpha_j, \beta_j)$.

We write also

$$L_1(x_2, \ldots x_n) = l_0 + \sum_{j=2}^{n} l_j x_j.$$

so that

$$L(\mathbf{x}) = L_1(x_2, \ldots x_n) + l_1 x_1. \tag{4.49}$$

Since the coefficients of $L(\mathbf{x})$ have no common factor, we can find $(y_2, \ldots y_n) \in \mathbb{Z}^{n-1}$ such that

$$(L_1(y_2, \ldots y_n), l_1) = 1.$$

It follows that for any $\mathbf{x}' = (x_2, \ldots x_n) \in \mathbb{Z}^{n-1}$. satisfying

$$(x_2, \ldots x_n) \equiv (y_2, \ldots y_n) \pmod{l_1}.$$

we have

$$(L_1(x_2, \ldots x_n), l_1) = 1. \tag{4.50}$$

Hence, if

$$\mathcal{K}(P) = \left\{ \mathbf{x}' \in P\mathcal{B}^{n-1} \cap \mathbb{Z}^{n-1} : (L_1(\mathbf{x}'), l_1) = 1 \right\}.$$

then

$$|\mathcal{K}(P)| \gg P^{n-1}. \tag{4.51}$$

For each $\mathbf{x}' \in \mathcal{K}(P)$ we consider the real interval

$$J(P, \mathbf{x}') = (l_1 P\alpha_1 + L_1(\mathbf{x}'), l_1 P\beta_1 + L_1(\mathbf{x}')).$$

and we notice that

$$\mu_{\mathcal{L}}(J(P, \mathbf{x}')) = P(l_1\beta_1 - l_1\alpha_1).$$

On the other side, if

$$M = \max\{|l_0|, |l_2|, \cdots, |l_n|\}.$$

and

$$T = \max\{|\alpha_2|, \ldots |\alpha_n|, |\beta_2| \ldots |\beta_n|\}.$$

it is easy to show that

$$|L_1(x_2, \ldots x_n)| \leq M + (n-2)T \quad \forall (x_2, \ldots x_n) \in \mathcal{B}^{n-1}.$$

while, by (4.48) it is

$$l_0 \leq L_1(x_2, \ldots x_n) \quad \forall (x_2, \ldots x_n) \in \mathcal{B}^{n-1}.$$

Hence, there exists $\theta = \theta(\mathcal{B}, n, L)$ such that

$$J(P, \mathbf{x}') \subseteq [l_0, \theta P].$$

for every P large enough. It follows from E.9 that if

$$\mathfrak{P}_1(P) = \{p \in \mathbb{P} : p \in J(P, \mathbf{x}'), p \equiv L_1(\mathbf{x}') \mod (l_1)\}.$$

then

$$|\mathfrak{P}_1(P)| \gg \frac{P}{\log P}. \tag{4.52}$$

uniformly in $\mathbf{x}'$. The conclusion of the Lemma now follows from (4.49), (4.51), (4.52). □

Lemma 4.15. *Let* $\mathbf{x} = (x_1, \ldots x_n) \in \mathbb{R}^n$ *and* $\phi_1(\mathbf{x}), \ldots \phi_r(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$. ***If***

- ϕ_1 *is not constant.*
- $(\phi_1, \ldots \phi_r) = 1$.
- *There exist continuous functions* $U_i : \mathbb{R}^+ \to \mathbb{R}^+$, $i = 1...n$ *such that*
  - $\lim_{P \to +\infty} U_i(P) = +\infty \quad \forall i = 1 \ldots n.$

– *There exist* $\gamma_i > 0$ *and* $m_i > 0$ *and* $P_0 > 0$ *such that*

$$U_i(P) \leq \gamma_i P^{m_i} \qquad \forall P > P_0, \forall i = 1 \dots n.$$

- $\mathcal{K}(P) = \{\mathbf{x} \in \mathbb{Z}^n : |x_i| < P,\ \phi_1(\mathbf{x}) | \phi_j(\mathbf{x}),\ \ i = 1, \dots n, j = 2, \dots r\}$.

Then *for every* $\varepsilon > 0$

$$|K(P)| \ll \max_{1 \leq i \leq n} \frac{U(P)}{U_i(P)} P^{\varepsilon}.$$

where

$$U(P) = \prod_{j=1}^{r} U_i(P).$$

Proof. Since ϕ_1 is not constant we can suppose, by permuting the variables if necessary, that ϕ_1 does not depends by $x_2, ...x_n$ only. Also, since $\phi_1, ..., \phi_r$ have no common factor, it follows from Proposition E.10 that there exist polynomials

$$\begin{cases} \psi_1 = \psi_1(x_1 \dots x_n) \\ \vdots \\ \psi_r = \psi_r(x_1 \dots x_n) \end{cases} \in \mathbb{Z}(x_1 \dots x_n).$$

and

$$H = H(x_2 \dots x_n) \in \mathbb{Z}(x_2 \dots x_n).$$

with H not identically zero such that

$$\sum_{j=1}^{r} \phi_j(\mathbf{x}) \psi_j(\mathbf{x}) = H(\mathbf{x}) \quad \forall \mathbf{x} \in \mathbb{R}^n.$$

We observe that:

- If

$$K_1(P) = \{\mathbf{x} \in \mathbb{Z}^n : |x_i| < U_i(P)\ \ \forall i = 1, ..., n,\ \ H(x_2, \dots x_n) = 0\}.$$

then

$$|K_1(P)| \ll \frac{U(P)}{\max\limits_{2 \leq i \leq n} U_i(P)}.$$

- If

$$\begin{cases} \mathbf{x} \in \mathbb{Z}^n \\ |x_i| < U_i(P)\ \ \forall i = 1, ..., n. \end{cases}$$

then there exists $M > 0$ and $\gamma > 0$ such that $|H(x_2, \dots x_n)| \leq M P^{\gamma}$.

It follows that if $m = H(x_2, \ldots x_n) \neq 0$ then for every $\varepsilon > 0$ $\tau(m) \ll P^{\varepsilon}$ where τ is the function which counts the divisors of an integer. Let

$$\Gamma(P) = \{c \in \mathbb{Z} : \exists \mathbf{x} = (x_1, x_2, \ldots x_n) \in \mathcal{K}_1(P),\ \ H(x_2, \ldots x_n) \neq 0\}.$$

Since, if $\mathbf{x} \in \mathcal{K}_1(P)$ then

$$\phi_1(\mathbf{x}) | H(x_2, \ldots x_n).$$

it follows that

$$|\Gamma(P)| \ll P^{\varepsilon}.$$

The strategy now is to count,for each $c \in \Gamma(P)$, how many $\mathbf{x} \in \mathcal{K}(p)$ we can have. If $c \in \Gamma(P)$ and we consider the equation

$$\phi_1(x_1, x_2, \ldots x_n) = c.$$

we can rewrite it as

$$J_0(x_2, \ldots x_n) x_1^k + J_1(x_2, \ldots x_n) x_1^{k-1} + \cdots J_k(x_2, \ldots x_n) = 0.$$

where

- $k \geq 1$.
- J_0 is not identically zero.
- J_0 is independent of c.

If

$$\Omega(P) = \{(x_1, x_2, \ldots x_n) \in \mathcal{K}(P) : \phi_1(x_1, x_2, \ldots x_n) = c\}.$$

the we have

$$\Omega(P) = \Omega_1(P) \cup \Omega_2(P).$$

where

$$\Omega_1(P) = \{(x_1, x_2, \ldots x_n) \in \mathcal{K}(P) :\ \phi_1(x_1, x_2, \ldots x_n) = c, J_0(x_2, \ldots x_n) = 0.\}$$

and

$$\Omega_2(P) = \{(x_1, x_2, \ldots x_n) \in \mathcal{K}(P) :\ \phi_1(x_1, x_2, \ldots x_n) = c, J_0(x_2, \ldots x_n) \neq 0.\}$$

Now,

$$|\Omega_1(P)| \ll U_1(P) \left(\max_{2 \leq i \leq n} \frac{U(P)}{U_i(P) U_1(P)} \right).$$

since the set

$$\{(x_2, \ldots x_n) : \exists x_1, (x_1, x_2, \ldots x_n) \in \mathcal{K}(P), J_0(x_2, \ldots x_n) = 0\}.$$

has cardinality $\ll \max_{2 \leq i \leq n} \frac{U(P)}{U_i(P) U_1(P)}$ and the set of suitable x_1 has cardinality $\ll U_1(P)$. Also,

$$|\Omega_2(P)| \ll k \frac{U(P)}{U_1(P)}.$$

since the set

$$\{(x_2, \ldots x_n) : \exists x_1, (x_1, x_2, \ldots x_n) \in K(P), J_0(x_2, \ldots x_n) \neq 0\}.$$

has cardinality $\ll \frac{U(P)}{U_1(P)}$ and, by the Fundamental Theorem of Algebra, the set of suitable x_1 has cardinality $\ll k$. Hence

$$|\mathcal{K}(P)| \ll |\Gamma(P)| \{|\Omega_1(P)| + |\Omega_2(P)|\}.$$

and so

$$|\mathcal{K}(P)| \ll P^{\varepsilon} \left\{ U_1(P) \max_{2 \leq i \leq n} \frac{U(P)}{U_i(P) U_1(P)} + k \frac{U(P)}{U_1(P)} \right\}.$$

and finally

$$|\mathcal{K}(\mathcal{P})| \ll P^{\varepsilon} \max_{1 \leq i \leq n} \frac{U(P)}{U_i(P)}.$$

□

Lemma 4.16. *Let* $\mathbf{x} \in \mathbb{R}^n$ *and*

$$\phi(\mathbf{x}) = Q(\mathbf{x}) + L(\mathbf{x}) + N.$$

a quadratic polynomial, irreducible in $\mathbb{Q}[\mathbf{x}]$. ***If*** *:*

- $\phi(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$.
- *If we write*

$$\phi(\mathbf{x}) = \sum_{i=1}^{n} \sum_{j=1}^{n} r_{ij} x_i x_j + \sum_{i=1}^{n} k_i x_i + N.$$

  then

$$(r_{11} \ldots r_{1n}, r_{22} \ldots r_{2n}, \ldots r_{nn}, k_1 \ldots k_n, N) = 1.$$

- *There exists* $\mathbf{x}_0 \in \mathbb{Z}^n : \phi(\mathbf{x}_0) \not\equiv 0 \pmod 2$.

- *There exist two linear polynomials* $L_1(\mathbf{x})$, $L_2(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ *linearly independent on* $\mathbb{Q}$ *such that*

$$Q(\mathbf{x}) = L_1(\mathbf{x}) L_2(\mathbf{x}).$$

- $\mathbb{P}_\phi = \{p \in \mathbb{P} : \exists \mathbf{x} \in \mathbb{Z}^n, \phi(\mathbf{x}) = p\}$.

then

$$|\mathbb{P}_\phi| = +\infty.$$

Proof. Since $Q(\mathbf{x})$ factorises into distinct factors there exists a transformation

$$\underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_{\mathbf{x}} = \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}}_{\mathbf{A}} \underbrace{\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}}_{\mathbf{y}}.$$

such that

- $a_{ij} \in \mathbb{Z}$ for every $i, j = 1...n$.
- $\det \mathbf{A} = \pm 1$.
- $Q'(\mathbf{y}) = Q(\mathbf{A}\mathbf{y}) = y_1(ay_1 + by_2)$. with $a, b \in \mathbb{Z}$ and $b \neq 0$.

Such a transformation is permissible as it affects neither the hypotheses nor the conclusion of the Lemma. Just to make the notation more simple, we still write $Q(\mathbf{x}) = x_1(ax_1 + bx_2)$ in place of $Q'(\mathbf{y}) = y_1(ay_1 + by_2)$. In other words we rename the variables. We doing the same for $\phi'(\mathbf{y}) = \phi(\mathbf{A}\mathbf{y})$ and so, from now on we think to ϕ as the polynomial obtained after the application of the transformation. If ϕ contains a variable other than x_1 and x_2 , the it satisfies the conditions of Lemma 4.13 and the result follows. Hence we can suppose that ϕ is of the form

$$\phi(x_1, x_2) = x_1(ax_1 + bx_2) + cx_1 + dx_2 + e.$$

where $a, b, c, d, e \in \mathbb{Z}$ and $b \neq 0$. Let $m = abcde$: the polynomial ϕ satisfies the conditions of Lemma 4.2 and so there exist $X_1, X_2 \in \mathbb{Z}$ such that

$$(\phi(X_1, X_2), m) = 1. \tag{4.53}$$

Let $x_1 = X_1 + my$. We have

$$\phi(x_1, x_2) = x_2 \mathcal{L}_1(y) + \mathcal{Q}_1(y). \tag{4.54}$$

where

- $\mathcal{L}_1(y) = bmy + bX_1 + d$.
- $\mathcal{Q}_1(y) = am^2y^2 + m(2aX_1 + c)y + (aX_1^2 + cX_1 + e)$.

We observe that

- $\mathcal{L}_1(y)$ is not constant because $b \neq 0$.
- $\phi(x_1, x_2) = x_2(bx_1 + d) + (ax_1^2 + cx_1 + e)$.
- The polynomials $F(x_1) = bx_1 + d$, $G(x_1) = ax_1^2 + cx_1 + e$ have no common factor, as, would divide ϕ, cotradicting its irreducibility.

Hence there exist $A, B, C, D \in \mathbb{Z}$ with $D \neq 0$ such that

$$(Ax_1 + B)(bx_1 + d) + C\left(ax_1^2 + cx_1 + e\right) = D. \tag{4.55}$$

and so for any $x_1 \in \mathbb{Z}$ the greatest common divisor of the numbers $F(x_1)$ and $G(x_1)$ divides D. Thus for any integer y the greatest common divisor of $L_1(y)$ and $Q_1(y)$ divides D. Denote with

$$\lambda_1 = (bm, b, d).$$

Then $\lambda_1 | bm$ and so $\lambda_1 | m^2$. By Dirichlet's theorem on primes in arithmetic progression there are infinitely many $y \in \mathbb{Z}$ for which $L_1(y) = \lambda_1 p$ where $p \in \mathbb{P}$. Hence we can choose some integer Y for which

- $L_1(Y) = \lambda_1 p$.
- $p \not| D$.

For this Y, we have that if $\Lambda_1(Y) = (L_1(Y), Q_1(Y))$. then $\Lambda_1(Y) | \lambda_1$ On the other hand it follows from (4.53) that

$$(\phi(X_1 + my, X_2), m) = 1.$$

and hence by (4.54)

$$(\Lambda_1(Y), m) = 1.$$

Hence

$$(L_1(Y), Q_1(Y)) = 1.$$

Thus, again by Dirichlet's theorem on arithmetic progression, if

$$H(x_2) = x_2 L_1(Y) + Q_1(Y).$$

then $H(x_2) \in \mathbb{P}$ for infinitely many $x_2 \in \mathbb{Z}$. By (4.54) the result follows. □

Lemma 4.17. *Let* $\mathbf{x} = (x_1 \dots x_n) \in \mathbb{R}^n$. ***If***

$$Q_0(\mathbf{x}) \dots Q_r(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}].$$

are quadratic forms, not all vanishing identically, ***then*** *at least one of the following three propositions holds:*

(I) ***If***

$$\Theta(P) = \{(\lambda_1 \dots \lambda_r) \in \mathbb{Z}^r : \forall i = 1...r \ |\lambda_i| < P, r(Q(\mathbf{x})) \leq 2\}.$$

with

$$Q(\mathbf{x}) = Q_0(\mathbf{x}) + \sum_{i=1}^{r} \lambda_i Q_i(\mathbf{x}).$$

then

$$|\Theta(P)| \ll P^{r-1}.$$

(II) *There exists a transformation*

$$\underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_{\mathbf{x}} = \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}}_{\mathbf{A}} \underbrace{\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}}_{\mathbf{y}}.$$

such that

- $a_{ij} \in \mathbb{Z}$ *for every* $i, j = 1...n$.
- $\det \mathbf{A} = \pm 1$
- *If* $Q_i'(\mathbf{y}) = Q_i(\mathbf{A}\mathbf{y})$ *for* $i = 0...r$ *then* [2].

$$\frac{\partial}{\partial y_j} Q_i'(\mathbf{y}) = 0.$$

identically, for every $i = 0...r$ *and for every* $j = 3...n$

(III) *There exists a linear form* $L_c(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ *such that*

$$\begin{cases} L_c(\mathbf{x}) \,|Q_0(\mathbf{x}) \\ \vdots \\ L_c(\mathbf{x}) \,|Q_r(\mathbf{x}). \end{cases}$$

[2] i.e the forms Q_i' do not involve the variables $y_3, ...y_n$

Proof. For every $i = 0, ...r$ we express Q_i as

$$Q_i(\mathbf{x}) = q_{i,1}L_{i,1}^2(\mathbf{x}) + \cdots q_{i,k_i}L_{i,k_i}^2(\mathbf{x}).$$

where

- $q_{i,1}...q_{i,k_i} \in \mathbb{Q}$ for every $i = 0...r$.
- $L_{i,j}(\mathbf{x}) = \sum_{j=1}^{n} \alpha_{i,j}x_j$ with $\alpha_{i,j} \in \mathbb{Q}$ for every $i = 0...r$,$j = 1...n$.

We rename the linear form as

$$\begin{aligned} L_1(\mathbf{x}) &= L_{0,1}(\mathbf{x}) \\ L_2(\mathbf{x}) &= L_{0,2}(\mathbf{x}) \\ &\vdots \\ L_s(\mathbf{x}) &= L_{r,k_r}(\mathbf{x}). \end{aligned}$$

where $s = \sum_{i=0}^{r} k_i$ so that $\mathbf{L} = \{L_1(\mathbf{x}), \ldots, L_s(\mathbf{x})\}$. First we show that **if** no three of the linear forms in $\mathbf{L}$ are linearly independent over $\mathbb{Q}$ **then** (II) holds. Let $L_1(\mathbf{x}) = a_1x_1 + \cdots a_nx_n$. We can suppose, by taking a rational multiple of L_1 if necessary, that

- $a_1...a_n \in \mathbb{Z}$.
- $(a_1, ...a_n) = 1$.

so that there exists an integral unimodular transformation such that [3]

$$L_1(\mathbf{x}) = x_1.$$

If on making this substitution we have

$$\begin{cases} L_2(\mathbf{x}) = \beta_2 x_1 \\ \vdots \\ L_s(\mathbf{x}) = \beta_s x_1. \end{cases}$$

we have (II). Otherwise one of these linear forms, say L_2 is of the shape

$$L_2(\mathbf{x}) = b_1x_1 + b_2x_2 + \cdots b_nx_n.$$

where $b_2...b_n$ are not all zero. Taking a rational multiple of L_2 if necessary, we can suppose that

[3] As usual the unimodular transformation has the form $\mathbf{x} = \mathbf{A}\mathbf{y}$ and hence $L_1'(\mathbf{y}) = L_1(\mathbf{A}\mathbf{y})$. Of course we can always rename the variables in L_1' taking them from y_i to x_i so that we still express L_1 as function of x_i. With abuse of notation we still use L_1 in place of L_1' just to avoid further symbols

- $b_2 ... b_n \in \mathbb{Z}$.
- $(b_2, ... b_n) = 1$.

so that there exists an integral unimodular transformation such that the linear form

$$l_2 : \mathbb{R}^{n-1} \to \mathbb{R}^{n-1}$$
$$(x_2 \dots x_n) \to b_2 x_2 + \cdots b_n x_n.$$

takes the shape

$$l_2 (x_2 \dots x_n) = x_2.$$

After this transformation we have

$$L_2 (\mathbf{x}) = b_1 x_1 + x_2.$$

Since we are supposing that no three of the linear forms of $\mathbf{L}$ are linearly independent, the same transformation takes all the remaining elements of $\mathbf{L}$ into linear combinations of x_1 and x_2. Thus (II) holds. To prove the Lemma we can assume that at least three of the linear forms of $\mathbf{L}$ are linearly independent and that (I) does not hold and show that these assumptions imply that (III) holds. If for any $(\lambda_0 \dots \lambda_r) \in \mathbb{R}^{r+1}$ we have that $r (Q (\mathbf{x})) \geq 3$ with

$$Q (\mathbf{x}) = \sum_{i=0}^{r} \lambda_i Q_i (\mathbf{x}).$$

we have

(a) If $\mathbf{M}_Q$ is the associated matrix of Q we have that all its minors of order 3×3 considered as polynomials in the variables $\lambda_1 ... \lambda_r$ are not identically zero.

(b) If $M_{3\times 3} (\lambda_1 \dots \lambda_r)$ denotes a generic minor of order 3×3 of $\mathbf{M}_Q$ and

$$V_{M_{3\times 3}} = \{(\lambda_1 \dots \lambda_r) \in \mathbb{Z}^r : M_{3\times 3} (\lambda_1 \dots \lambda_r) = 0, \, |\lambda_i| < P \; i = 1 \dots r\}.$$

then, for (a), at for at least on $M_{3\times 3}$ we must have

$$\left|V_{M_{3\times 3}}\right| \ll P^{r-1}.$$

and hence for (b),it follows that(I) holds. Thus we can now suppose that for each of the quadratic forms $Q_0 ... Q_r$ it is $r(Q_i) \leq 2$ and we are going to consider separately the different cases that can arise. In each case we shall suppose, with generality, that L_1, L_2, L_3 are linearly independent. We shall indicate as $\Xi = \{Q_0 ... Q_r\}$ the set of our quadratic forms. First of all we notice that

- If $r\left(Q_l\left(\mathbf{x}\right)\right) \leq 2$ for $l = 0...r$.
- L_1, L_2, L_3 are linearly independent.

there are only four possible cases:

Case 1

$$\begin{cases} Q_i\left(\mathbf{x}\right) = aL_1^2\left(\mathbf{x}\right). \\ Q_j\left(\mathbf{x}\right) = bL_2^2\left(\mathbf{x}\right). \\ Q_k\left(\mathbf{x}\right) = cL_3^2\left(\mathbf{x}\right). \\ a, b, c \in \mathbb{Q} - \{0\}. \end{cases}$$

If

$$Q\left(\mathbf{x}\right) = Q_i\left(\mathbf{x}\right) + Q_j\left(\mathbf{x}\right) + Q_k\left(\mathbf{x}\right).$$

we have $r\left(Q\left(\mathbf{x}\right)\right) = 3$ and so, by our remark above, (I) holds.

Case 2

$$\begin{cases} Q_i\left(\mathbf{x}\right) = aL_1^2\left(\mathbf{x}\right) + bL_2^2\left(\mathbf{x}\right). \\ Q_j\left(\mathbf{x}\right) = cL_3^2\left(\mathbf{x}\right). \\ a, b, c \in \mathbb{Q} - \{0\}. \end{cases}$$

In this case $r\left(Q_i\left(\mathbf{x}\right)\right) = 2$ and $r\left(Q_j\left(\mathbf{x}\right)\right) = 1$. If

$$Q\left(\mathbf{x}\right) = Q_i\left(\mathbf{x}\right) + Q_j\left(\mathbf{x}\right).$$

we have $r\left(Q\left(\mathbf{x}\right)\right) = 3$ and so, by our remark above, (I) again holds.

Case 3

$$\begin{cases} Q_i\left(\mathbf{x}\right) = aL_1^2\left(\mathbf{x}\right) + bL_2^2\left(\mathbf{x}\right). \\ Q_j\left(\mathbf{x}\right) = cL_3^2\left(\mathbf{x}\right) + dL_4^2\left(\mathbf{x}\right). \\ a, b, c, d \in Q - \{0\}. \end{cases}$$

with L_1, L_2, L_3, L_4 linearly independent. In this case $r\left(Q_i\left(\mathbf{x}\right)\right) = 2$ and $r\left(Q_j\left(\mathbf{x}\right)\right) = 2$. If

$$Q\left(\mathbf{x}\right) = Q_i\left(\mathbf{x}\right) + Q_j\left(\mathbf{x}\right).$$

we have $r\left(Q\left(\mathbf{x}\right)\right) = 4$ and so, by our remark above, (I) again holds.

Case 4

$$\begin{cases} Q_i\left(\mathbf{x}\right) = aL_1^2\left(\mathbf{x}\right) + bL_2^2\left(\mathbf{x}\right). \\ Q_j\left(\mathbf{x}\right) = cL_3^2\left(\mathbf{x}\right) + dL_4^2\left(\mathbf{x}\right). \\ a, b, c, d \in Q - \{0\}. \end{cases}$$

with

- $L_4 = \alpha L_1 + \beta L_2 + \gamma L_3$, $\alpha, \beta, \gamma \in \mathbb{Q}$.
- $r\left(Q_i\left(\mathbf{x}\right)\right) = 2$.

- $r\left(Q_j\left(\mathbf{x}\right)\right)=2$.

In this case there is a rational non-singular transformation taking

- $Q_i\left(\mathbf{x}\right)$ into $ay_1^2+by_2^2$ with $a,b\in\mathbb{Q}$.
- $Q_j\left(\mathbf{x}\right)$ into $cy_3^2+d(l_1y_1+l_2y_2+l_3y_3)^2$ with $c,d,l_1,l_2,l_3\in\mathbb{Q}$ and l_1,l_2 not both zero.

Assume (I) does not hold and consider the quadratic form

$$Q\left(\mathbf{x}\right)=\lambda Q_i\left(\mathbf{x}\right)+\mu Q_j\left(\mathbf{x}\right)\quad\lambda,\mu\in\mathbb{R}.$$

It must be

$$r\left(Q\left(\mathbf{x}\right)\right)\leq 2\quad\forall\lambda,\mu\in\mathbb{R}.$$

otherwise we would have that (I) holds. This means that the determinant of $Q\left(\mathbf{x}\right)$ vanishes for all $\lambda,\mu\in\mathbb{R}$. This determinant is:

$$\Delta\left(\lambda,\mu\right)=\begin{vmatrix}\lambda a+\mu dl_1^2 & \mu dl_1l_2 & \mu dl_1l_3\\ \mu dl_1l_2 & \lambda b+\mu dl_2^2 & \mu dl_2l_3\\ \mu dl_1l_3 & \mu dl_2l_3 & c+\mu dl_3^2\end{vmatrix}.$$

and it is a polynomial in λ,μ. Since it is zero for all $\lambda,\mu\in\mathbb{R}$ it must have all its coefficients zero. The coefficient of $\lambda^2\mu$ is $ab(c+dl_3^2)$ and hence, since $ab\neq 0$, we must have

$$c=-dl_3^2. \tag{4.56}$$

Also the coefficient of $\lambda\mu^2$ is $cd(al_2^2+bl_1^2)$, since $cd\neq 0$, we must have $al_2^2+bl_1^2=0$, whence

$$\frac{l_1^2}{a}=-\frac{l_2^2}{b}. \tag{4.57}$$

Using (4.56) and (4.57) we can write

- $Q_i\left(y_1,y_2\right)=A\left(l_1^2y_1^2-l_2^2y_2^2\right)$.
- $Q_j\left(y_1,y_2\right)=d\left(l_1y_1+l_2y_2+l_3y_3\right)^2-dl_3^2y_3^2$.

where $A\in\mathbb{Q}-\{0\}$ and

$$F\left(y_1,y_2\right)=l_1y_1+l_2y_2.$$

is a rational common factor of Q_i and Q_j. Hence another rational non-singular transformation takes

- $Q_i\,(y_1, y_2)$ into $z_1 z_2$.
- $Q_j\,(y_1, y_2)$ into $z_1 z_3$.

We consider now another generic quadratic form in Ξ and we have two possibilities:

1. If $Q_k = eL_5^2 + fL_6^2$ is a form in Ξ and $r(Q_k) = 2$ we need to show that if (I) does not hold $G(z_1) = z_1$ is also a factor of Q_k. We observe that neither

$$\mathcal{L}_1 = \{L_1, L_2, L_5, L_6\}\,.$$

nor

$$\mathcal{L}_2 = \{L_3, L_4, L_5, L_6\}\,.$$

can be a linearly independent set of linear forms. For if so we should have the situation of ***Case 3*** which leads to (I). On the other hand it is impossible for both L_5 and L_6, being linearly independent, to be linear combinations of L_1, L_2 and of L_3, L_4. Hence, on interchanging the roles of Q_i and Q_j if necessary, we can suppose that just three of the forms L_1, L_2, L_5, L_6 are linearly independent. But this is just the situation considered above, an we deduce, on the hypothesis that (I) does not hold, that Q_i and Q_k have a common linear factor. This factor must be either z_1 or z_2. In the latter case at least three of the linear forms L_3,L_4,L_5,L_6 are linearly independent. If all four of these linear forms were linearly independent we should have again the situation of ***Case 3*** and (I) would follow; hence just three of them are independent and, since we are assuming that (I) does not hold, we deduce as before that Q_j and Q_k have a common linear factor, and this factor can be only z_3. Thus Q_k is of the form $Q_k = \alpha_k z_2 z_3$ and we have $r(Q) = 3$ where $Q = Q_i + Q_j + Q_k$. This leads to (I). hence on the assumption that (I) is false, the only possibility is that $G(z_1) = z_1$ is a factor of Q_k.
2. If $Q_l = gL_7^2$ is a form in Ξ and $r(Q_l) = 1$ and (I) does not hold, then $L_7 = \alpha_7 z_1 + \beta_7 z_2 \quad \alpha_7, \beta_7 \in \mathbb{Q}$ since otherwise we should have the situation of ***Case 2*** which lead to (I). Similarity $L_7 = \alpha_7' z_1 + \beta_7' z_3 \quad \alpha_7', \beta_7' \in \mathbb{Q}$. Thus $L_7 = k z_1$ and so $G(z_1) = z_1$ is a factor of Q_l.

Hence in ***Case 4*** either $I)$ holds or else all the quadratic forms of Ξ have a common rational linear factor which is (III).

□

4.10 Cubic polynomials

4.10.1 Introduction

In proving Theorem 4.2 we can always replace the polynomial $\phi(\mathbf{x})$ by a polynomial obtained from ϕ by an integral unimodular transformation, as such a transformation leaves unaltered the set

$$C_\phi = \{\mathbf{y} \in \mathbb{Z}^n : \mathbf{y} = \phi(\mathbf{x}), \mathbf{x} \in \mathbb{Z}^n\}.$$

and preserves the property of having integer coefficients, so that both the hypotheses and the conclusion of the Theorem are unaffected by the transformation. If $\phi(\mathbf{x})$ is any cubic polynomial, we already know that its cubic $C(\mathbf{x})$ can be written as

$$C(\mathbf{x}) = \sum_{i=1}^{h} L_i(\mathbf{x}) Q_i(\mathbf{x}). \tag{4.58}$$

and the number h is invariant under any linear non-singular transformation. It is always possible, by means of an integral unimodular linear transformation, arrange that the linear forms of (4.58) depend only by the variables $x_1 ... x_h$. If, at the same time, we call

$$\begin{cases} y_1 = x_{h+1} \\ \vdots \\ y_s = x_n. \end{cases}$$

where $s = n - h$, we have that the polynomial ϕ takes the form $\phi = \phi(\mathbf{x}, \mathbf{y})$ with

$$\phi(\mathbf{x}, \mathbf{y}) = \widetilde{C}(x_1, \ldots, x_h) + \sum_{1 \le i \le s} y_i \widetilde{Q_i}(x_1, \ldots, x_h) + \sum_{\substack{1 \le j \le s \\ 1 \le k \le s}} y_j y_k \widetilde{L}_{jk}(x_1, \ldots, x_h) \tag{4.59}$$

where

- $\widetilde{C} \in \mathbb{Z}[x_1 ... x_h]$ is a cubic polynomial.
- $\widetilde{Q}_i \in \mathbb{Z}[x_1 ... x_h]$ are quadratic polynomials.
- $\widetilde{L}_{jk} \in \mathbb{Z}[x_1 ... x_h]$ are linear polynomials.

Note 4.5. *Here some of the polynomials* $\widetilde{C}$, $\widetilde{Q}_i$, $\widetilde{L}_{j,k}$ *may vanish identically or have a degree less than their* apparent degree[4]*, but, since we are interested in a non degenerate cubic polynomial* ϕ *with* $n > h$*, not all the polynomials* $\widetilde{Q}_i$, $\widetilde{L}_{j,k}$ $(1 \leq i, j, k \leq s)$ *will vanish identically in our case.*

In order to prove the second Theorem of Pleasants we will show that the variables $x_1 ... x_h$ can be given integer values in such a way that the remaining quadratic or linear polynomial in the variables $y_1 ... y_s$ represent infinitely many primes.

Lemma 4.18. *Let* $\phi = \phi(\mathbf{x}, \mathbf{y})$ *like in* (4.59) *and let* μ *the product of its coefficients.* ***If*** ϕ *satisfies the conditions of Theorem 4.2* ***then*** *there exist*

- $\mathbf{X} = (X_1 \dots X_h) \in \mathbb{Z}^h$.
- $\mathbf{Y} = (Y_1 \dots Y_s) \in \mathbb{Z}^s$.

such that for every $\mathbf{x} \in \mathbb{Z}^h$ *satisfying*

$$\mathbf{x} \equiv \mathbf{X} \pmod{6\mu}. \tag{4.60}$$

it is

1. $(H(\mathbf{x}), 6\mu) = 1$.
2. $\phi(\mathbf{x}, \mathbf{Y}) \not\equiv 0 \pmod 2$.

where

$$H(\mathbf{x}) = \left(\widetilde{C}(\mathbf{x}), \widetilde{Q}_1(\mathbf{x}) \dots, \widetilde{Q}_s(\mathbf{x}), \widetilde{L}_{11}(\mathbf{x}), \widetilde{L}_{12}(\mathbf{x}) \dots \widetilde{L}_{ss}(\mathbf{x})\right) \in \mathbb{Z}.$$

Proof. Among the hypotheses of Theorem 4.2 we have that for every integer $m > 1$ there exists $\mathbf{x}(m) \in \mathbb{Z}^n$ such that

$$m \not| \phi(\mathbf{x}(m)).$$

Let $p_1 \dots p_k \in \mathbb{P}$ the prime factors of 6μ and let

$$\begin{cases} \mathbf{x}_1 = \mathbf{x}(p_1). \\ \vdots \\ \mathbf{x}_k = \mathbf{x}(p_k). \end{cases}$$

[4]The apparent degree of a polynomial is the degree which the polynomial should have. For instance if we talk about a polynomial of second degree in one variable, say ax^2+bx+c its apparent degree is 2 but if we choose $a = 0$ the degree is ≤ 1

such that

$$\begin{cases} p_1 \not| \phi(\mathbf{x}_1). \\ \vdots \\ p_k \not| \phi(\mathbf{x}_k). \end{cases}$$

and combining $\mathbf{x}_1 \dots \mathbf{x}_k$ in the same way as in the proof of Lemma 4.2 we obtain

$$(X_1 \dots X_h, Y_1, \dots, Y_s) = (\mathbf{X}, \mathbf{Y}) \in \mathbb{Z}^n.$$

such that

$$(\phi(\mathbf{X}, \mathbf{Y}), 6\mu) = 1.$$

The points $\mathbf{X}$ and $\mathbf{Y}$ have the properties required by the Lemma. □

Lemma 4.19. *Let $\phi = \phi(\mathbf{x}, \mathbf{y})$ like in (4.59) satisfying the conditions of Theorem 4.2.*

- *Let*

$$\begin{array}{l} U_i : \mathbb{R}^+ \to \mathbb{R}^+ \quad i = 1, ..., h \\ P \to U_i(P). \end{array}$$

  such that there exist $\alpha_i, \beta_i \in \mathbb{R}^+$ and l_i, m_i positive integers so that

$$\alpha_i P^{l_i} \leq U_i(P) \leq \beta_i P^{m_i} \quad i = 1, ..., h.$$

- *Let*

$$U(P) = \prod_{i=1}^{h} U_i(P).$$

- *Let*

$$\Omega = \left\{ \widetilde{Q}_1(\mathbf{x}) \dots, \widetilde{Q}_s(\mathbf{x}), \widetilde{L}_{11}(\mathbf{x}), \widetilde{L}_{12}(\mathbf{x}) \dots \widetilde{L}_{ss}(\mathbf{x}) \right\}.$$

- *Let $R(\mathbf{x}) \in \Omega$ a non- constant polynomial.*
- *Let μ as in Lemma 4.18.*
- *Let $\mathbf{X}, \mathbf{Y}$ as in Lemma 4.18.*

If

$$\Gamma(P) = \left\{ \mathbf{x} \in \mathbb{Z}^h : \left| \begin{array}{ll} (i) & |x_i| < U_i(P) \ \forall i = 1, ..., h \\ (ii) & \mathbf{x} \equiv \mathbf{X} \pmod{6\mu} \\ (iii) & R(\mathbf{x}) = mp \quad m | (6\mu)^3, \ p \in \mathbb{P} \end{array} \right. \right\}. \tag{4.61}$$

and

$$|\Gamma(P)| \gg \frac{U(P)}{\log P}.$$

then, *denoting with*

$$\Lambda(P) = \{\mathbf{x} \in \Gamma(P) : H(\mathbf{x}) = 1,\ \phi(\mathbf{x}, \mathbf{Y}) \not\equiv 0 \pmod 2\}.$$

we have

$$|\Lambda(P)| \gg \frac{U(P)}{\log P}.$$

being $H(\mathbf{x})$ *as in Lemma 4.18.*

Proof. If $\mathbf{x} \in \mathbb{Z}^h$ satisfies (ii) of (4.61) then, by Lemma 4.18 $(H(\mathbf{x}), 6\mu) = 1$. If in addition $\mathbf{x} \in \mathbb{Z}^h$ satisfies (iii) and $H(\mathbf{x}) \neq 1$ then $H(\mathbf{x}) = p$ because $H(\mathbf{x}) | mp$ and it is relative prime with 6μ. Hence

$$\begin{cases} p|\widetilde{C}(\mathbf{x}) \\ p|\widetilde{Q}_1(\mathbf{x}) \\ \vdots \\ p|\widetilde{Q}_s(\mathbf{x}) \\ p|\widetilde{L}_{11}(\mathbf{x}) \\ \vdots \\ p|\widetilde{L}_{ss}(\mathbf{x}). \end{cases}$$

and so

$$\begin{cases} R(\mathbf{x}) \,|\, (6\mu)^3 \widetilde{C}(\mathbf{x}) \\ R(\mathbf{x}) \,|\, (6\mu)^3 \widetilde{Q}_1(\mathbf{x}) \\ \vdots \\ R(\mathbf{x}) \,|\, (6\mu)^3 \widetilde{Q}_s(\mathbf{x}) \\ R(\mathbf{x}) \,|\, (6\mu)^3 \widetilde{L}_{11}(\mathbf{x}) \\ \vdots \\ R(\mathbf{x}) \,|\, (6\mu)^3 \widetilde{L}_{ss}(\mathbf{x}). \end{cases} \tag{4.62}$$

because $R(\mathbf{x}) = mp$. Since the polynomial ϕ is irreducible, the polynomials

$$\begin{cases} \widetilde{C}' = (6\mu)^3 \widetilde{C} \\ \widetilde{Q}_1' = (6\mu)^3 \widetilde{Q}_1 \\ \vdots \\ \widetilde{Q}_s' = (6\mu)^3 \widetilde{Q}_s \\ \widetilde{L}_{11}' = (6\mu)^3 \widetilde{L}_{11} \\ \vdots \\ \widetilde{L}_{ss}' = (6\mu)^3 \widetilde{L}_{ss}. \end{cases}$$

have no common factor and we can apply Lemma 4.15 with $\phi_1 = R$ and $n = h$. We deduce that if

$$\Psi(P) = \left\{ \mathbf{x} \in \mathbb{Z}^h : \left| \begin{array}{l} (4.61)\ (i)\ \textit{holds} \\ (4.62) \qquad " \end{array} \right. \right\}.$$

then

$$|\Psi\,(P)| \ll \max_{1 \le i \le h} \frac{U\,(P)}{U_i\,(P)} P^{\varepsilon}.$$

for any $\varepsilon > 0$. So, if

$$\Upsilon\,(P) = \left\{ \mathbf{x} \in \mathbb{Z}^h : \left| \begin{array}{l} (i)\ \textit{holds} \\ (ii)\ " \\ (iii)\ " \end{array} \right. , H\,(\mathbf{x}) > 1 \right\}.$$

we have

$$|\Upsilon\,(P)| \ll \max_{1 \le i \le h} \frac{U\,(P)}{U_i\,(P)} P^{\varepsilon} \ll \frac{U\,(P)}{\log P}.$$

for $\varepsilon > 0$ small enough. It follows that

$$|\mathrm{K}\,(P)| \gg \frac{U\,(P)}{\log P}.$$

where

$$\mathrm{K}\,(P) = \left\{ \mathbf{x} \in \mathbb{Z}^h : \left| \begin{array}{l} (i)\ \textit{holds} \\ (ii)\ " \\ (iii)\ " \end{array} \right. , H\,(\mathbf{x}) = 1 \right\}.$$

Finally we note that, by Lemma 4.18 it is

$$\phi\,(\mathbf{x}, \mathbf{Y}) \not\equiv 0 \pmod 2.$$

for any $\mathbf{x} \in \mathbb{Z}^h$ for which (4.61) (ii) holds. □

4.11 The proof of the second theorem of Pleasants

4.11.1 Introduction

In the proof of the Theorem 4.2 we need only consider cubic polynomials ϕ which are expressible in the form (4.59) and we shall suppose from now on that ϕ is of this form. We shall deal separately with the two principal cases:

Case A Not all the linear polynomials $\widetilde{L}_{jk}\,(x_1 \dots x_h) \quad (1 \le j, k \le s)$ are identically zero.

Case B The linear polynomials $\widetilde{L}_{jk}\,(x_1 \dots x_h) \quad (1 \le j, k \le s)$ are all identically zero.

4.11.2 The proof in Case A

Proof. By rearranging the terms of (4.59) we can write

$$\phi(\mathbf{x},\mathbf{y}) = \widetilde{C}(\mathbf{x}) + \sum_{1\le i\le s} y_i \widetilde{Q}_i(\mathbf{x}) + Q_0^*(\mathbf{y}) + \sum_{1\le i\le h} x_i Q_i^*(\mathbf{y}). \tag{4.63}$$

where

- $\mathbf{x} \in \mathbb{R}^h$.
- $\mathbf{y} \in \mathbb{R}^s$.
- $Q_0^*...Q_h^*$ are quadratic forms in $\mathbb{Z}[\mathbf{y}]$ not all identically zero. We shall denote their set as $.\mathbf{Q} = \{Q_0^*, \ldots, Q_h^*\}$.

In proving Theorem 4.2 **Case A** we shall consider separately the three cases that arise according as the quadratic forms $Q_0^*...Q_h^*$ satisfy alternatives (I) (II) (III) of Lemma 4.17. In this application we will have $r = h$ and $n = s$ being r, n the parameters employed in that Lemma.

Case I In this case the proof of Theorem 4.2 falls into three further cases depending on which of the following statements applies to ϕ.

(i) Not all the linear polynomial $\widetilde{L}_{jk}$ $(1 \le j,k \le s)$ occurring in (4.59) are constant.

(ii) The linear polynomial $\widetilde{L}_{jk}$ $(1 \le j,k \le s)$ are all constant but at least one of the quadratic polynomials $\widetilde{Q}_i$ $(1 \le i \le s)$ in (4.59) ha non vanishing quadratic part.

(iii) The linear parts of the polynomials $\widetilde{L}_{jk}$ $(1 \le j,k \le s)$ and the quadratic parts of the polynomials $\widetilde{Q}_i$ $(1 \le i \le s)$ are all identically zero but the cubic polynomial $\widetilde{C}$ has non-vanishing cubic part.

No other cases are possible since, otherwise, the cubic part of ϕ would vanishing identically.

Case I (i) We suppose that there exist j_0 and k_0 so that $\widetilde{L}_{j_0k_0}$ is not constant. It follows that not all of the quadratic forms $Q_1^*...Q_h^*$ of (4.63) vanish identically. Hence we can choose $\eta = (\eta_1 \ldots \eta_s) \in \mathbb{R}^s$ such that $Q_1^*(\eta) \ldots Q_s^*(\eta)$ are not all zero. Then we can find a point $\mathbf{a} = (a_1 \ldots a_h) \in \mathbb{R}^h$ such that

$$\sum_{i=1}^{h} a_i Q_i^*(\eta) > 0.$$

and a box $\mathcal{A} \subset \mathbb{R}^h$ such that $\mathbf{a} \in \mathcal{A}$ and a $\delta > 0$ such that

$$\sum_{i=1}^{h} \xi_i Q_i^* (\eta) > \delta > 0. \tag{4.64}$$

for every $\xi \in \mathcal{A}$. Let μ denotes, as usual, the product of the coefficients of ϕ and let $\mathbf{X} \in \mathbb{Z}^h$ the point given by Lemma 4.18. We make the transformation

$$\mathbf{x} = \mathbf{X} + 6\mu\mathbf{z}. \tag{4.65}$$

where

- $\mathbf{z} \in \mathcal{A}'(P) \cap \mathbb{Z}^h$.
- $\mathcal{A}'(P) = (6\mu)^{-1} P\mathcal{A}$.

Under this transformation the polynomial $\widetilde{L}_{j_0k_0}(\mathbf{x})$ becomes $L'_{j_0k_0}(\mathbf{z})$ where the coefficients of of the linear part of $L'_{j_0k_0}$ are just 6μ times the corresponding coefficients of $\widetilde{L}_{j_0k_0}$. It follows that if $\lambda_{j_0k_0}$ stands for the greatest common divisor of the coefficients of $L'_{j_0k_0}$, it is

$$\lambda_{j_0k_0} | 6\mu^2.$$

Now at least one of the polynomials

$$\begin{cases} M_{j_0k_0}(\mathbf{z}) = \quad (\lambda_{j_0k_0})^{-1} L'_{j_0k_0}(\mathbf{z}) \\ N_{j_0k_0}(\mathbf{z}) = -(\lambda_{j_0k_0})^{-1} L'_{j_0k_0}(\mathbf{z}). \end{cases}$$

satisfies the condition of Lemma 4.14 with respect to the box $\mathcal{A}'(P)$ defined before. From that Lemma we have that if

$$\mathcal{G}(P) = \left\{ \mathbf{z} \in \mathcal{A}'(P) \cap \mathbb{Z}^n, L'_{j_0k_0}(\mathbf{z}) = mp,\ m = \pm\lambda_{j_0k_0}, p \in \mathbb{P} \right\}.$$

then

$$|\mathcal{G}(P)| \gg \frac{P^h}{\log P}.$$

For every $\mathbf{z} \in \mathcal{G}(P)$ the corresponding $\mathbf{x}$ given by (4.65) is such that

- $\mathbf{x} \in P\mathcal{A} - \mathbf{X} = \mathcal{A}''(P)$.
- $\widetilde{L}_{j_0k_0}(\mathbf{x}) = mp$.

We now apply Lemma 4.19 to the polynomial ϕ with

- $R(\mathbf{x}) = \widetilde{L}_{j_0k_0}(\mathbf{x})$.
- $U_i(P) = cP \quad i = 1, ..., h$.
- c a suitable constant.

We observe that for every $\mathbf{x} \in \mathbb{Z}^h$

$$\psi\{\mathbf{y}\} = \phi(\mathbf{x}, \mathbf{y}).$$

is a **quadratic polynomial** and from Lemma 4.19 we deduce that if

$$\Lambda(P) = \{\mathbf{x} \in \mathcal{A}''(P) \cap \mathbb{Z}^n : H(\mathbf{x}) = 1, \exists \overline{\mathbf{y}} \in \mathbb{Z}^s : \psi\{\overline{\mathbf{y}}\} \not\equiv 0 \pmod 2\}.$$

then

$$|\Lambda(P)| \gg \frac{P^h}{\log P}.$$

Furthermore the quadratic part of $\psi(\mathbf{y})$ is

$$Q^*_{\mathbf{x}}(\mathbf{y}) = Q^*_0(\mathbf{y}) + \sum_{i=1}^{h} x_i Q^*_i(\mathbf{y}).$$

If $\mathbf{x} \in \mathcal{A}''(P)$ we can write $\mathbf{x} = P\xi - \mathbf{X}$ where $\xi \in \mathcal{A}$ and then we have

$$Q^*_{\mathbf{x}}(\mathbf{y}) = Q^*_0(\eta) + \sum_{i=1}^{h} (P\xi_i - X_i) Q^*_i(\mathbf{y}) > P\delta + O(1).$$

by (4.64). Thus $Q^*_{\mathbf{x}}(\mathbf{y}) > 0$ if P is large enough. Hence for $\mathbf{x} \in \mathcal{A}''(P)$ the quadratic form $T(\mathbf{y}) = Q^*_{\mathbf{x}}(\mathbf{y})$ is neither negative definite nor negative semi-definite. Finally, since $Q^*_0 ... Q^*_h$ satisfy (I) of Lemma 4.17 we have that if

$$\Theta(P) = \{\mathbf{x} \in \mathcal{A}''(P) \cap \mathbb{Z}^s : r(Q^*_{\mathbf{x}}(\mathbf{y})) \leq 2\}.$$

then

$$|\Theta(P)| \ll P^{h-1}.$$

Hence for large enough P there is some $\overline{\mathbf{x}} \in \mathcal{A}''(P)$ for which $\phi(\bar{\mathbf{x}}, \mathbf{y})$ as a quadratic polynomial in $\mathbf{y}$ satisfies all the conditions of Corollary 4.1 and hence it **represents infinitely many primes**.

Case I (ii) Since in this case the linear polynomials $\widetilde{L}_{jk}$ are all constant, we have Q_i^* must be identically zero for $1 \leq i \leq h$. On the other hand, since we are supposing that $\widetilde{L}_{jk}$ are not identically zero, it follows that Q_0^* is not identically zero. Thus in this case $\mathbf{Q}$ contains only one non-vanishing form, namely Q_0^*, and since we are supposing that this set satisfies (I) of Lemma 4.17, we have $r(Q_0^*) \geq 3$. Suppose that the linear polynomial $\widetilde{L}_{j_0k_0}$ does not vanish identically so that

$$\widetilde{L}_{j_0k_0}(\mathbf{x}) = l_{j_0k_0} \ \ \forall \mathbf{x} \in \mathbb{R}^h.$$

with $l_{j_0k_0} \in \mathbb{Z} - \{0\}$ and denote by $\mathbf{Q}' = \{Q_1', \ldots, Q_s'\}$ the set of the quadratic parts of the polynomials $\widetilde{Q}_1(\mathbf{x}) ... \widetilde{Q}_s(\mathbf{x})$ of (4.59). By (ii) it follows that $\widetilde{Q}_1(\mathbf{x}) ... \widetilde{Q}_s(\mathbf{x})$ are not identically zero. We fix a point $\mathbf{a} = (a_1 \ldots a_h) \in \mathbb{R}^h$ such that $Q_1'(\mathbf{a}), \ldots, Q_s'(\mathbf{a})$ are not all zero and then a point $\mathbf{b} = (b_1 \ldots b_s) \in \mathbb{R}^s$ such that

$$Q_0^*(\mathbf{b}) + \sum_{i=1}^{s} b_i Q_i'(\mathbf{a}) > 0.$$

Now we can choose a box $\mathcal{B} \subset \mathbb{R}^s$ such that $\mathbf{b} \in \mathcal{B}$ and

$$e_1 < Q_0^*(\eta) + \sum_{i=1}^{s} \eta_i Q_i'(\mathbf{a}) < e_2 \qquad \forall \eta \in \mathcal{B}. \tag{4.66}$$

where e_1 and e_2 are suitable positive real numbers. We also choose f_1 and f_2 so that

$$0 < f_1 < e_1 < e_2 < f_2. \tag{4.67}$$

If $\mathbf{X}$, $\mathbf{Y}$ are the integer points given by Lemma 4.18 then for any $\mathbf{x} \in \mathbb{Z}^n$ satisfying (4.60) we have that, if $H(\mathbf{x})$ has the same meaning as in Lemma 4.18 then

- $(H(\mathbf{x}), 6\mu) = 1$.
- $\phi(\mathbf{x}, \mathbf{Y}) \not\equiv 0 \pmod 2$.

But $H(\mathbf{x}) | l_{j_0k_0}$ and $l_{j_0k_0} | \mu$ and so $H(\mathbf{x}) = 1$ for every such a $\mathbf{x}$. Now for any P large enough we consider the point $\mathbf{a}' = P^{1/2}\mathbf{a} \in \mathbb{R}^h$ and the set

$$N(\mathbf{a}') = \left\{ \mathbf{x} \in \mathbb{Z}^h : |\mathbf{x} - \mathbf{a}'| \leq \frac{1}{2} \right\}.$$

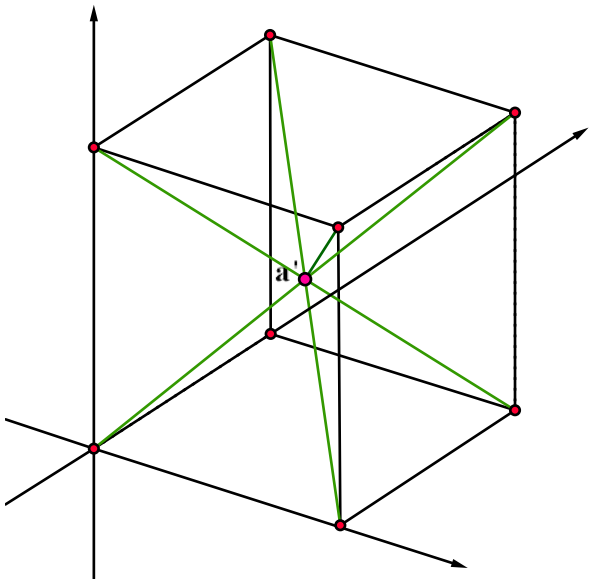

Figure 4.3: The set $N(\mathbf{a}')$ can contains more than one point but all of them have the same distance from $\mathbf{a}'$

Either $N(\mathbf{a}')$ contains a single point or each of its point has the same distance from $\mathbf{a}'$ Let $\mathbf{x}(P)$ any point of $N(\mathbf{a}')$. If $\mathbf{y} \in P\mathcal{B}$ we have $\mathbf{y} = P\eta$ and substituting $\mathbf{x}(P)$ and $\mathbf{y}$ in (4.63) and remembering that the quadratic forms Q_i^* for $i = 1, ..., h$ are identically zero we obtain

$$\phi(\mathbf{x}(P), \mathbf{y}) = \widetilde{C}(\mathbf{x}(P)) + \sum_{1 \le i \le s} y_i \widetilde{Q}_i(\mathbf{x}(P)) + Q_0^*(\mathbf{y}).$$

and hence

$$\phi(\mathbf{x}(P), \mathbf{y}) = P^2 \left(Q_0^*(\eta) + \sum_{i=1}^{s} Q_i'(\mathbf{a}) \right) + O\left(P^{3/2}\right).$$

From (4.66) and (4.67) it follows that

$$f_1 P^2 < \phi(\mathbf{x}(P), \mathbf{y}) < f_2 P^2.$$

for every P large enough and for every $\mathbf{y} \in P\mathcal{B}$. Now, the polynomial

$$\phi_P(\mathbf{y}) = \phi(\mathbf{x}(P), \mathbf{y}).$$

considered as polynomial in $\mathbf{y}$, has quadratic part $Q_0^*(\mathbf{y})$ with constant coefficients and such that $r(Q_0^*) \ge 3$. The coefficients

of the other terms of $\phi_P(\mathbf{y})$ depend on P and so ϕ_P is **weakly dependent** on P and we have shown that together with the box $\mathcal{B}$ it satisfies all the conditions of the Theorem 4.1. We deduce that ϕ **represent infinitely many primes**.

Case I (iii) In this case, as in Case I (ii), we have Q_i^* identically zero for $i = 1...n$ and $r\left(Q_0^*\right) \geq 3$. Also, as in Case I (ii), if $\mathbf{X}$, $\mathbf{Y}$ have the same meaning as in Lemma 4.18, then for any $\mathbf{x} \in Z^n$ such that (4.60) holds it is

- $H\left(\mathbf{x}\right) = 1$.
- $\phi\left(\mathbf{x}, \mathbf{Y}\right) \not\equiv 0 \pmod 2$.

We denote by $C'\left(\mathbf{x}\right)$ the cubic part of $\widetilde{C}\left(\mathbf{x}\right)$. Since by (iii) C' is not identically zero, we can find a point $\mathbf{a} \in R^h$ such that $C'\left(\mathbf{a}\right) > 0$. The we can choose a box $\mathcal{B} \subset R^s$ such that $\mathbf{0} \in \mathcal{B}$ and

$$e_1 < C'\left(\mathbf{a}\right) + Q_0^*\left(\eta\right) < e_2 \quad \forall \eta \in \mathcal{B}. \tag{4.68}$$

where e_1 and e_2 are suitable positive real numbers. We choose also f_1 and f_2 such that

$$0 < f_1 < e_1 < e_2 < f_2. \tag{4.69}$$

Now for any P large enough we consider the point $\mathbf{a}'' = P^{2/3}\mathbf{a} \in \mathbb{R}^h$ and the set

$$N\left(\mathbf{a}''\right) = \left\{\mathbf{x} \in \mathbb{Z}^h : |\mathbf{x} - \mathbf{a}''| \leq \frac{1}{2}\right\}.$$

As before, either $N\left(\mathbf{a}''\right)$ contains a single point or each of its point has the same distance from $\mathbf{a}''$. If $\mathbf{y} \in P\mathcal{B}$ we have $\mathbf{y} = P\eta$ and substituting $\mathbf{x}\left(P\right)$ and $\mathbf{y}$ in (4.63) and remembering that the quadratic forms Q_i^* for $i = 1, ..., h$ are identically zero we obtain

$$\phi\left(\mathbf{x}\left(P\right), \mathbf{y}\right) = \widetilde{C}\left(\mathbf{x}\left(P\right)\right) + \sum_{1 \leq i \leq s} y_i \widetilde{Q}_i\left(\mathbf{x}\left(P\right)\right) + Q_0^*\left(\mathbf{y}\right).$$

and

$$\phi\left(\mathbf{x}\left(P\right), \mathbf{y}\right) = P^2\left(C'\left(\mathbf{a}\right) + Q_0^*\left(\eta\right)\right) + O\left(P^{5/3}\right) + O\left(P^{4/3}\right). \tag{4.70}$$

The term $O\left(P^{5/3}\right)$ arises from the fact that, by (iii), the polynomials $\widetilde{Q}_i$ $i = 1...s$ have degree at most one. If now proceeding as in Case I (ii) we obtain as well that ϕ **represent infinitely many primes**.

Case II Since in this case there exists an integral unimodular transformation taking the quadratic forms $Q_0^*, ..., Q_s^*$ of the variables $y_1, ..., y_s$ simultaneously into quadratic forms involving only y_1, y_2 the polynomial ϕ takes the form

$$\phi(\mathbf{x}, \mathbf{y}) = \widetilde{C}(\mathbf{x}) + \sum_{1 \le i \le s} y_i \widetilde{Q}_i(\mathbf{x}) + y_1^2 \widetilde{L}_{11}(\mathbf{x}) + y_1 y_2 \widetilde{L}_{12}(\mathbf{x}) + y_2^2 \widetilde{L}_{22}(\mathbf{x}).$$

where $\mathbf{x} \in \mathbb{R}^h$. Since we are dealing with **Case A**, at least one of the linear polynomials $\widetilde{L}_{11}$,$\widetilde{L}_{12}$,$\widetilde{L}_{22}$ is not identically zero. We shall denote it as $\widehat{L}$. Also the quadratic polynomials $\widetilde{Q}_3, ...\widetilde{Q}_s$ are not identically zero as in that case ϕ would not involve the variables $y_3, ..., y_s$, whereas the hypotheses of Theorem 4.2 state that ϕ is non-degenerate and $n \ge h+3$. By permuting the variables $y_3, ..., y_s$, if necessary, we can suppose that $\widetilde{Q}_3$ is not identically zero. Now let $\mathbf{X}$, $\mathbf{Y}$ as in Lemma 4.18. We have two further cases

(i) $\widehat{L}$ is **constant**.

(ii) $\widehat{L}$ is **not constant**.

Case II (i) We proceeding as in Case I (ii) so for any $\mathbf{x} \in \mathbb{Z}^n$ satisfying (4.60) we have that

- $H(\mathbf{x}) = 1$.
- $\phi(\mathbf{x}, \mathbf{Y}) \not\equiv 0 \pmod 2$.

Case II (ii) As in Case I (i), if

$$\widetilde{\Lambda}(P) = \left\{\mathbf{x} \in \mathbb{Z}^h : |\mathbf{x}| < P, H(\mathbf{x}) = 1, \phi(\mathbf{x}, \mathbf{Y}) \not\equiv 0 \pmod 2\right\}.$$

then

$$\left|\widetilde{\Lambda}(P)\right| \gg \frac{P^{h-1}}{\log P}.$$

In **either Cases**, since $\widetilde{Q}_3$ is not identically zero, if

$$\Omega(P) = \left\{\mathbf{x} \in \mathbb{Z}^h : |\mathbf{x}| < P, \widetilde{Q}_3(\mathbf{x}) = 0\right\}.$$

then

$$|\Omega(P)| \ll \frac{P^{h-1}}{\log P}.$$

and so there exists $\overline{\mathbf{x}}$ such that

- $H(\overline{\mathbf{x}}) = 1$.

- $\phi(\overline{\mathbf{x}}, \mathbf{Y}) \not\equiv 0$.
- $Q_3(\overline{\mathbf{x}}) \neq 0$.

It follows that the quadratic polynomial

$$T(\mathbf{y}) = T(y_1, \ldots y_s) = \phi(\overline{\mathbf{x}}, \mathbf{y}).$$

contains the variable y_3 in the **linear part** but not in its **quadratic part** and satisfies all the other conditions of Lemma 4.13 Hence ϕ **represents infinitely many primes**.

Case III In this case, after an integral unimodular transformation of the variables $y_1, ...y_s$ if necessary, we can suppose that y_1 is a common factor of $Q_1^*, ..., Q_h^*$ and the ϕ has the shape

$$\phi(\mathbf{x}, \mathbf{y}) = \widetilde{C}(\mathbf{x}) + \sum_{1 \leq i \leq s} y_i \widetilde{Q}_i(\mathbf{x}) + \sum_{1 \leq j \leq s} y_1 y_j \widetilde{L}_{1j}(\mathbf{x}). \tag{4.71}$$

Since we are dealing with Case A, not all the linear polynomials $\widetilde{L}_{11}, ...\widetilde{L}_{1s}$ are identically zero. Moreover, we can suppose that $\widetilde{L}_{12}, ...\widetilde{L}_{1s}$ are not all identically zero since otherwise $\phi(\mathbf{x}, \mathbf{y})$ would be of the form considered in Case II. Thus there is at least one among such polynomials which is not identically zero and we shall denote it as $\widehat{L}$. Now, just as in the cases we have already considered, if

$$\widehat{\Lambda}(P) = \left\{ \mathbf{x} \in \mathbb{Z}^h : |\mathbf{x}| < P, \left| \begin{array}{l} \widehat{H}(\mathbf{x}) = 1 \\ \exists \mathbf{Y} \in \mathbb{Z}^s, \phi(\mathbf{x}, \mathbf{Y}) \not\equiv 0 \pmod 2 \\ \widehat{L}(\mathbf{x}) \neq 0 \end{array} \right. \right\}.$$

then

$$\left| \widehat{\Lambda}(P) \right| \gg \frac{P^h}{\log P}.$$

where, in this case, $\widehat{H}(\mathbf{x}) = \left(\widetilde{C}(\mathbf{x}), \widetilde{Q}_1(\mathbf{x}) \ldots \widetilde{Q}_s(\mathbf{x}), \ldots \widetilde{L}_{1s}(\mathbf{x}) \right)$.
A priori, we have two further cases

(i) There is $\overline{\mathbf{x}} \in \widehat{\Lambda}(P)$ such that the polynomial $T(\mathbf{y}) = \phi(\overline{\mathbf{x}}, \mathbf{y})$ is irreducible over $\mathbb{Q}$.

(ii) For every $\mathbf{x} \in \widehat{\Lambda}(P)$ the polynomial $T(\mathbf{y}) = \phi(\mathbf{x}, \mathbf{y})$ factorizes.

We shall show now that while Case III (i) leads to the conclusion that ϕ represent infinitely many primes, Case III (ii) is impossible.

Case III (i) In this case the quadratic polynomial $T(\mathbf{y})$ satisfies all the condition of Lemma 4.16 since the quadratic part of $\phi(\overline{\mathbf{x}}, \mathbf{y})$ has y_1 as a factor but is not of the form ay_1^2. Hence ϕ represent **infinitely many primes**.

Case III (ii) We shall show that this Case is impossible because it leads to a contradiction. We consider the projective space

$$\mathbb{R}\mathbb{P}^s = \left(\mathbb{R}^{s+1} - \{\mathbf{0}\}\right) / \sim.$$

and the homogeneous coordinates $\widehat{\mathbf{y}} = \left(y_1' \dots y_{s+1}'\right)$. We have

$$\phi(\mathbf{x}, \mathbf{y}) = \widetilde{C}(\mathbf{x}) + \left\{ \sum_{1 \leqslant i \leqslant s} y_{s+1} y_i' \frac{\widetilde{Q}_i(\mathbf{x})}{(y_{s+1})^2} + \sum_{1 \leqslant j \leqslant s} y_1' y_j' \frac{\widetilde{L}_{1j}(\mathbf{x})}{(y_{s+1})^2} \right\}.$$

We indicate by

$$\phi_1(y_1', ..., y_s', y_{s+1}) = \sum_{1 \leqslant i \leqslant s} y_{s+1} y_i' \frac{\widetilde{Q}_i(\mathbf{x})}{(y_{s+1})^2} + \sum_{1 \leqslant j \leqslant s} y_1' y_j' \frac{\widetilde{L}_{1j}(\mathbf{x})}{(y_{s+1})^2}.$$

We can think to ϕ_1 as a quadratic forms in the variables $y_1', ..., y_s', y_{s+1}$ and coefficients in the field of rational functions $\mathbb{Q}(\mathbf{x})$ so that we can write $\phi_1(\widehat{\mathbf{y}}) = \phi_1(y_1' \dots y_s', y_{s+1})$ If

$$\mathcal{M}_{s+1} = \{\mathbf{M} = (a_{i,j}),\ a_{i,j} \in \mathbb{Q}(\mathbf{x}) \quad i, j = 1, ..., s+1\}.$$

denotes the set of matrices of order $s+1$ with element in the field $\mathbb{Q}(\mathbf{x})$ we indicate by $\mathbf{A} = \mathbf{A}(\mathbf{x}) \in \mathcal{M}_{s+1}$ the symmetric matrix associated with ϕ_1. Now if

$$\overline{\overline{\Lambda}}(P) = \left\{\mathbf{x} \in \mathbb{Z}^h : |\mathbf{x}| < P, \phi_1(\widehat{\mathbf{y}}) = \overline{L_1}(\widehat{\mathbf{y}})\, \overline{L_2}(\widehat{\mathbf{y}})\right\}.$$

where $\overline{L_1}(\widehat{\mathbf{y}}), \overline{L_2}(\widehat{\mathbf{y}})$ are linear forms with coefficients in $\mathbb{Q}(\mathbf{x})$ we have

$$\left|\overline{\overline{\Lambda}}(P)\right| \gg \frac{P^h}{\cdot} \log P$$

and for every $\mathbf{x} \in \overline{\overline{\Lambda}}(P)$ $r(\mathbf{A}) \leqslant 2$ being r the rank of $\mathbf{A}$. We deduce that the minors 3×3 of $\mathbf{A}$ all vanish identically,is these minors are polynomials in the variables $x_1, ..., x_h$ and if one of them did not vanish identically it would vanish over a set of integer points $\mathbf{x}$,with $|\mathbf{x}| < P$, of cardinality $\ll P^{h-1}$. Hence, identically,

$r(\mathbf{A}) \leqslant 2$ and so ϕ_1 factorizes over $\mathbb{K} = \mathbb{K}(\mathbf{x})$, the algebraic closure of $\mathbb{Q}(\mathbf{x})$. Thus

$$\phi_1(\widehat{\mathbf{y}}) = (a_1 y_1' + \ldots + a_{s+1} y_{s+1})(b_1 y_1' + \ldots + b_{s+1} y_{s+1}). \quad (4.72)$$

where $a_l, b_l \in \mathbb{K}$, $l = 1, ..., s+1$. But $\mathbb{K}[\mathbf{y}']$, the ring of polynomials in the variables $\mathbf{y}' = (y_1', ..., y_s')$ over $\mathbb{K}$, is a unique factorization domain, and it follows from (4.71) that the part of ϕ_1 not involving y_{s+1} factorizes into

$$y_1' \left(\widetilde{L_{11}} y_1' + \cdots \widetilde{L_{1s}} y_s' \right).$$

Hence, after exchanging an element oh $\mathbb{K}$ between the factors of ϕ_1 in (4.72) if necessary, we have

- $a_1 = 0$.
- $a_l = 0$ $2 \leq l \leq s$.
- $b_l = \widetilde{L}_{1l}(x_1, ..., x_h)$ $1 \leq l \leq s$.

We are supposing that there is at least one of $\widetilde{L}_{1j}$ $2 \leq j \leq s$ and we have already indicated it by $\widehat{L}$. If $2 \leq j_0 \leq s$ is such that $\widehat{L} = \widetilde{L}_{1j_0}$ we have that the coefficient of the term $y_{j_0}' y_{s+1}$ in ϕ_1, which belongs to $\mathbb{Q}(\mathbf{x})$, is $a_{s+1} b_{j_0} = a_{s+1} \widehat{L}$. Hence, since $\widehat{L}$ is not identically zero, $a_{s+1} \in Q(\mathbf{x})$. Also the coefficient of the term $y_1' y_{s+1}$ in ϕ_1 belongs to $\mathbb{Q}(\mathbf{x})$ and is equal to $b_{s+1} + a_{s+1} b_1$, and hence $b_{s+1} \in \mathbb{Q}(\mathbf{x})$, since

- $a_{s+1} \in \mathbb{Q}(\mathbf{x})$.
- $b_1 = \widetilde{L_{11}} \in \mathbb{Q}(\mathbf{x})$.

Thus ϕ_1 factorizes over $\mathbb{Q}(\mathbf{x})$ and hence, since the coefficients of ϕ_1 are all polynomials of $\mathbb{Q}[\mathbf{x}]$ it follows that ϕ_1 factorizes in $\mathbb{Q}[\mathbf{x}]$. On settings $y_{s+1} = 1$ this gives a factorization of $\phi(\mathbf{x}, \mathbf{y})$ in which both factors are linear in $y_1 ... y_s$. Since we are dealing with **Case A** in which ϕ has non-vanishing terms which are quadratic in $y_1 ... y_s$, neither of this factors can be constant and this contradicts the irreducibility of ϕ.

□

4.11.3 The proof in Case B

In this Case all the polynomials $\widetilde{L}_{jk}$ of (4.59) are identically zero, and so ϕ is of the form

$$\phi = \phi(\mathbf{x}, \mathbf{y}) = \widetilde{C}(x_1, \ldots, x_h) + \sum_{1 \leqslant i \leqslant s} y_i \widetilde{Q_i}(x_1, \ldots, x_h). \quad (4.73)$$

Thus ϕ is linear respect to the variables $y_1, ...y_s$. Since ϕ is non-degenerate with $n > h$ not all the quadratic polynomials $\widetilde{Q}_1, ..., \widetilde{Q}_s$ vanish identically and so, by permuting the variables $y_1, ...y_s$ if necessary, we can suppose that $\widetilde{Q}_1$ is not identically zero. We have to consider further cases. ***A priori*** we have

Case B1 In this Case we have either $h = 1$ or $h = 2$.

(i) $h = 1$. By rearranging the terms of (4.73) we can express ϕ in the form

$$\phi(\mathbf{x}, \mathbf{y}) = x_1^2 L_1^*(\widehat{\mathbf{x}}) + x_1 L_2^*(\widehat{\mathbf{x}}) + L_3^*(\widehat{\mathbf{x}}).$$

where

- $\widehat{\mathbf{x}} = (x_1, y_1, \dots y_{n-1})$.
- L_1^*, L_2^*, L_3^* are linear polynomials in $x_1, y_1, ..., y_{n-1}$.

Hence we can perform a unimodular transformation involving x_1, L_1^*, L_2^*, L_3^* as variables and we would have that ϕ is unimodularly equivalent to a polynomial in four variables. This is incompatible with condition (i) of 4.2. This means that **Case B1 (i)** can not occur.

(ii) $h = 2$. In this Case we have $s = n - 2$ and we can rearrange the terms of (4.73) to express ϕ in the form

$$\phi(\mathbf{x}, \mathbf{y}) = x_1^2 L_1^*(\widehat{\mathbf{x}}) + x_1 x_2 L_2^*(\widehat{\mathbf{x}}) + x_2^2 L_3^*(\widehat{\mathbf{x}}) + x_1 L_4^*(\widehat{\mathbf{x}}) + x_2 L_5^*(\widehat{\mathbf{x}}) + L_6^*(\widehat{\mathbf{x}}).$$

where

- $\widehat{\mathbf{x}} = (x_1, x_2, y_1, \dots y_{n-2})$.
- $L_1^*, L_2^*, L_3^*, L_4^*, L_5^*, L_6^*$ are linear polynomials in $x_1, x_2, y_1, ..., y_{n-2}$.

Hence we can perform a unimodular transformation involving $x_1, x_2, L_1^*, L_2^*, L_3^*, L_4^*, L_5^*, L_6^*$ as variables and we would have that ϕ is unimodularly equivalent to a polynomial in eight variables. This is incompatible with condition (i) of 4.2.

Case B2 $h \geq 3$.

(i) Suppose that $r(\overline{\overline{Q}}_1(\mathbf{x})) \geq 3$ where $\overline{\overline{Q}}_1(\mathbf{x})$ is the quadratic part of $\widetilde{Q}_1(\mathbf{x})$. Let $\mathbf{X}$ the integer point of Lemma 4.18. We make the substitution (4.65) and we consider the set

$$\Delta(P) = \left\{ \mathbf{z} \in \mathbb{Z}^h : |\mathbf{z}| < cP \right\}. \tag{4.74}$$

where c is a constant satisfying $0 < c < |6\mu|^{-1}$ being, as before, μ the product of the coefficients of ϕ. For a given $\mathbf{z} \in \Delta(P)$ let $\mathbf{x} = \mathbf{x}(P)$ so that (4.65) holds. If P is large enough it is $|\mathbf{x}| < P$. With this substitution from the polynomial $\widetilde{Q}_1(\mathbf{x})$ we obtain a polynomial $\widetilde{Q}_1'(\mathbf{z})$. Let $\overline{\overline{Q}}_1{}'(\mathbf{z})$ the quadratic part of $\widetilde{Q}_1'(\mathbf{z})$. We have that

$$\overline{\overline{Q}}_1{}'(\mathbf{z}) = (6\mu)^2 \overline{\overline{Q}}_1(\mathbf{x}).$$

Thus it is $r\left(\overline{\overline{Q}}_1{}'\right) \geqslant 3$. If λ_1 denotes the greatest common factor of the coefficients of $\widetilde{Q}_1'$ we have that $\lambda_1 | 36\mu^3$. The polynomial $F(\mathbf{z}) = \lambda_1^{-1}\widetilde{Q}_1'(\mathbf{z})$ has the following properties:

- The coefficients of $F(\mathbf{z})$ are co-primes.
- If $\exists \mathbf{z}_0 \in \mathbb{Z}^h$ such that.

$$2 \not| F(\mathbf{z}_0) .$$

then at least one of the quadratic polynomials

$$F_{\pm}(\mathbf{z}) = \pm F(\mathbf{z}).$$

satisfies the conditions of 4.1. We deduce that if

$$\mathcal{G}(P) = \left\{ \mathbf{z} \in \mathbb{Z}^h : |\mathbf{z}| < cP, \ \ \widetilde{Q}_1'(\mathbf{z}) = \pm\lambda_1 p, \ \ p \in \mathbb{P} \right\}.$$

then

$$|\mathcal{G}(P)| \gg \frac{P^h}{\log P}.$$

On the other hand, if $2|F(\mathbf{z}) \ \ \forall \mathbf{z} \in \mathbb{Z}^h$. we consider the polynomial

$$E(\mathbf{z}) = (2\lambda_1)^{-1} \widetilde{Q}_1'(\mathbf{z}).$$

This polynomial is integer valued for every $\mathbf{z} \in \mathbb{Z}^h$ and cannot be even at every of such a points. For if, the polynomial

$$D(\mathbf{z}) = (4\lambda_1)^{-1} \widetilde{Q}_1'(\mathbf{z}).$$

would be an integer valued quadratic polynomial having some coefficient with denominator 4 which is contrary to the conclusion of Lemma 4.1. Hence at least one of the polynomials

$$E_{\pm}(\mathbf{z}) = \pm E(\mathbf{z}).$$

satisfies the conditions of 4.1. We deduce that if

$$\mathcal{F}(P)=\left\{\mathbf{z}\in\mathbb{Z}^h:|\mathbf{z}|<cP\,,\ \ \widetilde{Q}_1'(\mathbf{z})=\pm 2\lambda_1 p,\ \ \ p\in\mathbb{P}\right\}.$$

then

$$|\mathcal{F}(P)|\gg\frac{P^h}{\log P}.$$

Thus, in any case, if

$$\mathcal{H}(P)=\left\{\mathbf{z}\in\mathbb{Z}^h:|\mathbf{z}|<cP,\ \widetilde{Q}_1'(\mathbf{z})=\lambda_1^* p,\ \lambda_1^*|(6\mu)^3\,,p\in\mathbb{P}\right\}.$$

then

$$|\mathcal{H}(P)|\gg\frac{P^h}{\log P}.$$

The corresponding points $\mathbf{x}$ satisfy

- $|\mathbf{x}|<P$.
- $\mathbf{x}\equiv\mathbf{X}\pmod{6\mu}$.
- $\widetilde{Q_1}(\mathbf{x})=\lambda_1^* p$.

and so the conditions of Lemma 4.19 are satisfied with

- $R(\mathbf{x})=\widetilde{Q_1}(\mathbf{x})$.
- $U_i(P)=P\qquad(i=1,...,h)$.

It follows that there exists $\overline{\mathbf{x}}\in\mathbb{Z}^h$ such that

- $\left(\widetilde{C}(\overline{\mathbf{x}}),\widetilde{Q_1}(\overline{\mathbf{x}}),...,\widetilde{Q_s}(\overline{\mathbf{x}})\right)=1$.
- $\widetilde{Q_1}(\overline{\mathbf{x}})\neq 0$.

The polynomial

$$\psi(\mathbf{y})=\phi(\overline{\mathbf{x}},\mathbf{y}).$$

is a linear polynomial in $\mathbf{y}$ satisfying the conditions of Lemma 4.14 with s in place of n. Hence $\psi(\mathbf{y})$ represents **infinitely many primes**.

(ii) Suppose that $r(\overline{\overline{Q}}_1(\mathbf{x}))\leq 2$. In this case, after an integral unimodular transformation of the variables $x_1,...,x_h$ if necessary, we can suppose that $\widetilde{Q}_1$ is of the form

$$\widetilde{Q_1}(\mathbf{x})=\sum_{i=1}^{h-2}a_i x_i+Q_1^*(x_{h-1},x_h).$$

where

- Q_1^* is a quadratic polynomial in x_{h-1}, x_h.
- $a_1, ..., a_{h-2} \in \mathbb{Z}$.

We shall consider two further cases:

(ii)(a) Where we suppose $a_1 \neq 0$ If $a_1 \neq 0$ the variable x_1 occurs in the linear part of $\widetilde{Q}_1$ but not in the quadratic part. In this case we make the substitution (4.65) where $\mathbf{X}$ is the integer point given by Lemma 4.18 and μ is the product of coefficients of ϕ, and $\mathbf{z} \in J(P)$ where

$$\mathcal{J}(P) = \left\{ \mathbf{z} \in \mathbb{Z}^h : \left| \begin{array}{ll} |z_1| < cP^2 & \\ |z_i| < cP & (i = 2, ..., h) \\ 0 < c < |6\mu|^{-1} & \end{array} \right. \right\}.$$

The corresponding points $\mathbf{x}$ satisfy

- $|x_1| < P^2$.
- $|x_i| < P \ \ (i = 2, ..., h)$.

for P large enough. With this substitution the polynomial $\widetilde{Q_1}(\mathbf{x})$. becomes $\widetilde{Q_1}'(\mathbf{z})$, where z_1 occurs in the linear part of $\widetilde{Q_1}'(\mathbf{z})$ but not in its quadratic part. If λ_1 is the greatest common factor of the coefficients of $\widetilde{Q_1}'$ then $\lambda_1 | 36\mu^3$. Just as in **Case B2 (i)** either

$$F(\mathbf{z}) = \lambda_1^{-1} Q_1'(\mathbf{z}).$$

or

$$E(\mathbf{z}) = (2\lambda_1)^{-1} Q_1'(\mathbf{z}).$$

satisfy the conditions of Lemma 4.13. Hence we deduce that if

$$\widehat{\Lambda}(P) = \left\{ \mathbf{x} \in \mathbb{Z}^h : \left| \begin{array}{l} |x_1| < P^2, \ |x_i| < P \ \ (i = 2, ..., h) \\ \mathbf{x} \equiv \mathbf{X} \pmod{6\mu} \\ \widetilde{Q_1}(\mathbf{x}) = \lambda_1^* p \\ \lambda_1^* | (6\mu)^3 \\ p \in \mathbb{P} \end{array} \right. \right\}.$$

then

$$\left| \widehat{\Lambda}(P) \right| \gg \frac{P^{h+1}}{\log P}.$$

We apply now Lemma 4.19 with

- $R(\mathbf{x}) = \widetilde{Q_1}(\mathbf{x})$.
- $U_1(P) = P^2$.
- $U_i(P) = P \qquad (i = 2, ..., h)$.

It follows that there exists $\overline{\mathbf{x}} \in \mathbb{Z}^h$ such that

- $\left(\widetilde{C}(\overline{\mathbf{x}}), \widetilde{Q_1}(\overline{\mathbf{x}}), ..., \widetilde{Q_s}(\overline{\mathbf{x}})\right) = 1$.
- $\widetilde{Q_1}(\overline{\mathbf{x}}) \neq 0$.

The polynomial

$$\psi(\mathbf{y}) = \phi(\overline{\mathbf{x}}, \mathbf{y}).$$

is a linear polynomial in $\mathbf{y}$ satisfying the conditions of Lemma 4.14. Hence $\psi(\mathbf{y})$ represents **infinitely many primes**.

(ii)(b) Where we suppose $a_1 = 0$. If on the other hand $a_1 = 0$ then $\widetilde{Q_1}$ is a polynomial in $x_2, ..., x_h$ only which is not identically zero and we can find $(x_2^*, ...x_h^*) \in \mathbb{Z}^{h-1}$ satisfying

- $x_i^* \equiv X_i \pmod{6\mu} \quad (i = 2 \dots h))$.
- $\widetilde{Q_1}(x_2^*, ...x_h^*) \neq 0$.

where $\mathbf{X}$ is the integer point given by Lemma 4.18 and μ is the product of coefficients of ϕ. Now either the polynomial $\widetilde{C}(x_1 \dots x_h)$ of (4.73) contains a term x_1^3 or else one of the polynomials $\widetilde{Q}_2, ..., \widetilde{Q}_s$ of (4.73) contains a term x_1^2, for otherwise every term of the cubic part of ϕ would contain one of the variables $x_2, ..., x_h$, contrary to the minimality in the definition of h. Let $R(\mathbf{x}) = R(x_1 \dots x_h)$ one of these polynomials. We have that

- $\partial R(\mathbf{x}) = d = \begin{cases} 2 \\ 3 \end{cases}$ where d is the degree of R.
- The coefficient of x_1^d in $R(\mathbf{x})$ is not zero.

We shall show that there exists $x_1^* \in \mathbb{Z}$ such that

- $x_1^* \equiv X_1 \pmod{6\mu}$.
- If $p \in \mathbb{P}$ and

$$\begin{cases} p | R(x_1^*, ...x_h^*) \\ p | \widetilde{Q_1}(x_1^*, ...x_h^*) = \widetilde{Q_1}(x_2^*, ...x_h^*). \end{cases}$$

then $p | 6\mu$.

If we make the substitution

$$\begin{cases} x_1 = X_1 + 6\mu z_1 \\ x_i = x_i^* \ \ (i = 2 \dots h) . \end{cases}$$

the polynomial $R(x_1 \dots x_h)$ becomes $R_1(z_1)$ where

$$R_1(z_1) = \sum_{i=0}^{d} c_i z_1^{d-i}.$$

with

- $c_0 \neq 0$.
- $c_0 | 6^3 \mu^4$.

If $p \in \mathbb{P}$ and $p \nmid 6\mu$ then

$$R_1(z_1) \equiv 0 \pmod{p} .$$

is not identically true. By a well-know theorem of Lagrange [5] about polynomial congruence, we know that $R_1(z_1) \equiv 0 \pmod{p}$. has at most d incongruent solutions $(\mathrm{mod}\, p)$. Since $p > 3 \geq d$, there is $\overline{z_1} \in \mathbb{Z}$ such that

$$R_1(\overline{z_1}) \not\equiv 0 \pmod{p} .$$

Let

$$P_{\widetilde{Q_1}} = \left\{ p \in \mathbb{P} : \ p | \widetilde{Q_1}(x_2^*, ...x_h^*) , p \nmid 6\mu \right\} .$$

and

$$Z_{\widetilde{Q_1}} = \left\{ \overline{z_1} \in \mathbb{Z} : \exists p \in P_{\widetilde{Q_1}}, R_1(\overline{z_1}) \not\equiv 0 \pmod{p} \right\} .$$

It is plain that $Z_{\widetilde{Q_1}}$ is a finite set and combining its elements as in the proof of Lemma 4.2 we obtain $z_1^* \in \mathbb{Z}$ such that if

$$\begin{cases} p \in \mathbb{P} \\ p | R_1(z_1^*) \\ p | \widetilde{Q_1}(x_2^*, ...x_h^*) . \end{cases}$$

then $p | 6\mu$. Then the integer $x_1^* = X_1 + 6\mu z_1^*$ has the properties we require. Now

$$\mathbf{x}^* \equiv \mathbf{X} \pmod{6\mu} .$$

[5] See, for example, [39]

and so, it follows from Lemma 4.18 if

$$\overline{\overline{H}}(\mathbf{x}^*) = \left(\widetilde{C}(\mathbf{x}^*), \widetilde{Q_1}(\mathbf{x}^*), ..., \widetilde{Q_s}(\mathbf{x}^*)\right).$$

then

$$\left(\overline{\overline{H}}(\mathbf{x}^*), 6\mu\right) = 1.$$

Hence, we must have $\overline{\overline{H}}(\mathbf{x}^*) = 1.$ because

- $\overline{\overline{H}}(\mathbf{x}^*) \,|R(\mathbf{x}^*)$.
- $\overline{\overline{H}}(\mathbf{x}^*) \,|\widetilde{Q_1}(\mathbf{x}^*)$.

Thus the polynomial $\psi(\mathbf{y}) = \phi(\mathbf{x}^*, \mathbf{y})$. satisfies the conditions of Lemma 4.14 and so it represents **infinitely many primes**.

Part III

Some results

First part

Chapter 5

Results about the invariant h and h^*

5.1 Introduction

In the next paragraphs we shall illustrate some results obtained during this research. Is we need to use some know result it is cited with references. What is not quoted is due to ourself as the best of our knowledge.

5.2 Results about the h invariant

5.2.1 Introduction

So far the invariant h does has algebraic meaning only but it is easy to show that it has a geometric and a diophantine meaning as well. Namely, by definition we have that h is the smaller positive integer such that

$$C(\mathbf{x}) = C\left(x_1 \dots x_n\right) = \sum_{j=1}^{h} L_j\left(x_1 \dots x_n\right) Q_j\left(x_1 \dots x_n\right).$$

where L_j are linear forms and Q_j are quadratic forms respectively and so, if we consider

$$\begin{cases} L_1\left(x_1 \dots x_n\right) = 0 \\ \\ \vdots \\ L_h\left(x_1 \dots x_n\right) = 0. \end{cases}$$

it define a linear space V_h of dimension $r = n - h$ contained into the cubic hypersurface of equation $C(\mathbf{x}) = 0$.

Of course, if

$$\begin{aligned}\mathbf{v}^1 &= (x_1^1 \dots x_n^1)\,.\\ &\vdots\\ \mathbf{v}^r &= (x_1^r \dots x_n^r)\,.\end{aligned}$$

denotes any basis of V_h and if

$$\mathbf{v} = \sum_{j=1}^{r} m_j \mathbf{v}^j \quad m_j \in \mathbb{Z}.$$

we have $C(\mathbf{v}) = 0$. So, if one is able to find s solutions of the equation $C(\mathbf{x}) = 0$ such that any linear integer combination of them is still a solution of the same equation, the he can say that $h \leq n - s$. In particular, if the diophantine equation has only the trivial solution then $h(C) = n$.

Note 5.1. *The diophantine meaning of h let us understand why it is so difficult to find it!*

If a cubic form is such that $h \geq 8$ we say that it satisfies the **first Theorem** of Pleasants. If a non degenerate cubic form is such that $h \geq 2$ and $n \geq 9$ we say that it satisfies **the second Theorem** of Pleasants. We shall give now an example of polynomial in **nine** variables which satisfies the **first Theorem** of Pleasants.

5.2.2 Example

Lemma 5.1. *Let $F(x, y, z)$ a cubic form such that*

1. *$F(x, y, z) = 0$ if and only if $(x, y, z) = \mathbf{0}$.*
2. *There is a prime p such that $p|F(x, y, z)$ if and only if $p|(x, y, z)$ for every $(x, y, z) \in \mathbb{Z}^3$.*

Let

$$C\,(x_1 ... x_9) = F(x_1, x_2, x_3) + pF(x_4, x_5, x_6) + p^2 F(x_7, x_8, x_9).$$

then the diophantine equation

$$C\,(x_1 ... x_9) = 0.$$

has only the trivial solution.

Proof. For if $(\theta_1 \dots \theta_9)$ is a non-trivial solution then

$$F(\theta_1, \theta_2, \theta_3) + pF(\theta_4, \theta_5, \theta_6) + p^2 F(\theta_7, \theta_8, \theta_9) = 0$$

and so $p|F(\theta_1, \theta_2, \theta_3)$. It follows that $p|(\theta_1, \theta_2, \theta_3)$ where k_i and so we have

$$\theta_1 = pk_1 \quad \theta_2 = pk_2 \quad \theta_3 = pk_3$$

From this we have

$$p^2 F(k_1, k_2, k_3) + F(\theta_4, \theta_5, \theta_6) + pF(\theta_7, \theta_8, \theta_9) = 0$$

Proceeding In same way we obtain

$$F(k_1, k_2, k_3) + pF(k_4, k_5, k_6) + p^2 F(k_7, k_8, k_9) = 0$$

Now we observe that $|k_i| = |\theta_i| \Leftrightarrow \theta_i = 0$ and so it is not possible to have $k_i = \theta_i$ for every $i = 1...9$ because, by hypotesis, $(\theta_1 \dots \theta_9)$ is not the trivial solution. In this case we would have an infinite descent and this is a contradiction. □

In [24] Mordell proved that:

Lemma 5.2. *If*

$$F(x, y, z) = x^3 + 2y^3 + 4z^3 + xyz.$$

then it satisfies the hypotesis of Lemma 5.1 ad so we proved the:

Theorem 5.1. *Let*

$$C(\mathbf{x}) = C(x_1 ... x_9).$$

is a cubic form as in 5.2. ***If:***

- $Q(x_1 ... x_9)$ *is a* ***quadratic form*** *in* $\mathbb{Z}[x_1 ... x_9]$.
- $L(x_1 ... x_9)$ *is a* ***linear form*** *in* $\mathbb{Z}[x_1 ... x_9]$.
- $N \in \mathbb{Z}$
- *There exists* $\mathbf{x} \in \mathbb{Z}^9$ *so that* $\phi(\mathbf{x}) > 0$
- $\phi(x_1 ... x_9) = C(x_1 ... x_9) + Q(x_1 ... x_9) + L(x_1 ... x_9) + N$ *does not have* ***fixed divisors***.

then: *the polynomial* ϕ *satisfies the* ***first*** *Theorem of Pleasants.*

In particular, we have that:

Corollary 5.1. *If $C(\mathbf{x}) = C(x_1 ... x_9)$ is a cubic form as in 5.2 then*

$$\phi(x_1 \dots x_9) = C(x_1 \dots x_9)$$

*satisfies the **first** Theorem of Pleasants.*

Proof. We have only to check that:

1. There is $\mathbf{x} \in \mathbb{Z}^9$ so that $\phi(\mathbf{x}) > 0$
2. There are no fixed divisors.

Both these tasks are easy. □

Note 5.2. *By setting down $x_9 = 0$ we have an example of a cubic form in **eight variables** which does not have any non-trivial solution. For this cubic we have $h = 8$ and so for it the Pleasants's First Theorem holds.*

5.2.3 Further examples

First example

Lemma 5.3. *Let $C_1(x, y, z, w)$, $C_2(x, y, z, w)$ be non-singular cubic forms such that $h(C_1) \leq 3$ and $h(C_2) \leq 2$. Let $A \in \mathbb{Z} - \{0\}$. Then*

$$C(\mathbf{x}) = C_1(x_1, x_2, x_3, x_4) + C_2(x_5, x_6, x_7, x_8) + Ax_9^3.$$

is a non-singular cubic such that $2 \leq h(C) \leq 6$.

Proof. We have

$$J(C) = \begin{cases} \frac{\partial C}{\partial x_1} = \frac{\partial C_1}{\partial x}(x_1 \cdots x_4) \\ \frac{\partial C}{\partial x_2} = \frac{\partial C_1}{\partial y}(x_1 \cdots x_4) \\ \frac{\partial C}{\partial x_3} = \frac{\partial C_1}{\partial z}(x_1 \cdots x_4) \\ \frac{\partial C}{\partial x_4} = \frac{\partial C_1}{\partial z}(x_1 \cdots x_4) \\ \frac{\partial C}{\partial x_5} = \frac{\partial C_2}{\partial x}(x_5 \cdots x_8) \\ \frac{\partial C}{\partial x_6} = \frac{\partial C_2}{\partial y}(x_5 \cdots x_8) \\ \frac{\partial C}{\partial x_7} = \frac{\partial C_2}{\partial z}(x_5 \cdots x_8) \\ \frac{\partial C}{\partial x_8} = \frac{\partial C_2}{\partial w}(x_5 \cdots x_8) \\ \frac{\partial C}{\partial x_9} = 3Ax_9^2. \end{cases}$$

and so, by hypotesis, we have:

$$\frac{\partial C}{\partial x_1} = \frac{\partial C_1}{\partial x}(x_1 \cdots x_4) = 0 \Leftrightarrow (x_1 \cdots x_4) = \mathbf{0}.$$

The same holds for every partial derivative, so C in non-singular and hence non degenerate as well. This means $h(C) > 1$. Moreover

$$C_1(x_1, x_2, x_3, x_4) = \sum_{j=1}^{h(C_1)} L_j(x_1, x_2, x_3, x_4) Q_j(x_1, x_2, x_3, x_4).$$

and

$$C_2(x_5, x_6, x_6, x_8) = \sum_{j=1}^{h(C_2)} L_j(x_5, x_6, x_7, x_8) Q_j(x_5, x_6, x_7, x_8).$$

Hence, if $\mathbf{u} = (x_1, x_2, x_3, x_4)$ and $\mathbf{v} = (x_5, x_6, x_7, x_8)$, we have

$$C(\mathbf{x}) = C(\mathbf{u}, \mathbf{v}, x_9) = \sum_{j=1}^{h(C_1)} L_j^{(1)}(\mathbf{u}) Q_j^{(1)}(\mathbf{u}) + \sum_{j=1}^{h(C_2)} L_j^{(2)}(\mathbf{v}) Q_j^{(2)}(\mathbf{v}) + A x_9 x_9^2.$$

where $L_j^{(1)}, L_j^{(2)}$ are linear forms and $Q_j^{(1)}, Q_j^{(2)}$ are quadratic forms in their respective domains. This means that $h(C) \leq 6$. □

Lemma 5.4. ***If***
$C_1(x, y, z, w)$ is any of the following forms ***then*** *$h(C_1) \leq 3$ and the cubic form C_1 is non-singular:*

1 $C_1(x, y, z, w) = ax^3 + ay^3 + az^3 + ab^3w^3$ *with* $a, b \in \mathbb{Z} - \{0\}$.

2 $C_1(x, y, z, w) = ax^3 + ay^3 + az^3 + 2ab^3w^3$ *with* $a, b \in \mathbb{Z} - \{0\}$.

3 $C_1(x, y, z, w) = ax^3 + by^3 + cz^3 + (a + b + c)w^3$ *with* $a, b, c \in \mathbb{Z} - \{0\}$.

4 $C_1(x, y, z, w) = ax^3 + ay^3 + acz^3 + 2aw^3$ *with* $a, c \in \mathbb{Z} - \{0\}$.

5 $C_1(x, y, z, w) = Ax^3 + By^3 - z^2w + Cw^3$ *where:*

- **1** $A = ab^2$, $B = 1$, $C = (27ab)^2$ *with* $a, b \in \mathbb{Z} - \{0\}$.
  or
- **3** $A = a$, $B = b$, $C = 16a^2b^2$ *with* $a, b \in \mathbb{Z} - \{0\}$.
  or
- **3** $A = (6l^2 + 6l - 1)$, $B = (6l^2 - 6l - 1)$, $C = (11 - 12l^2)$ *with* $l \in \mathbb{Z} - \{0\}$.

Proof. We consider the equation

$$C_1(x, y, z, w) = 0. \tag{5.1}$$

We have that

1 $x = 1, y = -1, z = b, w = 1$ is a non-trivial solution for (5.1). Moreover C_1 is non-singular as every diagonal cubic.

2 $x = b, y = b, z = 0, w = -1$ is a non-trivial solution for (5.1). Moreover C_1 is non-singular as every diagonal cubic.

3 $x = 1, y = 1, z = 1, w = -1$ is a non-trivial solution for (5.1). Moreover C_1 is non-singular as every diagonal cubic.

4 $x = 6c^2 - 1$, $y = -6c^2 - 1$, $z = 6c$, $w = 1$ is a non-trivial solution for (5.1). Moreover C_1 is non-singular as every diagonal cubic.

5 We have that:

1 In [26] Mordell proved that this equation has non-trivial solutions.

2 In [26] Mordell proved that this equation has non-trivial solutions.

3 In [25] Mordell proved that this equation has non-trivial solutions.

hence in is enough to prove that the cubic form

$$C_1(x, y, z, w) = Ax^3 + By^3 - z^2w + Cw^3.$$

is non-singular. We have

$$J(C_1) = \begin{pmatrix} \frac{\partial C_1}{\partial x} \\ \\ \frac{\partial C_1}{\partial y} \\ \\ \frac{\partial C_1}{\partial z} \\ \\ \frac{\partial C_1}{\partial w} \end{pmatrix} = \begin{pmatrix} 3Ax^2 \\ 3By^2 \\ -2zw \\ -z^2 + 3Cw^2 \end{pmatrix}.$$

and so we must study the solutions of

$$\begin{cases} 3Ax^2 = 0 \\ \\ 3By^2 = 0 \\ \\ -2zw = 0 \\ \\ -z^2 + 3Cw^2 = 0. \end{cases}$$

Of course, immediately we have $x = y = 0$. If $z = 0$ then from the last equation it follows that $w = 0$ as well. The same happens if $w = 0$ so the cubic is non-singular.

□

Lemma 5.5. *If*

$$C_2(x, y, z, w) = Ex^3 + Ey^3 - z^2w + Gw^3.$$

with $G, E \in \mathbb{Z} - \{0\}$ *then* C_2 *is non-singular and* $h(C_2) = 2$

Proof. As we already proved C_2 is non singular and $h(C_2) > 1$. On the other side, trivially

$$C_2(x, y, z, w) = E(x + y)\left(x^2 - xy + y^2\right) + w\left(-z^2 + Gw\right).$$

Hence, $h(C_2) = 2$. □

So we proved the following:

Theorem 5.2. ***If***

- C_1 *is a cubic form as in 5.3.*
- C_2 *is a cubic form as in 5.5.*
- $C(\mathbf{x}) = \lambda_1 C_1(x_1, x_2, x_3, x_4) + \lambda_2 C_2(x_5, x_6, x_7, x_8) + \lambda_3 x_9^3$, $\lambda_i \in \mathbb{Z} - \{0\}$, $i = 1, 2, 3$.
- *There exists a* $\mathbf{x} \in \mathbb{Z}^{\mathbf{9}}$ *so that* $C(\mathbf{x}) > \mathbf{0}$.
- C *has* ***not*** *fixed divisors.*

then:

$$\phi(\mathbf{x}) = C(\mathbf{x})$$

satisfies the ***second*** *Theorem of Pleasants.*

Second example

Lemma 5.6. *Let* $C_1(x, y, z, , t, w)$, $C_2(x, y, z, w)$ *be non-singular cubic forms such that* $h(C_1) \leq 4$ *and* $h(C_2) \leq 2$. *Then*

$$C(\mathbf{x}) = C_1(x_1, x_2, x_3, x_4, x_5) + C_2(x_6, x_7, x_8, x_9).$$

is a non-singular cubic such that $2 \leq h(C) \leq 6$.

Proof. As in 5.3. □

In [8] **V. Demjanenko** proved the following result

Lemma 5.7. ***If*** $n \in \mathbb{Z}$ *and* $n \not\equiv \pm 4 \pmod 9$ ***then*** *the diophantine equation:*

$$x^3 + y^3 + z^3 + t^3 = n.$$

has a ***non trivial*** *solution.*

hence we have that

Lemma 5.8. *If* $n \in \mathbb{Z}$ *and* $n \not\equiv \pm 4 \pmod 9$ *and*

$$C_1(x, y, z, t, w) = x^3 + y^3 + z^3 + t^3 + nw^3.$$

then $2 \leq h(C_1) \leq 4$

It follows that:

Theorem 5.3. ***If:***

- C_1 *is as in Lemma 5.8.*
- C_2 *is as in Lemma 5.5*
- $C\left(x_1 \dots x_9\right) = \lambda_1 C_1(x_1 \dots x_5) + \lambda_2 C_2(x_6 \dots x_9)$ *with* $\lambda_1,\ \lambda_i \in \mathbb{Z} - \{0\}$, $i = 1, 2$.
- *There exists a* $\mathbf{x} \in \mathbb{Z}^{\mathbf{9}}$ *so that* $C(\mathbf{x}) > \mathbf{0}$.
- C *has* ***not*** *fixed divisors.*

then:

$$\phi\left(\mathbf{x}\right) = C\left(\mathbf{x}\right)$$

satisfies the ***second*** *Theorem of Pleasants.*

Note 5.3. *It has been conjectured from long time that the equation*

$$x^3 + y^3 + z^3 + t^3 = n.$$

has a ***non trivial*** *solution for every* $n \in \mathbb{Z}$.

Third example

Lemma 5.9. *Let $C_i(x,y,z)$ $i=1,2,3$ be non-singular cubic forms; if*

$$C(x_1 \dots x_{10}) = \sum_{i=1}^{3} \lambda_i C_i(x_{3i-2}, x_{3i-1}, x_{3i}) + A_{10} x_{10}^3.$$

with

$$\begin{cases} \lambda_i \in \mathbb{Z} - \{0\} \;\; i=1,2,3 \\ A_{10} \in \mathbb{Z} - \{0\}. \end{cases}$$

then it is a non-singular cubic such that $2 \leq h(C) \leq 10$.

Proof. As in 5.3. □

Lemma 5.10. *If $C(x,y,z)$ is one of the following cubic form then it is non-singular:*

1 *$C(x,y,z) = x^3 + y^3 + z^3 - kxyz$ with $k \in \mathbb{Z}$ and $k \neq 3$.*

2 *$C(x,y,z) = ax^3 + ay^3 + bz^3 - 3ax^2y + 3axy^2$ with $a, b \in \mathbb{Z}$.*

Proof. We have

1

$$J(C_1) = \begin{pmatrix} \frac{\partial C}{\partial x} \\ \\ \frac{\partial C}{\partial y} \\ \\ \frac{\partial C}{\partial z} \end{pmatrix} = \begin{pmatrix} 3x^2 - kyz \\ \\ 3y^2 - kxz \\ \\ 3z^2 - kxy \end{pmatrix}$$

hence we have to study

$$\begin{cases} 3x^2 - kyz = 0 \\ \\ 3y^2 - kxz = 0 \\ \\ 3z^2 - kxy = 0 \end{cases}$$

If $(\theta_1, \theta_2, \theta_3)$ is a non-trivial solution and $\theta_1 = 0$ then by means of the second and third equations, immediately we see that $\theta_2 = \theta_3 = 0$. The same is true if $\theta_2 = 0$ or $\theta_3 = 0$. Hence there are no non-trivial solutions with $\theta_1\theta_2\theta_3 = 0$ On the other side, if $(\theta_1, \theta_2, \theta_3)$ is a non-trivial solution with $\theta_1\theta_2\theta_3 \neq 0$ then, from the first and the second equations we have

$$\frac{\theta_1^2}{\theta_2^2} = \frac{\theta_2}{\theta_1}$$

as well as

$$\frac{\theta_1^2}{\theta_3^2} = \frac{\theta_3}{\theta_1}$$

by considering the first and the third equations. This means that $\frac{\theta_1^2}{\theta_3^2} = \frac{\theta_3}{\theta_1}$. By Euler's theorem on homogeneus functions we have that $(\theta_1, \theta_2, \theta_3)$ would be a solution of the equation

$$x^3 + y^3 + z^3 - kxyz = 0$$

and so

$$3\theta_1^3 - k\theta_1\theta_2\theta_3 = 0$$

Hence

$$27\theta_1^3 = k^3\theta_1^3\theta_2^3\theta_3^3$$

and so

$$\left(27 - k^3\right)\theta_1^3 = 0$$

and this means that $\theta_1 = 0$ because $k \neq 3$. This is a contradiction.

2

$$J(C) = \begin{pmatrix} \frac{\partial C}{\partial x} \\ \\ \frac{\partial C}{\partial y} \\ \\ \frac{\partial C}{\partial z} \end{pmatrix} = \begin{pmatrix} 3ax^2 - 6axy + 3ay^2 \\ \\ -3ax^2 - 6axy + 3ay^2 \\ 3bz^2 \end{pmatrix}.$$

Hence we have to solve

$$\begin{cases} 3ax^2 - 6axy + 3ay^2 = 0 \\ -3ax^2 - 6axy + 3ay^2 = 0 \\ 3bz^2 = 0. \end{cases}$$

By subtracting the second equation from the first we have $x = 0$ and so $y = 0$ as well as $z = 0$.

□

From Lemma 5.9 and 5.10 we have:

Theorem 5.4. ***If:***

$$C\left(x_1 \ldots x_{10}\right) = \sum_{i=1}^{3} \lambda_i C_i\left(x_{3i-2}, x_{3i-1}, x_{3i}\right) + A_{10}x_{10}^3.$$

where:

- $C_i\left(x_{3i-2}, x_{3i-1}, x_{3i}\right) = x_{3i-2}^3 + x_{3i-1}^3 + x_{3i}^3 - k_i x_{3i-2} x_{3i-1} x_{3i},\ \ i = 1, 2, 3.$

  or:

- $C_i\left(x_{3i-2}, x_{3i-1}, x_{3i}\right) = a_i x_{3i-2}^3 + a_i x_{3i-1}^3 + b_i x_i^3 - 3a_i x_{3i-2}^2 x_{3i-1} + 3a_i x_{3i-2} x_{3i-1}^2$, $i = 1, 2, 3.$

and ***if:***

- *There exists a* $\mathbf{x} \in \mathbb{Z}^{\mathbf{10}}$ *so that* $C(\mathbf{x}) > \mathbf{0}$.
- C *has* ***not*** *fixed divisors.*

then: $C\left(x_1 \dots x_{10}\right)$ *either satisfies the* ***first*** *or the* ***second*** *theorem of Pleasants.*

5.3 A result about h^*

Lemma 5.11. *If*

$$C\left(x_1 \dots x_n\right) = a_1 x_1^3 + \dots a_n x_n^3.$$

is a cubic form with integer coefficients then $h^* \geq n$.

Proof. It follows directly from the definition of h^*. □

Lemma 5.12. *Let*

$$F\left(x, y\right) = a^3 x^3 + 3a^2 b x^2 y + 3abxy^2 + cy^3.$$

be a cubic form such that

- $a, b, c \in \mathbb{Z} - \{0\}$
- $c \neq b^3$.

There exist a non-singular linear transformation

$$\begin{array}{l} T : \mathbb{R}^2 \to \mathbb{R}^2 \\ (X, Y) \to (x, y)\,. \end{array}$$

such that $T\left(\mathbb{Z}^2\right) \subseteq \mathbb{Z}$ *and if* $G = F \circ T$ *then*

$$G(X, Y) = a^3 X^3 + a^3\left(c - b^3\right) Y^3.$$

Proof. Let

$$T : R^2 \to R^2$$

such that

$$\begin{cases} x = X - bY \\ y = aY. \end{cases}$$

Then

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

and so T is non-singular and $G = F \circ T$ □

With the help of the last lemma is easy to get:

Lemma 5.13. *Let*

$$F_j\left(x_{2j-1}, x_{2j}\right) = a_j x_{2j-1}^3 + 3a_j^2 b_j x_{2j-1}^2 x_{2j} + 3a_j b_j^2 x_{2j-1} x_{2j}^2 + c_j x_{2j}^3.$$

be cubic forms such that

- $a_j, b_j, c_j \in \mathbb{Z} - \{0\}$.
- $c_j \neq b_j^3$.

for $j = 1...4$. *Let be:*

$$C\left(x_1 \dots x_8\right) = \sum_{j=1}^{4} F_j\left(x_{2j-1}, x_{2j}\right).$$

then $h^* \geq 8$.

Proof. If we consider the non-singular linear transformation:

$$T : \mathbb{R}^8 \to \mathbb{R}^8.$$

such that

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} = \begin{pmatrix} 1 & -b_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -b_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -b_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -b_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_4 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \\ X_7 \\ X_8 \end{pmatrix}.$$

we have that:

$$C'(X_1, \cdots X_8) = (C \circ T)(X_1, \cdots X_8).$$

is given by

$$C'(X_1, \cdots X_8) = \sum_{j=1}^{4} a_j^3 X_{2j-1}^3 + a_j^3 \left(c_j - b_j^3\right) X_{2j}^3.$$

By lemma 5.11 the result follows. □

Hence we proved the:

Theorem 5.5. ***If:***

- $C(x_1 \dots x_8)$ *is a cubic form as in Lemma 5.13*
- *There exists a* $\mathbf{x} \in \mathbb{Z}^{\mathbf{8}}$ *so that* $C(\mathbf{x}) > \mathbf{0}$.
- C *has* ***not*** *fixed divisors.*

then: $C(x_1 \dots x_8)$ *either satisfies the* ***first*** *or the* ***second*** *theorem of Pleasants.*

In the **same way** we can prove that:

Theorem 5.6. ***If:***

- $s \in \mathbb{N}$ *with* $1 \leq s \leq 3$.
- $C(x_1 \dots x_8) = \sum_{j=1}^{s} F_j(x_{2j-1}, x_{2j}) + \sum_{i=2s+1}^{8} a_i' x_i^3$, *where the* F_j *are the same as in Lemma 5.13.*
- $a_i' \in \mathbb{Z} - \{0\}$ *for* $i = (2s+1)...8$.
- *There exists a* $\mathbf{x} \in \mathbb{Z}^{\mathbf{8}}$ *so that* $C(\mathbf{x}) > \mathbf{0}$.
- C *has* ***not*** *fixed divisors.*

then: $C(x_1 \dots x_8)$ *either satisfies the* ***first*** *or the* ***second*** *theorem of Pleasants.*

Second part

Chapter 6

Algorithms

6.1 How to find the primes of the form x^2+y^4

6.1.1 Introduction

As quoted in Theorem 2.2 the polynomial

$$P(x,y) = x^2 + y^4.$$

represented infinitely many primes. If we want to find them we must be able to develop an algorithm Erathostenes's sieve procedure alike, which let us able to detect them or at least to reduce the number of computations. The following proposition help us in doing this.

Proposition 6.1. *Let $(a,b) \in \mathbb{Z}^2$ and let $M = P(a,b)$. Assume that M is not a prime. If p is any prime divisor of M, h,$k \in \mathbb{Z}$, and*

$$\begin{cases} x_h = ph + a \\ y_k = pk + b. \end{cases}$$

then $P(x_h, y_k)$ is a composite integer.

Proof. With generality we can consider only the positive values of x and y. We have

$$P(x_k, y_k) = a^2 + b^4 + p\{H(p,h,a) + K(p,k,b)\}.$$

where

- $H = H(p,h,a) = 2ah + ph^2$.
- $K = K(p,k,b) = 4kb^3 + 6pk^2b^2 + 4p^2k^3b + p^3k^4$.

So

$$P(x_k, y_k) = p\{H + K + N\}.$$

where $M = pN$ and the result follows. □

In a similar way we prove the following

Proposition 6.2. *Let $(a, b) \in \mathbb{Z}^2$ and let $P(a, b) = p \in \mathbb{P}$. Let*

$$\begin{cases} x_h = ph + a \\ y_k = pk + b. \end{cases}$$

where $h, k \in \mathbb{Z}$. If H, K are the same as in 6.1 and $H+K \neq 0$, then $P(x_h, y_k)$ is a composite integer.

We observe that if $a > 0, b > 0$, $h, k \in \mathbb{N}$ and least one in non zero, then trivially at least on of H, K is positive and so

Corollary 6.1. *With the conditions of 6.2, if $a > 0, b > 0$, $h, k \in \mathbb{N}$ and least one in non zero then $P(x_k, y_k)$ is a composite number.*

6.1.2 The algorithm

Suppose we want to find all the primes generated by the given polynomial which are not greater than a given positive real value N. With generality it is enough to consider only the positive values of x and y. We consider the plane region bounded by

$$\begin{cases} x^2 + y^4 \leq N \\ x \geq 0 \\ y \geq 0 \end{cases}$$

The subset

$$\mathcal{A}_N = \left\{(x, y) \in \mathbb{Z}^2, x > 0, y > 0, x^2 + y^4 = p \in \mathbb{P}, p \leq N\right\}.$$

is contained in this region.

- If x, y are both even then $P(x, y)$ is even and greater than 2 and hence composite. If x, y are both odd and greater than 1 then $P(x, y)$ is also even and greater than 2 and hence composite. Thus, for first we delete from the region all these points. (Fig 6.1)

- We apply now Proposition 6.2 and we obtain further cancelations (Fig 6.2)

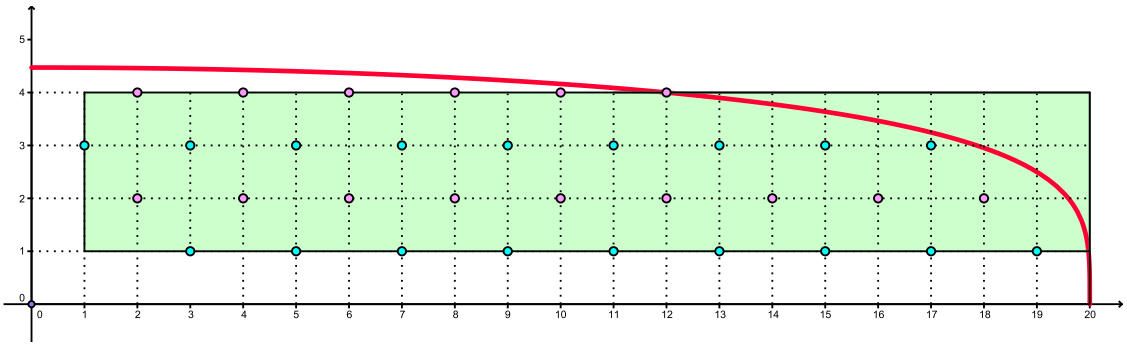

Figure 6.1: All the points whose coordinates have the same parity, with the exception of $(1, 1)$ are deleted at the first step

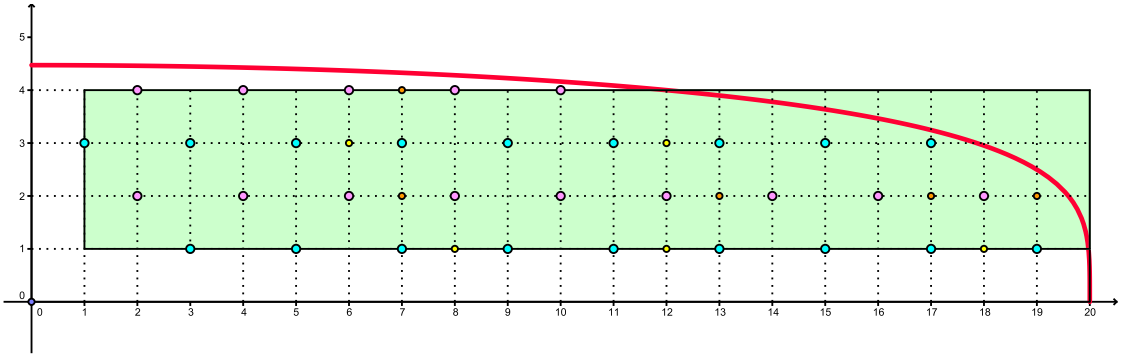

Figure 6.2: The application of Proposition 6.2 produces new cancelations

- Now we have only points whose coordinates have different parity. If we consider them $(\mathrm{mod}\, 10)$ and we list the values of $P(x, y)$ $(\mathrm{mod}\, 10)$ we have

$(x,y)_{(\mathrm{mod}\ 10)}$	1	3	5	7	9
0	1	1	5	1	1
2	5	5	9	5	5
4	7	7	1	7	7
6	7	7	1	7	7
8	5	5	9	5	5

$(x,y)_{(\mathrm{mod}\ 10)}$	0	2	4	6	8
1	1	7	7	7	7
3	9	5	5	5	5
5	5	1	1	1	1
7	9	5	5	5	5
9	1	7	7	7	7

Hence, with the exception of $(2, 1)$, we obtain further cancelations also. (Fig 6.3)

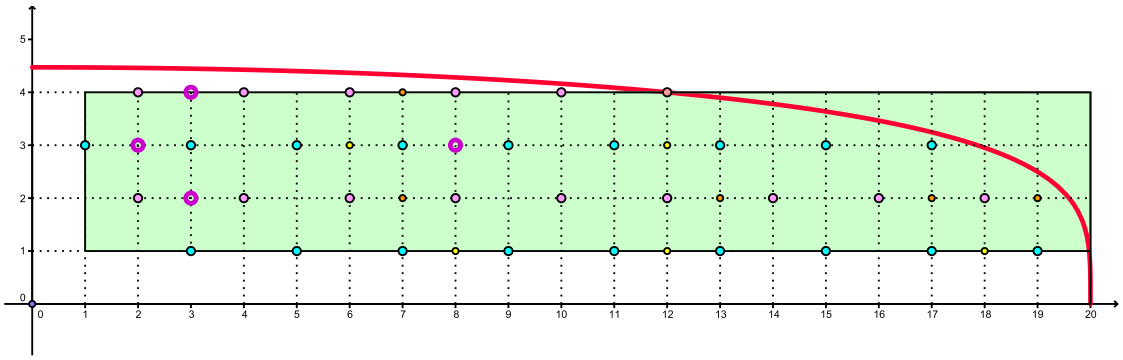

Figure 6.3: New cancelations are obtained with the congruences (mod 10)

- We apply now Proposition 6.2 and we obtain further cancelations. [1]
- We consider the square Q_1 as in figure C.4 and we choose all the integer points on is boundary, which coordinates are both non-zero, i.e $(1,1)$: we have $P(1,1) = 2$ so we must cancel from the region all the points which coordinates are

$$\begin{cases} x_h = 2h+1 \\ \\ y_k = 2k+1. \end{cases}$$

  where $h, k \in \mathbb{N}$ and not both zero.

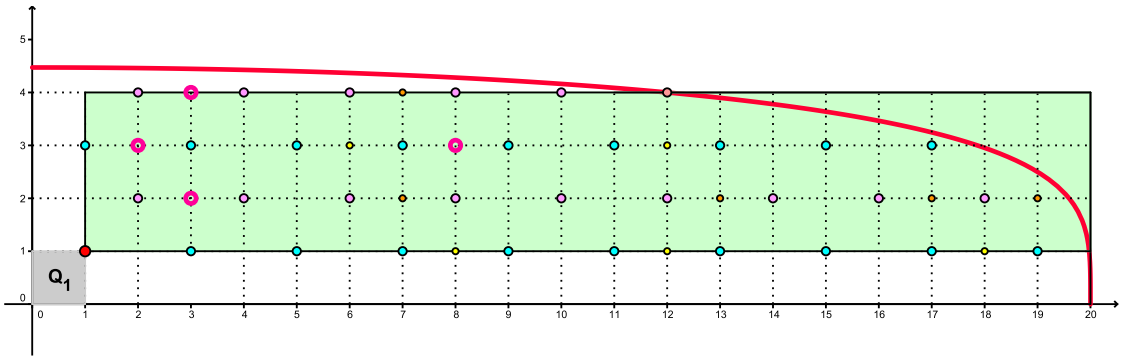

Figure 6.4: In this case no new cancelations

- Now we consider the square Q_2 as in figure 6.4 and we choose all the integer points on is boundary, which coordinates are both non-zero and which survived to the first step, i.e $(1,2)$ $(2,2)$,$(2,1)$.We have

[1] Not illustrated here

– $P(1,2) = 17$ so we must cancel form the region all the points which coordinates are

$$\begin{cases} x_h = 17h + 1 \\ y_k = 17k + 2. \end{cases}$$

where $h, k \in \mathbb{N}$ and not both zero.

– $P(2,2) = 20$ so we must cancel form the region all the points which coordinates are

$$\begin{cases} x_h = 2h + 2 \\ y_k = 2k + 2. \end{cases}$$

as well as all the points which coordinates are

$$\begin{cases} x_h = 5h + 2 \\ y_k = 5k + 2. \end{cases}$$

where $h, k \geq 0$

– $P(2,1) = 5$ so we must cancel form the region all the points which coordinates are

$$\begin{cases} x_h = 5h + 2 \\ y_k = 5k + 1. \end{cases}$$

where $h, k \in \mathbb{N}$ and not both zero.

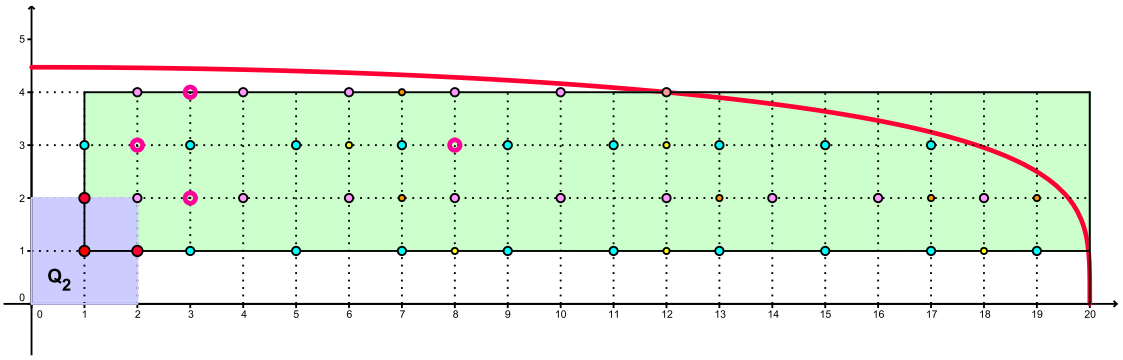

Figure 6.5: The square Q_2 with red points representing the points where $P(x, y)$ takes prime values

- We continuate this procedure until all the points of the region have been either canceled or they get a prime value.

6.2 How to find the primes of the form x^3+2y^3

The procedure is similar to the previous but there something is different because, in this case, we have a polynomial of odd degree. First of all, if we fix positive real number N and we consider the set

$$\mathcal{A}_N = \left\{(x,y) \in \mathbb{Z}^2, x^3+2y^3 = p \in \mathbb{P}\,, p \leq N\right\}$$

could be not finite. So we must consider a better set like

$$\mathcal{A}_{N,a,b} = \left\{(x,y) \in \mathbb{Z}^2,\ x \geq a\,, y \geq b,\ x^3+2y^3 = p \in \mathbb{P}\,, p \leq N\right\}$$

which is contained in the region

$$\begin{cases} x^3+2y^3 \leq N \\ x \geq a \\ y \geq b. \end{cases}$$

- First of all, we notice that all the points on the axis must be deleted as well as all the points with the coordinates that are both even (Fig. 6.6)

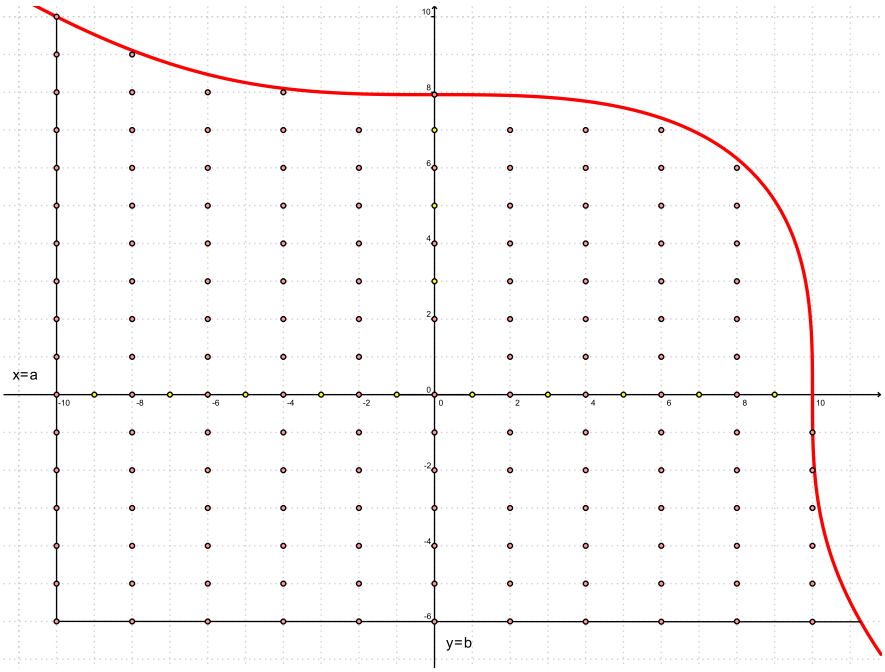

Figure 6.6: All the points of the axis and all the points with coordinates both even must be canceled.

- Next we make use of congruences (mod 10) and we obtain further cancelations. (Fig 6.7)

$(x,y)_{(\text{ mod } 10)}$	0	1	2	3	4	5	6	7	8	9
1	1	3	7	5	9	1	3	7	5	9
3	7	9	3	11	5	7	9	3	11	5
5	5	7	1	9	3	5	7	1	9	3
7	3	5	9	7	1	3	5	9	7	1
9	9	1	5	3	7	9	1	5	3	7

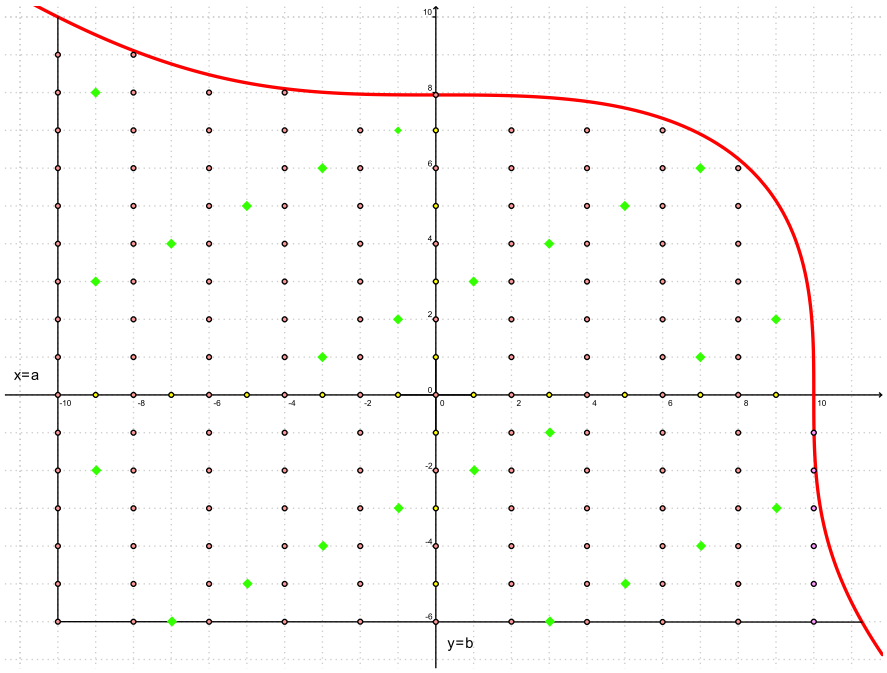

Figure 6.7: Further cancelations form congruences (mod 10)

- Then we procede as before considering the square Q_1. We notice that if $P(a,b) = p$ and if $(-a,-b)$ i still in the considered region, immediately we can use the fact that $P(-a,-b) = -p$. (Fig 6.8)
- Then we shall consider a square Q_2 and repeat the procedure.
- We continuate this procedure until all the points of the region have been either canceled or they get a prime value.

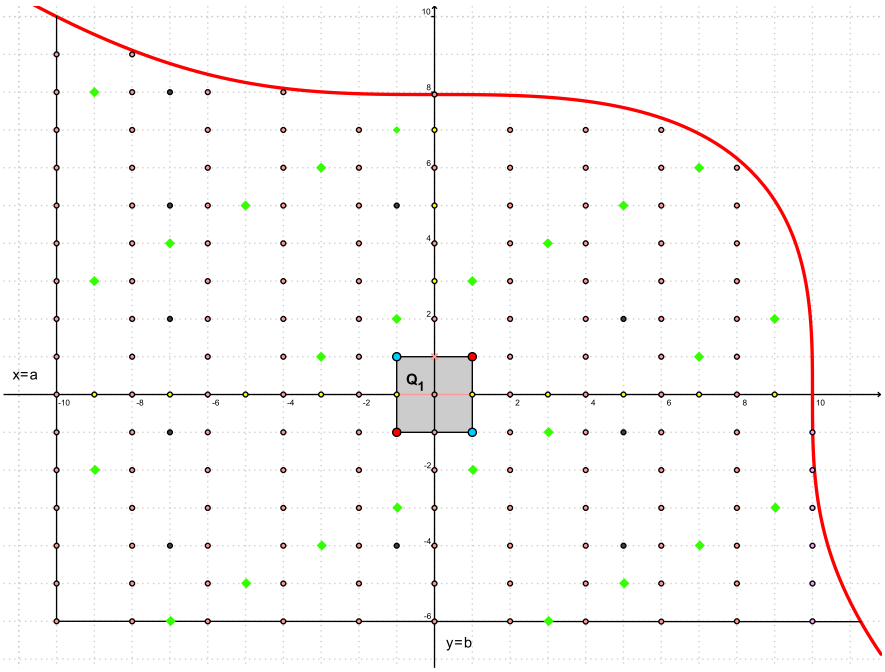

Figure 6.8: Further cancelations from the red points where $P(x, y)$ takes prime values, by means of Proposition 6.1

6.3 How to find the primes of the forms x^2+1

Even dough it is not known if there are infinitely many primes of the form $x^2 + 1$ it is quite simple to find them within a given bound. First if $P(x) = x^2 + 1$ is prime and greater than 2 trivially x must be even. Let N a given bound and let x even; if $x^2+1 \leq N$ is a composite number then it must have an odd prime factor $p \leq \left[\sqrt{N}\right]$. By quadratic reciprocity law if p is odd and $p|p(x)$ then $p \equiv 1 \pmod 4$ and conversely. So if p is an odd prime then there is an integer a so that

- $1 \leq a \leq p - 1$.
- $a^2 + 1 \equiv 0 \pmod p$.
- If $b = p - a$ then $b^2 + 1 \equiv 0 \pmod p$.

Hence

- We start with $x = 1$ and we obtain $p(1) = 2$ (the only case where x is odd).

- All the points $x = 2k + 1$ $k > 0$ must be canceled.
- Since $x = 2$ and $x = 4$ have not been canceled it follows that $p(2)$ and $p(4)$ must be prime numbers.
- We consider the points of the form

  (5a) $x = 5k + 2$ $k \geq 1$.

  (5b) $x = 5k + 3$ $k \geq 0$.

  and we cancel all of them. Since $x = 6$, $x = 10$ have not be canceled $p(6)$, $p(10)$ must be prime numbers.
- We consider now the points of the form

  (13a) $x = 13k + 5$ $k \geq 0$.

  (13b) $x = 13k + 8$ $k \geq 0$.

  and we cancel all of them. Since $x = 14$, $x = 16$ have not be canceled $p(14)$, $p(16)$ must be prime numbers.
- We continuate this procedure until all the primes of the form $p \equiv 1 \pmod 4$ not greater than $\left[\sqrt{N}\right]$ have been considered.
- The remaining point x have the properties that $P(x) = x^2 + 1$ is a prime number. For instance if $N = 1000$ we have to consider only the points $x = 1, 2, 4, 6, 10, 14, 16, 20, 24, 26$ in order to obtain primes of the form $x^2 + 1 \leq 1000$. (Fig 6.9)

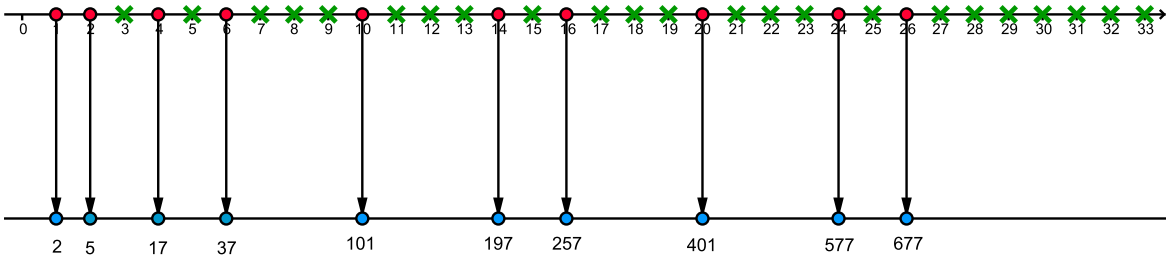

Figure 6.9: The red points representing the values of x such that $x^2 + 1$ is prime and not greater than 1000

Part IV

Appendices

Appendix A

The polynomial of Heath-Brown

Let

$$P(m,n) = \left(n^2+15\right)\left\{1-\left(m^2-23n^2-1\right)^2\right\}-5$$

If we consider the diophantine equation

$$m^2-23n^2-1=0$$

we notice that this is a special case of the so called " Pell equation" with fundamental solution $m_0 = 24$, $n_0 = 5$. As it is well known from the theory of Pell's equations, the recurrences

$$\begin{cases} m_{k+1} = m_1 m_k + 23 n_1 n_k \\ n_{k+1} = m_1 n_k + n_1 m_k \end{cases}$$

for every $k \in \mathbb{N}\,, k > 1$ get us the whole set of positive integral solutions. It follows that

$$P(m_{k+1}, n_{k+1}) = n_{k+1}^2 + 10$$

and so P takes **arbitrarily large positive values** because, as it is easy to see by induction, the sequence of integers $(n_k)_k$ is strictly increasing. Assume that $P(m,n)$ admits a fixed divisor d. We have that $P(0,0) = -5$ so only the values $d = \pm 5$ are possible and so any for any other value of $P(m,n)$ it would be $5|P(m,n)$. But $P(-4,1) = -1013$ and this get us a contradiction. So $P(m,n)$ **does not admit any fixed divisors**. Now we are going to prove that $P(m,n)$ is **irreducible** in $\mathbb{Z}[m,n]$. For if

$$P(m,n) = T(m,n)S(m,n)$$

where $T(m,n)$, $S(m,n)$ are non trivial factors in $\mathbb{Z}[m,n]$, then

$$P(0,n) = T(0,n)S(0,n)$$

as polynomial in $\mathbb{Z}[n]$ would be reducible, because the degree of $P(0,n)$ is still 6 (as the degree of $P(m,n)$. But as it easily seen, in our case

$$p(n) = 529n^6 + 7981n^4 + 690n^2 + 5$$

which is irreducible in $Z[m]$ and this is a contradiction.

Appendix B

A very brief survey on Sieve Methods

B.1 Sieve of Eratosthenes-Legendre

The theory of "Sieve Methods" has is root in the Sieve of Eratosthenes, the well known algorithm for finding all the primes. This algorithm rests on the fact that a natural number n si prime if and only if it is not divisible by any other prime smaller than itself. To find all the primes lesser than a give positive real number x, we write down the list

$$2, 3, 4 \ldots [x] .$$

Since 2 is prime, it is left untouched but every proper multiple of it is crossed out. The next number in the sequence is 3 and it has not been crossed out yet. Hence it is prime. Therefore it is left in the list and we cross out every proper multiple of it. Since, if an integer $n \leq x$ is composite at least one of its prime factors has to be not greater than $\sqrt{x}$, we continue this process up to $[\sqrt{x}]$. The numbers which have not been crossed out are exactly the primes not greater than x. following Legendre, we can set up this procedure into an "analytical framework". Let z any positive real number and let $P(z)$ be the product of all primes less than z. A positive integer n does not have any prime factor less than z if and only if $(n, P(z)) = 1$. Hence the characteristic function of the set of all such integers is expressed as

$$\sum_{d|(n,P(z))} \mu(d). \tag{B.1}$$

where μ is the Moebius function. Hence (B.1) could be identified with Eratosthenes' Sieve. It follows that

$$\pi(x) - \pi\left(\sqrt{x}\right) + 1 = \sum_{n \leq x} \sum_{d|(n, P(\sqrt{x}))} \mu(d).$$

and so

$$\pi(x) - \pi\left(\sqrt{x}\right) + 1 = x \sum_{d|P(\sqrt{x})} \frac{\mu(d)}{d} + \sum_{d|P(\sqrt{x})} \mu(d) \left\{ \left[\frac{x}{d}\right] - \frac{x}{d} \right\}.$$

But

$$\sum_{d|P(\sqrt{x})} \frac{\mu(d)}{d} = \prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right).$$

and so we obtain the exact formula

$$\pi(x) - \pi\left(\sqrt{x}\right) + 1 = x \prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right) + \sum_{d|P(\sqrt{x})} \mu(d) \left\{ \left[\frac{x}{d}\right] - \frac{x}{d} \right\}.$$

We would like consider

$$x \prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right).$$

as the "main term" and

$$\sum_{d|P(\sqrt{x})} \mu(d) \left\{ \left[\frac{x}{d}\right] - \frac{x}{d} \right\}.$$

as an "error term". But this is hopeless because we cannot do much better than

$$\left\{ \left[\frac{x}{d}\right] - \frac{x}{d} \right\} = O(1).$$

and so we have that

$$\sum_{d|P(\sqrt{x})} \mu(d) \left\{ \left[\frac{x}{d}\right] - \frac{x}{d} \right\} = O\left(2^{\pi(\sqrt{x})}\right).$$

This of course, is much greater than the "main term". Anyway, the same underlying ideas cam be used to obtain estimates for the number of integers not greater than x and coprime by any prime lesser than z provided z is much smaller than $\sqrt{x}$. For instance, if we choose $z = \log x$ then we obtain that

$$\pi(x) \ll \frac{x}{\log \log x}.$$

This result is weak compare to the statement of PNT or even to Chebyshev's bounds [4]but nevertheless it tell us that the set of prime numbers has density 0.

B.2 Brun's Sieve

In 1915 Brun [3] had a very clever rather simple idea: he threw out the exact formula (B.1) and replaced it by an inequality bounding the characteristic function from above and below so that he could gain an effective control over the size of participating factors of $P(z)$. His idea is embodied in

$$\sum_{\substack{d|(n,P(z))\\ \upsilon(d)\leq 2l+1}} \mu(d) \leq \sum_{d|(n,P(z))} \mu(d) \leq \sum_{\substack{d|(n,P(z))\\ \upsilon(d)\leq 2l}} \mu(d). \tag{B.2}$$

with $\upsilon(d)$ the number of different prime factors of d. These inequalities are called at the present "Brun's Sieve" and they are the basis of the modern theory of the Sieve Method. By means of them it is possible to show that if

$$\pi_2(x) = \left|\{p \in \mathcal{P} :\ p \leq x,\, p+2 \in \mathcal{P}\}\right|.$$

then

$$\pi_2(x) \ll \frac{x\left(\log\log x\right)^2}{\left(\log x\right)^2}.$$

and so

$$\sum_{\substack{p\in\mathcal{P}\\ p+2\in\mathcal{P}}} \frac{1}{p} < +\infty.$$

B.3 The Selberg Sieve

Let $\mathcal{A}$ any finite set of positive integers. Let $\mathfrak{P}$ any finite set of primes and let $P = \prod_{p\in\mathfrak{P}} p$. Let

$$S\left(\mathcal{A},\mathfrak{P},x\right) = \sum_{\substack{n\in\mathcal{A}\\ (n,P)=1}} 1.$$

Let $|\mathcal{A}| = N \in \mathbb{N}$. For every $d \in \mathbb{N}$ let

$$A_d = \left\{n \in \mathcal{A} : d|n\right\}.$$

Suppose there exists a multiplicative function $f(d)$ such that

$$|A_d| = \frac{f(d)}{d}N + R(d).$$

where $|R(d)| \leq f(d)$ and $d > f(d) > 1$. In [36] Selberg proved that

$$S(\mathcal{A}, \mathfrak{P}, x) \leq \frac{N}{Q_x} + x^2 \prod_{\substack{p \in \mathfrak{P} \\ p \leq x}} \left(1 - \frac{f(p)}{p}\right)^{-2} \tag{B.3}$$

where

$$Q_x = \sum_{\substack{d|P \\ d \leq x}} g^{-1}(d).$$

and

$$g(n) = \prod_{d|n} \frac{\mu(n/d)\, d}{f(d)}.$$

The Selberg's sieve is better than the Brun's sieve, for instance if applied to the Twin's problem it get

$$\pi_2(x) \ll \frac{x}{(\log x)^2}.$$

which is a better than the result from Brun's sieve.

B.4 The Large Sieve

Let $N \in \mathbb{N}$ and for every prime $p \leq \sqrt{N}$ let $f(p)$ residue classes modulo p be given with $0 \leq f(p) < p$. Given a set I_N of N consecutive natural numbers we call I_N as " interval of natural numbers of length N" and we indicate it as I_N. In A_N denotes the subset of I_N which elements are not in any of the $f(p)$ residue classes, then it is possible to show that

$$|A_N| \leq \frac{(1+\pi)\, N}{\sum\limits_{p \leq \sqrt{N}} p - f(p)}.$$

This inequality is called "Large sieve inequality" and it is due to the work of Linnik [22]. Roughly speaking the reason for the name is the following: for each prime $p \leq \sqrt{N}$ we eliminate $f(p)$ classes mod p where $f(p)$ can gets large as p does.

B.5 The parity problem

The following example due to Selberg [38] shows a severe limitation of the sieve methods, now know as " **parity problem**". Let $1 \leq z \leq x$ real

numbers.
Let A_{odd} (respectively A_{even}) the set of natural numbers n such that

1. $n \leq x$
2. If $p \in \mathbb{P}$ is a divisor of n then $p \geq z$
3. The number of prime factors of n counted with multiplicity, is **odd**.(respectively **even**)

Let

$$\Phi_{odd}(x,z) = |A_{odd}|.$$

$$\Phi_{even}(x,z) = |A_{even}|.$$

Suppose that ρ_d is a bounded sequence of real numbers satisfying

$$\sum_{d|n} \mu(d) \leq \sum_{d|n} \rho(d).$$

with $\rho_d = 0$ for $d > z$. Then, by means of Selberg's sieve, it is possible to show that for any $0 < \theta < 1$ and for $z < x^\theta$ one has

$$\Phi_{odd}(x,z) \leq \frac{x}{2} \sum_d \frac{\rho(d)}{d} + O\left(x (\log z) \exp\left(-c_1 (\log x)^{1/2}\right)\right).$$

and

$$\Phi_{even}(x,z) \leq \frac{x}{2} \sum_d \frac{\rho(d)}{d} + O\left(x (\log z) \exp\left(-c_2 (\log x)^{1/2}\right)\right).$$

for suitable c_1 and c_2 **positive** real constants. In particular for $\Phi_{odd}(x, \sqrt{x})$ and $\Phi_{even}(x, \sqrt{x})$ the method gives the same upper bound:

$$(2 + o(1)) \frac{x}{\log x}.$$

whereas it is possible to show that

$$\Phi_{even}\left(x, \sqrt{x}\right) = 0.$$

and

$$\Phi_{odd}\left(x, \sqrt{x}\right) = (1 + o(1)) \frac{x}{\log x}.$$

Thus the sieve method is unable to give a useful upper bound for the first set, and overestimate the upper bound on the second set by a factor of 2. Roughly speaking we can say that without other tools the sieve methods are unable to distinguish between a set whose elements are all products of an odd number of primes and a set whose elements are all products of an even number of primes.

Appendix C

Some graphics

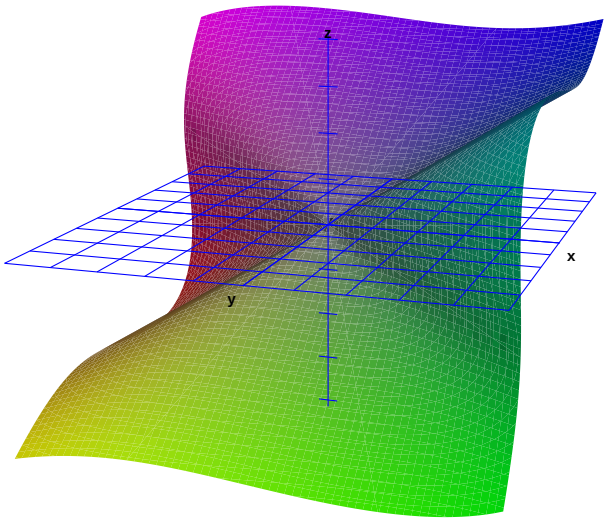

Figure C.1: The surface $x^3 + 2y^3 + 4z^3 + xyz = 0$ used in Lemma 5.1

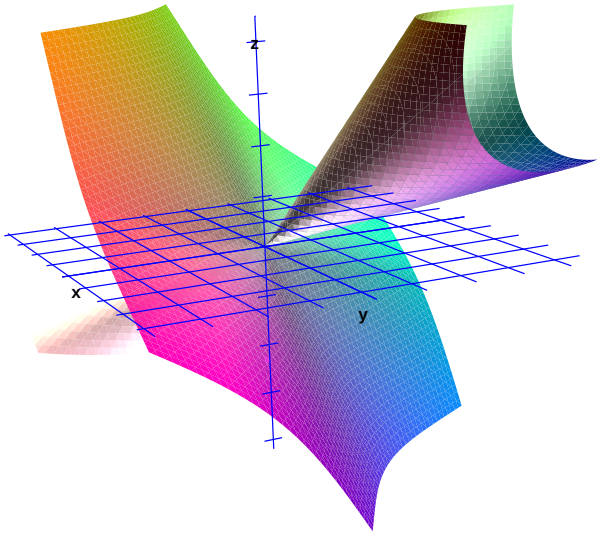

Figure C.2: The surface $x^3 + y^3 + z^3 - 5xyz = 0$ used in Lemma 5.10

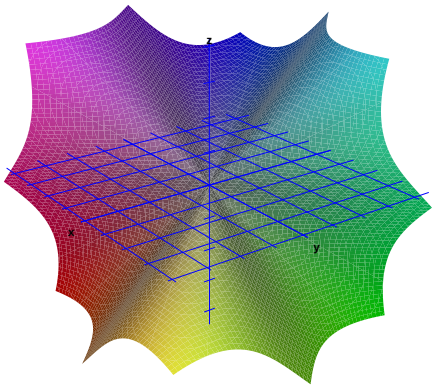

Figure C.3: The surface $x^3 + y^3 + z^3 + 3xyz = 0$ used in Lemma 5.10

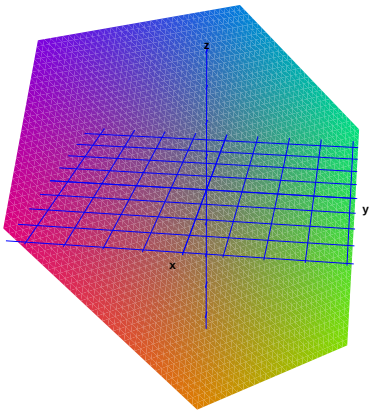

Figure C.4: The surface $x^3 + y^3 + z^3 - 3xyz = 0$

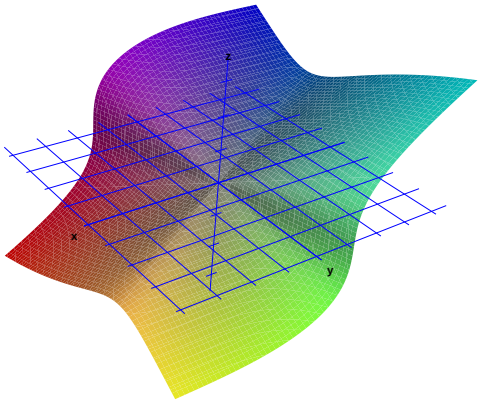

Figure C.5: The surface $x^3 + y^3 + 10z^3 - 3x^2y + 3xy^2 = 0$ used in Lemma 5.10

Appendix D

Notation

D.1 Sets

- $\mathbb{N}$ is the set of natural numbers.
- $\mathbb{Z}$ is the set of integer numbers.
- $\mathbb{Q}$ is the set of rational numbers.
- $\mathbb{R}$ is the set of real numbers.
- $\mathbb{C}$ is the set of real numbers.
- $\mathbb{P}$ is set of ordinary prime numbers.
- I is the interval $(0, 1)$.
- $\overline{I}$ is the interval $[0, 1]$.
- $\mathbb{R}^n_{\mathbf{x}}$ is the ordinary $\mathbb{R}^n$ space where we choose the variable $\mathbf{x}$ to indicate its points.
- If A is a finite set $|A|$ denotes its cardinality
- If A is a set we write $|A| = \infty$ to say that it is an infinite set.
- $\widetilde{A}_R = \{\mathbf{x} \in \mathbb{Z}^n : |\mathbf{x}| < R\}$.
- $\widetilde{A}^2_R = A_R \times A_R$.
- $A_R = \{\mathbf{x} \in \mathbb{Z}^n : 0 < |\mathbf{x}| < R\}$.
- $A^2_R = A_R \times A_R$.

- $\mathfrak{A}_R = \{\mathbf{x} \in \mathbb{Z}^n : 0 < |\mathbf{x}| \ll R\}$.
- $\mathfrak{A}_R^2 = \mathfrak{A}_R \times \mathfrak{A}_R$.
- $\mathfrak{A}'_R = \{\mathbf{x} \in \mathbb{Z}^n : |\mathbf{x}| \ll R\}$.

D.2 Algebra

- If f_1 and f_2 are polynomial of $\mathbb{Z}[\mathbf{x}]$ with $\mathbf{x} \in \mathbb{R}^n$ then (f_1, f_2) denotes their maximum common divisor.
- $\mathbb{Q}(x_1, \ldots, x_n)$ denote the field of rational functions of $x_1, ..., x_n$.
- If $\mathbf{A}$ is a matrix $r(\mathbf{A})$ denotes its rank.
- If Q is a quadratic form $r(Q)$ denotes its rank.
- If B is a bilinear form $r(B)$ denotes its rank.
- If P is a polynomial ∂P denotes its total degree.

D.3 General Functions

- If $x \in \mathbb{R}$ then $|x|$ is the usual absolute value.
- If $z \in \mathbb{C}$ then $|z|$ is the usual absolute value.
- $e(t)$:
$$\begin{array}{l} e : [0,1] \to R \\ t \to e^{2\pi i t}. \end{array}$$

D.4 Arithmetical Functions

- If a and b are non zero integers then (a, b) denotes their maximum common divisor.
- If we have $a_1...a_n \in \mathbb{Z}$ and we want to say that they have no non-trivial common factors, we write $(a_1...a_n) = 1$.
- If $\mathbf{x} \in \mathbb{Z}^{\mathbf{n}}$: $|\mathbf{x}| = \max\limits_{i=1...n} \{|x_i|\}$.
- If x is any real number:
$$\|x\| = \min\{x - [x], [x] + 1 - x\}.$$

- If $\mathbf{x} = (x_1 \dots x_n) \in \mathbb{Z}^n$ and $q > 1$ is any positive integer, then $\mathbf{x} \pmod q = \mathbf{y} = (y_1 \dots y_n) \in \mathbb{Z}^n$ where:

$$\begin{cases} y_i \equiv x_i \pmod q & \forall i = 1 \dots n \\ 0 \leq y_i \leq q-1 & \forall i = 1 \dots n. \end{cases}$$

- If n is a positive integer then $\mu(n)$ denotes the Möbius function.
- If n is a positive integer then $\varphi(n)$ denotes the Euler's totient function.
- If x is a real number, then $[x]$ denotes the integer part of x i.e the greatest integer such that $m \leq x$.

D.5 Miscellaneous

- $\mu_{\mathcal{L}}$ denotes the usual Lebesgue measure on $\mathbb{R}$.
- If $\mathbf{x} \in \mathbb{R}^n$ is a column vector,$\mathbf{x}^t \in \mathbb{R}^n$ is its transpose i.e a row vector.
- $\ll_{something}$ means that the implied constant depend on "something" only. The same for $_{something} \gg$.

Appendix E

Some useful results

We collect here some results from various parts of Mathematics, without proofs. We refer to [6] for further details.

Proposition E.1. *Given a cubic polynomial $\phi(\mathbf{x})$ in n variables with cubic part $C(\mathbf{x})$ let $H(\mathbf{x})$ the determinant of the hessian matrix of $C(\mathbf{x})$. If $C(\mathbf{x}) \neq 0$ for every $\mathbf{x} \in \mathbb{Z}^n - \{\mathbf{0}\}$, then $H(\mathbf{x})$ does not vanish identically.*

Proposition E.2. *Let $f_1(\mathbf{x}), \cdots f_N(\mathbf{x})$ homogeneous polynomials in $\mathbb{Z}^n[\mathbf{x}]$. Let ∂f_i be the degree of f_i Let*

$$\mathcal{A}_R = \{\mathbf{x} \in \mathbb{Z}^n - \{\mathbf{0}\} : f_1(\mathbf{x}) = 0, \cdots f_N(\mathbf{x}) = 0, \, |\mathbf{x}| < R\}.$$

where $R \in \mathbb{R}^+$. Assume that there exists two continuous functions $\alpha : \mathbb{R} \to \mathbb{R}^+$, $\beta : \mathbb{R} \to \mathbb{R}^+$, $\gamma : \mathbb{R} \to \mathbb{R}^+$.

- *$N \leq \alpha(n)$ for every $n \in \mathbb{N}$.*
- *$\max\{\partial f_1, \ldots \partial f_N\} \leq \beta(n)$.*
- *$|\mathcal{A}_{\mathcal{R}}| > AR^{n-1}$ where $A > \gamma(n)$ for every $n \in \mathbb{N}$.*

If

$$J(\mathbf{x}) = \begin{pmatrix} \frac{\partial f_1(\mathbf{x})}{\partial x_1} & \cdots & \frac{\partial f_1(\mathbf{x})}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_N(\mathbf{x})}{\partial x_1} & \cdots & \frac{\partial f_N(\mathbf{x})}{\partial x_1} \end{pmatrix}.$$

then *there exists $\mathbf{x}_0 \in \mathcal{A}_R$ such that*

$$\nu(J(\mathbf{x}_0)) \leq r - 1.$$

where ν is the rank of the matrix J.

Proposition E.3. *Let*

$$\begin{cases} a_{11}y_1 + \dots a_{1n}y_n = 0 \\ \vdots \\ a_{m1}y_1 + \dots a_{mn}y_n = 0. \end{cases}$$

*be a system of homogeneous linear equations with exactly r linearly independent **integral** solutions. Then there exists r linearly independent integral solutions $\mathbf{y^{(1)}} \dots \mathbf{y^{(r)}}$ such that:*

- *every integral solution $\mathbf{y}$ is expressible (uniquely) as*

$$\mathbf{y} = u_1\mathbf{y^{(1)}} + \dots u_r\mathbf{y^{(r)}}. \tag{E.1}$$

  where $u_1, \dots u_r \in \mathbb{Z}$.

- *We have*

$$\left|\mathbf{y^{(1)}}\right| \leq \left|\mathbf{y^{(2)}}\right| \dots \leq \left|\mathbf{y^{(r)}}\right|. \tag{E.2}$$

- *There exist $c = c(r,n) \in \mathbb{R}^+$ such that if $\mathbf{y}$ is any solution expressed as in* (E.1) *then*

$$|u_1|\left|\mathbf{y^{(1)}}\right| + \dots |u_r|\left|\mathbf{y^{(r)}}\right| \leq c\left|\mathbf{y}\right|. \tag{E.3}$$

Proposition E.4. *Let the cubic form C such that $C(\mathbf{x}) \neq 0$ for every $\mathbf{x} \in \mathbb{Z}^n - \{\mathbf{0}\}$ ad it **does not** split. **Then** for every $\varepsilon > 0$ there exist $R_0 = R_0(n,\varepsilon)$ such that if $R > R_0$*

$$|\mathcal{Z}_C(R)| < R^{n-n^{-1}+\varepsilon}. \tag{E.4}$$

where

$$\mathcal{Z}_C(R) = \left\{ (\mathbf{x},\mathbf{y}) \in \mathbb{Z}^n \times \mathbb{Z}^n : \ \forall j = 1...n \ \Rightarrow B_j(\mathbf{x}|\mathbf{y}) = 0, \ \begin{cases} 0 < |\mathbf{x}| < R. \\ 0 < |\mathbf{y}| < R. \end{cases} \right\}$$

and

$$B_j(\mathbf{x}|\mathbf{y}) = \sum_{i=1}^{n}\sum_{k=1}^{n} c_{i,j,k}x_iy_k \ \ j = 1...n.$$

are the bilinear equations associated with the cubic form C.

Proposition E.5. *Let*

$$\widehat{L} = \{L_j : \mathbb{R}^n \to \mathbb{R} \quad j = 1 \dots n\}.$$

a set of linear forms in n variables such that

$$L_j(\mathbf{u}) = \sum_{k=1}^{n} \lambda_{j,k}u_k.$$

with $\lambda_{j,k} = \lambda_{k,j}$ *for every* j *and* k. *Let* $A > 1$ *and* $0 < Z < 1$. *Let* [1]

$$V(Z) = \left\{ \mathbf{u} \in \mathbb{Z}^n : 0 < |\mathbf{u}| < ZA,\ \|\mathbf{L}(\mathbf{u})\| < ZA^{-1} \right\}. \tag{E.5}$$

If $|V(Z)| > 0$ ***then*** *there exists* $\mathbf{u} \in \mathbb{Z}^n$ *such that*

$$\begin{cases} 0 < |\mathbf{u}| \ll ZA\,|V(Z)|^{-\frac{1}{n}} \\ \|\mathbf{L}(\mathbf{u})\| \ll ZA^{-1}\,|V(Z)|^{-\frac{1}{n}}. \end{cases}$$

Further, ***if*** *there exists a suitable constant* $c = c(n)$ *such that*

$$cZ\,|V(Z)|^{-\frac{1}{n}} \leq Z_1 \leq Z. \tag{E.6}$$

then

$$|V(Z_1)| \gg \left(\frac{Z_1}{Z}\right)^n |V(Z)|. \tag{E.7}$$

Proposition E.6. *Let* $\alpha \in [0,1)$ *and let* $\theta > 0$ *a real parameter such that*

$$|S(\alpha)| > P^{n-\frac{1}{4}n\theta}.$$

for P *"large enough". Let* $0 < \delta < \theta$. *For any* $\varepsilon > 0$ *we have one of the following three alternatives: either*

I ***If***

$$\mathcal{C}_1 = \left\{ (\mathbf{x}, \mathbf{y}) \in A^2_{P^{\theta+2\varepsilon}}, \mathbf{B}(\mathbf{x}|\mathbf{y}) = 0 \right\}.$$

then

$$|\mathcal{C}_1| \gg P^{n\theta - n\delta}.$$

or

II ***If***

$$\mathcal{C}_2 = \left\{ \mathbf{x} \in A_{P^{\theta+2\varepsilon}} : \exists \mathbf{y} \in A_{P^{\theta+2\varepsilon}}, \|\alpha \mathbf{B}(\mathbf{x}|\mathbf{y})\| < P^{-3+2\theta+4\varepsilon} \right\}.$$

then

$$|\mathcal{C}_2| \gg P^{n\theta - n\delta}.$$

or

III α *has a rational approximation* a/q *such that*

- $(a, q) = 1$.

[1] As for bilinear forms, the symbol $\mathbf{L}(\mathbf{u})$ is a shortcut to say that a given condition must be satisfied for every form $L_j(\mathbf{u})$ with $j = 1...n$

- $1 \leq q \leq P^{2\theta-\delta+5\varepsilon}$.
- $|q\alpha - a| < P^{-3+2\theta+5\varepsilon}$.

Proposition E.7. *Let*

$$H : \mathbb{R}^n \to \mathbb{R}.$$
$$E : \mathbb{R}^n \to \mathbb{R}.$$

with

$$H\left(x_1 \dots x_n\right) = \sum_{i_1=1}^{n} \cdots \sum_{i_d=1}^{n} a_{i_1 \dots i_d} x_{i_1} \dots x_{i_d}$$

$$E\left(x_1 \dots x_n\right) = \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} b_{i_1 \dots i_{d'}} x_{i_1} \dots x_{i_{d'}}.$$

be forms with integer coefficients, not identically zero of degrees d and d' respectively. Let $d > d'$. Let

$$\begin{cases} p_{\mathbf{x}} \in \mathbb{Z} : p_{\mathbf{x}} = H(\mathbf{x}) \\ q_{\mathbf{x}} \in \mathbb{Z} : q_{\mathbf{x}} = H(\mathbf{x}). \end{cases}$$

the integer values of the forms, corresponding to a given $\mathbf{x}$. For any $\varepsilon > 0$ let

$$\mathcal{I} = \left\{ \mathbf{x} \in \mathbb{Z}^n : |\mathbf{x}| < R,\ p_{\mathbf{x}} \neq 0,\ p_{\mathbf{x}} | q_{\mathbf{x}} \ \right\}.$$

If *there exist a positive integer $\overline{m}$ such that*

$$\begin{cases} |a_{i_1 \dots i_d}| < R^{\overline{m}} & \forall \left(i_1 \dots i_d\right) \in \left\{1 \cdots n\right\}^d \\ \left|b_{i_1 \dots i_{d'}}\right| < R^{\overline{m}} & \forall \left(i_1 \dots i_d\right) \in \left\{1 \cdots n\right\}^d. \end{cases}$$

as R is a "large" real number, ***then***

$$|\mathcal{I}| \ll R^{n-1+\varepsilon}.$$

For the following Proposition, we quote [34] VI, Satz 3.3.

Proposition E.8. *Let $N \in \mathbb{N}$ be any positive integer, let be $\xi \in [0,1]$, let be*

$$S_N\left(\xi\right) = \sum_{p \leq N} e\left(p\xi\right).$$

Let be u and t any positive real numbers. If

- $q \leq \log^u N$.
- $|\beta| \leq N^{-1} \log^t N$.

then

$$S_N\left(\frac{a}{q}+\beta\right)=\widetilde{S_N}\left(q,\beta\right)+O\left(Ne^{-c\sqrt{\log N}}\right)\qquad N\to\infty\,. \tag{E.8}$$

where

$$\widetilde{S_N}\left(q,\beta\right)=\frac{\mu\left(q\right)}{\phi\left(q\right)}\sum_{2\leq n\leq N}\frac{e\left(n\beta\right)}{\log n}.$$

For the following Proposition, we quote [19] , Satz 382

Proposition E.9. *If k l are positive integers and $(k,l)=1$ then*

$$\pi\left(x,k,l\right)=\sum_{\substack{p\in\mathbb{P}\\ p\leq x\\ p\equiv l\,(\bmod\ k)}}1=\frac{1}{\varphi(k)}\int_2^x\frac{du}{\log u}+O\left(xe^{-\alpha\sqrt{\log x}}\right).$$

where $\alpha>0$ is an absolute constant and in particular

$$\pi\left(x,k,l\right)=\sum_{\substack{p\in\mathbb{P}\\ p\leq x\\ p\equiv l\,(\bmod\ k)}}1=\frac{1}{\varphi(k)}\frac{x}{\log x}+o\left(\frac{x}{\log x}\right)$$

For the following Proposition we quote [29]

Proposition E.10. *Let $\mathbb{K}$ a field and $\mathbf{x}=(x_1,\ldots x_k)\in\mathbb{K}^k$. If*

$$F_1\left(\mathbf{x}\right),\ldots F_n\left(\mathbf{x}\right)\in\mathbb{K}\left[\mathbf{x}\right].$$

and F_1 is not identically zero, then there are

$$\Phi_1\left(\mathbf{x}\right),\ldots\Phi_n\left(\mathbf{x}\right)\in\mathbb{K}\left[\mathbf{x}\right].$$

such that

$$\sum_{i=1}^{n}\Phi_i\left(\mathbf{x}\right)F_i\left(\mathbf{x}\right)=d\left(\mathbf{x}\right)\Omega\left(\mathbf{x}\right).$$

identically, where

- $d\left(\mathbf{x}\right)$ *is the greatest common divisor of the given polynomials.*
- $\Omega\left(\mathbf{x}\right)$ *is a polynomial in $\mathbb{Z}\left[\mathbf{x}\right]$not identically zero, such that the formal partial derivative*

  $$\frac{\partial\Omega\left(\mathbf{x}\right)}{\partial x_1}=0.$$

  identically.

Appendix F

Elementary algebra of cubic forms and polynomials

F.1 Cubic forms

We are going to see some algebra of a cubic form that let us understand better the useful role of bilinear forms.

Proposition F.1. *Let C be a cubic form in n variables. If*

$$G(\mathbf{x},\mathbf{y},\mathbf{z}) = C(\mathbf{z}+\mathbf{x}+\mathbf{y}) - C(\mathbf{z}+\mathbf{x}) - C(\mathbf{z}+\mathbf{y}) + C(\mathbf{z}.)$$

then

$$G(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{j=1}^{n} z_j B_j(\mathbf{x}|\mathbf{y}) + \eta(\mathbf{x},\mathbf{y}).$$

where $B_j(\mathbf{x}|\mathbf{y})$ $j = 1...n$ are the associated bilinear forms and $\eta((\mathbf{x}|\mathbf{y})$ is a polynomial which does not depends from the variable $\mathbf{z}$.

Proof. We have

$$C(\mathbf{z}+\mathbf{x}+\mathbf{y}) = \sum_{i,j,k=1}^{n} c_{i,j,k}(z_i+x_i+y_i)(z_j+x_j+y_j)(z_k+x_k+y_k)$$

$$C(\mathbf{z}+\mathbf{x}) = \sum_{i,j,k=1}^{n} c_{i,j,k}(z_i+x_i)(z_j+x_j)(z_k+x_k)$$

$$C(\mathbf{z}+\mathbf{y}) = \sum_{i,j,k=1}^{n} c_{i,j,k}(z_i+y_i)(z_j+y_j)(z_k+y_k)$$

$$C(\mathbf{z}) = \sum_{i,j,k=1}^{n} c_{i,j,k} z_i z_j z_k.$$

Let

$$P_1 = P_1(i,j,k) = (z_i + x_i + y_i)(z_j + x_j + y_j)(z_k + x_k + y_k)$$

$$P_2 = P_2(i,j,k) = (z_i + x_i)(z_j + x_j)(z_k + x_k)$$

$$P_3 = P_3(i,j,k) = (z_i + y_i)(z_j + y_j)(z_k + y_k)$$

$$P_4 = P_4(i,j,k) = z_i z_j z_k.$$

If we consider

$$S = S(i,j,k) = P_1 - P_2 - P_3 + P_4.$$

it is an elementary calculation to check that

$$S = T_1 + T_2.$$

where

$$T_1 = (x_i y_j z_k + x_i y_k z_j + x_j y_i z_k + x_j y_k z_i + x_k y_i z_j + x_k y_j z_i).$$

$$T_2 = (x_i x_j y_k + x_i x_k y_j + x_j x_k y_i + x_i y_j y_k + x_j y_i y_k + x_k y_i y_j).$$

Now

$$G(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{i,j,k=1}^{n} c_{i,j,k} S(i,j,k).$$

hence

$$G(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{i,j,k=1}^{n} c_{i,j,k} T_1(i,j,k) + \sum_{i,j,k=1}^{n} c_{i,j,k} T_2(i,j,k).$$

If we call

$$\eta(\mathbf{x},\mathbf{y}) = \sum_{i,j,k=1}^{n} c_{i,j,k} T_2(i,j,k).$$

we have

$$G(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{i,j,k=1}^{n} c_{i,j,k} T_1(i,j,k) + \eta(\mathbf{x},\mathbf{y}).$$

But, by definition, $c_{i,j,k}$ in invariant by any permutation of indices an so

$$\sum_{i,j,k=1}^{n} c_{i,j,k} T_1(i,j,k) = 6 \sum_{i,j,k=1}^{n} c_{i,j,k} x_i y_j z_k = \sum_{i,j,k=1}^{n} c'_{i,j,k} x_i y_j z_k.$$

Hence

$$G(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{j=1}^{n} z_j B_j(\mathbf{x}|\mathbf{y}) + \eta(\mathbf{x},\mathbf{y}).$$

□

F.2 Cubic polynomials

If we a have a cubic polynomial ϕ instead a cubic form we have a similar result:

Proposition F.2. *Let ϕ be a cubic polynomial in n variables. If*

$$H(\mathbf{x},\mathbf{y},\mathbf{z}) = \phi(\mathbf{z}+\mathbf{x}+\mathbf{y}) - \phi(\mathbf{z}+\mathbf{x}) - \phi(\mathbf{z}+\mathbf{y}) + \phi(\mathbf{z}).$$

then

$$H(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{j=1}^{n} z_j B_j(\mathbf{x}|\mathbf{y}) + \eta(\mathbf{x},\mathbf{y}).$$

where $B_j(\mathbf{x}|\mathbf{y})$ $j = 1...n$ are the bilinear forms associated with the cubic part of the polynomial ϕ and $\xi(\mathbf{x}|\mathbf{y})$ is a polynomial which does not depends from the variable $\mathbf{z}$.

Proof. It is enough to show that the linear part as well as the quadratic part of ϕ gives rise to a contribution which does not depends from the variable $\mathbf{z}$. If

$$L(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i.$$

denotes the linear part, we have that

$$L(\mathbf{z}+\mathbf{x}+\mathbf{y}) - L(\mathbf{z}+\mathbf{x}) - L(\mathbf{x}+\mathbf{y}) + L(\mathbf{z}) = 0 \ \forall \mathbf{x},\mathbf{y},\mathbf{z} \in \mathbb{R}^n.$$

If

$$Q(\mathbf{x}) = \sum_{i,j=1}^{n} q_{i,j} x_i x_j .$$

denotes the quadratic part, we have that

$$Q(\mathbf{z}+\mathbf{x}+\mathbf{y}) - Q(\mathbf{z}+\mathbf{x}) - Q(\mathbf{x}+\mathbf{y}) + Q(\mathbf{z}) = \sum_{i,j=1}^{n} (x_i y_j + y_i x_j).$$

Hence, by setting

$$\xi(\mathbf{x}|\mathbf{y}) = \sum_{i,j=1}^{n} q_{i,j}(x_i y_j + y_i x_j).$$

the result follows.

□

Appendix G

The polynomial of Matiyasevich

G.1 Introduction

Definition G.1. *We say* [1] *that set* $A \subseteq Z$ *is* ***diophantine*** *if there exists a polynomial*

$$p(t, \mathbf{x}) \in \mathbb{Z}[t, x_1 \dots x_n].$$

such that

$$A = \{a \in \mathbb{Z} : \exists \mathbf{x}_a \in \mathbb{Z}^n,\ p(a, \mathbf{x}_a) = 0\}.$$

Example G.1. *The subset* $\mathbb{N}$ *of* $\mathbb{Z}$ *is diophantine because if we choose*

$$p(t, \mathbf{x}) = x_1^2 + x_2^2 + x_3^2 + x_4^2 - t.$$

we have that

$$\{a \in \mathbb{Z} : \exists \mathbf{x}_a \in \mathbb{Z}^n,\ p(a, \mathbf{x}_a) = 0\} = \mathbb{N}$$

Definition G.2. *We say that set* $A \subseteq Z$ *is* ***listable*** *if there is an algorithm that prints* A*, i.e., a Turing machine such that* A *is the set of integers it prints out when left running forever.*

Example G.2. *The set of integers expressible as a sum of three cubes is listable. Namely,*

1. *Print out*

$$F(x, y, z) = x^3 + y^3 + z^3.$$

with

$$\begin{cases} 0 \leq |x| \leq 10 \\ 0 \leq |y| \leq 10 \\ 0 \leq |z| \leq 10. \end{cases}$$

[1] We have borrowed extensively from the survey of B. Poonen [33].

2. Print out

$$F(x,y,z) = x^3 + y^3 + z^3.$$

with

$$\begin{cases} 0 \leq |x| \leq 100 \\ 0 \leq |y| \leq 100 \\ 0 \leq |z| \leq 100. \end{cases}$$

3. ecc. ecc.

Note G.1. *A similar argument shows that any diophantine subset of $\mathbb{Z}$ is listable.*

Definition G.3. *We say that set $A \subseteq Z$ is **computable** if there is an algorithm for deciding membership in A , i.e., an algorithm that takes as input an integer a and outputs **YES** or **NO** according to whether $a \in A$.*

Any **computable** set is **listable**, since given an algorithm for deciding membership in A, we can apply it successively to $0, 1, -1, 2, -2, ...$ and print each number for which the membership test returns **YES**. The converse is **false**: in 1936 A. Turing proved, among others, that:

Theorem G.1. *(Turing) There exists a listable set that is not computable.*

In 1970 Davis, Putnam, Robinson, Matiyasevich, proved the following remarkable theorem:

Theorem G.2. *(DPRM) A subset of $\mathbb{Z}$ is listable if and only if it is diophantine.*

As a consequence of this theorem we have:

Theorem G.3. *There exists a polynomial*

$$F(x_1 \dots x_n) \in \mathbb{Z}[x_1 \dots x_n].$$

such that if we consider the associated polynomial function

$$F : \mathbb{N}^n \to \mathbb{Z}.$$

*we have that the **positive integers** in its range are exactly the **prime numbers**.*

Proof. The natural number version of the DPRM theorem gives a polynomial $p(t, \mathbf{x})$ such that for $a \in \mathbb{N}$, the equation

$$p(a, \mathbf{x}) = 0.$$

is solvable in natural numbers if and only if a is prime. We define

$$F(t, \mathbf{x}) = t\left\{1 - [(p(t, \mathbf{x}))]^2\right\}.$$

This polynomial can be positive only when

$$p(t, \mathbf{x}) = 0.$$

and in this case, t is prime and

$$F(t, \mathbf{x}) = t.$$

Conversely, every prime arises this way. □

A reasonably simple prime-producing polynomial in 26 variables was constructed in [18] J. P. Jones, D. Sato, H. Wada, and D. Wiens. Later, Matiyasevich constructed a 10-variable example.

Appendix H

The "road maps" of the FTP and STP

We present here two graphics conceptual maps about the First and the Second Theorem of Pleasants. In every item of each of them it is indicated the number of the correspondent section in the text where the mentioned argument is developed. In this way we think it is more easy to follow the path of the proof.

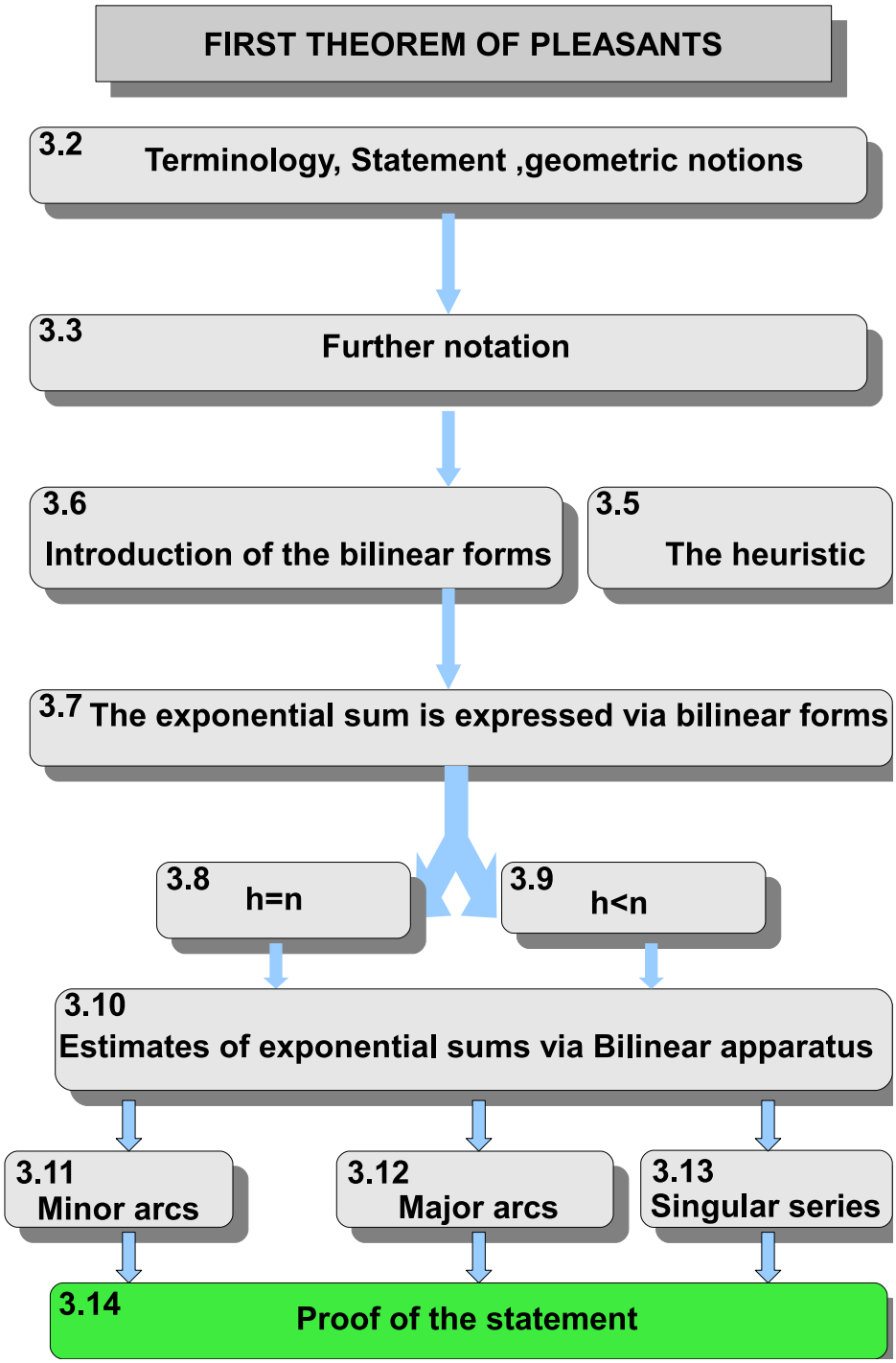

Figure H.1: The road map of FTP.

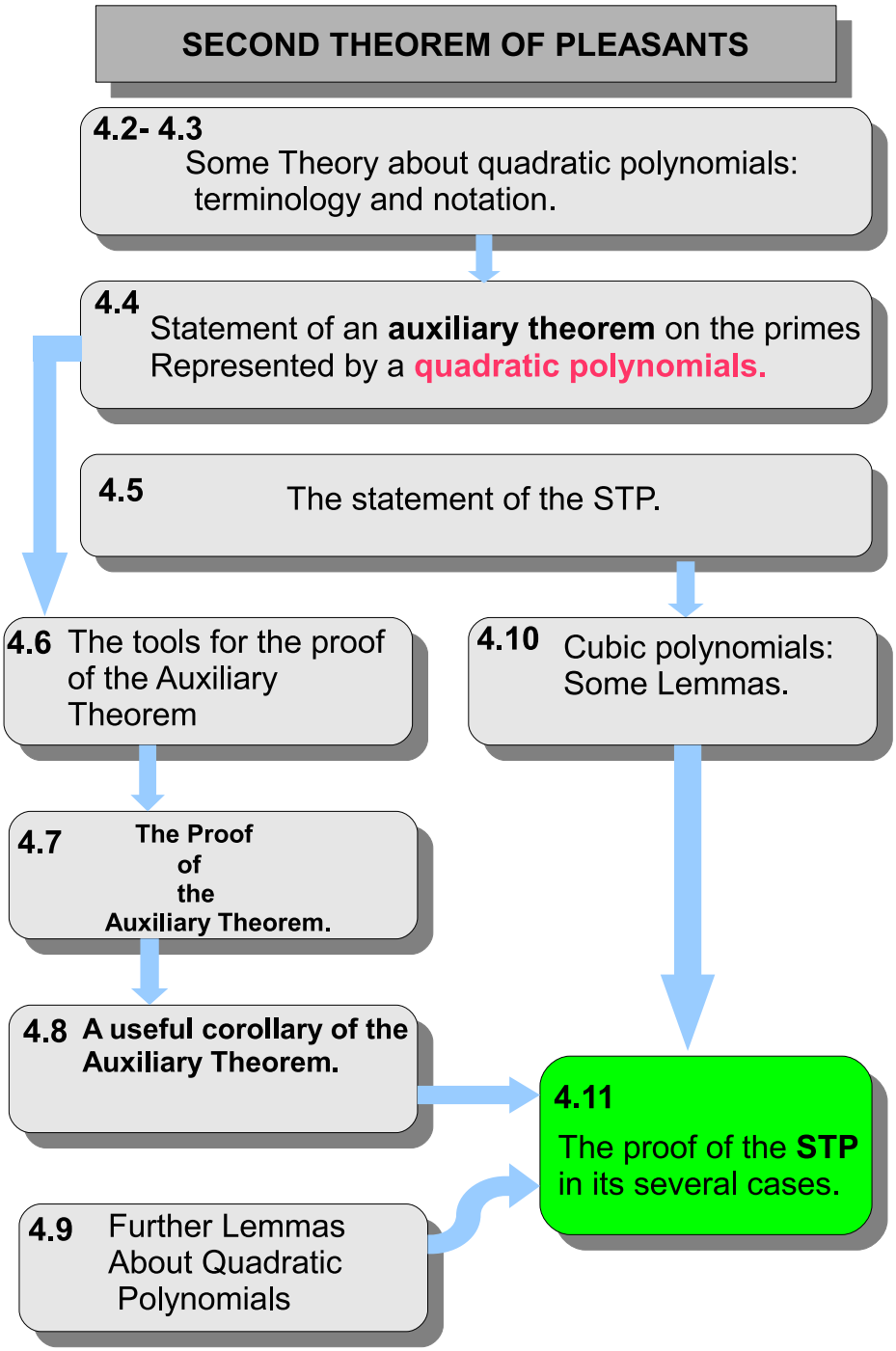

Figure H.2: The road map of STP.

List of Figures

Bibliography

[1] P.T. Bateman and R.A. Horn, *A Heuristic Asymptotic Formula concerning the Distribution of Prime Numbers*, Mathematics of Computation **79** (1962), 363–367.

[2] V. Bouniakowski, *Sur les diviseurs numériques invariables des fonctions rationelles entières*, Mem. Acad. Sci. St. Petersburg **6** (1857), 305–329.

[3] V. Brun, *Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare*, Arch. Mat. Natur. **B34** (1915), 3–19.

[4] P. L. Chebyshev, *Sur la fonction qui détermine la totalité des nombres premiers inferiures à une limite donnée*, J. Math. Pures App.(1) **17** (1853), 366–390.

[5] H. Davenport, *Cubic Forms in Thirty-Two Variables*, Philosophical Transactions of the Royal Society of London **251** (1959), 193–232.

[6] ———, *Cubic forms in sixteen variables*, Proc. London Math Soc. **272** (1963), 285–303.

[7] H. Davenport and D.J. Lewis, *Non-homogeneus cubic equations*, Journ. London Math. Soc. **39** (1964), 657–671.

[8] V. Demjanenko, *On sums of four cubes*, Izvestia Vischik Outchetsnik Zavedenii Mathematika **54** (1966), 64–69.

[9] L.E. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Mathematics **33** (1904), 155–161.

[10] P.G.L. Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abhand. Ak. Wiss. Berlin **48** (1837), 45–81.

[11] Euclid, *Elementa. I-XIII, English translation: T.L. Heath, The Thirteen books of Euclid's Elements*, Dover, 1956.

[12] L. Euler, *Opera Omnia*, vol. I14, Teubner, 1924.

[13] G.H. Hardy and J.E. Littlewood, *Some problems of 'Partitio numerorum'III: On the expression of a number as sum of primes*, Acta Mathematica **44** (1923), 1–70.

[14] G.H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatorial analysis*, Proc. London Math. Soc. **17** (1918), 75–115.

[15] D.R. Heath-Brown, *Primes represented by* $x^3 + 2y^3$, Acta Mathematica **186** (2001), 1–84.

[16] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Acta Arithmetica **24** (1974), 435–459.

[17] J.Friedlander and H.Iwaniec, *The polynomial* x^2+y^4 *captures its primes*, Annals of Mathematics 2 **148** (1998), 945–1040.

[18] J.P. Jones, D. Sato, H. Wada, and D. Wiens, *Diophantine Representation of the Set of Prime Numbers*, American Mathematical Monthly **83** (1976), 449–464.

[19] E. Landau, *Vorlesungen über Zahlentheorie II*, Chelsea-Publishing Company, 1955.

[20] A.M. Legendre, *Théorie des Nombres*, Didot, 1830.

[21] Hongze Li, *A hybrid of theorems of Goldbach and Piatetski-Shapiro*, Acta Arith. **107** (2003), 307–326.

[22] Yu. V. Linnik, *The large sieve*, Dokl. AN USSR **30** (1941), 290–292.

[23] H.Q. Liu and J. Rivat, *On the piatetski-shapiro prime number theorem*, Bull. London Math. Soc. **24** (1992), 143–147.

[24] J. L. Mordell, *A remark on indeterminate equations in several variables*, J. Lond. Math. Soc. **12** (1937), 127–129.

[25] J.L. Mordell, *Note on the integer solutions of* $z^2-k^2 = ax^3+by^3$, Ganita **5** (1954), 103–104.

[26] ———, *Diophantine Equations*, Academic Press, 1969.

[27] R. Murty, *Primes in certain arithmetic progressions*, Journal of the Madras University **51** (1988), 161–169.

[28] M.B. Nathanson, *Additive number theory: the classical basis*, Springer-Verlag, 1996.

[29] O. Perron, *Algebra Vol I*, De Gruyter, 1951.

[30] I.I. Piatetski-Shapiro, *On the distribution of prime numbers in the sequence of the form* $[f(n)]$, Mat. Sb. **33** (1953), 559–566.

[31] P.A.B. Pleasants, *The representation of primes by cubic polynomials*, Acta Arithmetica **XII** (1966), 23–44.

[32] ———, *The representation of primes by quadratic and cubic polynomials*, Acta Arithmetica **XII** (1966), 132–163.

[33] B. Poonen, *Undecidability in number theory*, Notices of the Amer. Math. Soc. **55** (2008), 344–350.

[34] K. Prachar, *Primzahlverteilung*, Springer-Verlag, 1957.

[35] A. Schinzel and W. Sierpinski, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arithmetica **4** (1958), 185–208.

[36] A. Selberg, *On an elementary method in the theory of primes*, Norske Vid. Selsk. Forh. Trondhjem **19** (1947), 64–67.

[37] ———, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Annals of Mathematics **2** (1950), 297–304.

[38] ———, *The general sieve method and its place in prime number theory*, Proc.Int. Congress of Mathematicians Cambridge **1** (1950), 262–289.

[39] J. Stillwell, *Elements of Number Theory*, Springer-Verlag, 2002.